33: Assisted Lab: Performing and Detecting CSRF

CySA+ (Exam CS0-003)

Congratulations, you passed!

Duration: 28 minutes, 31 seconds

☑ What would make the password change page more secure? (Select two) *Score: 1*

- ☑ Use HTTPS
- ☐ Ask to define security questions
- ☑ Require the current password to be provided
- ☐ Send a link to the password page via email
- ☐ Have a timer on the password change page

Congratulations, you have answered the question correctly.

☑ What other means is there to test if a password change was effective? *Score: 1*

- ○ Sending a URL via email
- ○ Sending a code via text message
- ◉ The primary login page
- ○ Calling the user on the phone

Congratulations, you have answered the question correctly.

☑ The core of this CSRF attack is tricking a victim into clicking on a link that will run commands against their account on a website where they have a pre-established session. (True/False) *Score: 1*

- ◉ True
- ○ False

Congratulations, you have answered the question correctly.

☑ This is evidence of a malicious event. *Score: 1*

- ○ True.
- ◉ False

Congratulations, you have answered the question correctly.

☑ Is this an IoC of CSRF without context? *Score: 1*

- ○ Yes
- ◉ No

Congratulations, you have answered the question correctly.

☑ What is the attack of CSRF dependant on? *Score: 1*

- ◉ A website trusting the requests of a visitor
- ○ A victim typing in malicious commands
- ○ A social engineering phone call to a victim
- ○ Malware pre-installed on a web server

Congratulations, you have answered the question correctly.

☑ What is the main vulnerability of the website in this lab that allowed for the CSRF attack? *Score: 1*

- ○ Passwords being hased
- ◉ Password changes via GET URL
- ○ Password changes in POST payloads
- ○ The use of HTTPS URLs

Congratulations, you have answered the question correctly.

☑ Based on the website from this lab, what is the final log record in the pattern that reveals a successful login took place? (Select one HTTP request and one HTTP referrer) *Score: 1*

- ☐ Req: GET /login.php HTTP/1.1
- ☐ Req: POST /login.php HTTP/1.1
- ☑ Req: GET /index.php HTTP/1.1
- ☑ Ref: http://dvwa.structureality.com/login.php
- ☐ Ref: http://dvwa.structureality.com/index.php
- ☐ Ref: http://dvwa.structureality.com/test_credentials.php

Congratulations, you have answered the question correctly.

☑ What mitigations should be implemented to address the CSRF risk of the website in this lab? (Select two) *Score: 1*

- ☑ Use HTTPS
- ☐ Use percent-encoding in the GET URL when changing passwords
- ☐ Hash passwords from the browser
- ☑ Transmit password changes in POST payloads
- ☐ Filter metacharacters

Congratulations, you have answered the question correctly.

☑ What is the direct evidence or IoC for CSRF? *Score: 1*

- ○ Password change occurred
- ○ Passwords sent via GET URL
- ○ Email received by victim
- ○ Login failures
- ◉ None of the above.

Congratulations, you have answered the question correctly.