UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Análise de Vulnerabilidades e Medidas de Prevenção em Aplicações *web* do Governo de Moçambique

Caso de Estudo: Portal Electrónico do Governo de Moçambique

Valter Ramudala Cheque

Supervisor:

Engº. Délcio Arnaldo Chadreca

Maputo, Julho de 2017

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Análise de Vulnerabilidades e Medidas de Prevenção em Aplicações *web* do Governo de Moçambique

Caso de Estudo: Portal Electrónico do Governo de Moçambique

Valter Ramudala Cheque

Supervisor:

Engº. Délcio Arnaldo Chadreca

Maputo, Julho de 2017

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

TERMO DE ENTREGA DE RELATÓRIO DE TRABALHO DE LICENCIATURA

Declaro que a estudante **Valter Ramudala Cheque** entregou no dia 28/07/2017 as __ cópias do relatório do Trabalho de Licenciatura com a referência 2017EITLD8 intitulado: Análise de Vulnerabilidades e Medidas de Prevenção em Aplicações *web* do Governo de Moçambique (Caso de Estudo: Portal Electrónico do Governo de Moçambique).

Maputo, __ de _____de 2017

O chefe da Secretaria

_____

Aos meus pais Ramudala Cheque e Matilde Manuel

Aos meus irmãos Zarina, Azamate, Cheque, Márcia e Daniba

Agradecimentos

Aos meus pais Ramudala Cheque e Matilde Manuel, que desde cedo apostaram em mim, investindo tudo o que tinham e um pouco mais para que não faltasse o básico na minha vida académica. MUITO OBRIGADO.

Agradecer aos meus irmãos que sentiram-se privados de certos mimos por parte dos meus pais durante o período do curso e pelo apoio incondicional proporcionado.

Agradecer a todos docentes do curso de Licenciatura em Engenharia Informática da Faculdade de Engenharia pelos ensinamentos, pela paciência e dedicação demonstrada durante estes últimos 9 semestres.

Agradecimentos especiais ao meu supervisor engº Délcio Chadreca pela entrega, pela paciência, pelas orientações e por se ter transformado no holofote que precisava para a concepção deste trabalho e ao dr. Vali Issufo pela abertura e pelos *insigth*.

Aos colegas da Faculdade de Engenharia, particularmente do curso de Engenharia Informática, especialmente a turma de 2013, muito obrigado pela amizade e pelo companheirismo.

Aos colegas que hoje tenho o prazer de chamar de amigos, Eunice Muzime, Muarucha Assane, Domingos Palave, Rosete Bandeira, Júlia Nelma, António Latibo, Edson Michaque, Densque Jamal, Emilson Vontade, Deize Rosa, Ana Paula Tâmbula, Idelson Mindo, Natalício Culuze, Neúsia Pelembe, Gizela Alexandre e aos que aqui não mencionei, meu muito obrigado pelo respeito e pela irmandade.

Aos amigos que tornaram-se irmãos para mim, Salvador Muchidão, Honesto Marroda, Honório Boné e Leila Maria, muito obrigado pelo apoio, pela convivência e pelos momentos bons partilhados.

Agradecer particularmente ao Júlio Mudubai que serviu como modelo de inspiração durante minha vida académica, por ter acreditado no meu potencial e pelos conselhos oportunos dados durante a formação.

Resumo

A Internet permite que instituições quebrem barreiras e limitações físicas impostas pela localização geográfica e contribui para a criação de meios que aproximam estas aos seus utentes, disponibilizando informações e vendendo produtos e serviços de forma rápida e universal.

Governos de diversos países têm se aproveitado da facilidade e abrangência oferecidas pelas Tecnologias de Informação e Comunicação e massificação do acesso a Internet para difundir informações sobre a vida do país aos seus cidadãos e fornecer serviços básicos como água, saúde, electricidade entre outros.

O presente trabalho foca-se na análise de vulnerabilidades e na proposição de medidas de prevenção para as vulnerabilidades identificadas nas aplicações *web* do Governo de Moçambique (o portal Electrónico do Governo e portais dos diferentes ministérios).

Para a efectivação da análise de vulnerabilidades, apresentou-se os critérios mínimos de segurança que aplicações *web* deve conter, as vulnerabilidades mais incidentes de acordo com organizações internacionais como a OWASP, a metodologia de testes de intrusão, selecção e comparação de scanners de vulnerabilidades *web*, realização dos testes, apresentação e classificação das vulnerabilidades encontradas e as medidas de correcção destas.

Com base neste estudo, conclui-se que as aplicações do Governo de Moçambique não apresentam um nível de segurança satisfatório e que devem ser levadas a cabo medidas urgentes e de forma rotineira de modo a garantir que as informações contidas nestas aplicações estejam seguras.

Palavras-chave: aplicação web, governo electrónico, vulnerabilidade, informação, segurança, prevenção, teste de intrusão.

“**Obstáculos são aquelas coisas assustadoras que você vê quando desvia seus olhos da sua meta**”.

(Henry Ford)

Índice

Lista de abreviaturas e acrónimos

CSRF	*Cross-Site Request Forgery*
DoS	*Denial of Service*
DRA	Direcção do Registo Académico
FEUEM	Faculdade de Engenharia da UEM
FTP	*File Transfer Protocol*
HTML	*HyperText Markup Language*
HTTP	*HyperText Transference Protocol*
ISSAF	*Information System Security Assessment Framework*
MASA	Ministério da Agricultura e Segurança Alimentar
MEDH	Ministério da Educação e Desenvolvimento Humano
MINEC	Ministério de Negócios Estrageiros e Cooperação
MJD	Ministério da Juventude e Desporto
MTC	Ministério dos Transportes e Comunicação
OSSTMM	*Open Source Security Testing Methodology Manual*
OWASP	*Open Web Application Security Project*
RAV	*Risk Assessment Values*
SQL	*Structured Query Language*
SSL	*Secure Socket Layer*
TIC	Tecnologias de Informação e Comunicação
UEM	Universidade Eduardo Mondlane
URL	*Uniform Resource Locator*
WVS	*Web Vulnerability Scan*
WWW	*World Wide Web*
XSS	*Cross-Site Scripting*

Lista de figur

Lista de tabelas

1. CAPÍTULO I – INTRODUÇÃO

1.1. Contextualização

A sociedade contemporânea está marcada pelo crescimento e pela expansão significativa das Tecnologias de Informação e Comunicação (TIC). Estas tecnologias permitiram a ligação de pessoas e organizações criando-se assim novo tipo de sociedades que possuem como base para a sua existência as TIC e em que o principal recurso partilhado entre os intervenientes destas é a informação.

Para Castells & Cardoso (2006), a Internet e as redes de computadores não só contribuíram para grandes transformações na relação entre o sujeito e o mundo, alavancando diversas dimensões da vida humana, dentre as quais podem destacar-se: relações entre o trabalho e a produção, instituições, práticas sociais, códigos culturais, espaços e processos formativos, entre outros mas também originaram novas formas de relacionamentos que possibilitaram com que diferentes actividades que antigamente eram realizadas de forma tradicional passassem a ser efectuadas com suporte às TIC, melhorando significativamente o seu desempenho e explorando novas áreas de conhecimento.

Como dito anteriormente, a informação é o principal recurso compartilhado na *web*[1]. Aquando da sua criação, os criadores da *Internet* não consideraram o factor "segurança" como muito importante porque ela foi desenvolvida com o propósito de compartilhar informação, sem restrições, entre os utilizadores da *Internet.* Com o passar do tempo, o número de utilizadores da Internet cresceu significativamente e as empresas/organizações que usavam esta tecnologia para o compartilhamento de dados ou informações entre as diferentes filiais das suas companhias, sentiram a necessidade de proteger estes de outros usuários curiosos e indesejados.

Actualmente, a segurança de informação é uma das discussões que se tem levado a cabo a nível mundial pela crescente actividade registada na Internet e principalmente pelo crescimento de utilizadores que tem acesso a esta plataforma no dia-a-dia e pelo

1 Sinónimo usado para se referir a word wide web.

elevado volume de dados que é transmitida. Para Faller (2005), a espionagem industrial é de relativamente pouca preocupação para a maioria das pessoas, mas, dentro de cada empresa moderna, existem indivíduos ou departamentos responsáveis por manter os segredos da empresa a salvo.

A utilização de aplicações *web* têm-se mostrado imprescindível em algumas áreas tais como: comércio electrónico, *homebanking*, gestão empresarial, governação electrónica, entre outras. Tais aplicações necessitam de soluções mais seguras pelo facto de algumas processarem informações sigilosas. Portanto, deve se prestar maior atenção durante a fase de concepção, para que se garanta que sejam considerados aspectos de segurança no que concerne a escolha de tecnologias, a fim de garantir maior segurança a estas.

1.2. Descrição do Problema

Com o advento da Internet e das Tecnologias de Informação e Comunicação, diversas entidades governamentais e não-governamentais têm buscado formas de prover informações e fornecer serviços aos seus clientes/utentes com vista a satisfazer as necessidades destes de forma cómoda e segura.

No contexto do desenvolvimento electrónico, o Governo da República de Moçambique com o intuito de tornar-se cada vez mais próximo do cidadão, disponibiliza informações e serviços sobre o país no Portal Electrónico do Governo.

Sendo uma aplicação *web,* o portal do governo encontra-se vulneráveis à inúmeros ataques porque assume-se que este possui informações de grande valor para o estado moçambicano e associado ao baixo risco de exposição dos criminosos. As tecnologias utilizadas durante a fase de concepção, a forma como as aplicações são desenvolvidas e geridas constituem os principais factores que contribuem para o elevado número de vulnerabilidades detectadas em aplicações *web*.

Informações de fontes não oficiais indicam que as aplicações *web* do Governo moçambicano têm sido vítimas constantes de diversos ataques orquestrados por piratas informáticos. Alguns destes ataques têm como consequência a indisponibilidade das páginas, privando aos cidadãos o acesso a informação e deste modo violando o ponto nº 1 do Artigo 49 da Lei das Transacções Electrónicas que refere a disponibilidade da informação (ver anexo 1).

É necessário que se criem políticas de segurança de modo a reduzir a incidência dos ataques e consequente redução dos efeitos causados por estes. De modo a identificar as vulnerabilidades presentes nas aplicações *web* do Governo de Moçambique e propor medidas de segurança que visam mitigá-las, surge a necessidade da elaboração do presente trabalho.

1.3. Motivação

A motivação para a escolha desse tema de pesquisa por parte do autor do trabalho é pessoal e profissional. É pessoal pois deve-se à curiosidade, interesse e a preocupação do autor pela área de segurança de informação. Quanto a área profissional, permitirá conciliar os conhecimentos teóricos adquiridos durante a sua formação pois, a realização de ataques e testes de intrusão num ambiente real fará com que este compreenda de prático as preocupações relativas a segurança existentes nas aplicações *web* e as competências profissionais obtidas da realização desse exercício serão de grande valia na carreira profissional do autor permitindo que este possa futuramente contribuir no desenvolvimento de sistemas seguros.

Com a realização deste trabalho será também possível contribuir para a melhoria da segurança das aplicações do Governo de Moçambique.

1.4. Objectivos

1.4.1. Objectivo geral

Realizar análise de vulnerabilidades nas Aplicações *web* do Governo de Moçambique e propor medidas de segurança.

1.4.2. Objectivos específicos

- Apresentar critérios mínimos de segurança em aplicações *web*;
- Descrever o portal do Governo Electrónico de Moçambique;
- Comparar ferramentas usadas para o *scan* de vulnerabilidades *web;*
- Efectuar *scan* de vulnerabilidades;
- Propor medidas de prevenção.

1.5. Metodologia

De forma a materializar os objectivos propostos no trabalho e a responder as questões de pesquisa acima colocadas, usou-se uma metodologia de pesquisa.

1.5.1. Classificação da metodologia de Pesquisa

Quanto a classificação, a metodologia utilizada no desenvolvimento do presente trabalho pode ser:

- **Quanto a abordagem**

No que concerne a abordagem utilizada, usou-se a abordagem qualitativa no decurso do desenvolvimento da pesquisa. Nesta abordagem, o pesquisador ou investigador busca aprofundar-se na compreensão dos fenómenos por si estudados e as acções dos indivíduos, grupos ou organizações em seu ambiente e contexto social. Como afirma Terence & Escrivão Filho (2006), a abordagem qualitativa é usada quando o intuito do pesquisador é de compreender de forma profunda os fenómenos estudados durante a pesquisa e interpretá-los de acordo com uma certa perspectiva sem se preocupar com representatividade numérica, generalizações estatísticas ou mesmo com as relações de causa e efeito.

- **Quanto ao método**

Referente ao método de abordagem, procurou-se adoptar o raciocínio hipotético-dedutivo. De acordo com Marques *et al* (2014), o método hipotético-dedutivo busca construir e testar possíveis soluções ou respostas para os problemas decorrentes de factos ou conhecimentos teóricos, algo que se encontra intimamente relacionado com a sua experimentação.

- **Quanto aos objectivos**

Quanto aos objectivos da pesquisa, esta pode ser classificada como combinação de analítica e de avaliação.

A pesquisa pode ser considerada analítica pois, trata-se de um "tipo de estudo que visa (...) analisar uma dada situação (objecto de estudo), mediante procedimentos de decomposição do todo estudado, visando não apenas conhecer seus elementos constituintes, mas sobretudo como eles se articulam entre si" (Marques et al, 2014, p. 52). Neste caso em particular, as aplicações *web*.

A pesquisa também pode ser classificada como de avaliação, visto que esta "trata-se de pesquisa aplicada para avaliar principalmente instituições, programas sociais e políticas públicas visando melhoramento, como educação no sentido geral, saúde, métodos de ensino, treinamentos etc. As técnicas utilizadas são variadas, como por exemplo a entrevista, a observação sistemática e participante, formulários, questionários, discussão em grupo etc" (Marques et al, 2014, pp. 53-54). Neste caso, o portal do Governo de Moçambique.

- **Quanto à participação do pesquisador (relação sujeito-objecto de pesquisa)**

Em relação à participação do pesquisador, esta pode ser classificada como pesquisa-acção, visto que nela o pesquisador desenvolve acções de modo a resolver os problemas fundamentais identificados, pois este "desempenha papel activo no equacionamento dos problemas encontrados, não só faz a investigação, mas procura desencadear acções e avaliá-las com a participação da população envolvida" (Marques et al, 2014, p. 55).

1.5.2. Técnicas Colecta de Dados

Para a compilação das informações contidas no presente documento foram usadas duas técnicas, nomeadamente a pesquisa documental e entrevistas.

- **Pesquisa Documental**

Consultou-se documentos existentes que abordam questões relativas a implementação e gestão das aplicações que constituem o Governo Electrónico de Moçambique e documentos disponibilizados pela entendida responsável pela hospedagem das aplicações.

- **Entrevistas**

De modo a colher dados da entidade responsável pelo desenvolvimento e pela gestão das aplicações portais electrónicos do Governo de Moçambique, foi preparado um guião de entrevistas de servirá como base para o autor por forma a auferir por parte desta entidade sobre os mecanismos de segurança implementados nestes e sobre o histórico de ataques das aplicações (Vide em anexo 2).

1.5.3. Metodologia da Análise de Vulnerabilidades

A análise de vulnerabilidades será feito com recurso a uma ferramenta desenvolvida com o objectivo de identificar vulnerabilidades e falhas que podem levar ao comprometimento dos dados contidos em aplicações *web.*

Far-se-á uma comparação de algumas ferramentas existentes no mercado de modo a definir a que melhor se adequa a natureza do presente trabalho e que forneça uma variedade de alternativas de uso da mesma.

1.6. Estrutura do Trabalho

O trabalho está organizado em 8 capítulos. A seguir apresenta-se a descrição de cada capítulo.

Capítulo I – Introdução: contem a parte introdutória do trabalho, em que faz-se a descrição do problema a resolver e apresenta-se a metodologia utilizada para o alcance dos objectivos definidos.

Capítulo II – Revisão da Literatura: Apresentam-se diversos conceitos consultados em diferentes literaturas sobre o caso em estudo.

Capítulo III – Caso de Estudo: Aborda-se conceitos relativos a governação electrónica em Moçambique e faz a descrição do Portal Electrónico do Governo.

Capítulo IV – Desenvolvimento do Trabalho: Faz-se a apresentação dos relatórios dos *scan*s de vulnerabilidades efectuadas nas aplicações *web* e apresenta-se as medidas de prevenção para as vulnerabilidades médias encontradas.

Capítulo V – Discussão de Resultados: Avaliam-se os resultados apresentados pelos *scan* e verifica-se se estes condizem com o que se esperava.

Capítulo VI – Conclusões e Recomendações: apresentam-se as conclusões tiradas do trabalho e recomendações para trabalhos da mesma natureza.

Bibliografia: Aqui encontram-se dispostas as referências todas as obras e documentos utilizados para a concepção do presente trabalho.

Anexos: Apresenta-se partes da lei das transacções electrónicas vigente no país e imagens que complementam o capítulo IV.

2. CAPÍTULO II – REVISÃO DA LITERATURA

2.1. SEGURANÇA DE INFORMAÇÃO

Acredita-se que estamos a viver numa era que é equivocamente considerada a era e/ou sociedade de informação e do conhecimento pelo elevado domínio que as Tecnologias de Informação e Comunicação exercem sobre os aspectos básicos para a convivência da própria humanidade. Castells & Cardoso (2006) afirmam que apesar do crescimento significativo registado no ramo das TIC desde os finais do século XX e o aparecimento daquilo que hoje é considerada a sociedade em rede devido a rápida expansão das redes de computadores, não é suficiente para afirmar que somente nessa época o ser humano começou a preocupar-se com a informação pois esta vem acompanhando a evolução do próprio homem. “Nós sabemos que a tecnologia não determina a sociedade: é a sociedade. A sociedade é que dá forma à tecnologia de acordo com as necessidades, valores e interesses das pessoas que utilizam as tecnologias” (Castells & Cardoso, 2006, p. 17).

2.1.1. Informação

Acredita-se hoje que a informação é o tão precioso oxigénio usado para a sobrevivência das organizações. Para Messias (2005), a informação é o principal recurso que movimenta a economia mundial, apresentando-se como o elemento basilar de produção das sociedades desenvolvidas e em desenvolvimento. Messias (2005) afirma também que a fonte de renda e de poder das grandes nações agora passou a ser representada pela quantidade de informação acumulada, organizada e transformada em valor monetário, deixando assim de lado a moeda que era o motor da sociedade aquando da revolução industrial.

Segundo o dicionário da língua portuguesa, a informação é a reunião dos conhecimentos, dos dados, sobre um assunto ou pessoa. A informação aqui pode ser entendida como tudo aquilo que se sabe sobre um determinado campo.

Em várias literaturas consultadas pelo autor, a tentativa de definição do termo informação é frequentemente associada aos conceitos dados[2] e conhecimento[3]. Esses conceitos aparecem dispostos na seguinte ordem: **dados -> informação –> conhecimento**, mostrando assim uma interdependência entre estes. Shedroff (1999) afirma que não se pode considerar a informação como sendo os diversos estímulos ou percepções que extraísse da natureza e que bombardeiam os sentidos diariamente. Tais estímulos devem ser considerados meros dados e estes passam a ser considerados informação quando são organizados, transformados e dispostos de maneira a dar algum significado.

Para Davenport & Prusak (1998), a informação é uma mensagem, geralmente na forma de um documento ou uma comunicação audível e visível, e que dados são transformados em informações por via dos seguintes passos:

- **Contextualização**: sabe-se a finalidade dos dados colectados;
- **Categorização**: conhece-se as unidades de análise ou os componentes essenciais dos dados;
- **Cálculo**: os dados colectados podem ser analisados matematicamente os estatisticamente;
- **Correcção**: os erros cometidos no processo de recolha dos dados são eliminados;
- **Condensação**: os dados podem ser resumidos em uma forma mais concisa.

2.1.2. Classificação da Informação

Para Rezende & Abreu (2000) citado em Laureano (2005), a informação desempenha papéis importantes tanto na definição quanto na execução de uma estratégia de segurança. A informação, como qualquer um activo da empresa, precisa ser protegida dos utilizadores indesejados.

2 Dado é o registro ou indício relacionável a algum objecto que lhe atribui um valor semântico quantitativo ou qualitativo.

3 Conhecimento é a informação compreendida, tomada como verdadeira e guardada na memória para usos futuros.

Laureano (2005) ainda afirma que é necessária a classificação da informação em determinados níveis de prioridade. Para a elaboração de melhores propostas de segurança, ela é comumente dividida em quatro classes de acordo com o valor que a mesma apresenta para a respectiva organização. As principais classes são:

- **Pública –** faz parte dessa classe, toda informação que quando exposta não origina consequências a empresa/organização e não prejudica ou interfere no funcionamento normal desta. Geralmente são informações para as organizações fornecem ao público por questões de *marketing* ou de localização.
- **Interna –** é toda aquela informação que deve ser mantida no seio da empresa. É considerada somente para uso interno e o acesso a mesma deve ser vedado aos indivíduos externos a mesma. Apesar da restrição colocada a esta classe, o acesso a informações destas por partes de terceiros não acarretam danos sérios a organização.
- **Confidencial –** é colocada nessa classe, toda informação restrita a empresa e que dizem respeito ao funcionamento da organização ou aos clientes e/ou parceiros da mesma. A divulgação desse tipo de informações deve ser evitada porque pode causar danos sérios a empresa/organização.
- **Secreta –** toda informação crítica para as actividades da empresa e restrita a um pequeno grupo de indivíduos dentro da organização. Ela deve ser preservado a todo e a qualquer custo pois é considerada informação vital para a empresa.

2.1.3. Segurança de Informação

Antes de entrar afundo sobre o conceito de segurança de informação, convém abordar antes sobre o conceito de segurança que tem a sua origem do latim "***securitas***" e implica minimizar ou eliminar qualquer tipo de risco na vida.

O termo segurança refere-se a um conjunto de medidas levadas a cabo para proteger-se ou prevenir-se de quaisquer actos de violência, ataques, roubos, espionagem, sabotagens entre outros. Ela implica necessariamente a qualidade ou o estado de sentir-se seguro. Este é frequentemente usado em diversos contextos diferentes e diversas áreas mas geralmente está associada a protecção de um determinado bem ou activo.

A informação é um recurso importante para a organização e está deve ser protegida. A segurança de informação consiste em garantir que toda informação pertencente a

empresa, independentemente do seu formato e modo de armazenamento, está segura e o acesso a esta é completamente vedado à utilizadores estranhos a organização, está sempre disponível quando esta é necessária por qualquer fim, e é confiável e autêntica.

Segundo Beal (2005), a segurança de informação é o processo de proteger a informação das diversas ameaças existentes de modo a garantir a sua integridade, disponibilidade e confidencialidade. Analogamente a Norma NBR ISO/IEC 27002:2005 define Segurança de Informação como a preservação da Confidencialidade, da Integridade, e da disponibilidade da informação; adicionalmente, algumas propriedades como autenticidade, responsabilidade, não repúdio e confiabilidade.

Em diversas bibliografias consultadas pelo autor, a Segurança de Informação é frequentemente associada as características da confidencialidade, integridade e disponibilidade. Sendo essas três características consideradas os pilares para a segurança de informação.

2.1.4. O trio CIA

Como referido acima, a segurança de informação é garantida pelos princípios da confidencialidade, integridade e disponibilidade comumente designadas por trio CIA (do inglês *Confidentiality*, *Integrity* and *Availability*).

2.1.4.1. Confidencialidade (*Confidentiality*)

A confidencialidade é o princípio que preconiza que somente indivíduos autorizados devem ter acesso às informações armazenadas ou transmitidas por meio das redes de comunicação.

O princípio preocupa-se com a protecção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso aos mesmos. O aspecto mais importante desse princípio e a garantia da autenticação e da identificação dos utilizadores do sistema. Garantir a confidencialidade é assegurar é assegurar o valor da informação e evitar a divulgação indevida.

Ocorre a violação da confidencialidade da informação quando, por algum motivo, indivíduos não autorizados possuam conhecimento ou tenham acesso ao seu conteúdo.

2.1.4.2. Integridade (*Integrity*)

O princípio da integridade da informação pressupõe que a informação deve ser retornada na sua forma original no momento em que está foi armazenada ou inserida no sistema. Ela sinaliza a conformidade dos dados com relação às inserções, alterações e processamentos autorizados efectuados. Garantir a integridade da informação significa assegurar que ela encontra-se na sua condição original.

Laureano (2005) esclarece que o princípio da integridade não pode ser confundido com confiabilidade do conteúdo da informação. Uma informação pode ser imprecisa, mas deve permanecer integra, ou seja, esta não deve sofrer qualquer alteração por pessoas não autorizadas.

Viola-se a integridade quando a informação é parcialmente ou totalmente corrompida, falsificada, alterada, roubada ou destruída.

2.1.4.3. Disponibilidade (*Availability*)

O princípio da disponibilidade consiste na garantia de que as informações estejam acessíveis aos utilizadores ou a outros sistemas devidamente autorizados, a qualquer momento requerido. Garantir a disponibilidade é assegurar o êxito da leitura, do trânsito e do armazenamento da informação, ou seja, garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito.

Diz-se que houve quebra do princípio da disponibilidade quando a informação não está disponível para ser utilizada, ou seja, ao alcance de seus usuários e destinatários, não podendo ser acedida no momento em que for necessário utilizá-la.

Várias literaturas defendem que somente o trio CIA não é suficiente para a garantia plena da segurança informação, apresentando mais factores. (Laureano, 2005, p. 12) reitera que para uma informação ser considera segura, o sistema que o administra ainda deve respeitar:

- **Autenticidade** – Garante que a informação ou o usuário da mesma é autêntico; Atesta com exactidão, a origem do dado ou da informação;
- **Não repúdio** – Não é possível negar (no sentido de dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação; Não é possível negar o envio ou recepção de uma informação ou dado;

- **Legalidade** – Garante a legalidade (jurídica) da informação; Aderência de um sistema à legislação; Característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os activos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.
- **Privacidade** – Foge do aspecto de confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada. Uma informação privada deve ser vista / lida / alterada somente pelo seu dono. Garante ainda, que a informação não será disponibilizada para outras pessoas (neste é caso é atribuído o carácter de confidencialidade a informação); É a capacidade de um usuário realizar acções em um sistema sem que seja identificado.
- **Auditoria** – Rastreabilidade dos diversos passos que um negócio ou processo realizou ou que uma informação foi submetida, identificando os participantes, os locais e horários de cada etapa. Auditoria em *software* significa uma parte da aplicação, ou conjunto de funções do sistema, que viabiliza uma auditoria; Consiste no exame do histórico dos eventos dentro de um sistema para determinar quando e onde ocorreu uma violação de segurança.

2.1.5. Níveis de Segurança de Informação

Laureano (2005) defende que a segurança de informação é a protecção de sistemas de informação contra as situações adversas ao funcionamento normal destes, ou seja, contra a negação de serviços a utilizadores autorizados, contra a intrusão, contra a modificação não-autorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças ao seu desenvolvimento.

O Código de Prática para a Gestão de Segurança da Informação ou simplesmente a norma NBR ISO/IEC 27002 (2005), estabelece directrizes e princípios geral de modo a implementar, manter e melhorar a gestão da segurança de informação dentro de uma organização. De acordo com a norma supra citada, a obtenção da segurança de informação é conseguida a partir da implementação de um certo conjunto de controlos adequados, desde políticas de segurança, processos, procedimentos, estruturas organizacionais e funções de *software* tanto quanto de *hardware*.

A norma NBR ISO/IEC 27002 (2005) recomenda que se estabeleça antes una política de segurança de informação[4] devidamente documentada dentro da organização e define três níveis principais para que a organização possa atingir uma segurança efectiva de informação. Estes níveis são: segurança em a nível dos Recursos Humanos, segurança a nível Física e do Ambiente e da Gestão das Operações e Comunicações ou simplesmente segurança a nível Tecnológico.

2.1.5.1. Segurança em Recursos Humanos

Neste nível, a norma aborda sobre aspectos referentes a contratação, formação e consciencialização dos funcionários e colaboradores da organização acerca da necessidade e responsabilidades destes em torno da manutenção da segurança de informação. Versa também sobre aspectos que vão desde as entrevistas de candidatos para ocupação de postos dentro da organização e a desvinculação de funcionários por forma a mitigar o risco de roubo, fraude ou até mesmo de mau uso dos recursos e equipamentos da instituição.

2.1.5.2. Segurança Física e do Ambiente

A segurança neste nível objectiva-se a prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização. Aqui, a norma trata sobre a necessidade da manutenção da segurança, com níveis e controles de acesso apropriados, incluindo protecção física nas instalações de processamento de informação críticas ou sensíveis da organização.

Os equipamentos também devem ser protegidos contra ameaças físicas e ambientais, incluindo aqueles utilizados fora do perímetro da organização mas que contribuem no processamento da informação. A protecção deve ser compatível com os riscos previamente identificados.

4 A política de segurança diz respeito as regras que devem ser elaboradas e seguidas pelos utilizadores dos recursos de informação da organização.

2.1.5.3. Segurança Tecnológica

Este nível preocupasse com a definição de procedimentos e responsabilidades pela gestão e operação de todos os recursos usados para o processamento de informação, ou seja, visa garantir a operação segura e correctas das TIC na organização.

Aqui faz-se o planeamento e prepara-se a disponibilidade e os recursos dos sistemas para minimizar as vulnerabilidades, bem como prever a capacidade futura dos sistemas, de modo a reduzir riscos decorrentes da sobrecarga dos sistemas. Deve-se também prevenir e detectar a introdução de códigos maliciosos que alterem o comportamento desejado dos sistemas e os utilizados devem ser capazes de fazer face a situação caso esta verifique-se.

A segurança a nível de rede, da aplicação, as políticas de cópia de segurança, mecanismos de monitoramento e controle de actividades, gestão dos eventos gerados pelo sistema, e todas outras formas de segurança relacionadas com a comunicação e transmissão de dados no formato digital dentro e fora da organização são aqui tidas em conta.

2.2. SEGURANÇA EM APLICAÇÕES *WEB*

O rápido crescimento da Internet impulsionou a migração de aplicações originalmente de ambientes *desktops*[5] para o ambiente *web* pelas enormes vantagens que este oferece. Segundo Oliveira (2012), a *web* é um conjunto de documentos *onlines* que podem conter diversas informações em diferentes formatos, normalmente texto, imagens e vídeos, e que são interligadas.

A massiva difusão da *Word Wide Web* (também comumente designada por WWW, W3 ou simplesmente *web*) tem gerado um impacto significativo na sociedade contemporânea. Sistemas *Web* incluem um esquema de formatação de texto conhecido como *Hyper Text Markup Language* (HTML), um protocolo de comunicação conhecido como *Hyper Text Transference Protocol* (HTTP) e um esquema de identificação de recursos acessíveis através deste protocolo, conhecido como *Uniform Resource*

5 Programas que podem ser instalados na em computadores pessoais ou de mesa e que a sua usados depende da conexão a Internet

Identifier (URI). Estes componentes utilizam-se dos navegadores (*browsers*), para exibição e captura de informações, e da Internet, para a transmissão das informações.

São consideradas aplicações *web*, todos os sistemas informáticos projectadas para o ambiente *web*, ou seja, desenvolvidas para utilização através de um *browser*, na internet ou redes corporativas privadas (Intranet). Micheletti (2011) citando Pressman & Lowe (2009), conclui que o veículo que adquire a informação, a estrutura, monta uma apresentação empacotada e a entrega é chamado de aplicação *web*. Quando uma aplicação *web* é combinada com *hardware* cliente e servidor, sistemas operacionais, *software* de rede e navegadores surge um sistema baseado na *web*. Ou seja, as aplicações *web* somente existem dentro dos sistemas *web*.

Viegas (2008) afirma que o desenvolvimento da tecnologia *web* está relacionado, entre outros factores, a necessidade de simplificar o processo da actualização e manutenção, mantendo o código-fonte em um mesmo local de onde ele é acedido pelos usuários das mesmas.

2.2.1. Critérios de Segurança

De acordo com a plataforma upGuard (2016), disponibilizar um aplicação na Internet, implica estar sujeito à tentativas de ataque como a varredura de portas, inspecção de tráfego e extracção de dados.

A protecção de um *website* depende de vários critérios. Uma das formas mais comuns usadas por utilizadores da Internet é a verificação de certificados em *websites* que podem indicar se o este é confiável ou não, contudo não é suficiente basear-se apenas neste detalhe. Dados como *cookies* fornecidos pelos *websites* devem ser também protegidos, uma vez que estes contém informações sensíveis que podem ser usados em ataques de personificação (ver o ponto 2.2.3).

Neste contexto, a upGuard (2016) sugere 13 critérios que devem ser seguidos para a garantia de segurança em uma aplicação *web*.

Tabela 1: Critérios de Segurança

Critério	Descrição
[C1.] Garantir o SSL em todo *website*	Tripton & Krause (2014) afirmam que o SSL é um protocolo de encriptação desenvolvido pela *NetScape* para proteger a comunicação entre um servidor *web* e um navegador, pode ser usado para garantir a segurança de um *website*, correio electrónico, FTP e tráfego Telnet. Para a upGuard (2016), todas as páginas do *website* devem estar disponíveis somente através do SSL, informações transmitidas sem o SSL, são em texto claro e podem facilmente ser interceptadas por qualquer pessoa.
[C2.] Verificar Certificados SSL	Certificados SSL possuem validade, por isso torna-se imperioso saber qual é a duração dos certificados do *website* que pretende-se proteger garantindo assim um melhor controlo dos mesmos. É importante também saber se os certificados são reconhecidos pelos principais navegadores
[C3.] Usar a encriptação SHA256	Certificados usando o padrão SHA1 já não são suportados, tendo sido substituídos por um padrão mais recente que é o SHA256, por isso torna-se também importante verificar que padrão os certificados do site estão usando.
[C4.] Desabilitar conjunto de cifras inseguras	A maioria dos servidores *web*, ainda usa conjuntos de cifras inseguras, estes devem ser explicitamente desabilitados no servidor *web* (Apache, IIS) de forma que indivíduos mal-intencionados não possam explorá-las.
[C5.] Esconder dados do cabeçalho	Disponibilizar informações como a versão do servidor *web* que está a ser usada poder facilitar tentativas de ataque. É recomendado que este tipo de informação sobre o *website*, não seja disponibilizada aos visitantes, vários servidores *web* disponibilizam esta informação por padrão.
[C6.] Activar a segurança de Transporte restrita HTTP	A segurança de Transporte restrita HTTP garante que navegadores *web*, comuniquem-se com *website*s apenas por SSL, requisições que não sejam em SSL serão automaticamente convertidas para SSL. Falhas no uso desta técnica podem resultar em ataques do tipo *man-in-the-middle* (ver 2.2.3 para mais detalhes).
[C7.] Usar *Cookies HTTPOnly*	Garantir a segurança de cookeis previne que informações privadas dos visitantes no *website* o dos utilizadores da aplicação *web*, possam ser exploradas. O HTTPOnly restringe o acesso aos *cookies* de forma que somente *scripts* do lado do cliente e as falhas de XSS possam tirar vantagem de *cookies* armazenados.

Critério	Descrição
[C8.] Usar *cookies* Seguros	*Cookies* seguros podem somente ser transmitidos por uma conexão SSL. Isto previne que *cookies* com informação sensível possam ser rastreados na conexão entre o cliente e o servidor. O uso de SSL em todo *website* implica também o uso de *cookies* seguros.
[C9.] Proteger os processos do servidor *Web*	Processos do servidor *Web* não devem correr com altos graus de privilégios. Em sistemas Linux, a maioria dos servidores *web* correm em uma conta de utilizador dedicado com privilégios limitados, no entanto deverão ser verificadas sempre as permissões do utilizador. Em sistemas da Microsoft, a conta de utilizador deverá ser trocada para uma conta de serviço dedicado, esta conta não deve ter privilégios de administrador e deverá apenas aceder recursos necessários, isto previne que outros recursos da aplicação estejam vulneráveis.
[C10.] Garantir formas de validar dados de entrada	Todos formulários que colectam dados do utilizador devem ser validados de forma que somente dados considerados seguros possam ser armazenados. Este é considerado o primeiro passo para a protecção contra ataques do tipo injecção e outros ataques que possam introduzir dados inválidos.
[C11.] Garantir Protecção contra injecção SQL	O segundo passo mais importante para a protecção contra ataques de injecção SQL é utilizar procedimentos armazenados bem implementados que efectuar consultas abertas à base de dados. Restringindo a aplicação de correr procedimentos armazenados, tentativas de introdução de código SQL em formulários irão falhar.
[C12.] Proteger o *website* ou da aplicação contra ataques de negação de serviço DoS	Ataques de negação de serviços inundam servidores com conexões ou pacotes até que elas não sejam capazes de responder a requisições legítimas. Não existe uma forma de prevenir este tipo de ataques de forma absoluta, porque estes ataques usam conexões legítimas, porém existem medidas que possam ser tomadas.
[C13.] Testes Regulares de configuração	Controlar a duração dos certificados SSL é um aspecto fundamental para tal podem ser usados mecanismos que avisem partes responsáveis pela gestão da aplicação *web*, quando a data da expiração esteja próxima de forma que possam ser actualizados. A maioria de provedores de certificados são automaticamente reconhecidos pela maioria dos navegadores, mas é sempre viável verificar junto à companhia onde são adquiridos os certificados, o estado de actualização dos mesmos.

2.2.2. Vulnerabilidades frequentes segundo OWASP Top 10 2013

Stuttard & Pinto (2011) afirmam que, como toda nova tecnologia em constante desenvolvimento, as aplicações *web* apresentam um leque de vulnerabilidades que podem ser facilmente exploradas. Stuttard & Pinto (2011) ainda salientam que os ataques mais devastadores são aqueles em que os atacantes apoderam-se de dados sensíveis para a organização ou em que ganham acesso irrestrito aos *back-end* do sistema *web* em que a aplicação se encontra hospedada.

Associada ao crescente uso e demanda por aplicações *web* nos últimos anos, criminosos e indivíduos curiosos têm criado formas cada vez mais sofisticadas para a invasão de sistemas. Como apontado em Stuttard & Pinto (2011), a área da segurança em aplicações *web* tornou-se hoje o campo de batalha mais intenso e significativo entre os atacantes e os gestores de dados e de recursos computacionais, e afirmam também que é provável que permaneça assim por longos anos.

Oliveira, *et al*. (2015) frisa que o grande problema em relação às aplicações *web* é que mesmo a rede de comunicações em que estas se encontram hospedadas sendo seguras, com *firewall* [6], controlo de acesso entre outros mecanismos frequentemente usados para a manutenção da segurança, ainda é possível que um utilizador mal intencionado possa, por via de formulários *web* para a entrada de dados na aplicação, executar diversos tipos de ataques que escapam completamente ao controle da equipe de segurança de redes.

Vulnerabilidade é uma falha presente na segurança de um elemento do sistema que pode ser utilizada por um atacante ou utilizador mal-intencionada para deturpar o comportamento esperado deste elemento, sujeitando o sistema afectado a problemas como indisponibilidade, obtenção indevida de acesso privilegiado e controlo externo por indivíduos não autorizados.

De modo a colmatar o elevado índice de falhas de segurança que as aplicações *web* geralmente apresentam, diversas instituições e/ou organizações buscam trazer, no seio dos desenvolvedores e dos administradores de sistemas, práticas e metodologias que

6 *Firewall* é uma solução de segurança adoptada em redes de computadores, podendo esta, ser implementada em termos de *hardware* ou de *software*.

ajudem estes a manter as aplicações seguras e confiáveis. É nesse contexto que surge a *Open Web Application Security Project* (OWASP).

"A OWASP é uma comunidade *online* aberta, dedicada a capacitar as organizações a desenvolver, adquirir e manter aplicações confiáveis. A comunidade cria e disponibiliza de forma gratuita artigos, metodologias, documentação, ferramentas e tecnologias no campo de segurança de aplicações *web*" OWASP (2013, p. 3).

Segundo Oliveira (2012), os projectos realizados pela OWASP são divididos em duas principais categorias: de desenvolvimento e de documentação. Um dos projectos mais populares na área de documentação levados a cabo pela OWASP é o OWASP Top 10. Oliveira (2012) afirma que o OWASP Top 10 é um documento de alto nível que apresenta as vulnerabilidades mais críticas encontradas em aplicações *Web*.

"O OWASP Top 10 para 2013 é baseado em 8 conjuntos de dados de 7 empresas que se especializam em segurança de aplicações, incluindo 4 consultorias e 3 fornecedores de ferramenta/*Software* (...). Estes dados abrangem mais de 500.000 vulnerabilidades em centenas de organizações e milhares de aplicações. Os itens Top 10 são seleccionados e priorizados de acordo com dados de prevalência, em combinação com estimativas do consenso da exploração, detecção e impacto" (OWASP, 2013, p. 4).

De modo a classificar e definir os riscos existentes nas aplicações *web*, a OWASP criou a *Risk Rating Methodology* (Metodologia de Classificação Riscos). A metodologia de classificação de risco do OWASP foi desenvolvida de modo genérico, preocupando-se somente na identificação dos riscos mais sérios para uma ampla gama de organizações.

Agentes de Ameaça	Vetores de Ataque	Prevalência da Vulnerabilidade	Detecção Vulnerabilidade	Impactos Técnicos	Impactos no Negócio
Específico da Aplicação	Fácil	Generalizada	Fácil	Severo	Específico do Negócio/ Aplicação
	Média	Comum	Média	Moderado	
	Difícil	Rara	Difícil	Pequeno	

Figura 1: Metodologia de classificação de risco sendo a OWASP

Fonte: (OWASP, 2013, p. 6)

A figura acima mostra as listas dos elementos que compõem a metodologia. Segundo a OWASP (2013), o “Agente de Ameaça” e o “Impacto de Negócio” são particularidades específicas de cada organização, ou seja, o impacto de negócio várias de organização para organização assim como variará o agente de ameaça.

Um atacante pode, eventualmente, percorrer diversos caminhos dentro da aplicação para a concretização do ataque. Estes caminhos podem ser fáceis ou extremamente difíceis de serem explorados de forma similar os danos causados podem variar conforme exemplifica a figura 02.

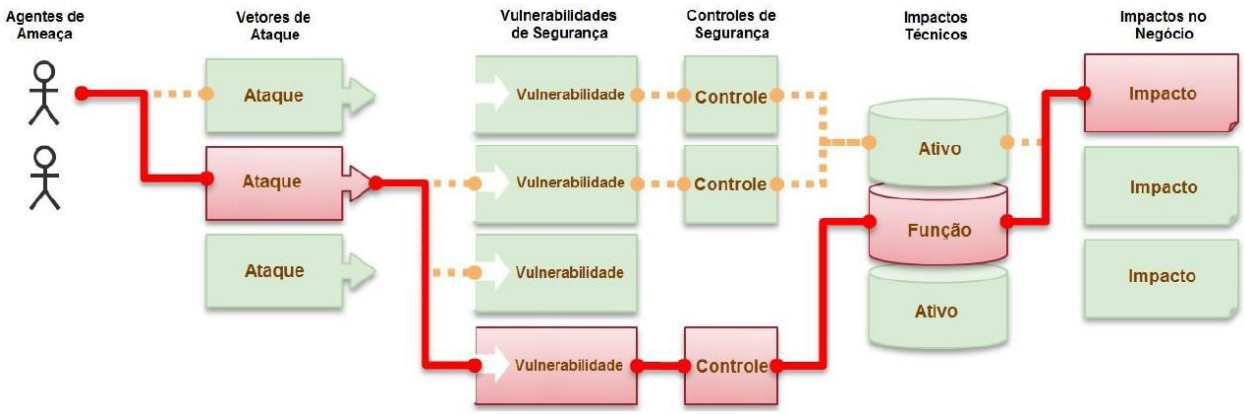


Figura 2: Caminhos percorridos pelo atacante

Fonte: (OWASP, 2013, p. 5)

Diante do exposto, apresenta-se de acordo com a pesquisa levada a cabo pela OWASP (2013), as 10 principais vulnerabilidades encontradas em aplicações *web*. A lista de vulnerabilidades está disposta de acordo com o grau de incidência da mesma e as vulnerabilidades possuem códigos de identificação na faixa de **A1 – A10**.

2.2.3.1. Injecção (A1)

A vulnerabilidade da injecção caracteriza-se pela possibilidade de qualquer utilizador do sistema, seja este interno devidamente credenciado, administrador ou mesmo atacante, enviar dados não confiáveis a base de dados do sistema. “As falhas de Injecção, tais como injecção de SQL, de SO (Sistema Operacional) e de LDAP, ocorrem quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta. Os dados manipulados pelo atacante podem iludir o interpretador para que este execute comandos indesejados ou permita o acesso a dados não autorizados” (OWASP, 2013, p. 7).

De acordo com o projecto OWASP (2013), a classificação do risco de injecção é a seguinte: o vector de ataque é simples pois pode ser constituído por qualquer fonte de dados. A detecção é media porque é fácil de identificar quando se faz uma verificação do código fonte da aplicação. A tabela abaixo apresenta de forma resumida a classificação do risco de injecção.

Tabela 2: Classificação do risco de Injecção

Fonte: adaptado de OWASP (2013)

Agentes de Ameaça	**Vectores de Ataque**	**Vulnerabilidade**		**Impactos Técnicos**	**Impactos no Negócio**
Específico da Aplicação	**Exploração**	**Prevalência**	**Detecção**	**Impacto**	Específico do Negócio/Aplicação
	Fácil	Comum	Média	Severo	

2.2.3.2. Quebra de Autenticação e Gestão de Sessão (A2)

Esta vulnerabilidade caracteriza-se quando a aplicação apresenta falhas em áreas como o gerenciamento de sessões, gestão de palavras-chave, questões secretas e de actualizações. “As funções da aplicação relacionadas com autenticação e gerenciamento de sessão geralmente são implementadas de forma incorrecta, permitindo que os atacantes comprometam senhas, chaves e *tokens* de sessão ou, ainda, explorem outra falha da implementação para assumir a identidade de outros usuários” (OWASP, 2013, p. 7).

Tabela 3: Classificação do risco de Quebra de Autenticação e Gestão de Sessão

Fonte: adaptado de OWASP (2013)

Agentes de Ameaça	**Vectores de Ataque**	**Vulnerabilidade**		**Impactos Técnicos**	**Impactos no Negócio**
Específico da Aplicação	**Exploração**	**Prevalência**	**Detecção**	**Impacto**	Específico do Negócio/Aplicação
	Média	Generalizada	Média	Severo	

2.2.3.3. *Cross-Site Scripting* (XSS) (A3)

De acordo com a OWASP Top 10 (2013), a XSS é a mais predominante falha de segurança em aplicações *web*. Constata-se este tipo de vulnerabilidade quando a aplicação inclui dados fornecidos pelo utilizador na página, enviados ao navegador, sem ter sido feita a devida validação ou filtro dos mesmos. As falhas de XSS são geralmente agrupadas em 3 grupos:

- **Persistentes:** são aquelas falhas em que os dados não seguros são armazenados em algum meio para que posteriormente sejam recuperados;
- **Reflectido:** este caracteriza-se por receber os dados não seguros de um determinado utilizador e encaminhá-los directamente para o *browser*;
- **XSS baseado em DOM:** actua criando ou manipulando código do lado do cliente na página.

De acordo com o projecto OWASP Top 10 (2013), a classificação do risco pode ser resumida na tabela abaixo.

Tabela 4: Classificação do risco de XSS

Fonte: adaptado de OWASP (2013)

Agentes de Ameaça	**Vectores de Ataque**	**Vulnerabilidade**		**Impactos Técnicos**	**Impactos no Negócio**
Específico da Aplicação	**Exploração**	**Prevalência**	**Detecção**	**Impacto**	Específico do Negócio/Aplicação
	Média	Muito difundida	Fácil	Moderado	

2.2.3.4. Referência Insegura e Directa a Objectos (A4)

Este tipo de vulnerabilidade verifica-se quando o programador e/ou desenvolvedor da aplicação *web* expõe uma referência a objectos internos da aplicação e o atacante consegue alterar esse parâmetro obtendo, deste modo, acesso a informações confidenciais contidas no sistema. De acordo com a OWASP Top 10 (2013), uma referência insegura e directa a um objecto ocorre quando um programador expõe uma referência à implementação interna de um objecto, como um arquivo, directório, ou registro da base de dados. Sem a verificação do controle de acesso ou outra protecção, os atacantes podem manipular estas referências para aceder dados não-autorizados.

Este tipo de ataque é geralmente perpetuado por utilizadores devidamente autenticados no sistema que alteram propositadamente o valor de um parâmetro, cujo este refere-se directamente a um objecto no sistema para um outro objecto no qual não possui autorização para o aceder. A tabela abaixo sintetiza a classificação do risco.

Tabela 5: Classificação do risco de Referência Insegura e Directa a Objectos

Fonte: adaptado de OWASP (2013)

Agentes de Ameaça	**Vectores de Ataque**	**Vulnerabilidade**		**Impactos Técnicos**	**Impactos no Negócio**
Específico da Aplicação	**Exploração**	**Prevalência**	**Detecção**	**Impacto**	Específico do Negócio/Aplicação
	Fácil	Comum	Fácil	Moderado	

2.2.3.5. Configuração Incorrecta de Segurança (A5)

A vulnerabilidade de configuração incorrecta de segurança pode verifica-se quando se esta presente diante dos seguintes casos:

- Quando actualizações não são instaladas;
- Quando os *softwares* não são devidamente configurados;
- Quando utilizadores e senhas que activam o *software* são mantidas.

A OWASP (2013) defende que para a manutenção de um nível aceitável de segurança, é necessário que se defina uma configuração segura e que esta seja implementada na aplicação, nos *frameworks*, nos servidores de aplicação, nos servidores *web*, na base de dados e na plataforma.

A exploração é considerada fácil pois o atacante utiliza-se, por exemplo, de contas criadas por padrão na instalação de sistemas. O impacto é moderado pois, uma vez esta vulnerabilidade é explorada, pode comprometer por completo o Sistema.

Tabela 6: Classificação do risco de Configuração incorrecta de segurança

Fonte: adaptado de OWASP (2013)

Agentes de Ameaça	**Vectores de Ataque**	**Vulnerabilidade**		**Impactos Técnicos**	**Impactos no Negócio**
Específico da Aplicação	**Exploração**	**Prevalência**	**Detecção**	**Impacto**	Específico do Negócio/Aplicação
	Fácil	Comum	Fácil	Moderado	

2.2.3.6. Exposição de Dados Sensíveis (A6)

De acordo com o projecto OWASP Top 10 (2013), muitas aplicações *web* não protegem devidamente os dados sensíveis, tais como cartões de crédito e credenciais de autenticação. Os atacantes podem roubar ou modificar esses dados desprotegidos com o propósito de realizar fraudes de cartões de crédito, roubo de identidade, ou outros crimes. Os dados sensíveis merecem protecção extra como criptografia no armazenamento ou em trânsito, bem como precauções especiais quando trafegadas pelo navegador.

Tabela 7: Classificação do risco de exposição de dados sensíveis

Fonte: adaptado de OWASP (2013)

Agentes de Ameaça	**Vectores de Ataque**	**Vulnerabilidade**		**Impactos Técnicos**	**Impactos no Negócio**
Específico da Aplicação	**Exploração**	**Prevalência**	**Detecção**	**Impacto**	Específico do Negócio/Aplicação
	Difícil	Rara	Média	Severo	

2.2.3.7. Falta de Função para Controle de Nível de Acesso (A7)

Aplicações nem sempre protegem adequadamente as funções de aplicação. De acordo com a OWASP (2013), a maioria das aplicações *web* verificam os direitos de acesso em nível de função antes de tornar essa funcionalidade visível na interface do usuário. No entanto, as aplicações precisam executar as mesmas verificações de controlo de acesso no servidor quando cada função é invocada. Se estas requisições não forem verificadas, os atacantes serão capazes de forjar as requisições, com o propósito de aceder a funcionalidade sem autorização adequada.

Tabela 8: Classificação do risco de falta de função para controle de nível de acesso

Fonte: adaptado de OWASP (2013)

Agentes de Ameaça	**Vectores de Ataque**	**Vulnerabilidade**		**Impactos Técnicos**	**Impactos no Negócio**
Específico da Aplicação	**Exploração**	**Prevalência**	**Detecção**	**Impacto**	Específico do Negócio/Aplicação
	Fácil	Comum	Médio	Moderado	

2.2.3.8. *Cross-Site Request Forgery* (CSRF) (A8)

A vulnerabilidade de CSRF verifica-se quando existe a possibilidade de um atacante conseguir falsificar uma requisição HTTP idêntica a uma requisição original. De acordo com a OWASP Top 10 (2013), este ataque caracteriza-se por forçar a vítima que possui uma sessão activa em um navegador a enviar uma requisição HTTP forjada, incluindo o *cookie* da sessão da vítima e qualquer outra informação de autenticação incluída na sessão, a uma aplicação *web* vulnerável.

Esta vulnerabilidade geralmente está associada ao uso de *cookies* de sessão. A tabela abaixo apresenta a classificação do risco.

Tabela 9: Classificação do risco de CSRF

Fonte: adaptado de OWASP (2013)

Agentes de Ameaça	**Vectores de Ataque**	**Vulnerabilidade**		**Impactos Técnicos**	**Impactos no Negócio**
Específico da Aplicação	**Exploração**	**Prevalência**	**Detecção**	**Impacto**	Específico do Negócio/Aplicação
	Médio	Comum	Fácil	Moderado	

2.2.3.9. Utilização de Componentes vulneráveis Conhecidos (A9)

São ataques direccionados a componentes que geralmente são executados com privilégios elevados, componentes tais como bibliotecas, *framework*s, e outros módulos de *software*. O projecto OWASP Top 10 (2013) afirma que se um componente vulnerável é explorado, um ataque pode causar sérias perdas de dados ou o comprometimento do servidor. As aplicações que utilizam componentes com vulnerabilidades conhecidas podem minar as suas defesas e permitir uma gama de possíveis ataques e impactos.

Tabela 10: Classificação do risco de exploração de componentes vulneráveis

Fonte: adaptado de OWASP (2013)

Agentes de Ameaça	**Vectores de Ataque**	**Vulnerabilidade**		**Impactos Técnicos**	**Impactos no Negócio**
Específico da Aplicação	**Exploração**	**Prevalência**	**Detecção**	**Impacto**	Específico do Negócio/Aplicação
	Médio	Generalizada	Difícil	Moderado	

2.2.3.10. Redireccionamentos e Encaminhamentos Inválidos (A10)

Uma das características principais das aplicações *web* é o facto delas funcionaram com base em redireccionamento e encaminhamento dos utilizadores em diversas páginas e *sites* internas ou externas a aplicação. A especificação da URL da página ou site de destino faz-se colectando dados directos dos navegadores.

O projecto OWASP Top 10 (2013) afirma que os erros de redireccionamento e encaminhamentos inválidos ocorrem quando um atacante aponta para um redireccionamento inválido enganando assim as suas vítimas. Tais redireccionamentos podem tentar instalar *malware* ou enganar as vítimas de modo que estas divulguem suas senhas ou outras informações sensíveis aos sistemas ou a organização.

O atacante usa encaminhamentos inseguros para evitar as verificações de segurança. A tabela abaixo apresenta o resumo do risco.

Tabela 11: Classificação do risco de redireccionamentos e encaminhamentos inválidos

Fonte: adaptado de OWASP (2013)

Agentes de Ameaça	**Vectores de Ataque**	**Vulnerabilidade**		**Impactos Técnicos**	**Impactos no Negócio**
Específico da Aplicação	**Exploração**	**Prevalência**	**Detecção**	**Impacto**	Específico do Negócio/Aplicação
	Média	Rara	Fácil	Moderado	

2.2.3. Tipos de Ataques

Os ataques mais comuns a aplicações *web* os de negação de serviços e os ataques intercepção de tráfego. Existem também outros ataques como os de personificação (em que o atacante obtém credenciais de utilizadores legítimos do sistema e faz-se passar por estes) mas são considerados uma variação dos de intercepção de tráfego. A seguir faz-se a descrição dos ataques mais comuns.

2.2.3.1. Ataque de Negação de Serviços

De acordo com Orinayo (2016), a negação de serviço é um tipo de ataque que visa prevenir a comunicação normal com um recurso, desabilitando o próprio recurso ou desabilitando um dispositivo de infra-estrutura que oferece conectividade a este. O recurso desabilitado pode ser na forma de dados do cliente, recursos da aplicação ou

um serviço específico. A forma mais comum de DoS é enviar requisições de diferentes meios a uma vítima que faram com que todos os recursos disponíveis do sistema fiquem sobrecarregados e incapazes de atender a novos pedidos. Normalmente o atacante inunda a rede ou a aplicação vítima com quantidades extremamente grandes de dados inúteis ou solicitações de dados, abrandando a rede e tornando-a inútil ou não disponível para usuários legítimos.

Quando um sistema encontra-se sobre esse tipo de ataque apresenta as seguintes características:

- Falta de disponibilidade de um recurso do sistema ou aplicação;
- Perda de acesso a aplicação;
- Desempenho lento;
- Aumento de *emails* de *spam*.

2.2.3.2. Ataque de Intercepção (*man-in-the-middle*)

Ataques de Intercepção ou sequestro de sessão são perpetrados por indivíduos que se posicionam entre um utilizador e o sistema, interceptando alguns pacotes de conexão. Orinayo (2016) afirma que os atacantes se colocam entre o usuário e a aplicação, permitindo-lhes monitorar o tráfego do usuário e lançar ataques específicos. Uma vez que ocorreu um roubo de sessão bem-sucedido, o atacante pode assumir o papel do usuário legítimo ou simplesmente monitorar o tráfego por momentos oportunos para injectar ou colectar pacotes específicos para criar o efeito desejado.

Orinayo (2016) ainda afirma que os ataques do tipo de roubo de sessão são fáceis de executar. As redes TCP / IP são vulneráveis, e a maioria das contramedidas, excepto criptografia, não funcionam contra este tipo de ataque. Também contribuem para este tipo de ataque os seguintes cenários:

- Não bloqueio de contas por excesso de tentativas falhadas de *login*.
- Manipulação insegura
- Algoritmos fracos para a geração de códigos de sessão;
- Sessões sem tempo de expiração;
- Dados transmitidos em texto puro;
- Códigos de sessões com poucos dígitos.

2.2.4. Testes de Intrusão

Sistemas são geralmente desenvolvidos para facilitar o compartilhamento de dados e informações importantes entre utilizadores de uma organização, assim sendo, é crucial garantir que estes apresentem um nível aceitável de segurança. Por forma a garantir a segurança física ou dos seus sistemas de informação, as organizações têm recorridos a práticas que simulem ou se assemelhem a ataques reais perpetrados por indivíduos mal-intencionados de modo a ganhar acesso ao perímetro interno da organização ou aos dados e informações contidas nos seus sistemas. Uma das formas que se tem recorrido regularmente são os testes de intrusão.

Tripton & Krause (2014) definem testes de penetração ou de intrusão como sendo um conjunto de procedimentos levados a cabo para quebrar ou enganar a segurança de um sistema ou duma organização com o intuito de testar a resistência do sistema ou da organização mediante a ocorrência de um ataque real. Geralmente, estes consistem em efectuar uma série de ataques a um sistema alvo de modo a identificar as vulnerabilidades deste e para determinar possíveis vias que atacantes podem usar para comprometer o sistema.

O objectivo geral de um teste de intrusão é de determinar a capacidade do sistema de resistir a um ataque por um intruso hostil. Para tal, é imperativo que o testador use truques e técnicas que um invasor da vida real pode usar. Esta estratégia de ataque simulada permite que a organização descubra e mitigue seus pontos fracos de segurança antes de um invasor real descobri-los. Para Tripton & Krause (2014), o sucesso ou falha dos ataques efectuados, e como o alvo reage a cada destes ataques, determinará o resultado do teste.

É importante salientar que testes de intrusão não só são realizados em sistemas computacionais. De acordo com o tipo de teste a ser efectuado, este pode incluir desde tentativa de invasão física (obter acesso as instalações da organização) até a invasão das aplicações da companhia.

Tripton & Krause (2014) salientam que existem três condições básicas que devem ser consideradas para se tirar maior proveito dos testes:

- O teste deve ter um objectivo definido e este deve ser claramente documentado. Quanto mais específicos forem os objectivos definidos, mais fácil será para avaliar o sucesso ou o fracasso do teste;
- Deve-se definir o tempo certo no qual realizar-se-ão os testes de modo que a actividade não interrompa os processos da organização. O tempo estipulado para a realização do teste deve ser definido de acordo com os objectivos, o tamanho do sistema e o nível da ameaça; e
- O teste deve ser autorizado pela gestão da organização onde decorrerá, visto que o testador usa técnicas similares as dos ataques. A autorização é importante para diferenciar um deste de penetração legítimo de uma tentativa de invasão maliciosa no sistema.

2.2.5.1. Vantagens dos Testes de Intrusão

De acordo com António (2013), os testes de intrusão oferecem as seguintes vantagens:

- Determinar a viabilidade de um determinado conjunto de vectores de ataque;
- Identificar vulnerabilidades de alto risco que resultam de uma combinação de vulnerabilidades de menor risco explorado em uma determinada sequência;
- Identificar vulnerabilidades que podem ser difíceis ou impossíveis de detectar com rede automatizada ou *software* de digitalização de vulnerabilidade de aplicativos;
- Na avaliação da magnitude do potencial de negócios e os impactos operacionais de ataques bem-sucedidos;
- Testar a capacidade dos defensores de rede para detectar e responder com sucesso aos ataques;
- Fornecer evidências para apoiar o aumento dos investimentos em pessoal de segurança e tecnologia.

2.2.5.2. Tipos de Testes de Intrusão

Os testes de penetração são agrupados de acordo com a quantidade de informação que *tester* contém sobre o sistema alvo e estes dividem-se em três principais categorias:teste da caixa branca (*white-box*), teste da caixa cinza (*grey-box*) e teste da caixa preta (*black-box*).

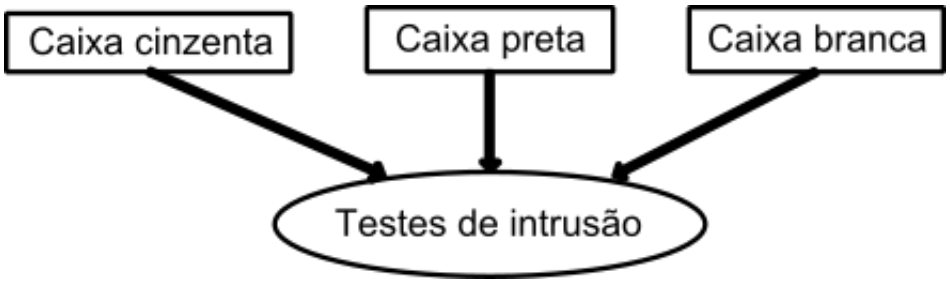


Figura 3: Tipos de Teste de Intrusão

Fonte: Autor

Caixa Branca

Neste tipo de teste, considera-se que o *tester* contém informações tais como, a arquitectura, o código fonte, detalhes do sistema operativo e do servidor, endereço IP entre outras, completa sobre sistema alvo. É normalmente considerado como um ataque proveniente de dentro da organização, ou seja, levado a cabo por alguém, que de certa forma, contém informações precisas sobre a empresa.

Caixa Preta

O oposto do *white-box*, neste tipo considera-se que o *tester* não dispõe de nenhuma informação sobre o alvo e nem como este será executado.

Caixa Cinzenta

Estes representam o meio-termo entre o *white-box* e *o black-box*, assume-se que o *tester* possui conhecimento limitado a respeito do sistema alvo. É considerado como sendo ataque de um individuo externo que teve acesso a informações da organização.

2.2.5.3. Metodologias de Testes

De forma a maximizar o resultado obtido em testes de penetração, muitas organizações tem usado como base metodologias e padrões reconhecidos internacionalmente. Guimarães (2013) afirma que as metodologias representam uma segurança tanto para o *tester*[7] quanto para a organização ou cliente requisitante do teste. O cliente tem a segurança de saber que o teste foi executado com base em padrões reconhecidos

7 *Tester* é o individuo ou empresa responsável pela realização dos testes de intrusão.

internacionalmente, assinada por profissionais da área de segurança de informação, garantindo assim que seja avaliada a maior quantidade de vulnerabilidades possíveis e este pode saber exactamente os pontos de falhas que foram testados no decurso do processo. Guimarães (2013) ainda afirma que para os profissionais que executam os testes, os padrões contribuem para que se faça uma análise muito mais rápida e assertiva.

Borges & Helena (2011) afirmam que a metodologia é a fundamental na execução de um teste de penetração, pois esta consiste justamente de um conjunto de procedimentos de ataque e registos, usados contra uma rede ou um sistema. As metodologias existentes diferenciam-se uma das outras pela forma como está realiza ou divide as fases durante a execução do teste, pois o objectivo final de todas é o mesmo (identificar pontos de falhas).

No presente trabalho abordar-se-á três das metodologias internacionais frequentemente usadas: *Open Source Security Testing Methodology Manual* (OSSTMM), *OWASP Testing Guide* e *Information System Security Assessment Framework* (ISSAF).

***Open Source Security Testing Methodology Manual* (OSSTM)**

Segundo Borges & Helena (2011), a metodologia OSSTMM foi desenhada para ser consistente e de resultados reproduzíveis, se baseando fortemente nos conceitos de segurança humana, física, sem fio, de telecomunicações e de redes de dados. De acordo com Bertoglio & Zorzo (2015, pp. 22-23), essa metodologia, os testes podem são divididos em seis padrões principais como mostra a figura abaixo.

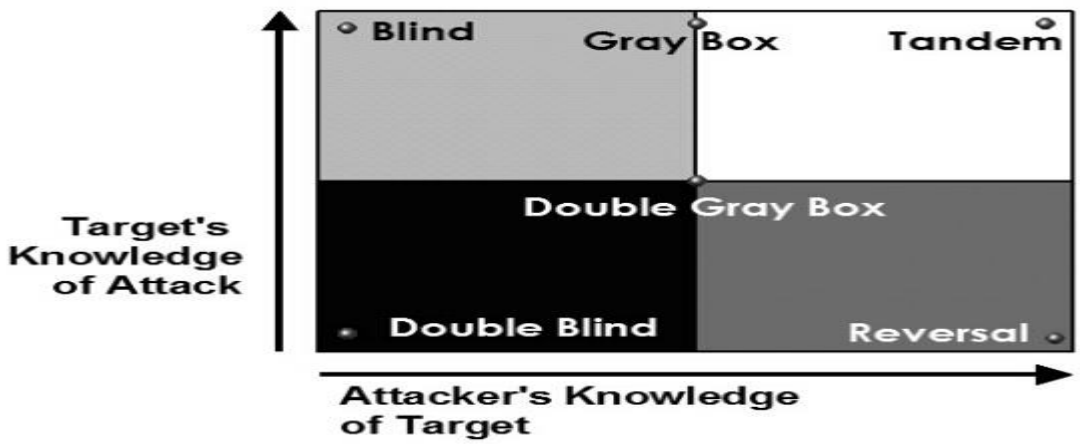


Figura 4: Tipos de acordo com OSSTMM[8]

- ***Blind*:** o teste é feito sem nenhum conhecimento do prévio do alvo sobre suas defesas, activos ou canais. O alvo é preparado para a auditoria, cujo objectivo principal pode ser considerado como o teste de habilidades do analista.
- ***Double Blind:*** similar ao *blind*, o *Double Blind* descreve um teste onde além do *tester* não ter nenhum conhecimento prévio sobre o alvo, o alvo também não recebe a notificação sobre o teste.
- ***Gray box:*** o teste é realizado com conhecimento limitado das defesas do alvo e seus activos, porém com completo conhecimento de seus canais. O alvo é preparado para a auditoria, sabendo todo o processo que será auditado. Este é também conhecido como Teste de Vulnerabilidade.
- ***Double gray box:*** diferencia-se do *gray box* pelo facto de que neste o alvo é notificado com antecedência apenas sobre o escopo e o tempo de duração da auditoria, mas este não contém informações sobre os canais testados ou vectores de teste.
- ***Tandem*:** neste tipo de teste, o alvo e o *tester* são preparados para a auditoria e possuem completo conhecimento sobre os detalhes da mesma, desconsiderando a avaliação do quanto o alvo está preparado para acções de teste e comportamentos desconhecidos dom ponto de vista de segurança. Este também é conhecido como Teste C*ristal Box*.
- ***Reversal*:** nesta abordagem, o *tester* tem em sua posse o pleno conhecimento sobre o alvo, e o alvo não possui nenhum conhecimento sobre o que, como e quando será o teste. O teste *Reversal* objectiva-se avaliar a preparação do alvo para as acções e comportamentos desconhecidos em relação a sua segurança.

Após a execução do teste, passa-se para a fase de análise e mensuração dos resultados obtidos. Bertoglio & Zonzo (2015) afirmam que a metodologia utiliza a ideia de *Risk Assessment Values* (RAV) para mensurar os resultados dos testes. Borges & Helena (2011) citando Fullerton (2010), esclarecem que cada secção receberá um valor RAV

8 Fonte: https://www.slideshare.net/floresj2003/osstmm3

correspondente. Este RAV será utilizado para mensurar a segurança de uma maneira consistente e reproduzível independente do auditor.

Guião de Testes OWASP (***OWASP Testing Guide***)

É uma metodologia completamente voltada para testes em aplicações *web* disponibilizada pela OWASP. De acordo com Santos & Nunes (2010), esta metodologia serve como guia que busca cobrir todas as características de um processo de testes de segurança de *software*, compreensivo e completo.

Bertoglio & Zonzo (2015) consideram que a metodologia propícia para testar aplicações *web* em execução, de maneira remota, para encontrar vulnerabilidades sem ter o conhecimento sobre os aspectos inerentes ao funcionamento da aplicação. A metodologia divide o processo de teste em três camadas:

- **Introdutória:** trata dos pré-requisitos para testar as aplicações *web* e também do escopo dos testes;
- **Intermediária:** apresenta o OWASP *Testing Guide Framework*, suas tarefas e técnicas relacionadas as diversas fases do ciclo de desenvolvimento de *software*;
- **Conclusiva:** etapa que descreve como as vulnerabilidades são testadas através da inspecção do código e dos testes de penetração.

Information System Security Assessment Framework (**ISSAF)**

A metodologia ISSAF sugere um método para evitar vulnerabilidades que possam ocorrer no sistema que será testado. Os principais testes da ISSAF estão relacionados com a segurança de rede, de *host*, de aplicação e da base de dados.

A metodologia ISSAF é dividida em três fases:

- Planeamento e preparação: fase onde são trocadas informações iniciais para planeamento e preparação dos testes para avaliação do sistema.
- Avaliação: é nesta fase em que se efectuam os testes propriamente ditos e ela divide-se em:
    1. Colecta de informações;
    2. Mapeamento da rede;
    3. Identificação de vulnerabilidades;

4. Penetração;
5. Acesso e escalação de privilégios;
6. Enumeração;
7. Comprometer usuários remotos;
8. Manutenção de acesso;
9. Cobrindo rastos.

- Relatórios e limpeza: nesta fase, é apresentado o relatório de todos os testes executados, mas se algum erro ou vulnerabilidade forem encontrados durante os testes, devem ser avisados antes do término da avaliação do sistema e geração dos relatórios.

2.2.5. Scanners de Vulnerabilidades Web

Como acima descrito, umas das fases importantes durante a realização dos testes de intrusão consiste na identificação de vulnerabilidades do sistema. Para a identificação de vulnerabilidades em aplicações *web*, especialista em segurança fazem uso de ferramentas automatizadas comumente designadas por *scanners* de vulnerabilidades.

Segundo Basso (2010), *scanners* de vulnerabilidade são ferramentas utilizadas para testar aplicações *web* em busca de falhas de segurança que podem ser aproveitadas por atacantes por forma a assumir o controlo destas. Eles são capazes de identificar automaticamente vulnerabilidades de segurança introduzidas no código fonte e podem ser utilizados durante o processo de concepção da aplicação.

De acordo com Basso (2010), tais ferramentas funcionam com base em três fases: configuração, rastreamento e exploração. Na fase de configuração, define-se URL da aplicação *Web* que se pretende identificar as vulnerabilidades e faz-se também a definição de demais parâmetros necessários, como, por exemplo, a utilização de *proxy*[9] ou certificados de segurança. Alguns *scanners* também apresentam, nessa fase, recursos para autenticação na aplicação.

Na fase de rastreamento, a maioria dessas ferramentas fornecem um mapa de como a aplicação *web* se encontra internamente estruturada. A partir da página inicial da aplicação *web*, o *scanner* examina o código procurando por ligações ou endereços de

9 Servidor intermediário entre o cliente e a internet.

outras páginas. Cada endereço encontrado é registado e repete-se o procedimento até que *links* e páginas não sejam mais encontrados.

É na fase de exploração onde os testes de intrusão são efectuados automaticamente contra a aplicação *web* simulando acções de um usuário (cliques em links e preenchimento de dados maliciosos em campos de entrada). Diversos testes são executados de acordo com o algoritmo interno da ferramenta e as requisições e respostas de cada teste são armazenadas e analisadas de acordo com as políticas de vulnerabilidades da ferramenta em uso. As respostas também são analisadas usando dados colectados durante a fase de rastreamento. Ao final, os resultados são exibidos ao usuário e podem ser salvos para uma análise posterior. A maioria dos *scanners* também fornecem informações sobre as vulnerabilidades detectadas e as maneiras de evitá-las ou corrigi-las.

Basso (2010) ainda afirma que os testes levados a cabo na fase de exploração baseiam-se em um conjunto de dados e informações que os *scanners* possuem sobre vulnerabilidades de segurança já conhecidas e estas são actualizadas de acordo com o surgimento e/ou descobrimento de novas vulnerabilidades. Essas ferramentas possuem um conjunto de testes predefinidos para cada uma das vulnerabilidades conhecidas.

Existem diferentes ferramentas que são utilizadas para a realização do *scan* vulnerabilidades e estás diferenciam-se umas das outras pela forma como executam cada umas acima expostas e pela forma como geram o relatório dos resultados do teste. Na tabela abaixo, apresentam-se algumas das ferramentas mais usadas para o *scan* de vulnerabilidades em aplicações *web*.

Tabela 12: Exemplos de *scan*ners de Vulnerabilidade

Ferramenta	Fabricante	Descrição	Tipo de Teste Disponibilizado	Frequência de Actualização
Acunetix WVS	Acunetix	Ferramenta que automaticamente avalia vulnerabilidades como injecções de SQL, SCRF, criação/exclusão de arquivos e os métodos de autenticação em aplicações *web*.	Caixa preta, cinza e branca	Regular
Burp Suite	Portswigger	Plataforma integrada para testes de segurança em aplicações *web*. Possuem várias ferramentas que suportam todo o processo de teste, desde o mapeamento inicial e a análise da superfície de ataque de um aplicativo até a busca e a exploração de vulnerabilidades de segurança.	Caixa branca	Não regular
*Web*Inspect	HP	Ferramenta automatizada e configurável para segurança em aplicações *web* e teste de intrusão que simula técnicas e ataques do mundo real, permitindo que seus clientes analisem minuciosamente vulnerabilidades de segurança em suas aplicações e serviços *web*.	Caixa branca	Regular
App*Scan*	IBM	Ferramenta que melhora a segurança das aplicações *web* e a segurança das aplicações móveis, melhora a gestão de programas de segurança de aplicativos e fortalece a conformidade regulamentar. Ao analisar suas aplicações *web* e móveis antes da implantação, *o AppScan* permite identificar vulnerabilidades de segurança, gerar relatórios e propor correcções.	Caixa preta ou branca	Regular
*Web*Scarab	OWASP	Ferramenta de testes de segurança para aplicações *web*. Ela funciona como um *proxy* que intercepta e permite que as pessoas alterem as solicitações da *web* do navegador (HTTP e HTTPS) e as respostas do servidor *web*. O *WebScarab* também pode registrar o tráfego para uma revisão posterior.	Caixa branca	Não regular

Para a realização do scan de vulnerabilidades, a ferramenta escolhida deve permitir que se possa efectuar qualquer um dos tipos de testes supra descritos (caixa branca, preta e cinza), tenha uma actualização regular [10] de modo que inclua todas possíveis vulnerabilidades identificadas e que seja possível gerar relatórios a partir desta.

Da Tabela 12, podem observar-se que as ferramentas Acunetix WVS e AppScan apresenta uma actualização regular e ambas permitem que o *tester* excute qualquer uma das modalidades de testes de intrusão. Contudo, há que salientar que ambos *softwares* são proprietários e requerem licenças para o seu uso pleno. De modo a colmatar isso, o autor fez uso de versões gratuitas desses *softwares* tendo este constado que o AppScan somente pode ser usado para testar aplicações previamente disponibilizadas pela empresa e que nesta versão não podiam ser realizadas testes a aplicações reais ao contrário da Acunetix WVS. Assim sendo, para o scan de vulnerabilidades das aplicações no escopo do presente trabalho, será usada a ferramenta Acunetix WVS.

2.2.5.1. **Acunetix WVS**

De acordo com o site da empresa proprietária do *software* Acunetix (2017), o Acunetix WVS é a ferramenta de scan de vulnerabilidade web mais avançada usada principalmente para testes de intrusão do tipo caixa preta. A ferramenta detecta de modo automatizado vulnerabilidades XSS, SQL *Injection*, verificador de arquivos e directórios, e outras em aplicações web.

Características principais

- Analisador automático de Java script, permitindo testes de segurança de Ajax e em aplicações Web;
- Possui sistema de testes de XSS e SQL *injection*;
- É um scanner multi-threads;
- Contém um rastreador que detecta o tipo de servidor web e linguagem da aplicação;

[10] São consideradas ferramentas com actualizações regulares aquelas que têm períodos curtos de actualizações (superior ou igual a 2 por ano) por forma a acomodarem novas vulnerabilidades descobertas. Grande número das ferramentas gratuitas foram desconsideradas por esse factor.

- Rastreia e analisa sites, incluindo conteúdo em Flash, SOAP e AJAX;
- Não é de código aberto, sendo um *software* proprietário, porém possui versão gratuita e funciona nas plataformas Microsoft Windows.

Olhando para os aspectos de segurança das aplicações web, a ferramenta apresenta as seguintes vantagens:

- O detalhamento de vulnerabilidades encontradas, como o tipo e local (directório e/ou ficheiro) onde se encontra na aplicação web testada;
- A classificação da vulnerabilidade em quatro níveis de ameaça (alto, médio, baixo e informativas) de acordo com o grau de exposição desta;
- Exibe a estrutura da aplicação alvo, bem como, os resultados encontrados na busca;
- Ela apresenta informações da aplicação web testada, como por exemplo, sistema operacional (UNIX Ubuntu) instalado no servidor, nome e versão do servidor web (Apache/2.2.22), tecnologias utilizada (PHP/ASP/ASP.Net entre outras) durante o teste e susceptibilidade da aplicação (sim/não);
- Estatísticas da aplicação, como tempo de verificação e número de requisições efectuadas durante o processo;
- Exibe uma janela de actividades, dividida em *logs* da aplicação e registros de erros. (Acunetix, 2017).

3. CAPÍTULO III – CASO DE ESTUDO: PORTAL ELECTRÓNICO DO GOVERNO DE MOÇAMBIQUE

3.1. Governação Electrónica

Hoje vivemos num mundo cada vez mais globalizado em que podemos realizar diversas tarefas usando os meios electrónicos, provocando assim mudanças significativas em muitas práticas organizacionais quem têm sido optimizadas.

O acesso à informação é um dos principais factores que proporciona o desenvolvimento das sociedades. Marisa *et al*. (2014) afirmam que o uso das TIC contribuíram substancialmente o nível de conhecimento da sociedade e das comunidades, pois estas permite-lhes estarem melhor equipadas sob o ponto de vista da acessibilidade da informação, diminuindo assim distâncias e facilitando múltiplas interacções entre cidadãos e os Governos de forma rápida e bruta, contribuindo para o empoderamento do acesso à informação, deixando as pessoas com conhecimentos relevantes e cruciais para desenvolver o País.

De forma a disponibilizar informações e serviços aos cidadãos e a outras entidades, diversos governos apoiam-se no uso das TIC. É neste contexto que surge o termo Governação Electrónica. De acordo com Martins & Ramos (2008), o governo pode ser definido como um conjunto de indivíduos responsáveis por decidir, operacionalizar e controlar as políticas de um determinado Estado[11].

Marisa *et al*. (2014) definem a governação electrónica como sendo a aplicação das TIC para governação através da difusão de informações de utilidade pública e da provisão de serviços públicos aos cidadãos, ao empresariado e à sociedade civil em geral. Martins & Ramos (2008) salientam ainda que é importante distinguir a Governação electrónica do Governo electrónico. A governação designa a maneira ou o processo de administração tendentes a alcançar certos objectivos, interesses e políticas traçadas pelo governo que por sua vez é a instituição ou o aparelho instituído para alcançar estes objectivos ou interesses.

[11] Corresponde ao Governo de um povo em determinado território, sendo que este governo pode ser democrático ou autocrático.

Segundo o relatório das Nações Unidas[12] citado em Marisa *et al* (2014), a governação electrónica assenta-se em cinco princípios básicos:

- Fornecimento de serviços básicos de acordo com à exigência dos cidadãos;
- Acessibilidade aos serviços fornecidos;
- Promoção da inclusão social;
- Fornecimento de informação de maneira segura e responsável; e
- Utilização das TIC e dos Recursos Humanos de forma eficiente e eficaz.

3.2. Governação Electrónica em Moçambique

De acordo com Marisa *et al*. (2014), o conceito de governação electrónica em Moçambique surge com a criação da comissão para a política de informática através do decreto presidencial nº 2/98 de 26 de Maio. Como dito acima, a governação electrónica assenta-se no uso das TIC para a sua materialização.

A política de informática de Moçambique realça que o uso das TIC tem contribuído significativamente para a melhoria das operações dos governos no mundo, disponibilizando melhores serviços e de forma rápida para os cidadãos, colocando a informação pública ao dispor dos cidadãos, facilitando a comunicação entre estes e os seus governantes, permitindo também o contributo dos cidadãos em áreas como saúde, educação, transporte, promoção da imagem de países, combate a corrupção entre outras, em suma, promovendo uma boa governação. Segundo a Estratégia do Governo Electrónico de Moçambique (2005), a política de informática identifica seis áreas prioritárias: educação, desenvolvimento de recursos humanos, saúde, acesso universal, infra-estrutura e boa governação.

De acordo com a Estratégia do Governo Electrónico de Moçambique (2005), a implementação da governação electrónica em Moçambique produzirá alterações sistémicas em processos, resultando numa maior transparência, melhoria na gestão e no manuseamento de dados, na monitoria e no acompanhamento mais focalizados de projectos, e na generalização e elevação de conjunto de habilidades no sector público.

12 Unites Nations Rapport: 2008

Segundo a Estratégia do Governo Electrónico de Moçambique (2005), o governo electrónico será testado com base em projectos definidos e apoiará a reforma do Sector Público colocando como foco o uso e aplicação das TIC às áreas prioritárias. “Tais projectos vão demonstrar a efectividade e objectivos da Reforma do Sector Público nos Ministérios e instituições que operam em áreas prioritárias, através da reengenharia dos seus processos, formação dos seus funcionários, desenvolvimento dos seus sistemas de disponibilização de informação e serviços, e generalização do uso das novas tecnologias” (Estratégia do Governo Electrónico de Moçambique, 2005, p. 8).

Chemane, et al. (2009) apresentam um *framework* de interoperabilidade para o Governo Electrónico em Moçambique e neste, apresenta-se uma estrutura abrangente baseada em: (i) uma arquitectura de referência juntamente com os padrões técnicos, (ii) um ciclo de vida de padronização, (iii) um modelo de maturidade, e (iv) algumas acções-chave destinadas a Iniciativa sustentável a longo prazo.

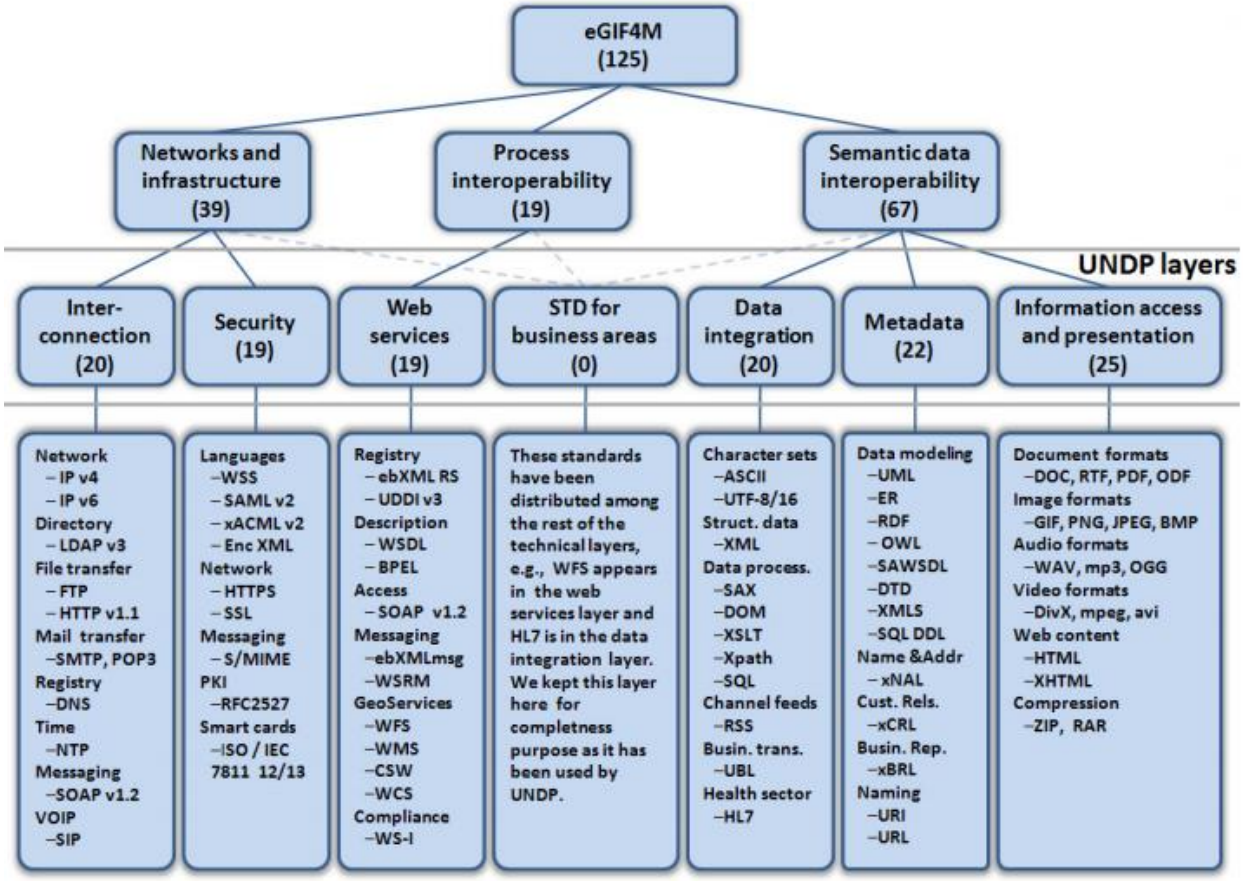


Figura 5: Padrões para implementação do Governo Electrónico em Moçambique

Fonte: (Chemane, et al., 2009, p. 333)

A Figura 5 apresenta os padrões descritos no *framework* proposto por Chemane, et al. (2009) para a materialização do Governo Electrónico e nesta encontram padrões relacionados com a redes e infra-estruturas, interoperabilidade do processo e a interoperabilidade dos dados semânticos.

3.2.1. Essência da Estratégia da Governo Electrónico

A Figura 6 apresenta a visão definida pela governação que é de permitir que o cidadão moçambicano tenha sempre acesso a informação relacionada as actividades do Governo.

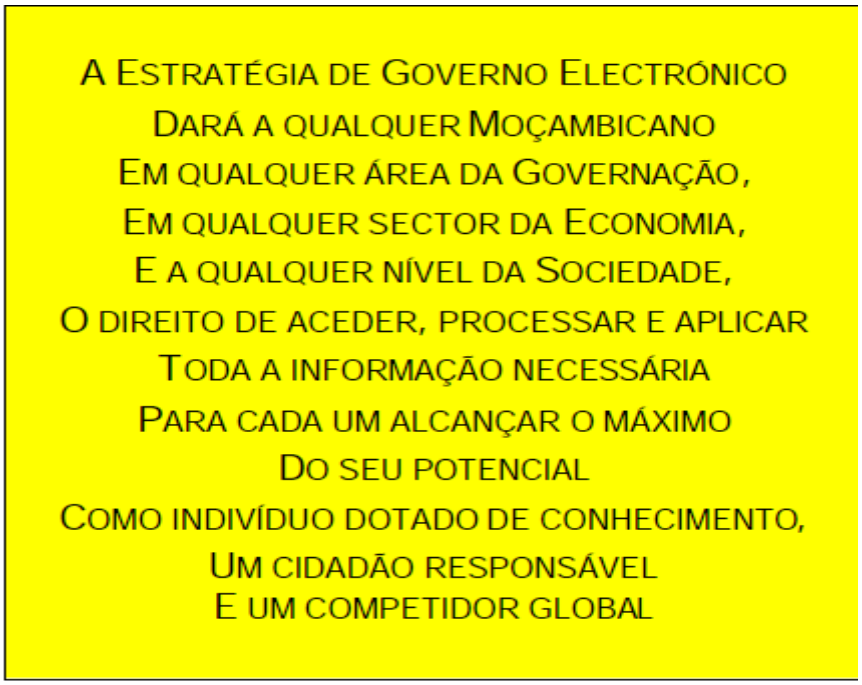


Figura 6: Visão da Estratégia do Governo Electrónico de Moçambique

Fonte: (Estratégia do Governo Electrónico de Moçambique, 2005, p. 11)

De modo a facilitar o alcance da visão, definiram-se certos objectivos concretos. Como descrito na Estratégia do Governo Electrónico de Moçambique (2005), os objectivos gerais desta são:

- Melhorar a eficiência e eficácia na prestação de serviços públicos;
- Assegurar a transparência e responsabilidade dos servidores públicos; e
- Dar acesso à informação para melhorar as actividades do sector privado e simplificar a vida dos cidadãos.

3.2.2. Elementos Chave da Estratégia do Governo Electrónico

De acordo com a Estratégia do Governo Electrónico de Moçambique (2005, p. 13), a implementação do Governo Electrónico requer:

- A conectividade e a interoperabilidade funcional de uma hierarquia de agências governamentais, seus sistemas de informação, e da informação com que elas lidam;
- Mecanismos através dos quais se possa garantir que as suas actividades são seguras, legais, honestas e susceptíveis de seguir até à sua origem; e
- Pessoas competentes para usar, administrar e manter os sistemas informáticos.

Para que isso se verifique, a Estratégia do Governo Electrónico de Moçambique (2005) faz menção de três elementos chave: uma plataforma comum de comunicação, políticas e regulamentos e capacitação institucional e humana.

3.2.2.1. Plataforma Comum de Comunicação

Com a criação do Governo Electrónico, objectiva-se permitir o compartilhamento de dados e informações entre os diferentes intervenientes do sistema de forma segura. Assim sendo, surge a necessidade de criação de mecanismos que possibilitam a comunicação entre os vários sistemas que compõem o Governo Electrónico.

Apesar do governo central, ministérios, governos provinciais ou municipais terem os seus sistemas desenvolvidos em diferentes plataformas ou linguagens de programação, estes devem ser capazes de operar ou comunicar uns com os outros e devem também ser capazes de trocar dados sem dificuldade. Isto torna-se possível com a criação de uma plataforma comum que permita a interacção destes sistemas independentemente da sua tecnologia.

3.2.2.2. Políticas e Regulamentação

O Governo Electrónico fornece dados e informações aos diversos utilizadores que interagem com o sistema, por essa razão, existe a necessidade de definir privilégios de autoridade, níveis de acesso dos utilizadores a informação que cada um, destes pode manipular.

De acordo com a Estratégia do Governo Electrónico de Moçambique (2005), alem das políticas de segurança de dados electrónicos, são necessários dispositivos legais como assinaturas digitais, sistemas de verificação de autenticação de terceiros e evidencia electrónica.

De modo a proteger a privacidade e os interesses dos cidadãos e do empresariado, é necessário que existam leis no país responsáveis por regular e para facilitar o uso amplo e autorizado da informação fornecida. Actualmente o país dispõem de leis que regulam actos envolvendo o uso das TIC em diferentes contextos da sociedade moçambicana, estas leis são:

- **Lei nº 3/2017 de 9 de Janeiro (Lei das Transacções Electrónicas)** – promulgada no dia 09 de Janeiro de 2017, a lei das transacções electrónicas regula as transacções electrónicas, o comércio electrónico e o governo electrónico. A lei, também visa garantir a protecção, segurança dos provedores e utilizadores das TIC;

- **Lei nº 35/2014 de 31 de Dezembro (Código Penal Moçambicano)** – título III, no seu capítulo I, aborda as penas referentes aos crimes informáticos, ou seja, o código penal moçambicano trata das penalizações decorrentes do uso das TIC na prática de crimes tipificados pela lei.

- **Estratégia Nacional de Cibersegurança** (ainda em elaboração) – inserido no plano de Acções dos países-membros da CTO, a elaboração da Estratégia Nacional de Segurança Cibernética em Moçambique visa adoptar medidas que garantam um ambiente *online* seguro, ou seja, onde utentes, negócios e o Governo estão devidamente protegidos, permitindo ao país usufruir dos benefícios das TIC em prol do desenvolvimento social e económico.

3.2.2.3. Capacitação Institucional e Humana

A área das TIC requer um certo nível de conhecimento técnico e actualizado pois diferentes metodologias e técnicas são desenvolvidas dia após dia, sendo por isso necessário que os profissionais desta mantenham sem informados e actualizados.

De acordo com a Estratégia do Governo Electrónico de Moçambique (2005), este elemento foca na necessidade de formação de profissionais altamente qualificados para o manuseamento e a gestão das plataformas do Governo Electrónico. Também defende-se a criação de políticas por forma a reter esses profissionais impulsionando assim o Sector Público.

3.3. Portal Electrónico do Governo de Moçambique

De acordo com Marisa *et al* (2014), a governação electrónica em Moçambique faz-se sentir efectivamente em Julho de 2006 com a aprovação da Estratégia do Governo Electrónico pelo conselho de ministros e com o lançamento oficial do Portal do Governo de Moçambique que pode ser acedido pelo *link* www.portaldogoverno.gov.mz.

Figura 7: Portal do Governo de Moçambique

Fonte: www.portaldogoverno.com

Pode-se afirmar categoricamente que o portal do governo encarna-se como sendo a governação electrónica em Moçambique. É a partir do portal que cidadãos singulares, empresários e a sociedade em geral têm acesso aos serviços e informações sobre o país.

O portal fornece informações como a história do país, a sua geografia, a população, a economia, cultura, turismo e também acerca da localização das embaixadas e dos consulados moçambicanos nos diversos países do Mundo.

Além de fornecer noticias sobre as várias actividades levadas a cabo pelo governo, encontram-se também *links* que redireccionam a *sites* dos ministérios, dos governos provinciais e distritais, dos conselhos municipais, documentos importantes para a gestão da vida pública nacional (orçamentos, políticas, estratégias nacionais e sectoriais, programas entre outros) e legislações importantes para o funcionamento do estado como a constituição da república, boletins da república e mais.

Para o cidadão comum, o portal disponibiliza serviços como o balcão de atendimento único (e-BAU), informações sobre emprego, saúde, educação, formulários e o portal do cidadão.

Aos empresários e agentes económicos, o portal oferece serviços para registo e licenciamentos de empresas, informações sobre taxas e impostos, sectores de actividades entre outros.

4. CAPITULO IV – DESENVOLVIMENTO DO TRABALHO

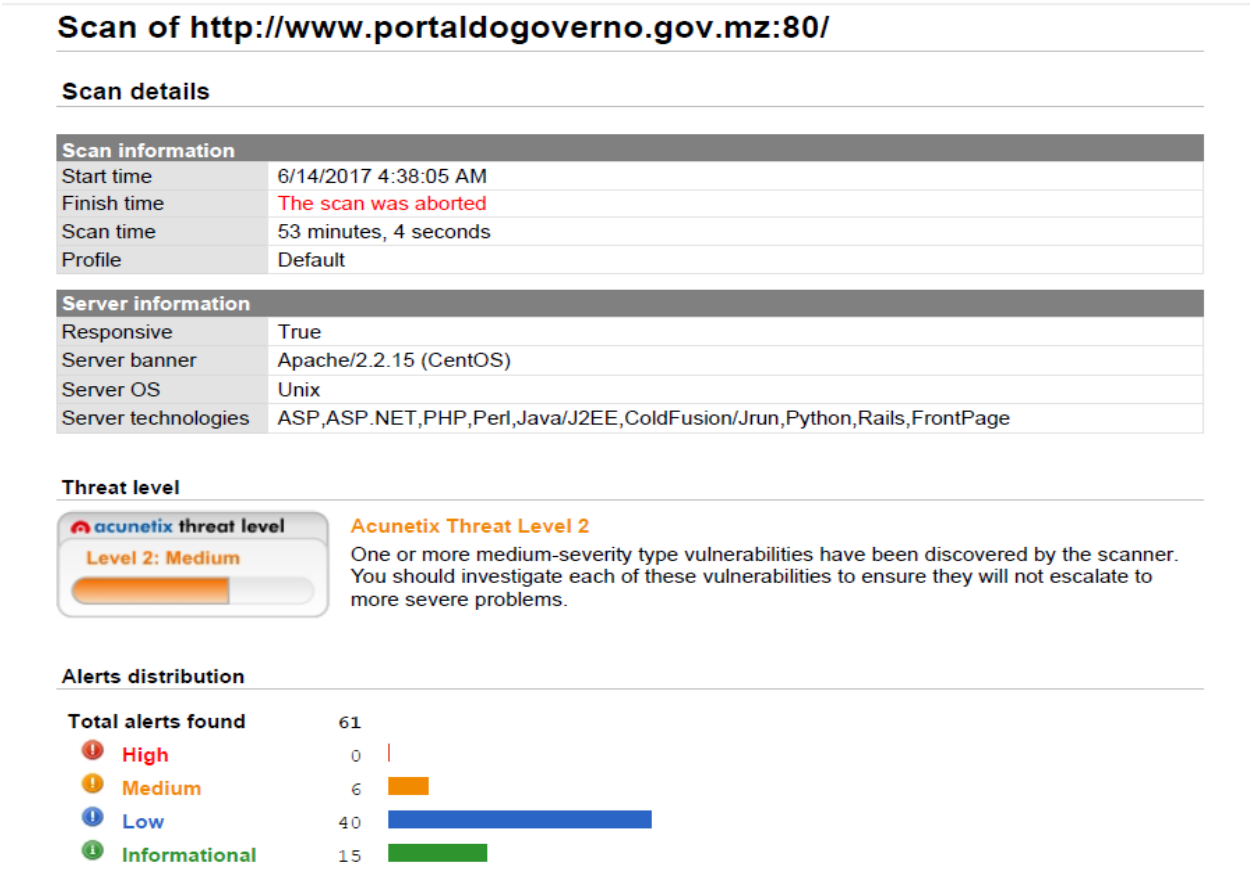
4.1. Resultados do *scan* de Vulnerabilidades

Como dito anteriormente, a realização do *scan* de vulnerabilidades foi efectuada com base numa das ferramentas descritas na Tabela 12, a Acunetix WVS. Foi utilizada a ferramenta porque para além de efectuar o *scan* de vulnerabilidades, esta apresenta diversas abordagens para a produção de relatórios de acordo com o tipo de interessados (desenvolvedores e executivos), permite também a elaboração de relatórios comparando resultados de diferentes *scan*s e possui uma versão *trial* para testes.

Os relatórios destinados aos desenvolvedores contem informações mais detalhadas sobre cada uma das vulnerabilidades identificadas (tipo, severidade, elementos que podem ser afectados quando exploradas, entre outros) e apresentam também recomendações para a prevenção destas.

A imagem a seguir é parte do relatório produzido pela aplicação Acunetix referente ao *scan* realizado no portal do governo. Constam na imagem informações sobre a duração do *scan*, a versão e o sistema operativo do servidor em qual a aplicação *web* encontra-se hospedada (facto que viola o critério [C5] descrito no ponto 2.2.1). É possível observar o nível de exposição da aplicação segundo a quantidade e classificação das vulnerabilidades encontradas.

Sendo um *software* proprietário, foi utilizado o *Acunetix Web Vulnerability Scanner* v9.5 *Free Edition* (versão gratuita da ferramenta). É de salientar que foi efectuado um teste do tipo caixa preta visto que o auditor não teve conhecimentos prévios sobre as aplicações e a organização não soube que seriam executados os testes.



Scan of http://www.portaldogoverno.gov.mz:80/

Scan details

Scan information	
Start time	6/14/2017 4:38:05 AM
Finish time	The scan was aborted
Scan time	53 minutes, 4 seconds
Profile	Default

Server information	
Responsive	True
Server banner	Apache/2.2.15 (CentOS)
Server OS	Unix
Server technologies	ASP,ASP.NET,PHP,Perl,Java/J2EE,ColdFusion/Jrun,Python,Rails,FrontPage

Threat level

acunetix threat level
Level 2: Medium

Acunetix Threat Level 2
One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	61
High	0
Medium	6
Low	40
Informational	15

Figura 8: Resultados do *scan* da Aplicação *web* do Governo de Moçambique

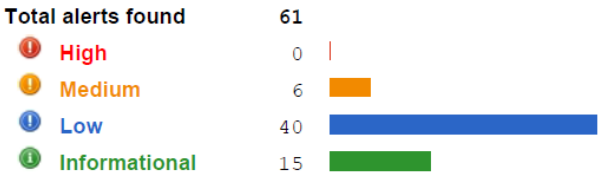
Fonte: Autor

A ferramenta classifica as vulnerabilidades encontradas em 4 principais grupos:

- **Altas:** são colocadas aqui todas as vulnerabilidades que quando exploradas levam a tomada total do sistema. Devem ser evitadas vulnerabilidades desse grupo pois são consideradas fatais. Da Figura 8, vê-se que o portal não possui nenhuma vulnerabilidade desse grupo.
- **Médias:** são agrupadas aqui todas vulnerabilidades que quando exploradas por atacantes podem ou não resultar no comprometimento da aplicação. Como se pode observar na Figura 8, do *scan* realizado no portal do governo foram identificadas 6 vulnerabilidades desse grupo.
- **Baixas:** vulnerabilidades que quando exploradas individualmente não representam grandes perigos para a aplicação *web*. Esse tipo de vulnerabilidade consideram-se devem ser mensuradas porque quando combinadas com as altas ou médias resultam em ataques mais graves. Foram encontradas 40 vulnerabilidades dessa categoria.

- **Informativas:** são informações sobre pequenos erros encontrado na aplicação. Estas não são consideradas graves pois não representam grandes perigos e a sua resolução não requer grandes esforços por parte dos gestores ou desenvolvedores. A Figura 8 aponta que existem 15 vulnerabilidades deste tipo.

A ferramenta também fornece uma lista das vulnerabilidades e a quantidade destas. A figura a seguir fornece as designações das vulnerabilidades identificadas.



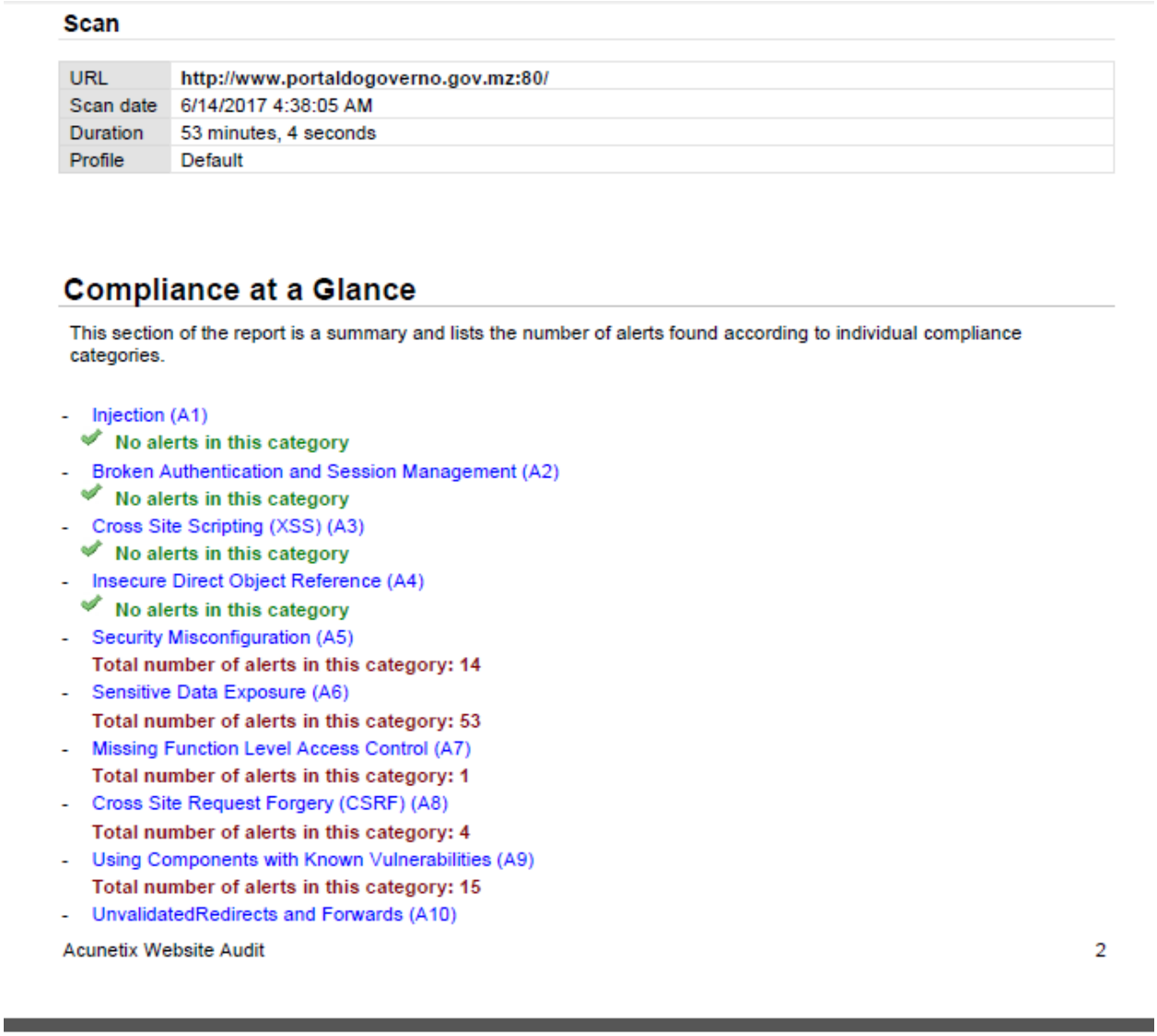
Executive summary

Alert group	Severity	Alert count
Apache httpd remote denial of service	Medium	1
HTML form without CSRF protection	Medium	4
User credentials are sent in clear text	Medium	1
Clickjacking: X-Frame-Options header missing	Low	1
Possible virtual host found	Low	1
Session Cookie without HttpOnly flag set	Low	1
Session Cookie without Secure flag set	Low	1
Session token in URL	Low	35
TRACE method is enabled	Low	1
Broken links	Informational	11
GHDB	Informational	2
Password type input with auto-complete enabled	Informational	2

Figura 9: Designação das vulnerabilidades encontradas

Fonte: Autor

De acordo com o OWASP Top 10 2013 (a tradução dos termos encontram-se descritas no ponto 2.2.2), as vulnerabilidades verificadas enquadram-se nas seguintes categorias.



Scan

URL	http://www.portaldogoverno.gov.mz:80/
Scan date	6/14/2017 4:38:05 AM
Duration	53 minutes, 4 seconds
Profile	Default

Compliance at a Glance

This section of the report is a summary and lists the number of alerts found according to individual compliance categories.

- Injection (A1)
  No alerts in this category
- Broken Authentication and Session Management (A2)
  No alerts in this category
- Cross Site Scripting (XSS) (A3)
  No alerts in this category
- Insecure Direct Object Reference (A4)
  No alerts in this category
- Security Misconfiguration (A5)
  Total number of alerts in this category: 14
- Sensitive Data Exposure (A6)
  Total number of alerts in this category: 53
- Missing Function Level Access Control (A7)
  Total number of alerts in this category: 1
- Cross Site Request Forgery (CSRF) (A8)
  Total number of alerts in this category: 4
- Using Components with Known Vulnerabilities (A9)
  Total number of alerts in this category: 15
- UnvalidatedRedirects and Forwards (A10)

Acunetix Website Audit 2

No alerts in this category

Figura 10: Classificação das vulnerabilidades de acordo coma OWASP Top 10 2013.

Fonte: Autor

Da Figura 10 é possível observar o número de vulnerabilidades distribuídas de acordo com cada uma das categorias que constam da OWASP Top 10 2013.

As imagens no **Anexo 3** mostram os resultados dos *scans* realizados nas aplicações de alguns dos Ministérios da República de Moçambique.

4.2. Medidas de Prevenção

O *scan* de vulnerabilidades no portal do governo resultou na identificação das vulnerabilidades indicadas na Figura 9. Podem evitar-se os impactos que podem advir da exploração destas por meio acções preventivas e correctivas com intuito de mitigá-las. A seguir apresentam-se medidas de prevenção para as vulnerabilidades do nível médio registadas durante o processo de scan.

4.2.1. Apache httpd remote denial of service

Quantidade:	1
Nível:	Média
Descrição:	Uma vulnerabilidade de negação de serviços foi encontrada na forma como os múltiplos intervalos de sobreposição são tratados pelo servidor Apache.
Impacto:	O ataque pode ser feito de forma remota, enviando um elevado número de requisições, saturando assim a memória do servidor. O *scan* foram identificadas ferramentas que emitem grossos números de requisições para o servidor.
Prevenção:	Actualizar a versão do Apache em uso para ultima disponibilizada (versão 2.2.20 ou mais recentes).

4.2.2. HTML form without CSRF protection

Quantidade:	4
Nível:	Média
Descrição:	É um tipo de exploração maliciosa de uma aplicação em que utilizadores legítimos transmitem comandos não autorizados de acordo com os privilégios destes no sistema. Durante a realização do *scan* foram encontrados formulários desprotegidos contra CSRF.
Impacto:	Um atacante pode forçar os utilizadores de uma aplicação *web* a executar acções da sua escolha. Uma exploração bem-sucedida pode comprometer os dados do utilizador final e a operação em caso de um utilizador final. Se o utilizador final direccionado for administrador do sistema, isso pode comprometer a aplicação.
Prevenção:	Validar todos os formulários contra ataques do tipo CSRF.

4.2.3. User credentials are sent in clear text

Quantidade:	1
Nível:	Média
Descrição:	As credenciais dos utilizadores são transportadas usando canais não criptografados. Esse tipo de informação deve ser sempre transportada utilizando canais encriptados para evitar a intercessão destas por atacantes.
Impacto:	Atacantes podem obter as credenciais dos utilizadores interceptando pacotes HTTP.
Prevenção:	Usar o protocolo HTTPs para a transferência de informações ao invés de HTTP.

As vulnerabilidades dos níveis médios e baixo são as que devem ser dadas mais atenção porque influenciam directamente no uso das aplicações. A exploração de vulnerabilidades desse nível podem causar dados severos e por este motivo que apresentam-se as medidas de prevenção para os nível médio e as do nível baixo no Anexo 4.

As vulnerabilidades do nível informativo podem ser resolvidas com a troca de algumas configurações no servidor *web* ou por uma inspecção directa no código fonte das aplicações, por essa razão não apresentam-se medidas de prevenção destas.

5. CAPITULO V - DISCUSSÃO DE RESULTADOS

No presente trabalho focou-se na identificação de vulnerabilidades nas aplicações *web* do Governo de Moçambique e na proposição de medidas de forma a prevenir-se destas. Para este efeito, o trabalho baseou-se na revisão da literatura (ver), em que apresentou-se a fundamentação teórica de tópicos relacionados com o assunto em estudo e procurou-se validar o problema definido e descrito na parte introdutória do trabalho (ver).

Com a revisão da literatura, foi possível analisar aspectos referentes a segurança de informação e as vulnerabilidades comummente encontradas em aplicações *web*. Foi possível também constatar que existem organizações a nível internacional preocupadas em desenvolver normas e padrões de forma a melhorar a segurança dos dados e das aplicações.

No capítulo IV (ver), foram apresentados os relatórios do *scan* de vulnerabilidades efectuados usando ferramenta Acunetix WVS descrita na Tabela 12 e também foram apresentadas medidas de prevenção de acordo com os erros encontrados. Optou-se em mostrar as medidas para as vulnerabilidades do nível médio por estas serem consideradas mais graves e merecerem maior atenção por parte dos gestores das aplicações.

Com o guião de entrevistas no Anexo 2, o autor procurou saber sobre os mecanismos de segurança implementados nas aplicações por parte da instituição gestora destas por forma a verificar se os dados obtidos durante o processo de scan de vulnerabilidades condiziam com os implementados.

Como tentativa de aproximar a entidade gestora das aplicações *web* do Governo de Moçambique, o autor submeteu credenciais na instituição mas este não foi recebido. Em termos de segurança de informação, diversos autores consideram esse comportamento como sendo “segurança através da obscuridade” e está pode ser entendida como a falta de informação sobre o contexto em que o activo a ser preservado se encontra, ou informações sobre o activo no qual se deseja avaliar a sua segurança.

Geralmente defende-se que, num sistema em que a segurança baseia-se através da obscuridade, dificulta a exploração de vulnerabilidades pois assume-se que não se tendo conhecimento de como a segurança do sistema foi implementada será difícil executar um ataque contra este. Contudo, diversos autores não concordam com essa pratica,

estes defendem que quanto mais exposto um sistema é, mais facilmente pode-se modelar e analisar sua segurança de forma metódica e cientifica.

Os resultados apresentados no capítulo IV mostram que as aplicações do governo de Moçambique apresentam vulnerabilidades médias e uma parte considerável está associada ao uso do protocolo HTTP. Para eliminar essas vulnerabilidades, é importante que se siga as indicações do ponto 4.2 e a migração do protocolo HTTP para o HTTPs como também sugere a Figura 5 no que concerne a segurança.

É de salientar que as medidas de prevenção propostas no ponto 4.2 servem apenas para resolver alguns dos erros verificados durante o processo de scan de vulnerabilidades, sendo estas não são suficientes para afirmar que as aplicações *web* do Governo encontram seguras.

O conceito “segurança total e completa” é considerado uma utopia quando trata-se de segurança de informação pois diversas falhas são descobertas dia apos dias e métodos utilizados outrora para garantir a segurança mostram-se ineficazes com o passar do tempo. Há uma necessidade urgente de investir-se seriamente em questões de segurança pois só assim podem-se pensar em um Governo Electrónico verdadeiramente seguro para o cidadão, para as empresas, para a função pública e também para a segurança dos segredos do estado.

6. CAPÍTULO VI – CONCLUSÕES E RECOMENDAÇÕES

6.1. Conclusões

Consoante os objectivos específicos evidenciados no ponto 1.4.2, pode-se tirar as seguintes conclusões:

(i) O primeiro objectivo (apresentar critérios mínimos de segurança em aplicações *web*) foi alcançado como pode-se observar na Tabela 1. Toda aplicação *web* que cumprir com estes critérios pode ser considerada momentaneamente segura;

(ii) Descreveu-se o portal electrónico do Governo de Moçambique no capítulo III do presente trabalho, considerando-se o objectivo satisfatoriamente alcançado;

(iii) A Tabela 12 apresenta a comparação de algumas das ferramentas utilizadas para o *scan* de vulnerabilidades em aplicações *web* e posteriormente fundamenta-se a aplicação da aplicação utilizada para o scan. Este objectivo foi atingindo com sucesso;

(iv) Conseguiu-se efectuar o *scan* de vulnerabilidades como se pode constatar observando as imagens dos relatórios expostos extraídos pela ferramenta Acunetix no ponto 4.1 como resultado deste processo;

(v) No ponto 4.2 encontram-se as medidas de prevenção para as vulnerabilidades encontradas. Esse objectivo foi também alcançado com sucesso.

Com base no acima exposto, conclui-se que todos os objectivos inicialmente definidos para a orientação do trabalho foram satisfatoriamente alcançados.

6.2. Recomendações

O presente trabalho somente focou-se na identificação de vulnerabilidades nas aplicações *web* do Governo de Moçambique e na proposição de medidas que corrigissem as falhas analisadas. Como exposto no 2.1.5, essa actividade enquadra-se no terceiro nível de classificação da segurança de informação (nível tecnológico), não sendo suficiente para garantir uma segurança desejável.

Futuros trabalhos do género devem procurar abordar mais sobre todos aspectos mencionados no ponto 2.1.5 e procurar averiguar se a instituição responsável pela concepção, gestão e hospedagem das aplicações do governo dispõe de políticas de seguranças e procurar buscar inteirar-se o porquê do não cumprimento de alguns destes como apresentados na Figura 5.

7. Bibliografia

[1]. Acunetix, 2017. *acunetix.com.* [Online]
Available at: https://www.acunetix.com/
[Acedido em 30 June 2017].

[2]. António, 2013. *grupotreinar.com.* [Online]
Available at: http://www.grupotreinar.com.br/blog/2013/9/23/penetration-test-ou-teste-de-penetra%C3%A7%C3%A3o-%E2%80%93-saiba-porque-isto-%C3%A9-importante.aspx
[Acedido em 10 Maio 2017].

[3]. Basso, T., 2010. *repositorio.unicamp.* [Online]
Available at: http://www.repositorio.unicamp.br/bitstream/REPOSIP/261545/1/Basso,%20Tania_M.pdf
[Acedido em 18 Maio 2017].

[4]. Beal, A., 2005. *Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações.* n.d ed. São Paulo: Atlas.

[5]. Bertoglio, D. D. & Zorzo, A. F., 2015. *Um Mapeamento Sistemático sobre Testes de Penetração,* s.l.: s.n.

[6]. Borges, C. G. & Helena, E. A. d. S., 2011. *cristiano.eti.br.* [Online]
Available at: http://www.cristiano.eti.br/Documentos/Artigo-Pentest-Cristiano.pdf
[Acedido em 10 Maio 2017].

[7]. Castells, M. & Cardoso, G., 2006. *A Sociedade em Rede Do Conhecimento à Acção Política.* edição 1012466 ed. s.l.:Impresa Nacional - Casa da Moeda.

[8]. Chemane, L. et al., 2009. *http://disi.unitn.it.* [Online]
Available at: http://disi.unitn.it/~pavel/Publications/eGIF4M@egov'09.pdf
[Acedido em 15 Junho 2017].

[9]. Davenport, T. & Prusak, L., 1998. *Conhecimento Empresarial: como as organizações gerenciam o seu capital intelectual.* 2nd ed. Rio de Janeiro: Campus.

[10]. Dias, A. & Pinheiro, M. M. K., s.d. *academia.edu.* [Online]
Available at: http://www.academia.edu/3846902/POL%C3%8DTICA_DE_GOVERNO_ELETR%C3%94NICO_DE_MO%C3%87AMBIQUE_UM_OLHAR_NA_PERSPETIVA_D

E_UMA_CULTURA_DE_INFORMA%C3%87%C3%83OResumen
[Acedido em 30 May 2017].

[11]. Estratégia do Governo Electrónico de Moçambique, 2005. *Colocar os Serviços Públicos Junto do Cidadão,* Maputo: s.n.

[12]. Faller, A., 2005. *A Internet e seus Protocolos.* 1st ed. s.l.:Elsevier Editora ltda.

[13]. Guimarães, E., 2013. *ibliss.com.br.* [Online]
Available at: https://www.ibliss.com.br/2013/07/26/testes-de-seguranca-padroes-e-metodologias/
[Acedido em 10 Maio 2017].

[14]. Laureano, M. A. P., 2005. *Gestão de Segurança da Informação.* n.d ed. n.d: n.d.

[15]. Marisa, S., Uate, R. & Perreira, M., 2014. *cdh.uem.mz.* [Online]
Available at: http://cdh.uem.mz/images/pdfs/Revista_Outubro_2014.pdf
[Acedido em 30 Maio 2017].

[16]. Marques et al, H. R., 2014. *Metodologia da Pesquisa e do Trabalho Cientifico.* 4th ed. Campo Grande: UCDB.

[17]. Martins, D. d. A. & Ramos, S. M. A., 2008. *scribd.* [Online]
Available at: https://www.scribd.com/document/338969997/2008-ENAPG305-pdf
[Acedido em 30 May 2017].

[18]. Messias, L. C. d. S., 2005. *Informação: um estudo exploratório do seu conceito em periódicos científicos brasileiros da área de Ciência da Informação.* 2nd ed. São Paulo: s.n.

[19]. Micheletti, F. A., 2011. *ANÁLISE DAS PRINCIPAIS VULNERABILIDADES DE APLICAÇÕES WEB TENDO COMO BASE A ARQUITETURA LAMP E AS TOP 10 VULNERABILIDADES DA OWASP,* São Paulo: s.n.

[20]. NBR ISO/IEC 27002, 2005. *fieb.org.br.* [Online]
Available at: http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf
[Acedido em 15 Julho 2017].

[21]. Oliveira, J. A. d., Campos, L. L. T. & Diniz, C. A. R. S., 2015. Segurança no Desenvolvimento de Aplicações Web. *Revista Pensar Tecnologia,* IV(2), pp. 1-12.

[22]. Oliveira, T. S. T. D., 2012. *bcc.ufla.br.* [Online]
Available at: http://www.bcc.ufla.br/wp-content/uploads/2013/09/TESTES-DE-SEGURAN%C3%87A-EM-APLICA%C3%87%C3%95ES-WEB-SEGUNDO-A.pdf
[Acedido em 20 April 2017].

[23]. Orinayo, S.-P., 2016. *Certified Ethical Hacking - Study Guide.* 9th ed. Canada: John Wiley & Sons.

[24]. OWASP Testing Guide, 2008. *www.owasp.org.* [Online]
Available at: https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf
[Acedido em 20 Maio 2017].

[25]. OWASP, 2013. *www.owasp.org.* [Online]
Available at: https://www.owasp.org/images/9/9c/OWASP_Top_10_2013_PT-BR.pdf
[Acedido em 20 April 2017].

[26]. REDE SEGURA TECNOLOGIA , s.d. *redesegura.com.br.* [Online]
Available at: https://www.redesegura.com.br/clientes-e-parceiros/o-risco-de-ataques-pela-web/
[Acedido em 18 Junho 2017].

[27]. Reis, B., Mota, J. C. & Oliveira, P. P. B. d., 2001. Classificação da Informação. *n.d*, 11 Agosto, pp. 1-10.

[28]. Rezende, D. A. & Abreu, A. F., 2000. *Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais.* São Paulo: Editora Atlas.

[29]. Santos, E. D. & Nunes, R. C., 2010. *http://ceseg.inf.ufpr.br.* [Online]
Available at: http://ceseg.inf.ufpr.br/anais/2010/05_wticg/artigo_03.pdf
[Acedido em 10 Maio 2017].

[30]. Shedroff, N., 1999. *Information interactiob design: a unified field theory of design.* 2nd ed. Londom: MIT Press..

[31]. Stuttard, D. & Pinto, M., 2011. *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.* 2nd ed. Indianapolis, Indiana: John Wiley & Sons, Inc..

[32]. Terence, A. C. & Escrivão Filho, E., 2006. *www.abepro.org.br.* [Online] Available at: http://www.abepro.org.br/biblioteca/enegep2006_tr540368_8017.pdf [Acedido em 2017 Maio 10].

[33]. Tripton, H. F. & Krause, M., 2014. *Information Security Management Handbook.* 5th ed. Florida: s.n.

[34]. upGuard, 2016. *UpGuard.com.* [Online] Available at: http://itsmf.cz/wp-content/uploads/2016/09/WS_sec_chlist.pdf [Acedido em 18 Maio 2017].

[35]. Viegas, A. L., 2008. *Segurança em Aplicações web: Hardering nos Servidores baseados em software livre,* Recife: s.n.

[36]. w3ii, s.d. *w3ii.com.* [Online] Available at: http://www.w3ii.com/pt/penetration_testing/default.html [Acedido em 10 Maio 2017].

ANEXOS

Anexo 1. Artigo 19 da Lei das Transacções Electrónicas

ARTIGO 49

(Disponibilização e acesso de informação e serviços públicos)

1. A informação para o público sobre as actividades e serviços do Governo e da Administração Pública nos níveis central, provincial, distrital e local providenciáveis via *Internet*, devem estar disponíveis através do Portal do governo, dos portais dos governos provinciais, dos portais dos governos distritais, bem como através de outros portais e páginas de *Internet* das instituições do Governo e Administração Pública.

2. Sem prejuízo das adaptações que se mostrem necessárias, a provisão de serviços de governo electrónico deve focar directamente a grupos-alvo identificados, incluindo o cidadão, os negócios e outras entidades governamentais, de acordo com a função ou assunto.

3. A autoridade competente para a prestação de serviços de governo electrónico deve implementar serviços acessíveis por um ponto único de acesso e através dos diversos dispositivos electrónicos disponíveis no País.

4. A autoridade competente para a prestação de serviços de governo electrónico deve promover a desmaterialização e desterritorialização dos processos relativos à provisão de serviços públicos e informação para o cidadão.

5. A informação do Governo disponível que é mantida nos portais e páginas de *Internet* de qualquer instituição do Governo e da Administração Pública deve ser providenciada de forma que haja protecção da privacidade, em conformidade com a legislação aplicável.

Figura A1- 1: Artigo 19 da Lei das Transacções Electrónicas

Fonte: Lei das Transacções Electrónicas

Anexo 2: Guião de Entrevistas

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

CURSO: **LICENCIATURA EM ENGENHARIA INFORMÁTICA**

DISCIPLINA: **TRABALHO DE LICENCIATURA**

ANÁLISE DE VULNERABILIDADES E MEDIDAS DE PREVENÇÃO EM APLICAÇÕES WEB DO GOVERNO DE MOÇAMBIQUE

QUESTÕES PARA ENTREVISTA

CONTEXTUALIZAÇÃO

O Governo de Moçambique, disponibiliza informações sobre o Estado e fornece alguns serviços na sua aplicação web designada portal do governo. Segundo o Instituto Gartner (2009), mais de 75% dos problemas de segurança na Internet são devidos à falhas exploráveis a partir das aplicações web, assim sendo, assume-se que as aplicações web do Governo (tanto o portal electrónico como os portais dos diferentes Ministérios) contém falhas e a exploração destas podem resultar não só na falha ao disponibilizar-se informação ao cidadão mas também no roubo de informação sigilosa.

Este questionário visa auferir, por parte dos gestores das aplicações web do Governo de Moçambique sobre o nível e os mecanismos de segurança implementados nestas.

Questões-guia para entrevista aos Administradores das Aplicações web do Governo de Moçambique.

Observação: *Os dados colhidos nesta entrevista serão usados apenas para a elaboração do Trabalho de Licenciatura do Entrevistador e, serão tratados de forma sigilosa.*

- *Os entrevistados poderão responder em anonimato.*

Instituição: _____

Função: _____

Nome: _____

1. O Governo de Moçambique implementa alguma política de segurança nas suas aplicações web (mencione algumas)?

   _____
   _____
   _____
   _____
   _____
   _____

2. No desenvolvimento das aplicações web, há alguma exigência de critérios de segurança que devem ser implementados?

   _____
   _____
   _____
   _____
   _____
   _____

3. Como são actualmente detectadas as vulnerabilidades nas aplicações do Governo?

_____
_____
_____
_____
_____
_____

4. Como são tratadas as vulnerabilidades quando identificadas?

_____
_____
_____
_____
_____
_____
_____

5. Já sofreram algum tipo de ataque web na aplicação (mencione caso tenham sofrido)?

_____
_____
_____
_____

   a. Que consequências teve o ataque?

_____
_____
_____

6. Como avalia a segurança das aplicações web do Governo de Moçambique?

_____
_____
_____

Observações e/ou comentários:

_____

_____

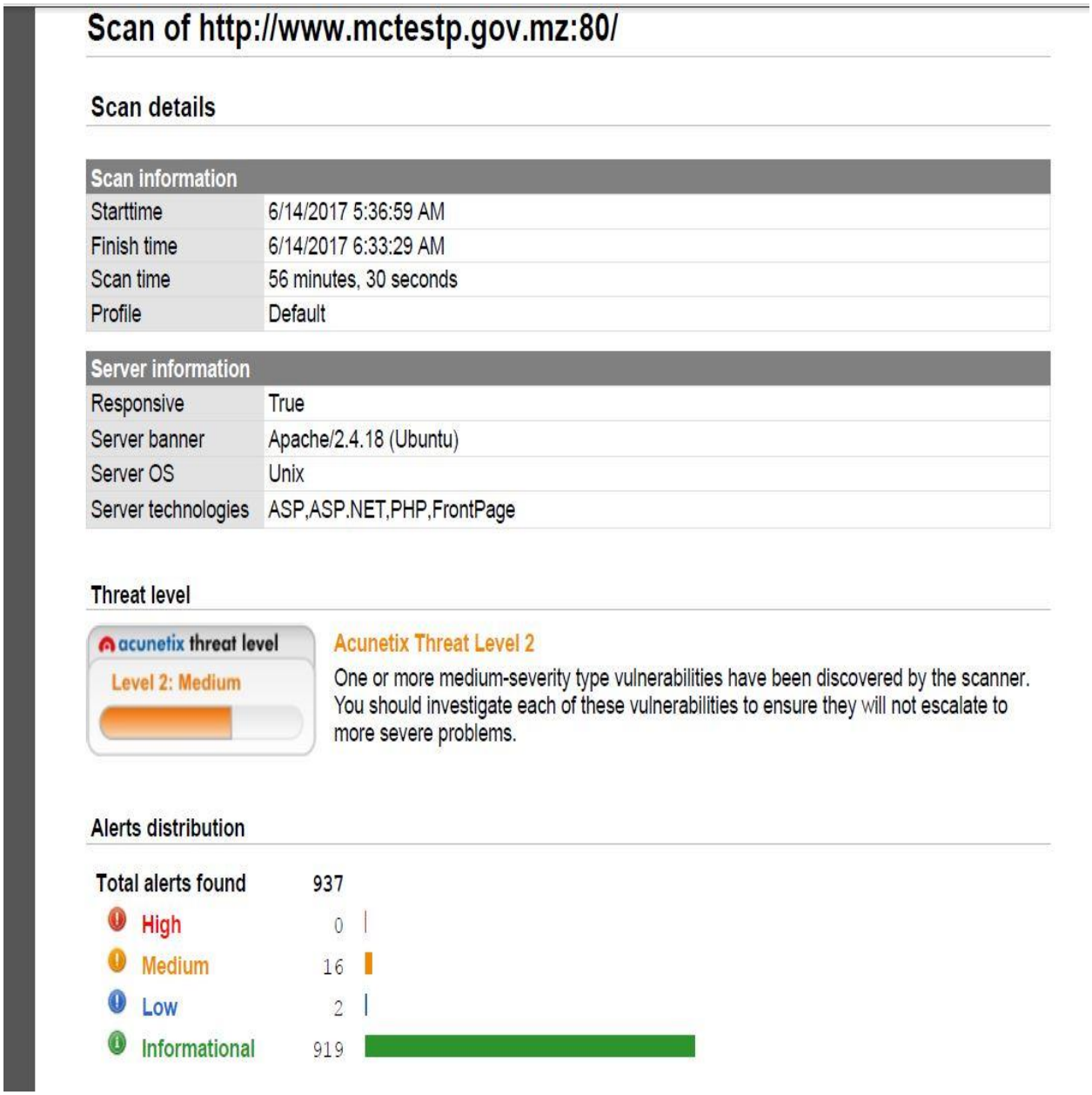
_____

_____

_____

Obrigado pela atenção dispensada.

Anexo 3. Relatórios de *scan* de Vulnerabilidades em Aplicações *Web* dos Ministérios da República de Moçambique



Scan of http://www.mctestp.gov.mz:80/

Scan details

Scan information	
Starttime	6/14/2017 5:36:59 AM
Finish time	6/14/2017 6:33:29 AM
Scan time	56 minutes, 30 seconds
Profile	Default

Server information	
Responsive	True
Server banner	Apache/2.4.18 (Ubuntu)
Server OS	Unix
Server technologies	ASP,ASP.NET,PHP,FrontPage

Threat level

acunetix threat level

Level 2: Medium

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	937
High	0
Medium	16
Low	2
Informational	919

Figura A3- 1: Resultados do scan de Vulnerabilidades na Aplicação web do MCTESTP

Scan of http://www.minec.gov.mz:80/

Scan details

Scan information	
Start time	6/14/2017 1:58:53 PM
Finish time	The scan was aborted
Scan time	10 minutes, 22 seconds
Profile	Default

Server information	
Responsive	True
Server banner	Apache
Server OS	Unknown
Server technologies	PHP

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Figura A3- 2: Resultados do scan de Vulnerabilidades na Aplicação web do MINEC

Scan of http://www.mec.gov.mz:80/

Scan details

Scan information	
Start time	6/14/2017 12:30:59 PM
Finish time	The scan was aborted
Scan time	1 hours, 19 minutes
Profile	Default

Server information	
Responsive	True
Server banner	Microsoft-IIS/7.5
Server OS	Windows
Server technologies	ASP.NET

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

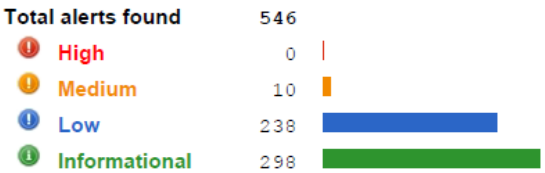


Figura A3- 3: Resultados do scan de Vulnerabilidades na Aplicação web do MEDH

Scan of http://www.mtc.gov.mz:80/

Scan details

Scan information	
Start time	6/14/2017 11:39:36 AM
Finish time	The scan was aborted
Scan time	47 minutes, 9 seconds
Profile	Default

Server information	
Responsive	True
Server banner	Apache/2.2.22 (Ubuntu)
Server OS	Unix
Server technologies	ASP,ASP.NET,PHP,FrontPage

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

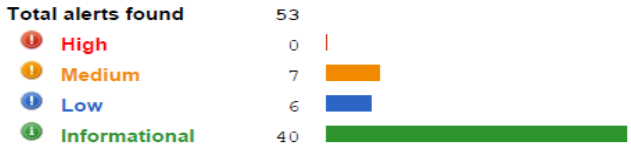


Figura A3- 4: Resultados do scan de Vulnerabilidades na Aplicação web do MTC

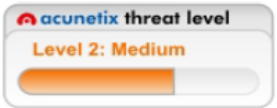
Scan of http://www.mjd.gov.mz:80/

Scan details

Scan information	
Start time	6/16/2017 1:45:04 PM
Finish time	The scan was aborted
Scan time	1 hours, 44 minutes
Profile	Default

Server information	
Responsive	True
Server banner	Apache/2.2.15 (CentOS)
Server OS	Unix
Server technologies	

Threat level



Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

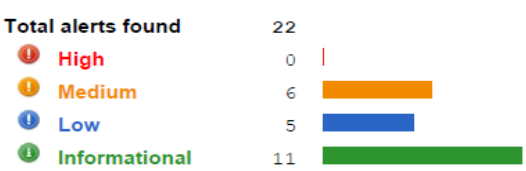


Figura A3- 5: Resultados do scan de Vulnerabilidades na Aplicação web do MJD

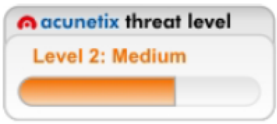
Scan of http://www.masa.gov.mz:80/

Scan details

Scan information	
Start time	6/16/2017 1:27:10 PM
Finish time	The scan was aborted
Scan time	16 minutes, 32 seconds
Profile	Default

Server information	
Responsive	True
Server banner	Apache
Server OS	Unknown
Server technologies	PHP

Threat level



Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

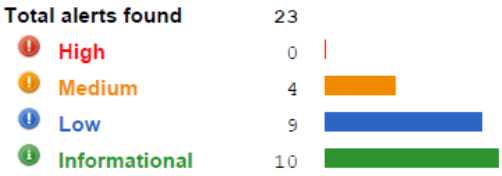


Figura A3- 6: Resultados do scan de Vulnerabilidades na Aplicação web do MASA

Anexo 4: Medidas de Prevenção

A4-1: *Clickjacking: X-Frame-Options header missing*

Quantidade	1
Nível	Baixo
Descrição	*Clickjacking* ou simplesmente ataque de reparo da interface do utilizador é uma técnica maliciosa usada para enganar um utilizador da aplicação *web* para clicar em algo diferente do que o utilizador pensa estar clicando, podendo este acabar por revelar informações confidenciais ao atacante ou o ataque pode assumir o controla do computador da vítima enquanto clica aparente em paginas inofensivas. O servidor não retornou um cabeçalho *X-Frame-Options*, o que significa que a aplicação pode estar em risco de um ataque de *Clickjacking*.
Impacto	O impacto depende muito da aplicação vítima. Utilizadores podem ser encaminhados a formulários em que devem fornecer algumas informações confidenciais.
Prevenção	Configurar o servidor *web* de modo a incluir um cabeçalho de *X-Frame-Options.* O cabeçalho de resposta *HTTP X-Frame-Options* é usado para indicar se um navegador deve ou não ser habilitado para redireccionar uma página em <*frame*> ou <*iframe*>.

A4-2: *Possible virtual host found*

Quantidade	1
Nível	Baixo
Descrição	*Virtual hosting* (hospedagem virtual) é um método para hospedar vários nomes de domínio (com manipulação separada de cada nome) em um único servidor (ou grupo de servidores). Isso permite que um servidor compartilhe seus recursos, como ciclos de memória e processador, sem exigir que todos os serviços fornecidos usem o mesmo nome de *host*. Durante a realização dos testes, o servidor *web* respondeu de forma diferente quando o cabeçalho do *host* foi manipulado e vários *hosts* virtuais comuns foram testados. Isso indica que existe um *hos*t virtual presente aplicação.
Impacto	Possível divulgação de informações sensíveis
Prevenção	Consultar a configuração do *host* virtual e verificar se este deve estar acessível ao público.

A4-3: *Session Cookie without HttpOnly flag set*

Quantidade	1
Nível	Baixo
Descrição	Este *cookie* não possui o conjunto de sinalizadores *HTTPOnly*. Quando um *cookie* é configurado com o sinalizador *HTTPOnly*, ele instrui o navegador de que o cookie só pode ser acedido pelo servidor e não por *scripts* do lado do cliente. Esta é uma protecção de segurança importante para *cookies* de sessão.
Impacto	Roubo de *cookies* de sessão
Prevenção	Configurar o sinalizador *HTTPOnly* para este *cookie*.

A4-4: Session Cookie without Secure flag set

Quantidade	1
Nível	Baixo
Descrição	Este *cookie* não possui o conjunto de sinalizadores seguros. Quando um *cookie* é configurado com a bandeira segura, ele instrui o navegador de que o cookie só pode ser acedido através de canais SSL seguros. Esta é uma protecção de segurança importante para *cookies* de sessão.
Impacto	Roubo de *cookies* de sessão
Prevenção	Configurar a bandeira segura para este *cookie*.

A4-5: *TRACE method is enabled*

Quantidade	1
Nível	Baixo
Descrição	O método *HTTP TRACE* encontra-se habilitado no servidor web. Na presença de outras vulnerabilidades entre domínios em *browsers*, informações de cabeçalho sensíveis podem ser lidas a partir de qualquer domínio que suporte o método *HTTP TRACE*.
Impacto	Os atacantes podem fazer o uso da funcionalidade *HTTP TRACE* para obter acesso a informações em cabeçalhos HTTP, como *cookies* e dados de autenticação.
Prevenção	Desabilitar a método *TRACE* no servidor *web.*