Cabrillo College

Lab 10: Hacking Web Servers

In this lab we will practice using reflected cross-site-scripting, stored cross-site scripting, cross-site forged requests and SQL injection to attack a website.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this lab you have authorization to hack the VMs in the VLab pod assigned to you.

Preparation

- Get the CIS 76 Login Credentials document. You will need usernames and passwords to log into VLab and each of the VMs. This document is on Canvas and the link is in the CIS 76 Welcome letter.
- Determine which VLab pod number you were assigned. See the link on the left panel of the class website.
- If you haven't already configured your pod in the previous labs, then follow the instructions here: https://simms-teach.com/docs/cis76/cis76-podSetup.pdf
- Review Lesson 12 here: https://simms-teach.com/docs/cis76/cis76lesson12.pdf

Part 1 – Reflected Cross-Site Scripting (XSS)

1) See related module in Lesson 12.
2) Insert code into the search field that both changes the text color to purple and displays a customized (with your first name) alert notice.
3) Include the inserted code in your report.

4) Include a screenshot of the alert notice in you report.
5) Include a screenshot of the purple text in your report.

Part 2 – Stored Cross-Site Scripting (XSS)

1) See related module in Lesson 12.
2) Make a message post titled “Malicious Post” that will display a custom Alert notice when read later.
3) Include a snapshot of the code in your report
4) Include a snapshot of the Alert notice in your report.

Part 3 - Cross-Site Request Forgery

1) See related module in Lesson 12.
2) Create new post titled “Trouble” with a malicious HTML <img> tag for a non-existent 1-by-1 pixel image that will instead use a forged URL to request a “funds transfer”.
3) Include a snapshot of the code pasted into the new message
4) Include a snapshot of Burp Suite showing the malicious “funds transfer” URL.

Part 4 - SQL Injection

1) See related module in Lesson 12
2) Create a new account for yourself.
3) Use SQL injection to login to your account without a password.
4) Capture a screenshot for your report.
5) Use SQL injection to list all user accounts and passwords.
6) Capture a screenshot of one of the pages showing all accounts with your account showing.

Submit your work

1) Prepare a report using the word processor and formatting of your choice. All screen shots should be captioned. Your report should contain the following:

    - Course name, lab assignment name, your name, and date.
    - Part 1 Reflected Cross-Site Scripting (XSS).
        - Inserted code
        - Pop-op Alert notice screenshot
        - Purple text color screenshot
    - Part 2 Stored Cross-Site Scripting (XSS).
        - New post showing malicious JavaScript screenshot.
        - Pop-up Alert notice screenshot.

- Part 3 Cross-Site Request Forgery.
  - New post showing malicious <img> tag screenshot.
  - Burp Suite showing forge URL screenshot.
- Part 4 SQL Injection.
  - Screenshot showing just your new account
  - Screenshot showing one page of all accounts including yours.

As an example you can see Benji Simms' report here:
https://simms-teach.com/docs/cis76/cis76-lab10-simben76.pdf

2) Email your report to: **risimms@cabrillo.edu**

Remember **late work is not accepted.** If you run out of time submit what you have completed for partial credit.

Grading Rubric (30 points)

2 points for the Part 1 inserted code
3 points for the Part 1 first screenshot
4 points for the Part 1 second screenshot
3 points for the Part 2 first screenshot
4 points for the Part 2 second screenshot
3 points for the Part 3 first screenshot
4 points for the Part 3 second screenshot
3 points for the Part 4 first screenshot
4 points for the Part 4 second screenshot