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 two SQL Injections, two XSS attacks and one CSRF attack. 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.

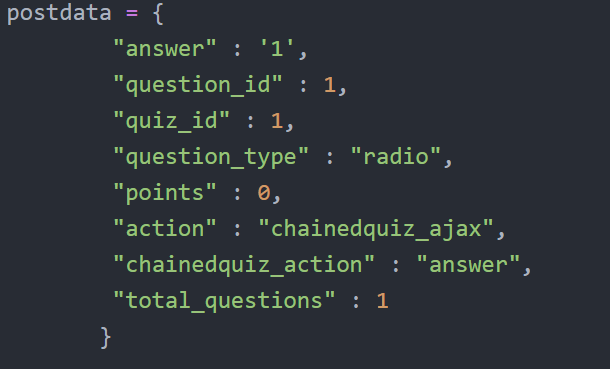
Implementation

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*:

### Victor CMS 1.0 'cat\_id' SQL-Injection

Vulnerability description

The Victor CMS 1.0 is a simple Content Management System coded in PHP by Victor Alagwu and offered for free on his GitHub page. This CMS has various vulnerabilities (there are five listed on [exploit-db.com](https://www.exploit-db.com/)), one of them is an SQL-Injection.

Causes of vulnerability

This CMS allows unauthorized users to execute SQL queries via the *cat\_id* parameter, which is vulnerable to SQL Injection. The problem is in the category.php page which does not do the proper sanitization of the user input.



Implementation

The aim of this exploit is to retrieve sensitive information from the database. The data we are going to retrieve are personal data such as users’ mails and passords, the database name and the verion of MySQL. These information should be kept private, but by exploiting the SQL Injection vulnerability by using the following payload, an attacker will be able to retrieve them.

"category.php?cat\_id=-1+UNION+SELECT+user\_id,user\_firstname,user\_name,randsalt,user\_password,user\_email,user\_role,user\_lastname,VERSION(),DATABASE()+FROM+users;+--"

In the cat\_id paramether we injected a malicious query. It does not return any post because the id of the category is set to -1, but then we make the union with all the private data of the users. Of course the number of columns of both sides of the query has to be equal, otherwise an error will occur. In this case the columns on the left side are 10 so we make sure to make the union with 10 columns.

By submitting this request we would normally get a page listing all the posts that matches the query. But in the case of this payload the result will not list any post. What we will see instead are the user data in the place of the post data.



The python script automates the request and parses all the data into a list.

## 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.

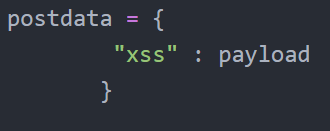
Implementation

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:



### Victor CMS 1.0 - 'comment\_author' Persistent Cross-Site Scripting

Vulnerability description

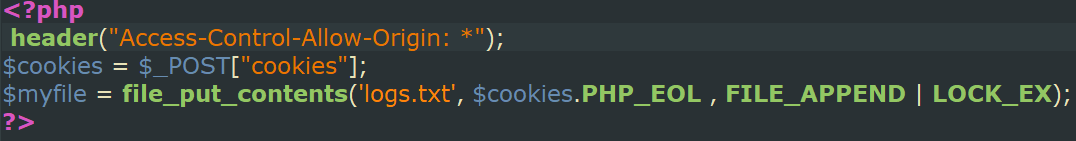
Another vulnerability of the Victor CMS is the Persistent XSS.

Implementation

The vulnerability lies in the comment feature of the CMS. In every article of the website there is a form that allows everyone to post a comment. The problem is in the comment\_author input, which is not correctly sanitized and lead to the XSS vulnerability. Moreover, since the comments are stored, the XSS is persistent. The aim of this exploit is to launch a script that steals the cookies of the users. To do this we prepared a javascript function that send the cookies of the victims to the attacker is on another website and it is the following.



We also need a function that saves the cookies on a file. The savecookies.php logs all the cookies into a txt file on the server.



Now that the background for the attack is ready we have to inject the javascript function into a comment. When the visitors open the article that has the malicious comment, the cookies will be stolen without that they notice. The automatization is the following:



Since the script that steals the cookies is on our website we can modify it as we want. In this way the malicious comment does not need to be changed to execute other code.

# References

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

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

Victor CMS SQL Injection: <https://www.exploit-db.com/exploits/48485>

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

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

WordPress Plugin Simple Membership 3.8.4 - Cross-Site Request Forgery: <https://www.exploit-db.com/exploits/47182>