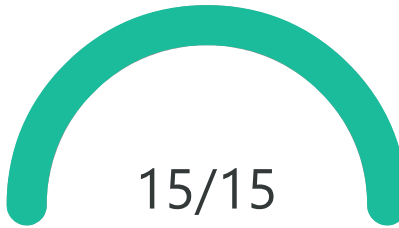


31: Assisted Lab: Performing and Detecting LFI/RFI

CySA+ (Exam CS0-003)



Congratulations, you passed!

Duration: 1 hour, 2 minutes

✓ What does the "R" parameter do in the ls command?

Score: 1

- ☐ Reveals hidden files
- ☒ Performs recursive display
- ☐ Returns only readable files
- ☐ Reveals only files associated with the current user

Congratulations, you have answered the question correctly.

✓ What is the hidden quote that you can now see through the Command Injection exploit?

Score: 1

- ☐ There is no do, there is only try.
- ☐ Bond, James Bond.
- ☒ Romeo, Romeo! Wherefore art thou Romeo?
- ☐ My name is Sherlock Holmes. It is my business to know what other people don't know.

Congratulations, you have answered the question correctly.

✓ What two files are in the ../hackable/uploads directory? (Select two)

Score: 1

- ☐ fi.php
- ☒ dvwa_email.png
- ☒ fi.txt
- ☐ admin.jpg

Congratulations, you have answered the question correctly.

✓ What are the explanations for why some parts of the fi.php file were not visible before extracting the fi.txt copy?

Score: 1

- ☒ PHP is executed on the server, not shown to the browser from .php files.
- ☐ HTML is rendered on the server before being sent to the client.
- ☐ Javascript is being used to hide elements of the PHP file.
- ☒ HTML comments are hidden by the browser from text files.

Congratulations, you have answered the question correctly.

☒ What is the point of the string "../..../.." in the previous exploit of file inclusion? Score: 1

- ☒ Use directory traversal to reach the root directory
- ☐ Use command obfuscation to avoid keyword filters
- ☐ Use special characters to avoid metacharacter escaping
- ☐ Trick the system into granting access to the file using root privileges

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

☒ There should be three files pulled as inclusion pages in the access.log which were coded as part of the website with direct hyperlinks. What are those page names? (Select three) Score: 1

- ☒ file1.php
- ☒ file2.php
- ☒ file3.php
- ☐ file4.php

Congratulations, you have answered the question correctly.

☒ Based on this HTTP request, what do you think was taking place with all of the prior references to /vulnerabilities/exec/? Score: 1

- ☒ Directory and folder discovery
- ☐ Network probing
- ☐ Privilege escalation
- ☐ SQLi

Congratulations, you have answered the question correctly.

☒ What is the user agent for this record? Score: 1

- ☐ Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
- ☐ Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36 Edg/110.0.1587.50
- ☒ Wget/1.21.3
- ☐ Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36

Congratulations, you have answered the question correctly.

☒ Which of the following is the clearest evidence of an RFI exploit? (assume these are the final parts of a log record's HTTP request) Score: 1

- ☐ ...?page=../../../../../../../../etc/shadow
- ☒ ...?page=http://10.1.16.66:9999/

- ☐ ...?page=rm+-r+/
- ☐ ...?page=../../hackable/flags/dvwa_email.png

Congratulations, you have answered the question correctly.

✓ Which of the following is true regarding file inclusion exploitation? *Score: 1*
(Select all that apply)

- ☒ It can reference local files.
- ☒ It can execute referenced files.
- ☒ It can reference remote files.
- ☐ It must be used in concert with command injection.

Congratulations, you have answered the question correctly.

✓ What is a means by which an LFI attack can access hidden files? *Score: 1*

- ☒ Command injection displaying directory contents
- ☒ Filename prediction based on naming conventions
- ☒ Filename guessing
- ☐ Reviewing web server documentation

Congratulations, you have answered the question correctly.

✓ How can an attacker determine that a website is vulnerable to LFI attacks? *Score: 1*

- ☐ Determine the web server version
- ☐ Figure out the server-side script languages
- ☒ Find URLs disclosing page inclusion
- ☐ Look at the security.txt file

Congratulations, you have answered the question correctly.

✓ What is the IoC observable that indicates an RFI exploit? *Score: 1*

- ☐ A system file object as the page reference.
- ☐ A data base reference object as the page reference.
- ☐ A listing port object as the page reference.
- ☒ A URL object as the page reference.

Congratulations, you have answered the question correctly.

✓ When using either LFI or RFI abuse, an attacker can directly combine what other exploitations? *Score: 1*

- ☒ Command injection
- ☒ Directory traversal
- ☐ SQLi
- ☒ XSS

Congratulations, you have answered the question correctly.

