Ira A. Fulton Schools of Engineering
Arizona State University

CSE 543: Information Assurance and Security

Pwn them all

Purpose

The purpose of this assignment is to test your understanding of common web vulnerabilities and guide you to exploit common web vulnerabilities in a controlled environment. You will learn how to perform block-box security audits of small websites without having access to its source code, as well as developing exploits to exploit the vulnerabilities that you find during security audits.

Objectives

Students will be able to:

- Read HTML and JavaScript code that is necessary to perform black-box security audit of web applications.
- Perform black-box security audit of small web applications.
- Develop exploits for common web vulnerabilities.
- Test and improve exploits so that they will work against the vulnerable target.

Technology Requirements

All vulnerable websites are hosted at pwnthemall.cse543.rev.fish. You must have Internet access to be able to work on this assignment. You will need a browser (Chrome, FireFox, or Microsoft Edge), an HTTP request sender (curl), and Burp Suite.

Project Directions

For this project, you will "hack" into a series of web applications: Find vulnerabilities in each website, develop exploits for the vulnerabilities that you find, launch your exploits, and then find the entry point to the next level! Your journey starts at http://pwnthemall.cse543.rev.fish:8081/.

All web challenges are under the domain of http://pwnthemall.cse543.rev.fish, from port 8081 (the first level) to port 8090 (the last level). Your goal is to exploit each level, find the secret message (which can be a password, a message, a note, a post, or the bank account login credentials of an important user), and compute the MD5 hash of that secret message to get the name of the HTML page of the next level. You must start from level 1 and exploit these levels one by one.

For each level, you are supposed to write a small paragraph of how you exploit the challenge. You should submit your paragraph at the submission system after finishing each level.

To make your life easier, the instructor will disclose the intended vulnerability of each level. However, remember that there can definitely be unintended vulnerabilities. It is acceptable if you exploit a level by exploiting unintended vulnerabilities!

Evaluation

You will earn 12.5 points for passing each level. There are 8 levels in all. You must solve these levels one-by-one. Partial credit will not be granted for this project.

Submission Directions for Project Deliverables

In the submission space in the course, you will need to submit a report.txt file. This must be in plaintext. Your report.txt file must contain your name, ID number, and a short description of how you broke each level. Your description does not need to be long, but it must be understandable by the instructor.

If you fail to include this information, or if your report.txt is not in the correct format, then you will not receive credit for breaking that level.