

Introduction to Web Applications:

Link to challenge: <https://academy.hackthebox.com/module/75>

(log in required)

Class: Tier 0 | Fundamental | General

Front End Components

HTML:

Question: What is the HTML tag used to show an image?

Answer:

Method:

Cascading Style Sheets (CSS):

Question: What is the CSS "property: value" used to make an HTML element's text aligned to the left?

Answer: text-align: left;

Method:

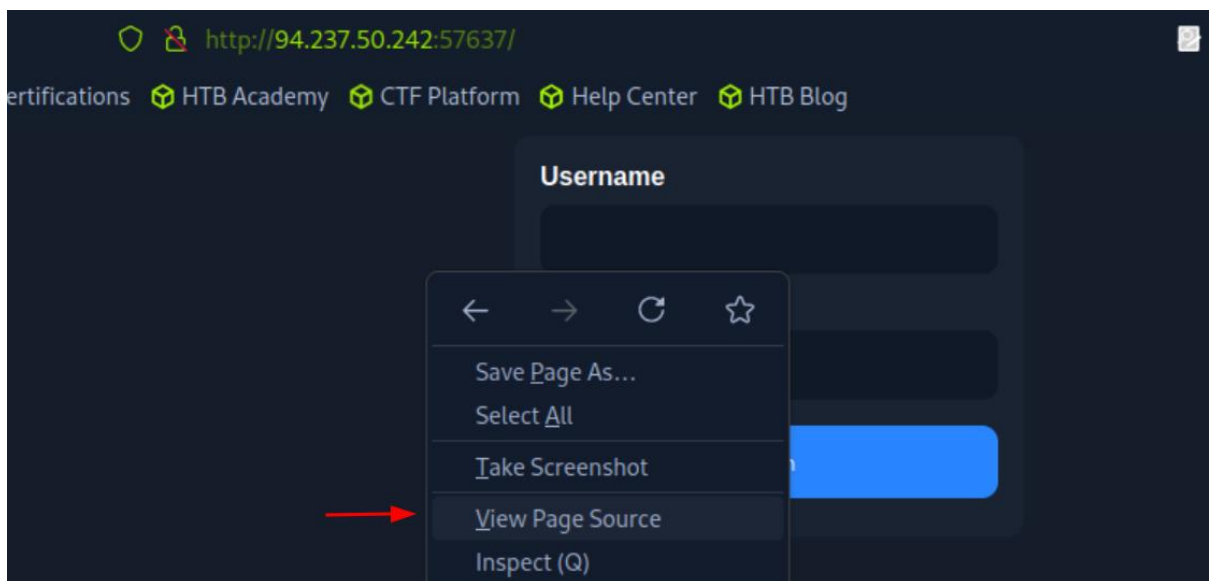
Front End Vulnerabilities

Sensitive Data Exposure:

Question: Check the above login form for exposed passwords. Submit the password as the answer.

Answer: HiddenInPlainSight

Method: in the website page we will right click it to view page source:



In the source code:

```
45     .container {
46         padding: 16px;
47     }
48 </style>
49 <form action="#" method="post">
50
51     <div class="container">
52         <label for="uname"><b>Username</b></label>
53         <input type="text" required>
54
55         <label for="psw"><b>Password</b></label>
56         <input type="password" required>
57
58         <!-- TODO: remove test credentials admin:HiddenInPlainSight -->
59
60         <button type="submit">Login</button>
61     </div>
62 </form>
```

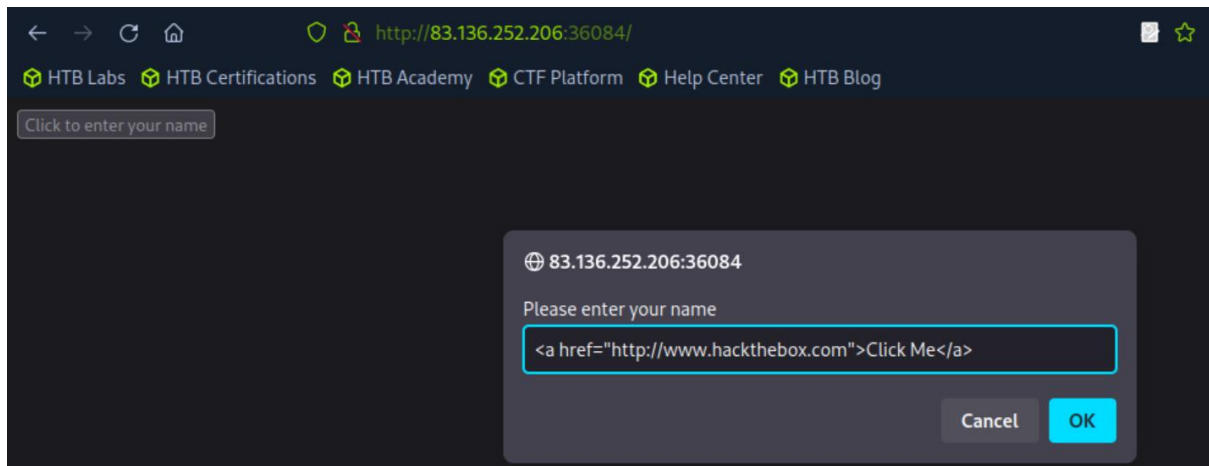
Another page will be opened, containing the password.

HTML Injection:

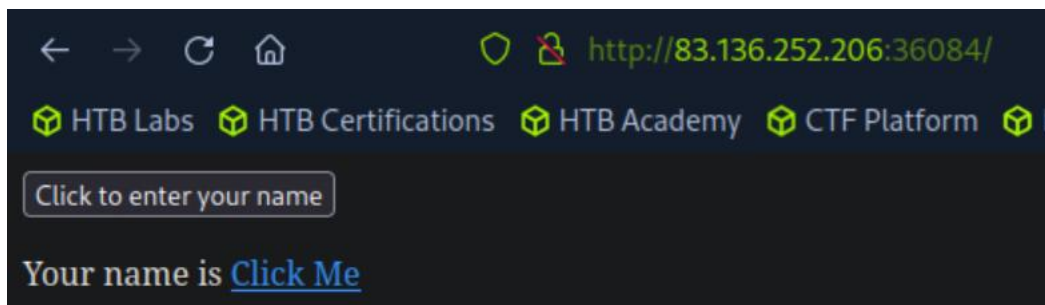
Question: What text would be displayed on the page if we use the following payload as our input: `Click Me`

Answer: Your name is Click Me

Method: Upon entry we are requested to enter our name, we will enter the payload:



→ the output is:



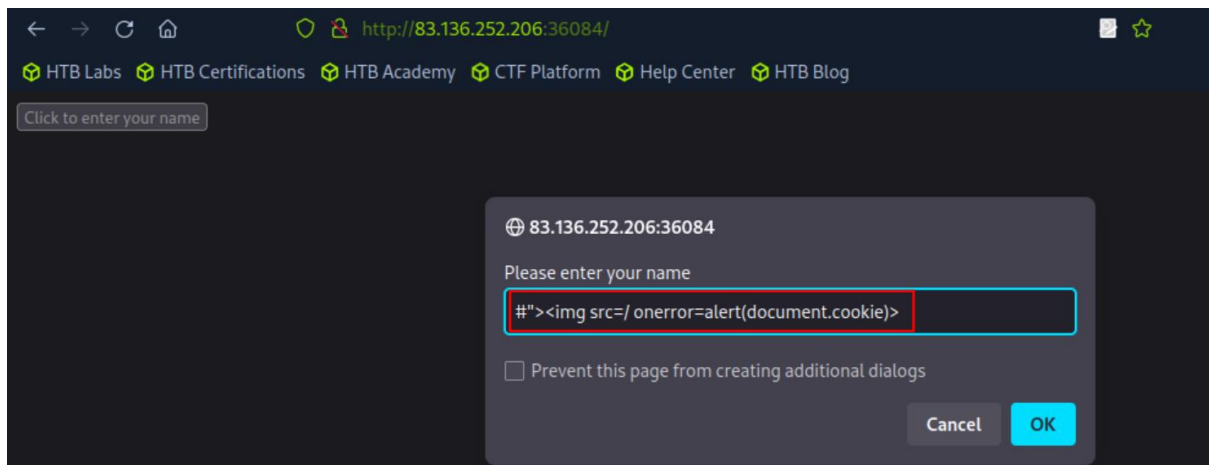
Cross-Site Scripting (XSS):

Question: Try to use XSS to get the cookie value in the above page

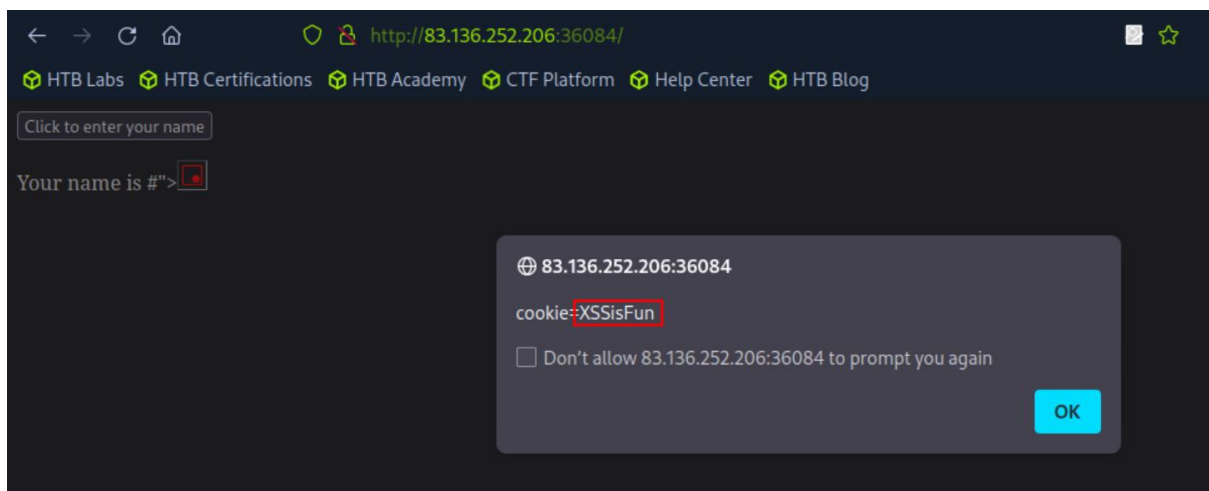
Answer: XSSisFun

Method: on the same website from the previous question – we will enter the payload:

```
#"><img src=/ onerror=alert(document.cookie)>
```



And upon entering:



Back End Components

Back End Servers:

Question: What operating system is 'WAMP' used with?

Answer: Windows

Method:

Combinations	Components
LAMP	Linux, Apache, MySQL, and PHP.
WAMP	Windows, Apache, MySQL, and PHP.
WINS	Windows, IIS, .NET, and SQL Server
MAMP	macOS, Apache, MySQL, and PHP.
XAMPP	Cross-Platform, Apache, MySQL, and PHP/PERL.

Web Servers:

Question: If a web server returns an HTTP code 201, what does it stand for?

Answer: Created

Method:

What does HTTP 201 mean?



201 Created

The HTTP 201 Created successful response status code indicates that **the HTTP request has led to the creation of a resource**. This status code is commonly sent as the result of a POST request. 6 Aug 2024

Databases:

Question: What type of database is Google's Firebase Database?

Answer: NoSQL

Method:

Is cloud firestore a relational database?

Cloud Firestore is a NoSQL, document-oriented database. Unlike a SQL database, there are no tables or rows. Instead, you store data in documents, which are organized into collections.

Development Frameworks & APIs:

Question: Use GET request '/index.php?id=0' to search for the name of the user with id number 1?

Answer: superadmin

Method: we sent the request to the API endpoint using the curl command:

```
curl http://<target-IP>:<target-port>/index.php?id=1
```

```
[eu-academy-2]-[10.10.15.30]-[htb-ac-1099135@htb-ilv3bm4owv]-[~]  
[*]$ curl http://83.136.252.160:42997/index.php?id=1  
superadmin [eu-academy-2]-[10.10.15.30]-[htb-ac-1099135@htb-ilv3bm4owv]-[~]
```

Back End Vulnerabilities

Common Web Vulnerabilities:

Question: To which of the above categories does public vulnerability 'CVE-2014-6271' belongs to?

Answer: Command Injection

Method: according to [this website](#) – 'A flaw was found in the way Bash (aka bourne-again shell) evaluated certain specially crafted environment variables. An attacker could use this flaw to override or bypass environment restrictions to execute shell commands.'

Public Vulnerabilities:

Question: What is the CVSS score of the public vulnerability CVE-2017-0144?

Answer: 9.3

Method: looking in this [CVE details page](#):

Metrics


CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 2.0 Severity and Vector Strings:

 **NIST:** NVD

Base Score: **9.3 HIGH**

Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C)

*make sure the option CVSS 2.0 selected, as instructed by the hint. *