Information Security Project

Giacomo Melacini, Matteo Messmer

Immagine che contiene bottiglia, segnale, nero, fotografia

Descrizione generata automaticamenteAcademic Year 2019-2020

Table of Contents

[Introduction 3](#_Toc41904210)

[Exploits 3](#_Toc41904211)

[SQL-Injection 3](#_Toc41904212)

[WordPress plugin Chained-Quiz SQL-Injection 3](#_Toc41904213)

[Cross-Site Scripting 4](#_Toc41904214)

[CodeIgniter XSS scripting attack 4](#_Toc41904215)

[References 6](#_Toc41904216)

CMSsite

<https://github.com/VictorAlagwu/CMSsite>

Install:

Do the following change the code in the **db.php**

* + $DB\_host = "";
  + $DB\_user = "";
  + $DB\_pass = "";
  + $DB\_name = "";
* Import the database file named "php\_cms.sql"

**SQL Injection**

<https://www.exploit-db.com/exploits/48485>

Retrieve Version e Database name

<https://www.exploit-db.com/exploits/48490>

<https://www.exploit-db.com/exploits/48484>

<https://www.exploit-db.com/exploits/48451>

# Introduction

This project aims to exploit different applications applying different kind of attacks. We searched for possible vulnerabilities in *exploitdb* and decided to proceed with x SQL Injections, y XSS attacks and z altra roba. In order to automatize the exploit we developed a python application, *main.py*, in which the user is asked to input a target. The target is identified by analyzing the content of the *url* and then a specific attack is executed. After a vulnerability has been exploited, the user can decide whether to continue with another attack or to close the application.

# Exploits

## SQL-Injection

### WordPress plugin Chained-Quiz SQL-Injection

Vulnerability description

The Chained-Quiz WordPress plugin lets the user create quiz where the next question depends on the answer of the previous one. This plugin, in the versions prior to 1.0.8 is vulnerable to time-based SQL injection.

Causes of vulnerability

This version of the plugin allows unauthorized users to execute SQL queries via the *answer* parameter. The problem lies on the *answer* backend variable.

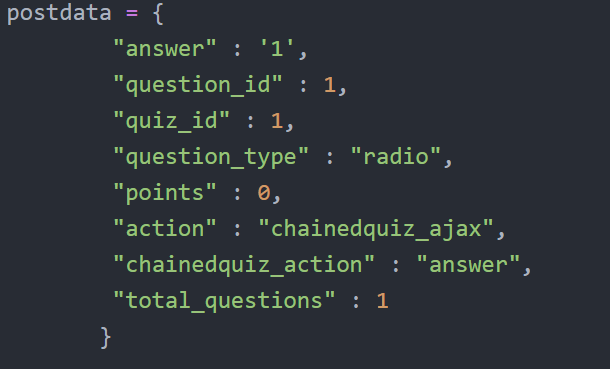
Implementation

The provided version of the plugin is v0.8.7. In order for the exploit to work, the database on which WordPress runs must be mySQL.

When we submit the answer of a question via a POST request, we can inject SQL commands to the parameter *answer* to check which database the web-application is using.

We are going to inject the command SLEEP(15), that is a mySQL command. This means that if the application by reading the request will sleep 15 seconds, the underlying database will be a mySQL database.

The parameters that are being passed in the POST request are the following:



The payload will be inserted in the answer parameter and it will be the following:



The POST request is executed with the python library *requests*:

## Cross-Site Scripting

### CodeIgniter XSS scripting attack

Vulnerability description

CodeIgniter is a PHP framework to create web applications. The version prior to v2.1.2 are vulnerable to XSS scripting attacks.

Causes of vulnerability

The cause of the vulnerability lies on the function *xss\_clean()*, that is a filter protection used to sanitize user inputs. The filter is not working correctly, therefore it is possible to execute a malicious script.

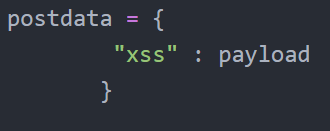
Implementation

The aim of this exploit is to launch a script rising an alert using the function *xss\_clean()*. This function is used to sanitize the input of the form.

The payload is the following:



This payload is inserted as parameter of the POST request:



The request is then executed using the python library *requests* and the script is shown to be present in the answer of the request:



# References

CodeIgniter XSS attack: <https://www.exploit-db.com/exploits/37521>

GitHub Repository: <https://github.com/matteomessmer/InformationSecurityProject>

WordPress plugin Chained-Quiz SQL-Injection: <https://www.exploit-db.com/exploits/45221>