Pwn Them ALL

The server is available at `http://pwnthemall.cse543.rev.fish:8081` to `:8088`.

Remember that the challenges are only accessible to you once you connect to the VPN. Your goal is to exploit each level of them, 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 Mike Pence), and compute the **MD5 hash** of that secret to get name of the HTML page of the next level.

You must start from level 1. For each level, you are supposed to write a small blurb of how you exploit the challenge. You should submit your blurb at http://pwnthemall.cse543.rev.fish:8100 after finishing each level.

Level 01

Simple request-dependent JavaScript. You will want to read the JavaScript, understand its logic, and get the correct username and password from it. This is a good time to start using Burp Suite!

Level 02

XML HTTP request. Read the source code of the webpage and find hidden parameters in HTML comments. One of the parameters is vulnerable to command line injection!

Level 03

Petition messages are all stored with predictable file names. How to predict the file names? You should submit a petition message to find out! The secret to find is what Mike Pence submitted. You will need his email address to access his message.

Level 04

The `filename` parameter allows a directory traversal attack. You can control that parameter to read the content of any files on your file system. All session information is stored in files under `/tmp`. You will want to read out the session of the user `mike_pence` and get his session secret. However, you do not know the name of his session file. Remember that you have a command line injection vulnerability in Level 2? You can use it to list files under `/tmp` and get the file name of the secret session file!

Level 05

This level is a bit tricky. Hidden parameter `admin` will allow you to read any files, which means you can get the source code of the CGI script `retrieve`. Then you will want to go from there. Your cookie takes a special key called `blacklist`. Maybe there is a vulnerability with how the web application deals with that key? Your goal is to read out the source code of the two CGI scripts `retrieve` and `store`. Then you will want to forge your cookie with `site=www.bank.com` and the correct password to retrieve the secret for user `mike_pence`.

Level 06

One field in your HTTP header allows remote PHP file inclusion. Note that the application will automatically add `.php` after the URL that you specify.

Level 07

SQL injection in a PHP application. The injection point is a bit difficult to find. It is during registration when the application checks whether the chosen username exists. The related code (includeing the vulnerable SQL query) looks like the following:

```
/* Checks if a user exists */
$query = "SELECT * FROM users WHERE username='" . $username . "'";
$rs = mysqli_query($db, $query);
if ($rs == false) {
   diefooter("Failed to execute query: " . $query);
}
if (mysqli_num_rows($rs) > 0) {
   print "<p>We found users already registered with this name</p>";
   while ($db_field = mysqli_fetch_assoc($rs) ) {
        print "<p>Username: " . $db_field['username'] . "</p>";
        print "<p>First: " . $db_field['firstname'] . "</p>";
        print "<p>Last: " . $db_field['lastname'] . "</p>";
   }
   diefooter("<p>A user with the specified name already exists.</p>");
}
```

You will need blind SQL injection to get the password for user `mike_pence`.

Level 08

This is the last level! No hints are given. Well, here is a small one: You will want to watch Burp Suite traffic really really carefully.

Good luck!