Universidade Paulista - UNIP

Leonardo Scherre Ragonha

VULNERABILIDADES EM APLICAÇÕES WEB

Limeira
2021

Universidade Paulista - UNIP

Leonardo Scherre Ragonha

VULNERABILIDADES EM APLICAÇÕES WEB

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade UNIP, como requisito parcial à obtenção do Bacharelado em ciência da computação sob a orientação do professor Me. Sergio Eduardo Nunes.

Limeira
2021
Leonardo Scherre Ragonha

VULNERABILIDADES EM APLICAÇÕES WEB

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade UNIP, como requisito parcial à obtenção do Bacharelado em ciência da Computação sob a orientação do professor Me. Sergio Eduardo Nunes.

Aprovada em XX de XXXXX de 201X.

BANCA EXAMINADORA

_____

Prof. Dr. Nome completo

_____

Prof. Me. Nome completo

_____

Prof. Esp. Nome completo

DEDICATÓRIA

Dedico este trabalho aos meus professores, familiares e colegas que me apoiaram durante esta jornada...

“O sucesso é ir de fracasso em fracasso sem perder o entusiasmo”.

(Winston Churchill)

RESUMO

Texto em parágrafo único, no máximo 500 palavras...

Palavra-Chave: até cinco palavras, separadas por ponto-e-vírgula.

ABSTRACT

Text...

Key Words: ...

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS

SUMÁRIO

1. INTRODUÇÃO

Os estudos sobre as vulnerabilidades mais comuns em sites, terá como auxilio, a lista publicada pela OWASP[1] com o objetivo de alertar as empresas e programadores das falhas mais comuns em serviços de aplicação web.

Vulnerabilidade são fraquezas presentes nos ativos de informação, que podem causar, intencionalmente ou não, a quebra de um ou mais dos três princípios de segurança da informação: confidencialidade, integridade e disponibilidade. (CAMPOS, 2006,pag. 11).

Para que um site seja considerado seguro ele precisa garantir os seguintes pilares da segurança da informação.

Confidencialidade: A confidencialidade tem como princípio o acesso das informações apenas pelos usuários autorizados. (Fontes, 2000, pag. 21).

Integridade: O princípio da integridade é respeitado quando a informação acessada está completa, sem alterações e, portanto, confiável. (Campos, 2006,pag. 6)

Disponibilidade: Este fator tem como principal finalidade a garantia de que as informações sejam passadas levando a empresa a atingir o nível de segurança adequado ao seu negócio, de forma correta para os usuários, com a participação dos associados na organização. (Campos, 2006,pag. 6)

[1]Open Web Application Security Project

1.1 Objetivo

O objetivo desse trabalho é utilizar um sistema operacional aberto com ferramentas de testes de invasão para realizar um escaneamento de um site em busca de falhas e atacar as vulnerabilidades existentes do site através do método de SQL Injection, avaliando o quanto de informações/dados é possível coletar ou alterar de uma aplicação web não programada nos melhores padrões de segurança.

Podendo então gerar um relatório do passo a passo e ferramentas utilizadas para conseguir invadir e obter informações do site estudado, que, segundo as normas de segurança e a lei geral de proteção de dados nenhum individuo a não ser o dono de tais dados deva ter acessso as mesmas.

Propondo assim, uma discussão a respeito dos parâmetros que alguns sites ainda possuem, mesmo com essas informações a respeito de falhas estando disponíveis na internet para pesquisa, reconhecimento e manutenção caso seja encontrada em seu site, desta forma podendo tornar determinado site mais seguro e passar uma segurança maior para seus usuários.

1.2 Justificativa

Com base na Lei Geral de Proteção de Dados, onde a função da mesma e garantir a proteção de dados pessoais sejam esses dados de pessoas fisícas, jurídicas ou privados, visando os direitos básicos de liberdade e privacidade do individuo, lei essa que já esta vigente desde setembro de 2020 e passará a ser sansionada a partir do dia 1º de agosto de 2021, tendo multas de até R$50 milhôes de acordo com a gravidade do caso.

Utilizando também a lei 12.737 para amparar usúarios onde tipificão como crime a invasão ou interrupção de dispositivos ligados ou não a rede, sancionada em 2012 ela vem como um meio de tentar proteger o usuário punindo o invasor mas não de fato cobrando uma segurança do fornecedor do serviço, a pena para este tipo de crime pode gerar reclusão de 3 meses a 2 anos de acordo com informações obtidas ou danos causados.

Sendo assim, com essas duas leis a favor da informatica onde tanto o infrator quanto o detentor da informações são punidos caso haja algum tipo de vazamento ou invasão, isto força os locais onde armazenamos nossos dados a se tornarem mais seguros e aptos para agir em caso de tentativa de obtenção ou destruição desses dados.

1.3 Metodologia

Para executar os testes de intrusão vamos utilizar o site www.bancocn.com, desenvolvido pela Solyd com intuito exclusivo para treinamentos do tipo. O sistema operacional a ser utilizado será o Kali-Linux, a escolha do Kali se da por ser um sistema operacional de código aberto específico para diversos testes na área de segurança da informação.

O primeiro passo para começar o ataque é fazer um footprint do alvo que queremos descobrir falhas, onde vamos analisar quais domínios estão atrelados ao http, se possui e-mails registrados para que possamos fazer ataques de engenharia social, procurar por brechas no código e assim podermos partir para segunda fase.

Na segunda fase vamos para o fingerprint, processo onde iremos reunir todas as informações que conseguimos no primeiro passo e utilizar para fazer os ataques, seja via [2]URL, brute force em senhas de login ou campos que permitam entrada de dados, com isso veremos quais vulnerabilidades determinada aplicação web possui a partir da falta das boas práticas de segurança da informação, onde o acesso a qualquer usuário não permitido significa a quebra dos pilares.

2. SEGURANÇA DA INFORMÇÃO

2.1 Lei nº 13.709

2.2 Lei nº 12.737

3. PROTOCÓLOS

3.1 HTTP

3.2 DNS

4. PENTEST

CONCLUSÃO

O trabalho permitiu...

REFERÊNCIAS BIBLIOGRÁFICAS

CAMPOS, André L. N. **Sistema de Segurança da Informação: Controlando os Riscos**. Florianópolis: Visual Books, 2006.

FONTES, Edison. **Vivendo a segurança da informação: orientações práticas para pessoas e organizações**. São Paulo: Sicurezza, 2000.

OLIVEIRA, G. D; et. Al. ARAÚJO, F. A. N. G; Gestão da segurança da informação. Disponível em:<https://brapci.inf.br/index.php/res/download/137280>. Acesso em 10 de mar. de 2021.

PIMENTA, M. S.; QUARESMA, R. F. C; A segurança da informação e o comportamento dos usuarios. Disponível em:<encurtador.com.br/afR48>. Acesso em 10 de mar. de 2021.