FUTURE_CS_01

Inter name: Vaibhav Gulati

Intern domain: Cyber Security

Task title: WEB APPLICATION SECURITY TESTING

Date: July 2025

Tool used: Burp-suite
Owasp Juice Shop Demo Site
Basic Inspect Tools

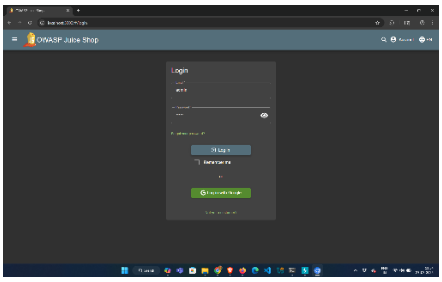
Objective:

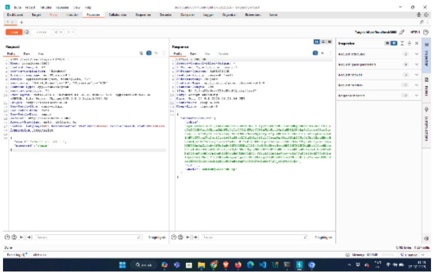
To perform basic web application security testing and identify common vulnerabilities like :

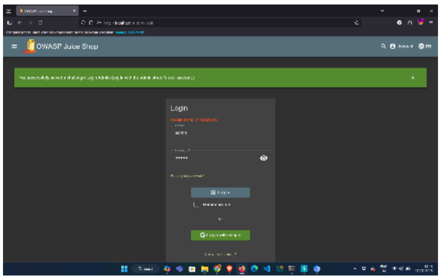
- SQL Injection
- Cross – site scripting (XSS)
- Authentication flaws

Task 1: SQL Injection(Admin Login Bypass)

1. Tried login with ‘admin’ , ‘admin’.
2. Then in Burp-suite the request is send to the repeater.
3. In repeater, we planted a code in email section “admin’ or 1=1--“, request is again sended to the server.
4. Got the authentication token/jack token.
5. Challenge completed.





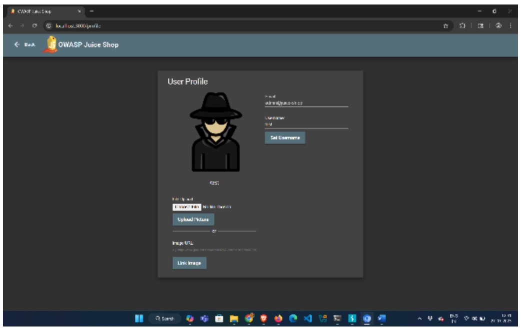


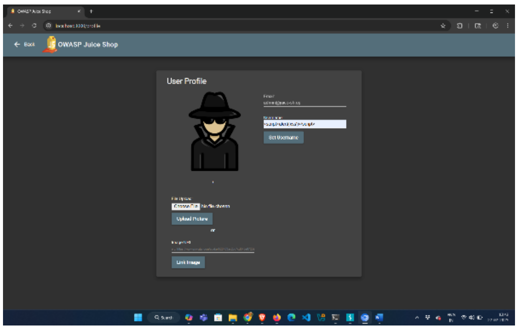
#Why It Worked?

The reason here is that, coincidentally the first user in the database was the administrator user and because of the first user in the user table we got authentication by implanting the code.

Task:2 Classic Stored XSS

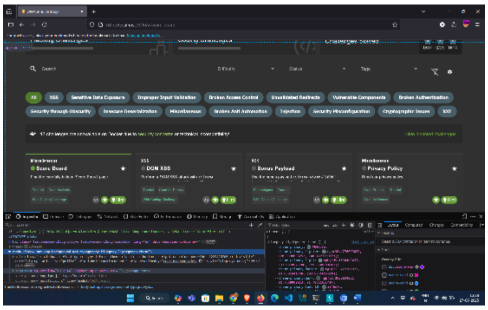
1. In hint we had given a payload <script>alert('xss')</script>, I copied it.
2. As we went to profile section , we get to see username column empty, for first I tried to name it 'test' and it worked.
3. Then I pasted the payload there and run it by chance if it works, but it didn't due to backend codes it resisted and tried to edit and narrow the script.
4. After multiple attempts and modification on payload. I checked through inspect mode what part it actually cutting it so, I duplicated the letters to trick it and the payload " <<script>sscript>alert('xss')</script>" worked.
5. Task completed although it is not showing might be due to frontend filters.

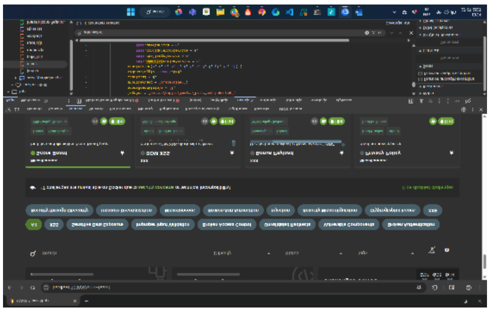


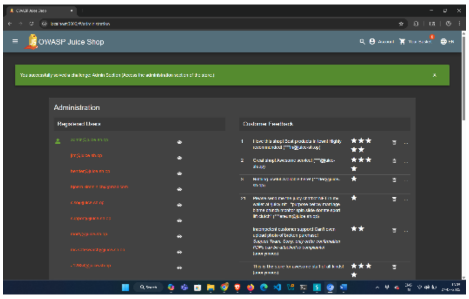


Task 3: Admin Section (Broken Access Control)

1. For admin section, firstly I open developer tool by clicking F1 from this I found '_ng' context many times from this, I got to known about that this site is build on angular site.
2. Learning about angular site , I get to known about that each route maps a URL path to a component.
3. From these information , I went to Debugger tool and used search functionality clicking to find administrat and after couple of things , I got something interesting there is a path saying administration.
4. Then I changes URL to administration and I got the access. There are lot of info about Customers review and Registered users.
5. Task Completed.







You successfully solved a challenge: Admin Section (Access the administration section of the store.)

Administration

Registered Users

Customer Feedback