Insecure Mate Web Shop
– Tasks –

October 2021

1 Cross-Site-Scripting (XSS)

The administrator reads all the messages one sends to him. Unfortunately, there are different kind of Cross-Site Scripting (XSS) attacks possible namely **reflected XSS**, **dom-based XSS** and **persistent XSS**.
The following two tasks requires you to perform two types of XSS attacks on the mate webshop. Read the tasks carefully to understand which kind of XSS you should perform.

1.1 AdminDiss

You are really upset about MateShop's reckless security behaviour and especially the expensive prices on the website for Mate and Chunk beverages - the websites admin blamed your low Mate consumption! Be persistent! Insult the administrator as a *dumb donkey* in an alarming way.
The goal of the task is that every time the admin calls the forum's site he or she will be insulted.

1.2 BugReport

After insulting the admin it is time to expose the admin even further. The admin is eager to fix the security issue from the insult and will be happy about every kind of help he or she can get.
Find out what kind of private stuff the admin hides from Google by stealing his or her identity! Perform a reflective XSS attack.
The goal is to steal the cookie value of the admin and log in as the admin. After that the flag is hidden in a file called private.php.

2 SessionHijack

Donald is a regular customer of the webshop and values the protection of his data provided there. Make the shop owners aware of how easy it is to steal their

customers data.
You should solve one task in this scenario which consists of stealing a session of an existing user of the webshop.
The goal is that you get the session ID of the user *Donald* and with his ID get access to his profile page that holds sensitive information such as the username and password for the webshop.
When you solve the task successfully, you can set Donald's cookie as yours and view his profile. The stolen sessionId will be the flag that needs to be found.

3 SQL Injection (SQLi) - Password Hack

Finally, we want to log in as the admin itself to the application and therefore trying to get his credentials. We want to make him rethink his current implementation.
This task aims to implement an effective SQL injection to read from the database. The goal of this task is to access the admins password which is stored as a not-salted MD5 hash in the database.