3º CONGRESSO NACIONAL DE INFORMÁTICA – BELÉM/PA.

UNAMA – Campus BR

PYOWNZ: FERRAMENTA PARA REALIZAR VARREDURA DE SQL INJECTION

Dennys Augustus Pinto de Oliveira[1]; Alan Marcel Fernandes de Souza[1]

[1]Universidade da Amazônia (UNAMA), Belém – PA

Resumo: Este trabalho apresenta protótipo de um script desenvolvido Python que realiza uma varredura na internet utilizando os motores de busca do Google para localizar os hosts e, em seguida, realizar testes de SQL Injection. Além disso, propõem-se formas de se defender do ataque.

Palavras-chave: SQL Injection, varredura, Google, Python.

1. Introdução

A cada dia, cresce o número de empresas que migram seus processos para plataformas computacionais com o intuito de armazenar em banco de dados (BD) as informações de maneira mais organizada, prática, acessíveis e seguras. Dessa forma, o BD se constitui como um dos bens mais valiosos de uma organização, pois, atualmente, as informações podem ser o diferencial competitivo das corporações empresariais. Portanto, é necessário proteger os dados contra ataques cibernéticos.

O SQL Injection é um tipo de ataque digital que injeta comandos de SQL, simples de ser feito, mas muito devastador para uma organização, pois pode desde vazar dados sigilosos até apagar permanentemente a base dados. Segundo MDS Engenharia (2018), 90% das empresas que de alguma maneira perderam seus dados seja por defeito em hardware, software, erro humano ou ataque cibernético fecharam dentro de dois anos.

Na grande maioria dos casos, essa vulnerabilidade decorre da não utilização de boas práticas de programação e pode ser facilmente evitada com a adoção de medidas que mantenham o código do projeto seguro e estável, boas políticas de backups/restauração.

O objetivo desse trabalho é descrever o funcionamento de um script, programado na linguagem Python (versão 2.7.12), executado e testado um ambiente Linux Ubuntu (16.04.05), sendo preciso a instalação das seguintes bibliotecas Requests, Sys, Re, Google e o controle de versão Git.

[1]Graduação, Unama/Curso Ciência da Computação. dennysaug@gmail.com

Há muitos scripts e programas que realizam testes de vulnerabilidades, mas nenhum disponível ao público que realiza a captura dos hosts utilizando a busca do Google, resolvendo os captchas, quando surgem, e testando se o host está vulnerável a SQL Injection ou não.

É importante ressaltar que a utilização dessa ferramenta é somente para fins de didáticos, qualquer outro fim será de inteira responsabilidade do utilizador.

2. Metodologia

A execução do script requer todas as bibliotecas mencionadas anteriormente, pois cada uma delas tem papel fundamental nas funções que o script necessita. Quando executar o script, se escolher a opção que para 1 ou 2 será realizado uma busca utilizando o Google para capturar os hosts e em seguida executará o teste adicionando na url capturada =1\' or \'1\' = \'1\" e se em alguma parte do corpo da página contiver a mensagem "You have an error in your SQL syntax", possivelmente um host vulnerável foi encontrado.

O SQL Map é uma ferramenta que realiza teste penetração, automatizando o processo de detecção e exploração de vulnerabilidades a SQL Injection. Após colher os resultados possivelmente vulneráveis, basta abrir o SQL Map e utilizar suas diversas opções para explorar a falha, que vão desde mostrar banco de dados e tabelas até drop table (remover a estrutura e os dados contidos em uma tabela) e drop database (remover por completo o banco de dados). Para visualizar todas as opções do SQL Map, o comando “sqlmap -help” pode ser usado.

A vulnerabilidade pode ser corrigida através do tratamento da consulta ao BD antes de sua execução, não permitindo que caracteres especiais sejam usados nas consultas. Em websites desenvolvidos em PHP, basta, por exemplo, tratar todos os dados vindos de formulários da seguinte forma (Devmedia, 2018):

a) Permitindo somente letras: $variavel = preg_replace('/[^[:alpha:]_]/', '',$variavel);
b) Permitindo alfanumérico: $variavel = preg_replace('/[^[:alnum:]_]/', '',$variavel);

Além disso, é importante manter os frameworks utilizados nos projetos atualizados, pois alguns já vêm com a proteção nativamente. Em PHP, o uso do PDO (PHP Data Objects) para realizar comunicação com o banco de dados também ajuda a se prevenir desse tipo de ataque, pois faz uso de *prepared statements* na formação das *queries*. Acima de tudo, sempre ter uma boa política de backup e restauração de sistema.

3. Resultados e Discussões

Os resultados obtidos com a varredura de uma lista de palavras de busca demonstram que há muitos servidores vulneráveis a SQL Injection (Figura 1).

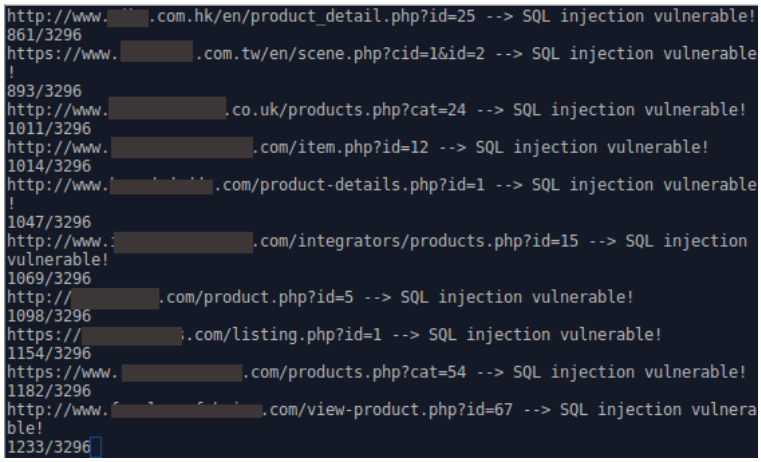

Figura 1. Resultado da varredura por vulnerabilidades.

O Sqlmap é uma ferramenta utilizada para auditorias de segurança em banco de dados. As opções que a ferramenta oferece são várias, para conhecer todas utilize o “help” da ferramenta ou consulte no site www.sqlmap.org.

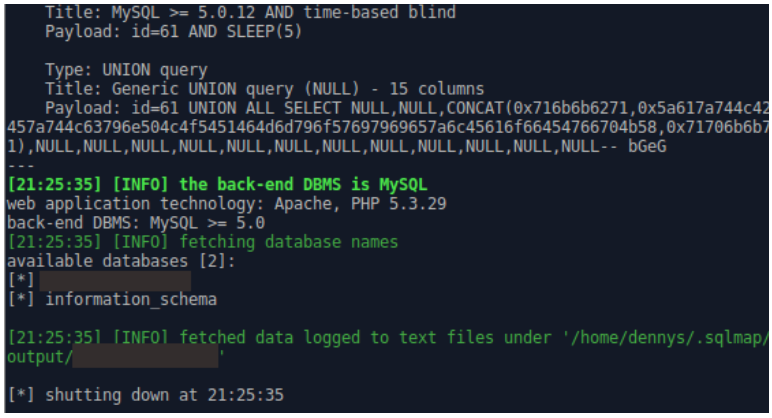

Figura 2. Sqlmap injetando comandos para retornar os bancos de dados

4. Conclusões

Este trabalho contribui com a comunidade para que ataques desse tipo sejam a cada momento menos frequentes, servindo para que administradores de sistemas web possam rever o seu código e corrigir a falha se houver, evitando assim prejuízos incalculáveis. A ferramenta, desenvolvida em Python, permite realizar essa detecção de brechas de segurança. Além disso, ela também pode ser modificada e aplicada para outros fins, como por exemplo, demonstrar ataques de força-bruta (testar vários logins e senhas automaticamente) em websites e realizar testes de sobrecarga de banco de dados.

6. Referências

Duffy, Christopher. Aprendendo Pentest com Python 1. ed. Tradução Edson Furmankiewicz; revisão técnica BrodTec. - São Paulo: Novatec Editora Ltda, 2016.

MDS Engenharia. 90% das empresas que perderam seus dados, fecharam dentro de 2 anos! -. Disponível em: <http://mdsengenharia.com.br/2016/09/09/ola-mundo> Acesso em: 30 set. 2018.

Devmedia. Evitando SQL Injection em aplicações PHP. Disponível em: <https://www.devmedia.com.br/evitando-sql-injection-em-aplicacoes-php/27804> Acesso em: 30 set. 2018.