Indian Institute of Technology Kanpur
Department of Computer Science and Engineering
CS628 Computer System Security - Fall 2023
Instructor - Angshuman Karmakar
Assignment 3 – Exploiting the Web Vulnerabilities (CSRF, XSS, SQLi)

Problem Statement:

You can access a vulnerable server DVWA (Damn Vulnerable web application), in your CS628 lab VM. In this lab exercise, you will learn to exploit vulnerabilities through SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF) attacks. Here are the steps to get started:

SQL Injection:

Accessing DVWA:

- Open your web browser and navigate to the DVWA server (http://localhost) running in your virtual machine (VM).
- Log in with the provided credentials: Username: **admin**, Password: **password**.

Adjusting Security Settings:

- After logging in, you will see a menu on the left. Click on 'DVWA Security.'
- Set the security level to 'medium' and click 'Submit.'

SQL Injection Attack:

- Return to the home page by clicking 'Home.'
- In the navigation menu, select 'SQL Injection.'
- On this page, you will see a section to view the source code (located on the bottom right as 'View Source'). Click on it.
- Study the source code carefully to understand the vulnerability present in it.
- Exploit the vulnerability using a SQL injection attack. Your objective is to retrieve usernames and their corresponding MD5 hash values for passwords.

Deliverables:

- **Detailed Explanation:** Describe the vulnerability you identified in the source code.

Explain how user inputs are handled and why this creates a potential SQL injection vulnerability. Detail the steps you took to exploit the SQL injection vulnerability. This should involve crafting SQL queries to retrieve usernames and their corresponding MD5 hash values for passwords.

- **Results and Data Retrieval:** Present the results of your SQL injection attack. Include the usernames and MD5 hash values you were able to retrieve.
- Share at least three different SQL payloads that achieve the required result.

Cross-Site Scripting (XSS) Attack:

Accessing the XSS Vulnerability:

- Go to the DVWA homepage and log in if you have not already used the provided credentials.

Reflected XSS Attack:

- From the DVWA homepage, select 'XSS reflected' from the navigation menu.
- Click 'View Source' at the page's bottom right. This will allow you to view the source code of the page.
- Study the source code closely to identify the vulnerability present in it. Pay attention to how user inputs are handled.
- you aim to exploit this vulnerability by performing a Reflected XSS attack. Specifically, you want to retrieve the session cookie and display it as a pop-up.

Testing with Different Security Levels:

- Perform the same attack twice:
- Once with the security level set to 'medium,' which makes the vulnerabilities more accessible.
- Once with the security level set to 'high' from the homepage's 'DVWA Security' section. This will challenge your skills further.

Deliverables:

- **Detailed Explanation:** Describe the vulnerability you identified in the source code. Explain how user inputs are handled and why this creates a potential XSS vulnerability. Describe the steps you took to exploit the XSS vulnerability. This should involve crafting an input that triggers the vulnerability and retrieves the session cookie.

- **Testing with Different Security Levels:** Perform the XSS attack twice, as instructed. Document the actions performed results of the first attack when the security level is set to 'medium'. Document the actions performed and results of the second attack when the security level is set to 'high'. Provide an analysis of any differences or challenges encountered between the two attacks due to security settings.
- Share at least three different XSS payloads that achieve the same result (displaying the session cookie as a pop-up) for each security level.

CSRF Attack:

Access DVWA:

- Go to the DVWA homepage and log in if you haven't already used the provided credentials. Set the security level to 'low' and click 'Submit.'

Exploring and Understanding the CSRF Vulnerability:

- From the DVWA homepage, select 'CSRF' from the navigation menu.
- In this section, your goal is to understand how a Cross-Site Request Forgery (CSRF) attack works. A CSRF attack tricks a user into performing actions on a web application without their knowledge or consent.
- The target of this exercise is to execute a CSRF attack to change the password of the currently logged-in user.
- To perform the CSRF attack, you will need to create an HTML page containing a hidden CSRF payload. The payload will initiate the password change when the user unknowingly loads the HTML page.
- Provide a step-by-step explanation of the attack, including the HTML code used to exploit the vulnerability.

Deliverables:

- **Detailed Explanation:** Create an HTML web page, including a hidden CSRF payload. You aim to perform the CSRF attack through the vulnerable html webpage you created. Provide a detailed step-by-step explanation of how you created the HTML page containing a hidden CSRF payload. Discuss any challenges faced due to the 'medium' security setting and how these challenges relate to CSRF protection.
- **HTML Code:** Include the actual HTML code of the page with the CSRF payload.
- **Impact Analysis:** Describe the impact of the CSRF attack, including any actions you could perform using the payload.

Submission Instructions:

You need to submit a total of three files.

1. After successfully performing SQLi, retrieve all the usernames along with passwords' md5 hash value from the SQL injection section and submit as **sqli.txt →file 1**
2. Include the actual HTML code of the page with the CSRF payload and submit as **csrf.html →file 2**
3. Submit A report that contains an explanation and reasons on how you have performed all 3 above mentioned exploitations with all payloads used as **report.pdf →file 3**
4. Make a zip that includes all three files (i.e., -sqli.txt, csrf.html, report.pdf) and go to (http://172.29.233.235/) from your browser inside your lab VM machine and upload the file named **ROLLNUMBER_NAME.zip.**

Grading Schema - Total 50 Marks:

1. Each attack deliverable corresponds to 20 marks.
2. Report with a proper explaination of how you performed the attacks- 30 marks

Instructions to access the Lab VM machine for the assignment:

1. Connect to your IITK Wi-Fi network before you open the URL sent to your mail. (https://172.29.233.235/). (preferably)
2. Open the URL in any browser and log in with your credentials.
3. You will then have access to the UBUNTU 20.04 machine with user cs628. You can access the machine by giving the password as cs628 (cs is small).

Instructions for Report Making: (Use the following template)

1. **Headings - Style** → Ubuntu, **Word Size** → 16
2. **Subheadings - Style** → Ubuntu, **Word Size** →14
3. **Normal Text - Style** → Ubuntu, **Word Size** → 12
4. **Figure Name/Description - Style** → Ubuntu, **Word Size** – 12

Important Note: Justify all the lines in the document. You are expected to write every sentence in your own words. You should not rely on manpages. Your report will be thoroughly checked in Turnitin and other AI tools for plagiarism. If the plagiarism is more than 20%, your submission is not considered for grading, although you have categorized every function correctly.

Caution: Once you have access to the machine, everything will be recorded and logged. You can do whatever is required to solve the assignment, but if you are found doing anything out of scope, there is a reduction in your marks by half. You will only be evaluated with half of the respective assignment marks.

Submission Deadline: 30.10.2023

There will be a 10% penalty for each 24-hour delay in submitting an assignment.