Assignment 1

OWASP Security Shepherd Responsible Disclosure Program

You have signed up for a responsible disclosure program for the OWASP Security Shepherd project.

Your task is to document the vulnerabilities you find in Security Shepherd.

Pick **4 different** vulnerabilities, e.g., SQL Injection, XSS, Poor Data Validation and Failure to Restrict URL Access.

Attempt to complete the harder challenges in the platform not just the lessons or the first few challenges.

For each of the vulnerabilities you must do the following;

1. Assign an appropriate title to the vulnerability referring to the OWASP Top 10 (title of the lesson/challenge)
2. Look up the CWE number of the vulnerability https://cwe.mitre.org/ and include it in the title
3. Write a short description of what the vulnerability is
4. Document the reproduction steps in clear and concise wording including any additional software needed e.g. Burp Suite
5. Assign a CVSS score using the calculator https://www.first.org/cvss/calculator/3.1
6. Put the rating of the CVSS score in the title e.g. **High: *title* [CWE-…]**
7. Order each vulnerability in terms of risk *according to the CVSS score
8. Take appropriate screenshots

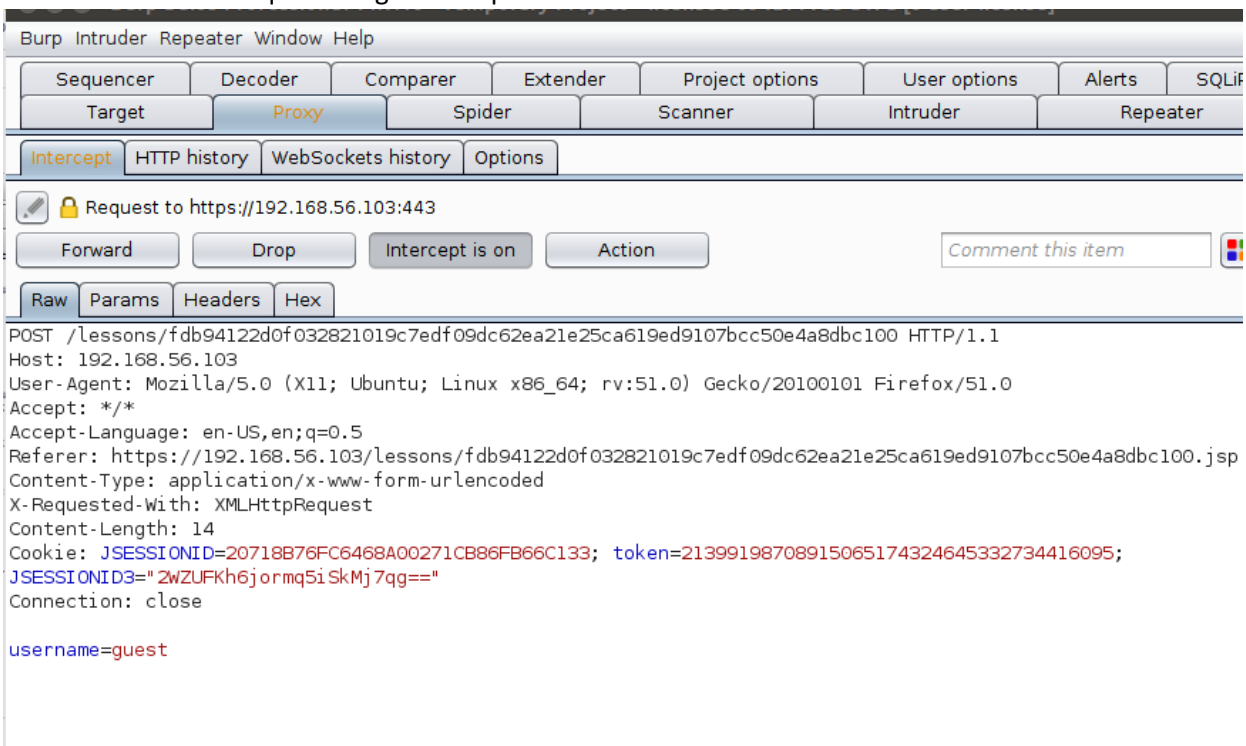
The OWASP Security Shepherd team has put together an example vulnerability write up;

High: Insecure Direct Object Reference in Lessons [CWE-639]

Insecure Direct Object Reference is where a malicious user can change the value of a parameter to bypass the authorisation of the application. The application fails to verify the authorisation for a target object in this case the 'username' parameter. Changing the value of the username will bypass the authorisation and allow an attacker to see other users details in the system for example the admin user.

Steps to reproduce

1. Download and run Burp Suite https://portswigger.net/burp/communitydownload (making sure you have Oracle Java Installed)
2. Utilising Firefox set the system proxy to route traffic through Burp - "Open Menu" button in the right hand corner -> Advanced -> Network (tab) -> Connection "Settings Button" -> Manual proxy configuration. The default for Burp is 127.0.0.1 with a port of 8080
3. Got to Security Shepherd https://192.168.1.200
4. Confirm that Burp can see and capture requests and turn off intercept in Burp
5. Go to Lessons -> Insecure Direct Object Reference
6. Turn on intercept in Burp
7. Press the "Refresh your Profile" button in the lesson
8. You should see the request caught in Burp



9. Modify the value for the parameter "username" in the body of the request from "guest" to "admin"

10. Press forward in Burp
11. Go back to the lesson and you will see that you have become the admin

CVSS Score 7.2

Attack Vector	**Network**
Attack Complexity	**Low**
Privileges Required	**None**
User Interaction	**None**
Scope	**Changed**
Confidentiality	**Low**
Integrity	**Low**
Availability	**None**