Horribly Insecure Web Application Lab Guide

Objective

In this lab, you will analyze a web application, identify vulnerabilities, and exploit them.

Preparation

Step 1. Start your Labtainers virtual machine.

Step 2. Launch the hiwa labtainer by issuing the command

```
labtainer hiwa
```

Step 3. Open Firefox ESR by clicking on the Applications menu. Then open

```
http://hiwa/login.php
```

Stage 1: Looking Around

In this lab packet, you will simulate participating in a Capture The Flag (CTF). A CTF is a gamified simulation of real-world security scenarios. You are presented with a number of challenges. The goal is to find "flags", which (in this game), are simply text strings. The strings always have the format hiwa{...} (where the ...) change for each challenge.

For each challenge, record a screenshot with the flag in the lab report. When asked, explain how you found the flag.

Challenge 1. Hidden in plain sight.

Most good clues are hidden in plain sight! Take a closer look at the web page and its HTML source.

Challenge 2. Mr. Robot

Search engines crawl whatever web sites they can find. If you don't want to have your websites indexed, you can use a special configuration file posted to your web server to do that.

However, where you don't want me to look, I'll gladly poke around!

Hint: the file is called `robots.txt` and, if it exists, will always be located in the root directory of the web site.

Challenge 3. Read That Fine Manual (RTFM)!

The URL box of the browser is fully under your control! By playing around with the filename (the part after the first `/`), you can sometimes find interesting information. Remove everything after the / in the URL, and then hit ENTER to load the page.

What is the flag that you find in the first file?

Challenge 4. Turn over every stone

Good coding practices can help, but they can also hurt. Look closely, to see what access you might have that wasn't necessarily meant for you.

Hint: Look in a place where programmers often leave hints for themselves. You may have to use “View Source” again!

What is the flag stored in the programming library’s comments?

Challenge 5. One More.

Just in case it isn’t abundantly clear yet. You should look at each and every page you can access. If it is readily available, inspect the rendered page, as well as its HTML source.

Find one more readily available flag.

Stage 2: Active attacks

In the next stage, you’re going to gain access to the application. Return to http://172.16.42.10/login.php

Challenge 6. Jump the turnstile!

To go in through the front door is easy when you have a key. Or when the lock is broken. Can you gain access to the application, even if you don't have a password?

Hint 1: Input validation is often the root of all evil.

Hint 2: SQL injection is sometimes an effective technique to bypass authentication systems. Try a SQLi attack against the password field on the login page!

Challenge 7. Elevate Privileges

As you navigate through the HIWA system, you will notice that several scripts are not accessible to you. Find a way to access the restricted pages.

Hint: Web applications use cookies to maintain sessions, and sessions maintain the state of the applications. Cookies should never contain information that is potentially sensitive, since they can be manipulated by the user. If a web app is written insecurely, you may be able to influence its behavior by messing around with cookies!

Challenge 8. Logo

Change the logo of the HIWA application in such a way that all users of the application see the new version. Simply editing the HTML locally in your browser is NOT sufficient.

Note: there is no specific flag associated with this challenge. Just describe what you did!

Hint: Look closely at the logo itself. Where is it stored? Can you control that location?

Stage 3: Advanced Techniques

Challenge 9: Hidden

What is the flag in the hidden database table?

Hint 1: carefully view the HTML source of the `products.php` page

Hint 2: you’ll need to use a SQLi technique that lets you access tables you normally don’t have access to.

Challenge 10: Secrets...

What is the password of the 'flag' user in the HIWA application?

Hint 1: carefully view the HTML source of the `products.php` page

Hint 2: you’ll need to use a SQLi technique that lets you access fields in tables you normally don’t have access to.

Challenge 11: Enumerate

Enumerate operating system users on the server running the application by exploiting a vulnerability in HIWA. The flag is in the home directory of the user who is labeled as having a flag.

Hint 1: We’re looking for operating system users. They are defined in `/etc/passwd`.

Hint 2: Can you run a shell command that shows you the contents of the password file?