30: Assisted Lab: Performing and Detecting XSS
CySA+ (Exam CS0-003)

11/11

Congratulations, you passed!

Duration: 45 minutes, 54 seconds

☑ The result of injecting an `alert` command through `script` tags proves what?   *Score: 1*

- ○ This site is secure.
- ○ This site allows for account takeover.
- ○ This site is vulnerable to privilege escalation.
- ◉ <u>This site is vulnerable to XSS.</u>

Congratulations, you have answered the question correctly.

☑ What does the %2F value replace near the end of the URL of the current page?   *Score: 1*

- ◉ <u>/</u>
- ○ \
- ○ <
- ○ >

Congratulations, you have answered the question correctly.

☑ **Use a script to confirm local web server is started**   *Score: 1*
Select the **Score** button to validate this task.
`Local web server detected ...`
`Task complete`

☑
- ○ A
- ◉ <u>B</u>
- ○ C
- ○ D

Score: 1

Congratulations, you have answered the question correctly.

☑ What was the HTTP response code for this log record?   *Score: 1*

- ○ 100
- ◉ <u>200</u>

○ 300
○ 400
○ 500

Congratulations, you have answered the question correctly.

☑ What is the HTTP referrer for the attack performed after the "testuser2" submission that obtained the user's session ID?   *Score: 1*

○ "dvwa.structurealty.com/vulnerabilities/xss_r/?
name=%3cscript%3ealert%28%22You+have+been+hacked%21+Again%21%22%29%3c%2fscript%3e
HTTP/1.1"
◉ "dvwa.structurealty.com/vulnerabilities/xss_r/"
○ "dvwa.structurealty.com/vulnerabilities/xss_r/?name=testuser"
○ "dvwa.structurealty.com/vulnerabilities/xss_r/?
name=%3cscript%3ealert%28document.cookie%29%3c%2fscript%3e"

Congratulations, you have answered the question correctly.

☑ What is the most common IoC to look for when searching for evidence of a XSS attack?   *Score: 1*

◉ The HTML script tag
○ The use of percent encoding
○ The presence of hex encoding
○ The existence of referrers
○ The occurrence of HTTP requests

Congratulations, you have answered the question correctly.

☑ Reflective cross-site scripting (XSS) attacks are often performed by tricking a victim into clicking on a malicious link that was crafted to include the attack script.   *Score: 1*

◉ True
○ False

Congratulations, you have answered the question correctly.

☑ Which of the following percent encoding values are commonly found in web log files related to XSS attacks?   *Score: 1*

☑ %3C
☑ %3E
☐ %99
☑ %3D
☐ %8C

Congratulations, you have answered the question correctly.

☑ How many fields are found by default in the Combined Log Format used by Apache2?   *Score: 1*

- ○ 13
- ○ 7
- ○ 17
- ◉ <u>9</u>

Congratulations, you have answered the question correctly.

☑ The HTTP response code of 200 is an indication of what   Score: 1

- ○ Informational response
- ◉ <u>Successful response</u>
- ○ Redirection message
- ○ Client error response
- ○ Server error response

Congratulations, you have answered the question correctly.