F14 18-487 Introduction to Computer Security, Network Security, and Applied Cryptography
Homework #3

David Brumley, Ed Schwartz, Greg Nazario, Jonathan Burket

Due: **2:00 pm on November 24, 2014**

1 Introduction

It's time for your final mission as a special agent from the `18487` hacking group. The villainous Evil Corp has set up an online, members-only shop for the purchasing of all sorts of evil products. After some investigation, you find that it is hosted at `http://debian.ece.cmu.edu:13706/`. Taking down the site would tip off Evil Corp, so your goal is to instead cheat them out of money by purchasing expensive products and not paying the full price. In particular, your mission will be a success if you infiltrate the site and manage to purchase the $99999 *Doom Laser* for only $1.

1.1 Grading

1.1.1 Rules

- You can discuss with others, but you must create *your own* exploits.
- Use Piazza to ask questions.
- **DO NOT** try to obtain root access on the systems, or administrative access to the database.
- **DO NOT** brute-force the systems. No aspect of this assignment involves brute-forcing anything.
- **DO NOT** intentionally delete or overwrite anything. Everything in this assignment involves either reading or appending new data. If you find yourself trying to delete a file or entry from the database, stop.
- **DO NOT** submit any real personal information on the target site, with the exception of your Andrew ID
- Intentionally violating these rules will result in a score of 0 for this assignment.

1.1.2 Criteria

This assignment consists of four separate exploits strung together. For each exploit, your report should contain the following:

- **Reversing (8 pts):** Describe the nature of the vulnerability (be specific).
- **Exploiting (8 pts):** Explain how you exploited the vulnerability. Please include any code or data relevant to your attack. If it took multiple steps to arrive at your final exploit, please explain these steps.
- **Repairing (4 pts):** Briefly explain how the site administrator could repair the vulnerability without compromising intended functionality of the site.

1.1.3 Submission

You need to submit a **writeup** describing the 3 criteria above for every attack you perform. Your writeup must be **UNDERSTANDABLE**! You do not need to use LaTeX, but it must be typed and submitted in PDF format. Multiple submissions are allowed, but only the final submission will be graded.

We will use database and server logs to verify that you completed the entire attack (worth 20 pts). In order to do this you need to use your Andrew ID when you make your final purchase of the *Doom Laser* for only $1. **DO NOT** use the Andrew ID of any other student in the class.

1.1.4 Extra Credit

The first five students to complete the challenge will receive an additional 3 points of extra credit. Note that completing the challenge here means successfully purchasing the *Doom Laser* for $1. You can verify that this has been recorded by visiting:
`http://debian.ece.cmu.edu:13706/scoreboard.php`
You do not need to complete your report early, though this is certainly encouraged as well.

2 Objective

Your goal is to (successfully) purchase the *Doom Laser* from the Evil Corp shop for only $1. In order to achieve this, you will likely need to perform four different attacks, using techniques we discussed in class.

3 Hints

3.1 The Database

- The Evil Corp shop is backed by a MySQL (version 5) database.
- Different SQL commands are executed with different privileges such that queries that are supposed to perform reads cannot perform writes.
- The Evil Corp database uses a table called `order_archive` to store information about older orders.
- Note that you can add an extra column to the results of a SQL query with the following sort of syntax: SELECT *, 5 FROM $things$. In this example, query will return the entire $things$ table, but then also add an additional column of all 5s.

3.2 Purchasing System

- Handling credit card data is a pain, so the Evil Corp shop, like many vile online merchants, refers customers to Villainous Payment Services, a third party payment service similar to PayPal.
- To complete a purchase, order information is sent from Evil Corp to Villainous Payment Services via a user redirect. The customer then pays for the order, and Villainous Payment Services sends back to Evil Corp information about the order, a receipt number, and a status (again via a user redirect). Finally, Evil Corp confirms that the correct amount was paid for the order by talking directly to Villainous Payment Services and asking how much the customer paid for a specific order. If the customer paid the full amount, the items are shipped and the customer is charged.

3.3 Membership Petitions

- Membership petitions can be viewed by Evil Corp employees via a web interface.
- An Evil Corp employee checks the list of membership petitions every few minutes using a browser with no special XSS-blocking features.

3.4 Tools

- You will probably need some way to receive HTTP requests, which means you will either need to setup a simple web server or use a service like `netcat`.
- It may be helpful to familiarize yourself with the developer tools included with many browsers, including Chrome and Firefox. You may also need a tool to view and modify cookies (something like the Chrome extension "Edit this Cookie"). The "Tamper Data" and "Edit Cookies" extensions for Firefox can also be fairly useful.
- Many modern browsers attempt to block code that looks like Cross-Site Scripting. Thus, a simple XSS attack may not work on your browser, but it could work on users using different browsers. It may be useful, therefore, to try to disable such protection for testing purposes, though this should not be necessary. Disabling XSS protection is often accomplished via a flag at the command line when starting the browser.

3.5 Additional Hints

Since this assignment effectively must be completed in a linear fashion and is fairly tricky, you may get stuck. If you are stuck and make no progress for an hour, you may request a hint via a private post on Piazza. We will do our best to respond promptly.