Assignment 2
Professional Ethical Hacking Report

Utilising the report writing skills acquired in assignment 1 you are tasked with writing a professional penetrating testing report.

[Section 1 Vulnerabilities]

You must choose 10 vulnerabilities from Security Shepherd and use some of the skills learned from assignment 1 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/3.0
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
9. **Recommend a mitigation** (look to the lectures or OWASP for recommended mitigations)

[Section 2 Report]

The report must be formatted into a professional report which must include;

1. Heading page
    1. The UCD logo
    2. Title
    3. Product name (Security Shepherd)
    4. Product Version (v3.0)
    5. Penetration testers name (your name)
    6. Who the document is prepared for (Project Lead of Security Shepherd)
2. Consultant information page
    1. Your name
    2. Your student email
    3. Location of where you are based (UCD School address)
    4. Manager Name / Supervisors Name
3. Sensitive Information Page
    1. A notice and a warning stating that the document contains sensitive information

4. Index Page
5. Executive summary
    1. Lead penetration testers name (your name)
    2. Number of days testing (the amount of time you spent on this assignment)
    3. Test start and end date
    4. Application information
        i. Release Date
        ii. Project Contact (Project Lead of Security Shepherd)
    5. Findings Summary
        i. Project Version
        ii. Name of Application
        iii. Number of Vulnerabilities
        iv. Number of Vulnerabilities within the OWASP Top 10
    6. Severity Summary – Defects rated from Low to Critical according to the CVSS score
6. Scope
    1. State the levels / challenges that were attempted.
    2. The time frame the testing was complete and time frame the report was complete
    3. List of user roles in the system (username you log in with) and their authorisation
    4. List of URLs

7. Test Cases carried out
    1. For each vulnerability state what test case from the OWASP Testing Guide v4 was used e.g. for SQL Injection you'd use; Input Validation -> OTG-INPVAL-005 Testing For SQL Injection
8. List of Vulnerabilities
    1. Start with the heading Critical and put all vulnerabilities rated as CVSS critical in there and work your way to Low
    2. Include all the information in Section 1
9. Recommendations and Conclusions
    1. Include any further recommendations to the development team
    2. Include your conclusions

EXAMPLE REPORT

[UCD LOGO]

Web Application

Penetration Testing Report

Product Name: Security Shepherd

Product Version: v3.0

Test Completion: 16/04/2021

Lead Penetration Tester: <your name>

Prepared for: Vsevolods Caka

Consultant Information

Name: <your name>

Email: <your student email>

Location: <UCD address>

Manager: Mark Scanlon

Manager email: <Mark's email>

NOTICE

This document contains confidential and proprietary information that is provided for the sole purpose of permitting the recipient to evaluate the recommendations submitted. In consideration of receipt of this document, the recipient agrees to maintain the enclosed information in confidence and not reproduce or otherwise disclose the information to any person outside the group directly responsible for evaluation of its contents.

WARNING

Sensitive Information

This document contains confidential and sensitive information about the security posture of the OWASP Security Shepherd Application. This information should be classified. Only those individuals that have a valid need to know should be allowed access this document.

Index Page

Executive Summary

Lead Tester: <your name>

Number of days testing: <amount of time you spent testing including this doc>

Test Start Date:

Test End Date:

Project Information

Application Name: Security Shepherd

Application Version: v3.0

Release Date:

Project Contact: Nikita Pavlenko

Findings:

OWASP Top 10:

Total Defects:

Severity	#Defects
Critical	
High	
Medium	
Low	

Scope

State the levels / challenges that were attempted.

The time frame the testing was complete and time frame the report was complete

List of user roles in the system (username you log in with) and their authorisation

List of URLs

Test Cases

For each vulnerability state what test case from the OWASP Testing Guide v4 was used e.g. for SQL Injection you'd use;

Input Validation: OTG-INPVAL-005 Testing For SQL Injection

Findings

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

10. Download and run Burp Suite https://portswigger.net/burp/download.html (making sure you have Oracle Java Installed)
11. 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
12. Got to Security Shepherd https://192.168.1.200
13. Confirm that Burp can see and capture requests and turn off intercept in Burp
14. Go to Lessons -> Insecure Direct Object Reference
15. Turn on intercept in Burp
16. Press the "Refresh your Profile" button in the lesson
17. You should see the request caught in Burp
18. Modify the value for the parameter "username" in the body of the request from "guest" to "admin"
19. Press forward in Burp
20. 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**

Mitigation

Relying on the value username as passed in the post request is an insecure method to determine levels of authorisation as this value is easily modified to gain access to another users account. It is

recommended that the session value JSESSIONID is utilised to determine levels of authorisation. This value is sudo random where it is not easily modified to gain horizontal or vertical access to another user's account.

Recommendations and Conclusions

Write a summary of your findings. Include any further recommendations you might consider to secure the application.