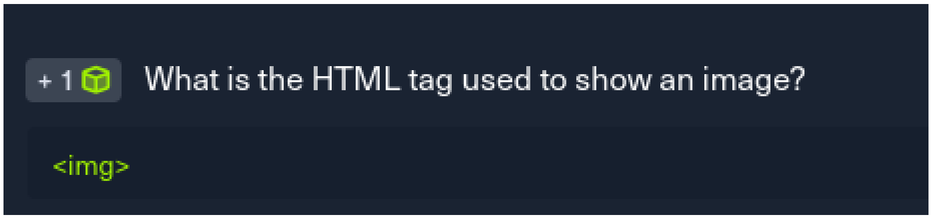
INTRODUCTION TO WEB APPLICATION

Introduction

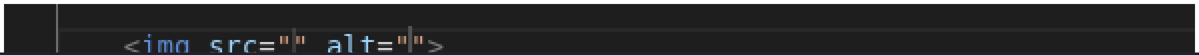
Web application are interactive applications that run on web browser. From this class the difference between websites and web applications came out clear; websites have static contents while web applications present dynamic contents as per users interaction.
Also, I came to learn the difference between web application and a native operating system. Basically web application are platform-independent and can run in a browser on any operating system instead native operating systems application have a high operation speed and the ability to utilize native operating system libraries and local hardware.

Q & A

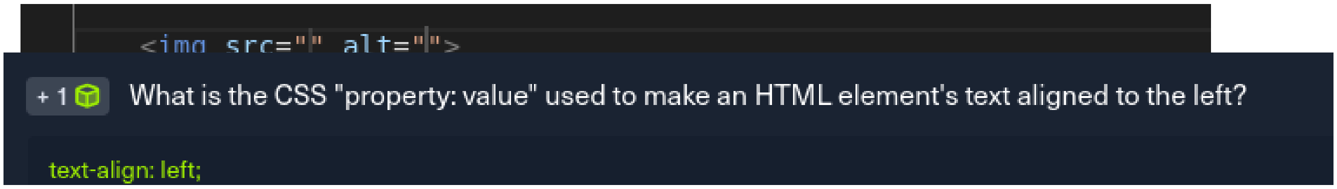


What is the HTML tag used to show an image?

`<img>`



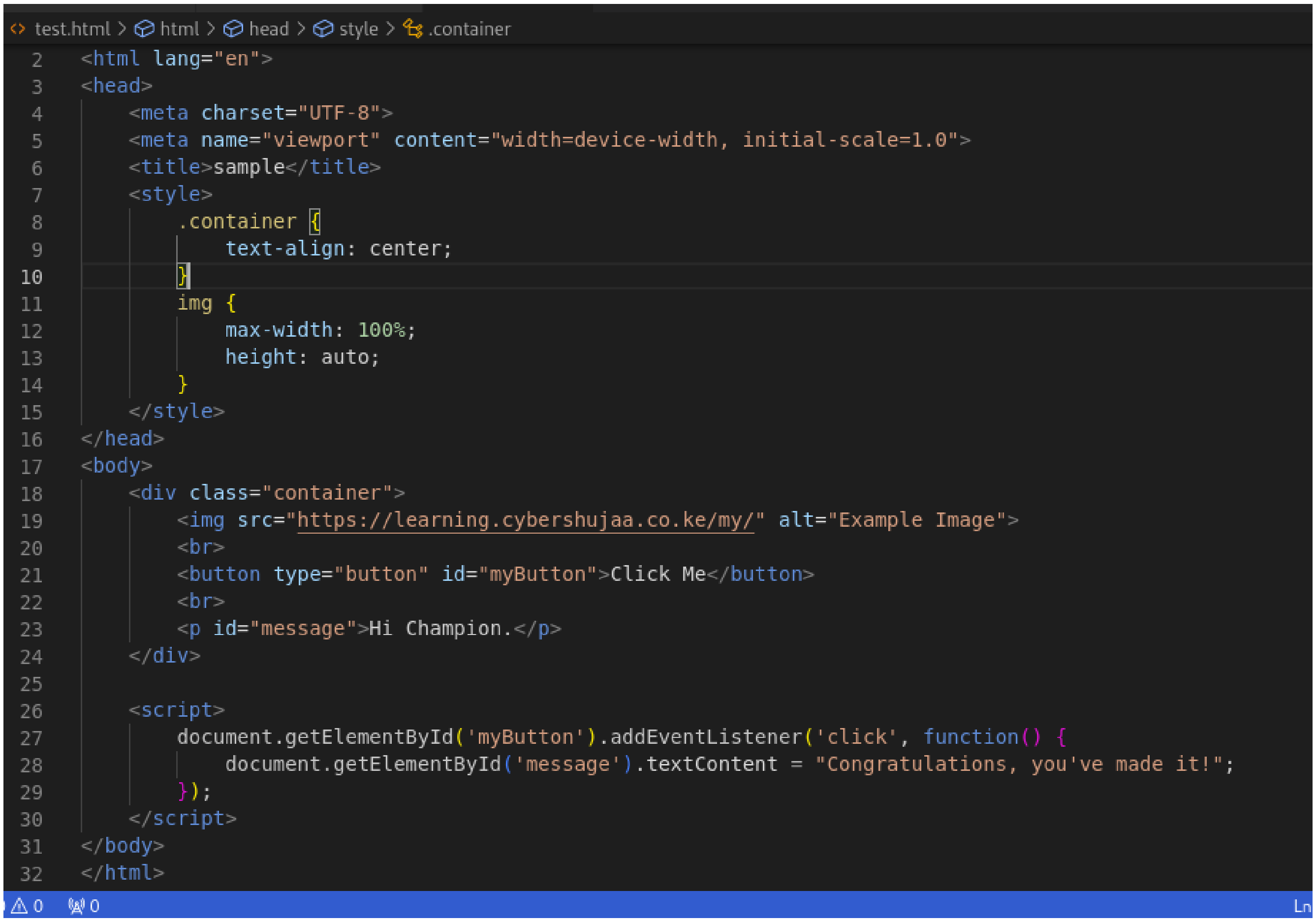
```
<img src="" alt="">
```



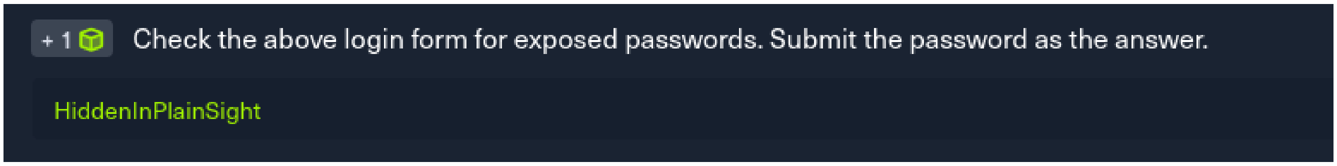
What is the CSS "property: value" used to make an HTML element's text aligned to the left?

`text-align: left;`

so here is a sample code I wrote to test the grasp of my concept inline with the above concept.



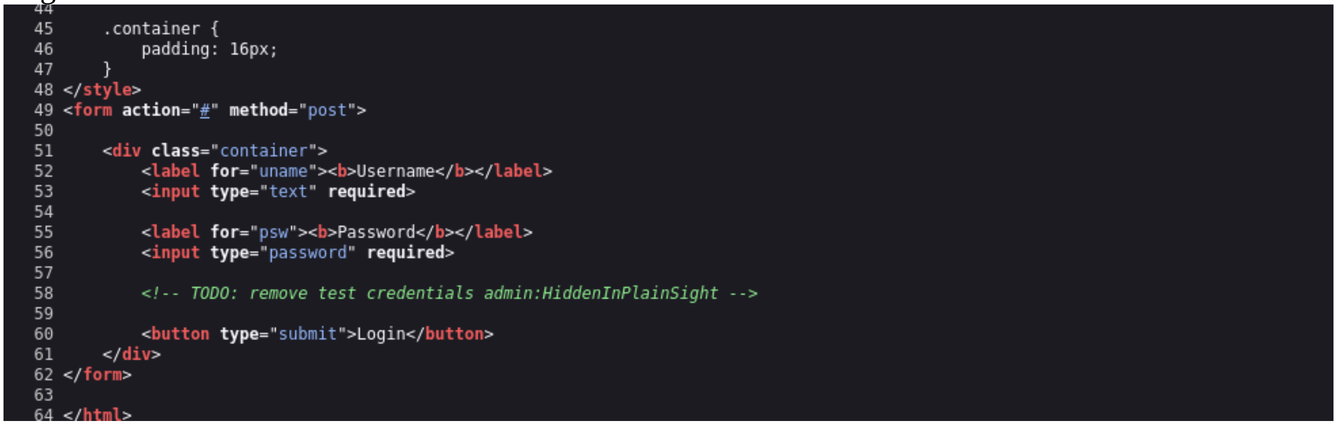
```html
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>sample</title>
    <style>
        .container {
            text-align: center;
        }
        img {
            max-width: 100%;
            height: auto;
        }
    </style>
</head>
<body>
    <div class="container">
        <img src="https://learning.cybershujaa.co.ke/my/" alt="Example Image">
        <br>
        <button type="button" id="myButton">Click Me</button>
        <br>
        <p id="message">Hi Champion.</p>
    </div>

    <script>
        document.getElementById('myButton').addEventListener('click', function() {
            document.getElementById('message').textContent = "Congratulations, you've made it!";
        });
    </script>
</body>
</html>
```



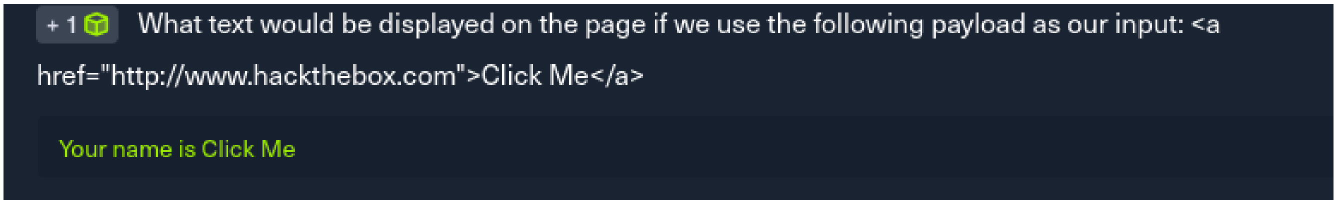
Check the above login form for exposed passwords. Submit the password as the answer.

HiddenInPlainSight

To tackle this question, I viewed the frontend source code by using the “ctrl + u” command just as shown below and extracted the login information from the comment section that seems a developer forgot to delete.



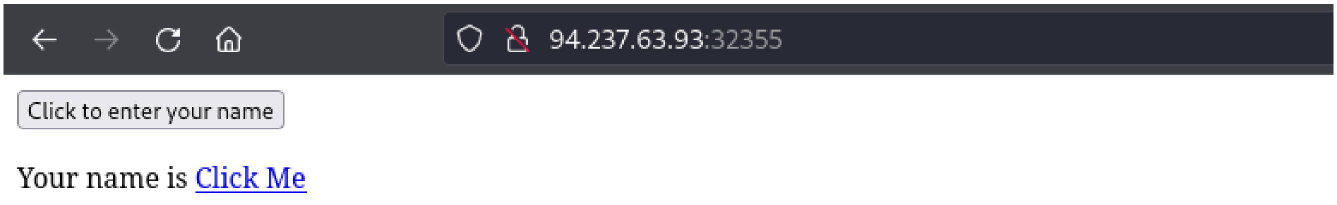
```html
    .container {
        padding: 16px;
    }
</style>
<form action="#" method="post">

    <div class="container">
        <label for="uname"><b>Username</b></label>
        <input type="text" required>

        <label for="psw"><b>Password</b></label>
        <input type="password" required>

        <!-- TODO: remove test credentials admin:HiddenInPlainSight -->

        <button type="submit">Login</button>
    </div>
</form>

</html>
```



What text would be displayed on the page if we use the following payload as our input: <a href="http://www.hackthebox.com">Click Me</a>

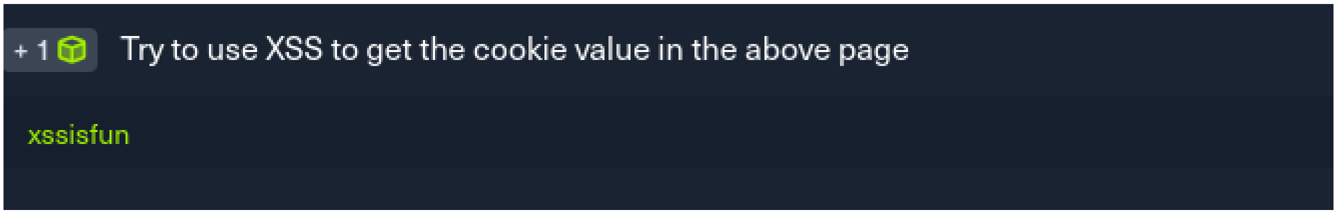
Your name is Click Me

here I was testing if the website was vulnerable to html injection, and from the result below, indeed it is.



94.237.63.93:32355

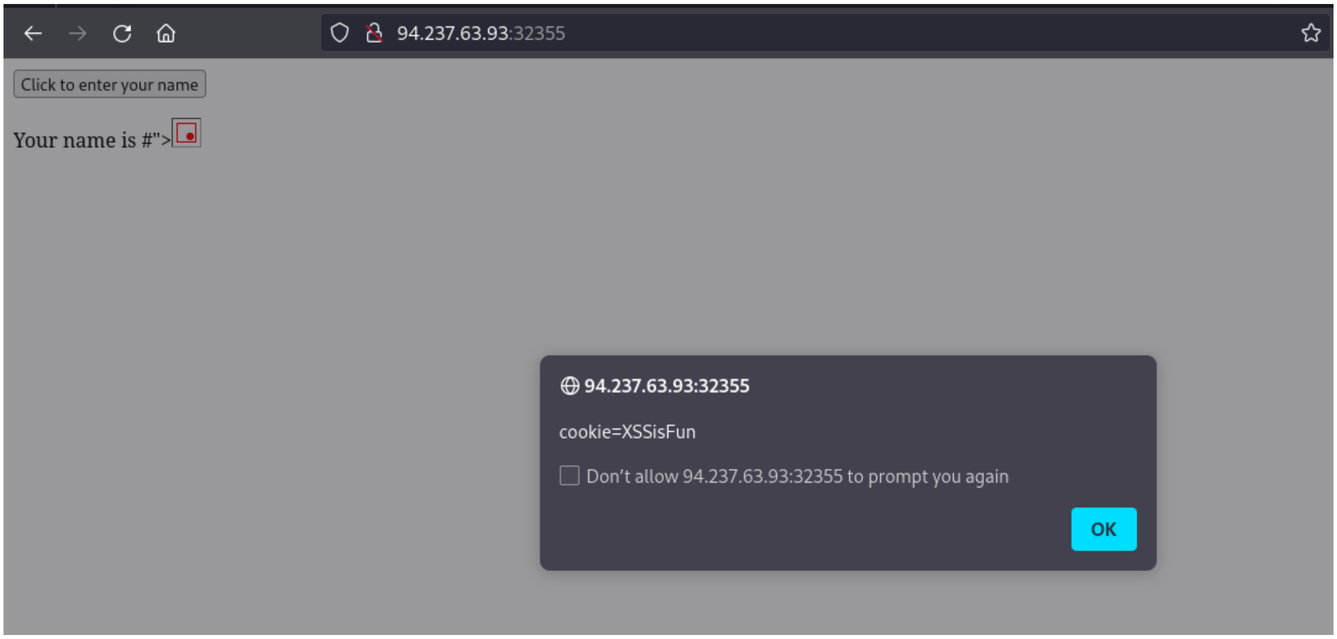
Your name is Click Me



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

xssisfun

Here I was testing if the site was vulnerable to xxs(cross-site scripting) and indeed it was. Besides, in most cases I noticed that webapp that is vulnerable to html injection most likely might also be vulnerable to xss and by this I as an attacker I can leverage my attack surface.



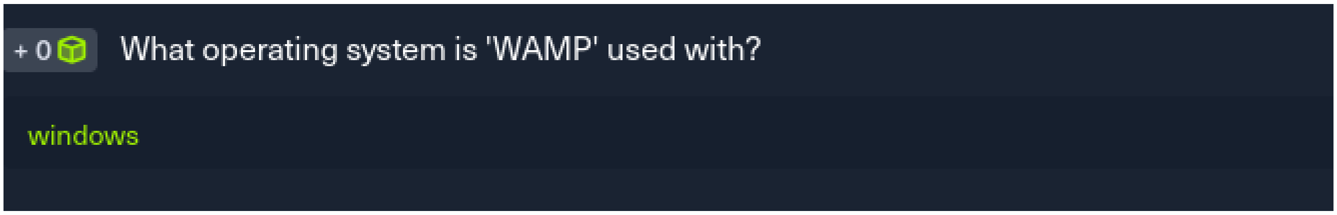
94.237.63.93:32355

Your name is #">

94.237.63.93:32355

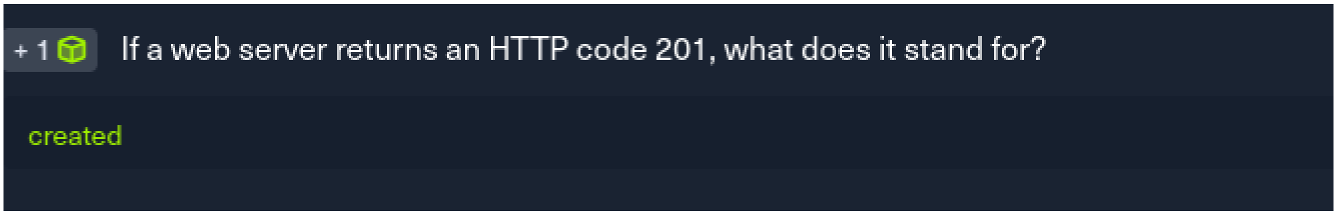
cookie=XSSisFun

□ Don't allow 94.237.63.93:32355 to prompt you again



+ 0 What operating system is 'WAMP' used with?

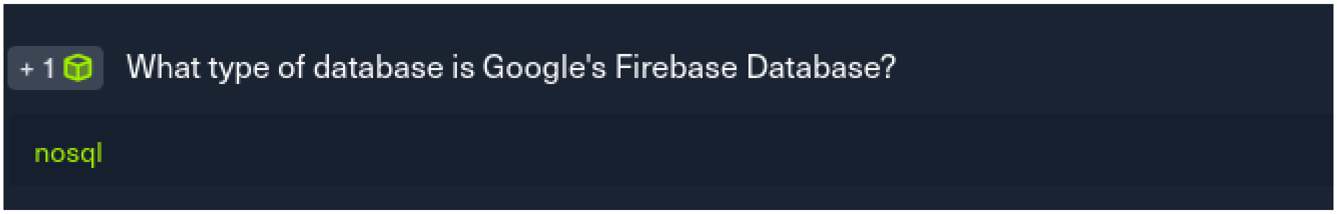
windows



+ 1 If a web server returns an HTTP code 201, what does it stand for?

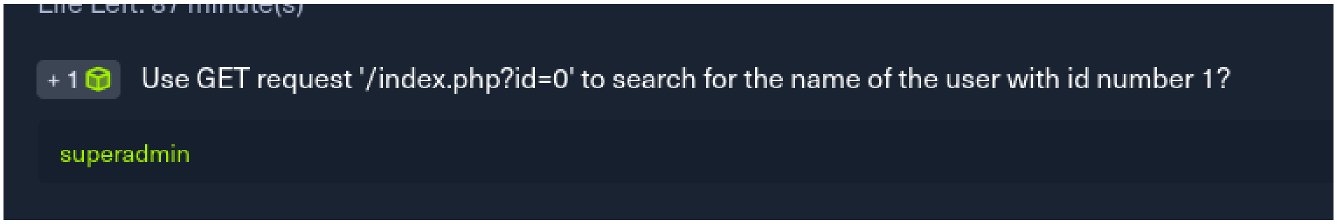
created

Besides, I learnt status code:
1xx = continue
2xx = SUCCESS, I.e OK,created,No content
3xx = redirection I.e moved permanently, FOUND
4xx = client error I.e bad request, unauthorized, not found.
5xx = server error I.e internal server error



+ 1 What type of database is Google's Firebase Database?

nosql

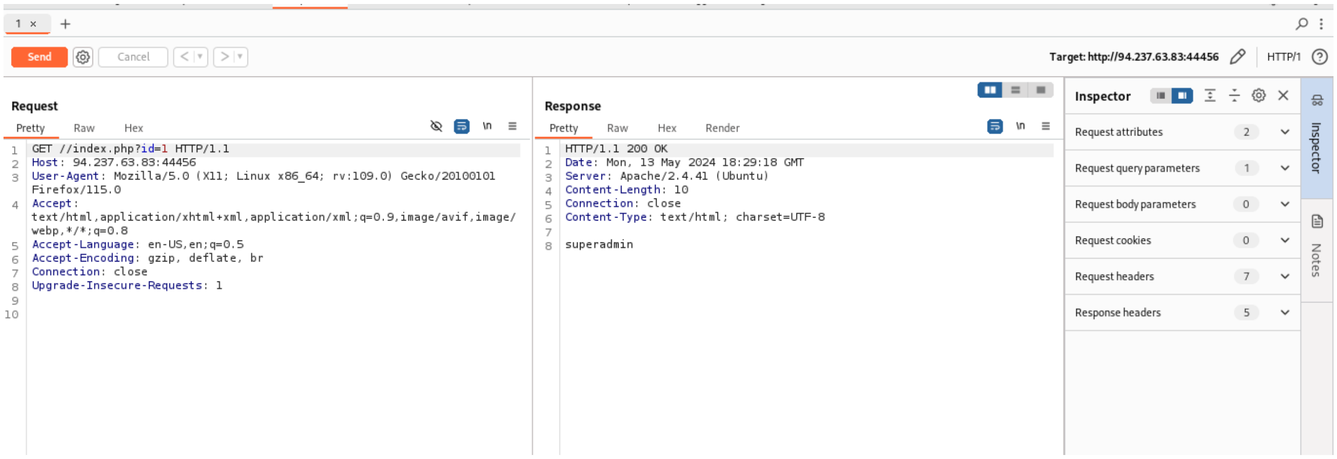


Life Left: 87 minute(s)

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

superadmin

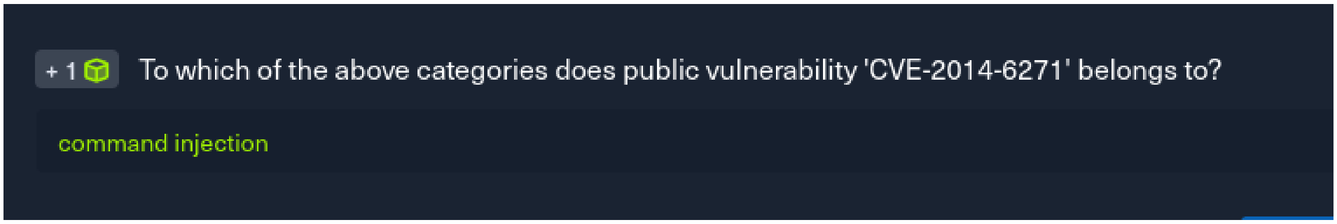
in this case I used the burpsuite tool to intercept request and did some little modifications before forwarding the request to its final destination just as shown in the image below.



```
GET //index.php?id=1 HTTP/1.1
Host: 94.237.63.83:44456
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

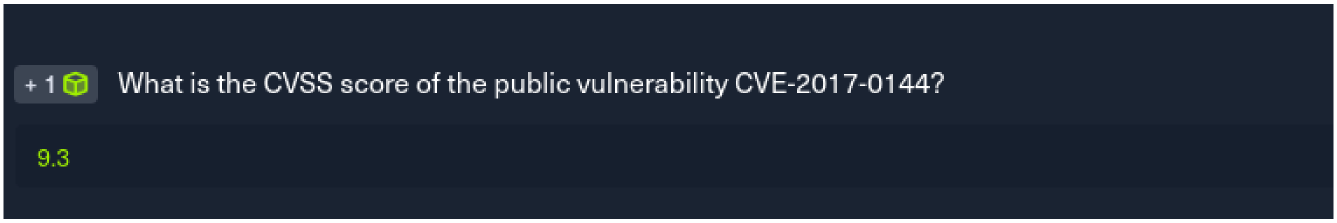
```
HTTP/1.1 200 OK
Date: Mon, 13 May 2024 18:29:18 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 10
Connection: close
Content-Type: text/html; charset=UTF-8

superadmin
```

Request attributes	2
Request query parameters	1
Request body parameters	0
Request cookies	0
Request headers	7
Response headers	5



+ 1 To which of the above categories does public vulnerability 'CVE-2014-6271' belongs to?

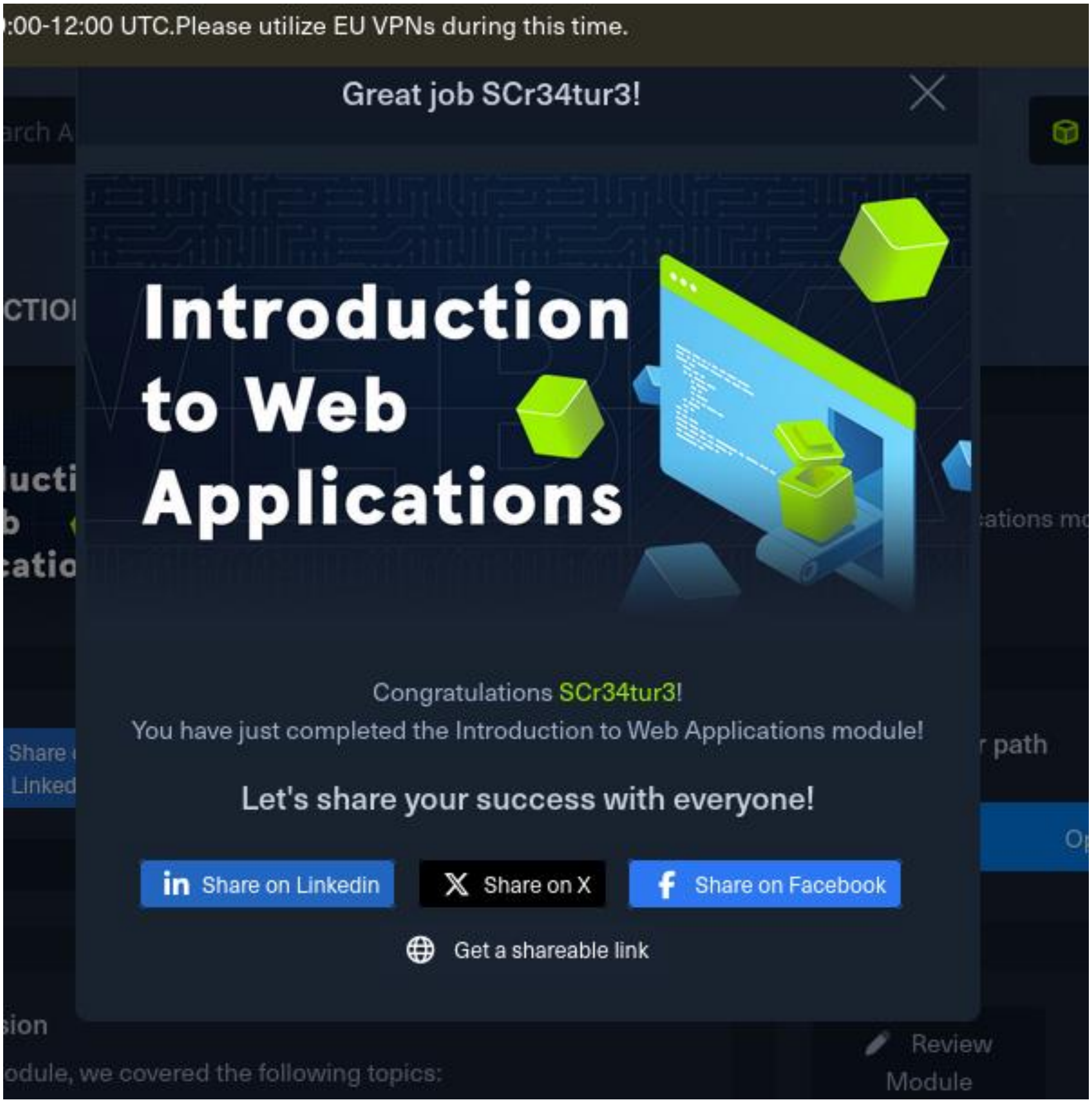
command injection



+ 1 What is the CVSS score of the public vulnerability CVE-2017-0144?

9.3

And this



:00-12:00 UTC.Please utilize EU VPNs during this time.

Great job SCr34tur3!

Introduction to Web Applications

Congratulations SCr34tur3!
You have just completed the Introduction to Web Applications module!

Let's share your success with everyone!

marked the end of my journey under introduction.

CONCLUSION

In conclusion, grasping and understanding how web applications works from its functionalities to the technologies used I very vital for security personel who engage in pentesting or rather the general security of this applications.
I have learnt a lot and I just need to stay updated with the current web vulnerabilities and how they can be prevented.

https://academy.hackthebox.com/achievement/1287818/75 to web.