10/25/2023

Penetration Testing Report

www.dvwa.com

Vinay Mangesh Farsole

Date:25/10/2023

Executive Summary: DVWA Penetration Testing Report

Introduction: This report outlines the results of a comprehensive penetration test conducted on www.dvwa.com, an instance of Damn Vulnerable Web Application. The primary objective was to assess the security posture of the web application and identify potential vulnerabilities that could be exploited by Hackers.

Help:

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

Key Findings:

1. **SQL Injection :**
    - Identified critical SQL injection vulnerabilities in multiple modules.
    - Demonstrated the potential for unauthorized access to sensitive data.
    - The 'id' variable within this PHP script is vulnerable to SQL injection
    - There are 5 users in the database, with id from 1 to 5.
    - There are 2 vulnerable column .

SQL INJECTION ON DVWA:

Level: Low

Step 1.

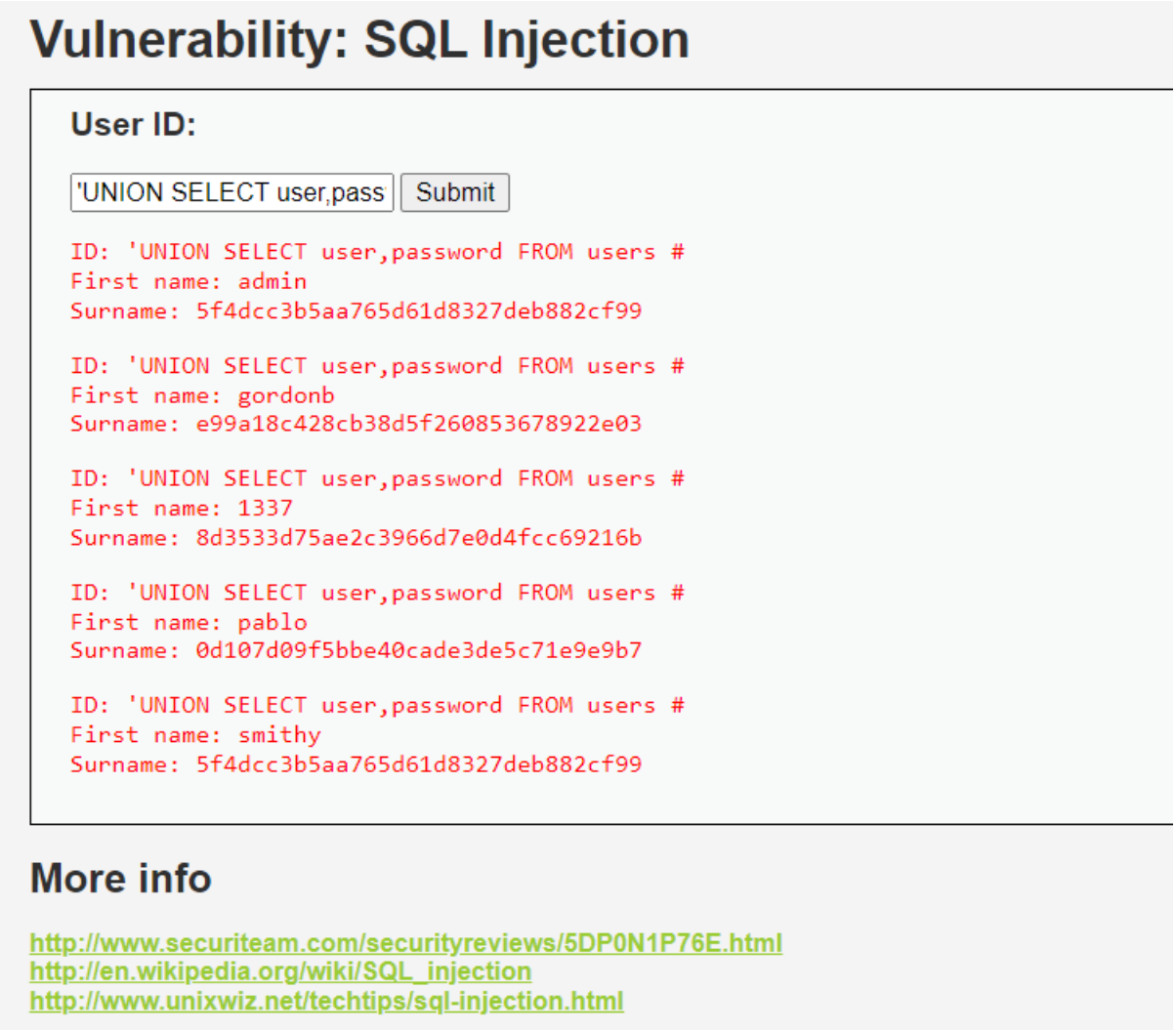
1. Enter the value in the user id box.

2. Enter any value data will display.

3. put the query that will show all the username , password from users table.

Payload: `1' Union select user,password from users #`

4. We Enter the Union query for search the user and password from the users table database

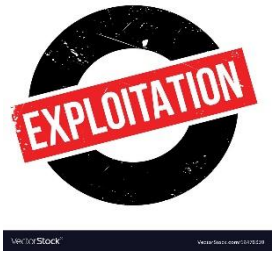


Risks: The identified vulnerabilities pose a significant risk to the confidentiality, integrity, and availability of the DVWA application. If exploited, these vulnerabilities could lead to unauthorized access, data breaches, and potential service disruptions.

Conclusion: The findings of this penetration test highlight the importance of addressing critical vulnerabilities to enhance the security posture of DVWA. Implementing the recommended measures will significantly reduce the risk of unauthorized access and data compromise.

This report aims to assist in strengthening the security of www.dvwa.com and fostering a proactive approach to cybersecurity.

CROSS SITE SCRIPTING ON DVWA:



Level: Low

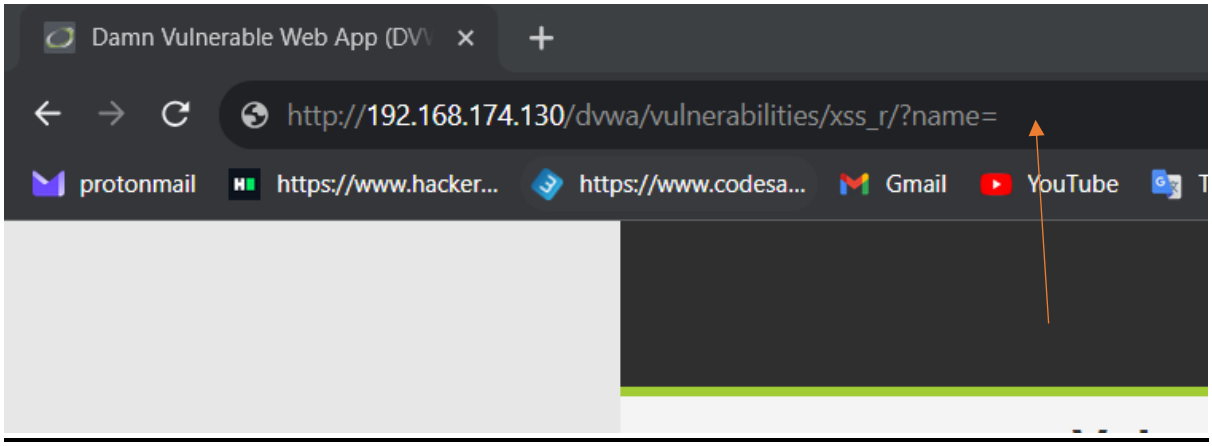
Vulnerability: XSS Reflected.

Step 1.

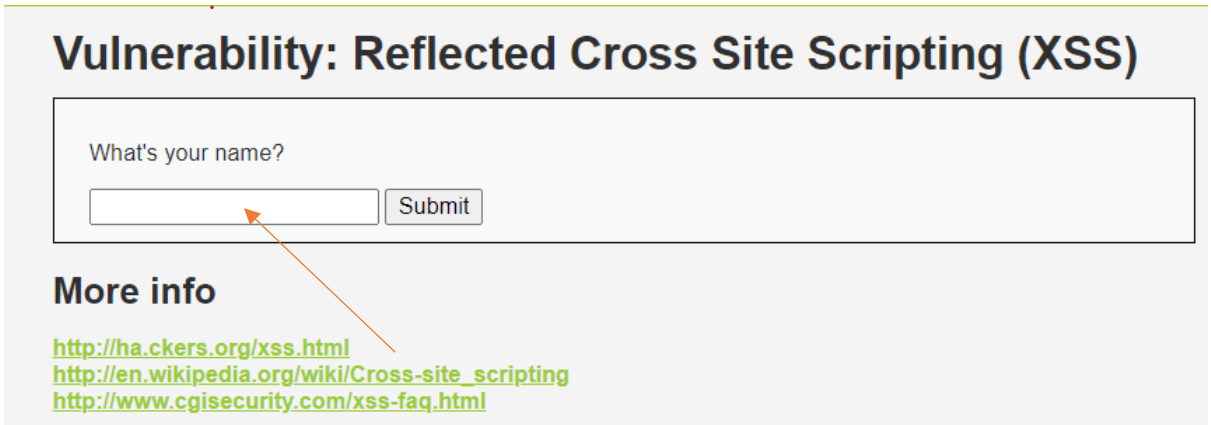
1. first find all the parameter which is vulnerable .
2. Both location have same name parameter vulnerable but at different locations .

- So ,We can put the payload in the URL.

.

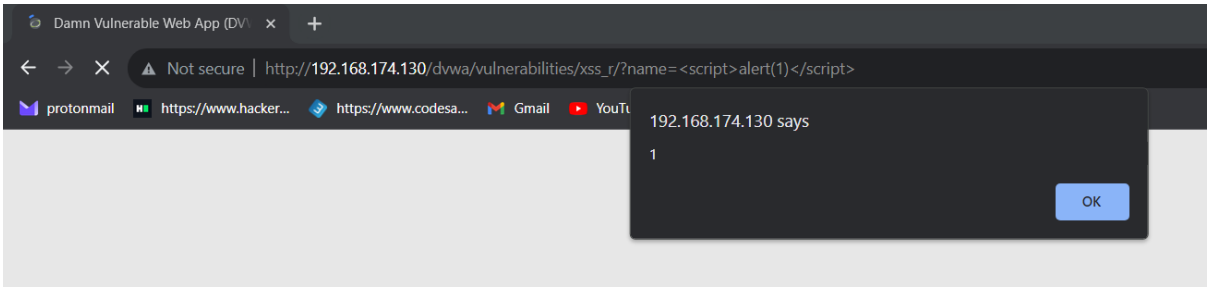


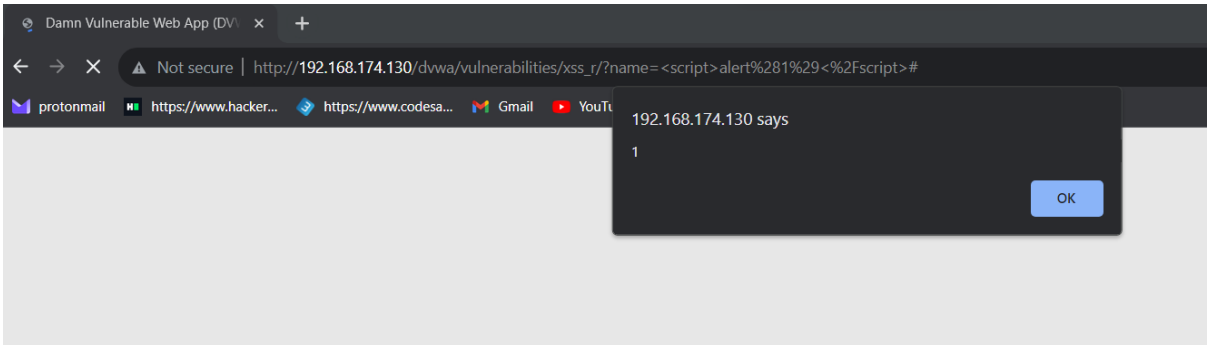
- Also , we found the 2nd parameter as the search box



2. Put the vulnerable payload on both paramters.
3. Payload : <script>alert(1)</script>

Poc:





4. As we can see both Parameter are vulnerable with the XSS Reflected Vulnerability.
5. Also , we see that there is no firewall as well as any particular type of filter to bypass the payload.

Potential Impact: An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by your browser and used with that site. These scripts can even rewrite the content of the HTML page.

- **Session Hijacking:** The attacker could steal user sessions, leading to unauthorized access.
- **Data Theft:** Personal or sensitive information may be exfiltrated.
- **Malicious Actions:** Perform actions on behalf of the user without their consent.

Conclusion: Addressing this Reflected XSS vulnerability is crucial to maintaining the integrity and security of www.dvwa.com. Implementing the recommended measures will significantly reduce the risk of XSS attacks and enhance the overall security posture of the web application.