15/18-330: Introduction to Computer Security
Evil Web Exercises

August 11, 2022

1 Introduction

It's time for your final mission as a special agent from the `330` hacking group. The villainous Evil Corp has set up an online, members-only shop for the purchasing of all sorts of evil products. 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 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 server. No aspect of these exercises involves brute-forcing the server in any way, including brute-forcing the entering of passwords. You should only attempt to enter a password that you believe is valid after doing some work to convince yourself the password is valid.
- **DO NOT** intentionally delete or overwrite anything. Everything in these exercises 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.
- **DO NOT** attack the systems in any way that would bring them down. If you're unsure of something, ask us!
- Intentionally violating these rules will result in a score of 0 for the corresponding homework.

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 five different attacks, many of which use techniques discussed in class.

3 Hints

3.1 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.

3.2 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.
- Performing a UNION operation requires that both components being operated on have the same number of columns.
- 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.
- What can you do to get a list of names of all the tables in the database?

3.3 Purchasing System

Handling credit card data is a pain (PCI compliance and all), so the Evil Corp shop, like many vile online merchants, refers customers to EvilPay, a third party payment service similar to PayPal. Pay close attention to how and what information is communicated between different parties.

3.4 Regarding passwords

- As the rules state, do NOT try random combinations of usernames and passwords hoping that one of them will work. Instead, you should gather clues and do some work beforehand to come up with a pair of username and password that you have confidence in.
- Maybe the password you are looking for is actually pretty common and potentially included in a list somewhere...
- Python packages such as `urllib.request` and `hashlib` may be helpful. If you find any libraries or resources online, please be sure to cite it.

3.5 Tools

3.5.1 Analyzing Websites

- It may be helpful to familiarize yourself with the developer tools included with many browsers, including Chrome and Firefox. Make sure to check the source code of pages. (Typically right-click → Inspect Element/View source or F12 on Firefox/Chrome.) The Network tab on these developer's console can also show request information if you find it useful. Other tabs allow you to directly modify cookies.
- Extensions such as Cookie-Editor, EditThisCookie can also be helpful in modifying cookies.
- Extensions to intercept and modify requests may also be very useful. We recommend `https://tamper.dev/` over manually trying to intercept requests, since it gives you more precise control. (If you are trying to execute one of the exploits without this extension, please be patient; some pages may hang for a bit and take a little longer to load. To counter this waiting for a smoother experience, we recommend using campus internet or vpn: `https://vpn.cmu.edu/`, however this is not required.)

3.5.2 Receiving Requests

You will probably need some way to receive HTTP requests, and the best way to do that is to use an existing web service.

We recommend `http://webhook.site`. It will give you a unique URL (something like http://webhook.site/XXXXXX-XXXX-XXXX-XXXXXXXXXXXX) that you can use as an endpoint. That means any requests anybody makes

to http://webhook.site/XXXXXX-XXXX-XXXX-XXXXXXXXXXXX or http://webhook.site/XXXXXX-XXXX-XXXX-XXXXXXXXXXXX/WHATEVER will be recorded.

3.5.3 XSS-Blocking Browsers

Some 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 for users using different browsers. It may be useful, therefore, to try to disable such protection for testing purposes. Disabling XSS protection is often accomplished via a flag at the command line when starting the browser. (Or pick another browser.)
The following browsers were tested for XSS blocking on Windows 10:

- **Chrome:** blocks XSS by default; disable by launching with "–args –disable-xss-auditor" (Remember to remove that when not working on the homework!)
- **Firefox:** by default doesn't seem to block common XSS
- **Edge:** by default doesn't seem to block common XSS

3.6 Additional Hints

Since these tasks effectively must be completed in a linear fashion and they are 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. **Please include as much detail into what you've tried, what you're have trouble with, etc. so we know how best to help you.** We will do our best to respond promptly.