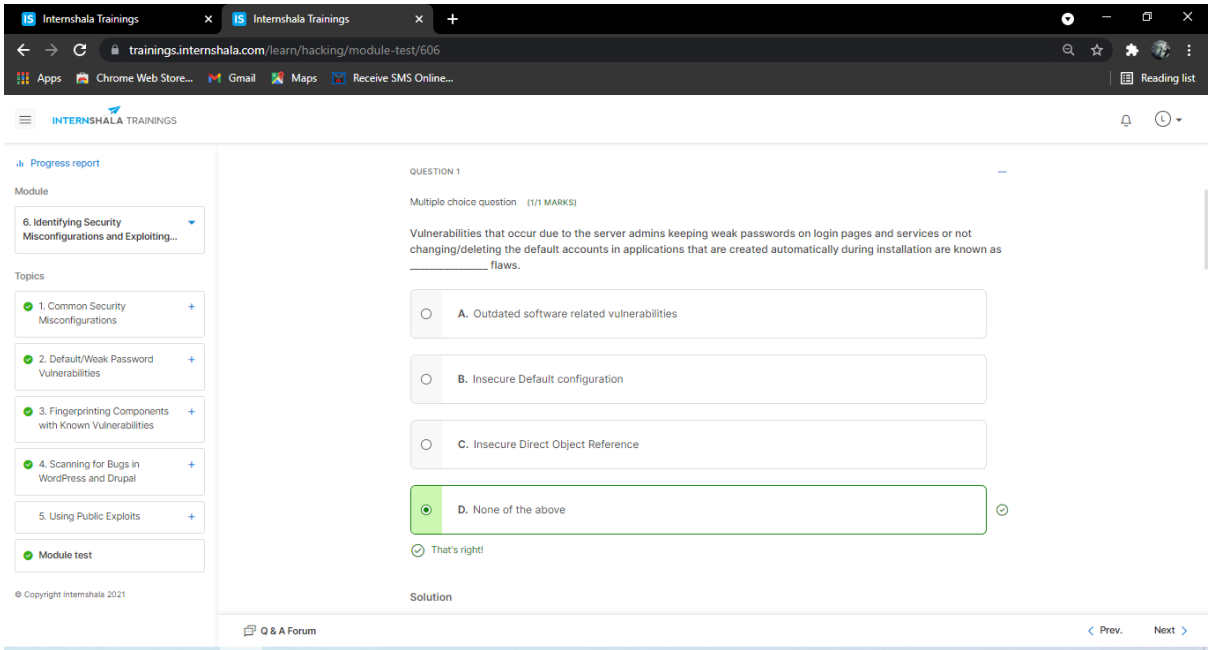
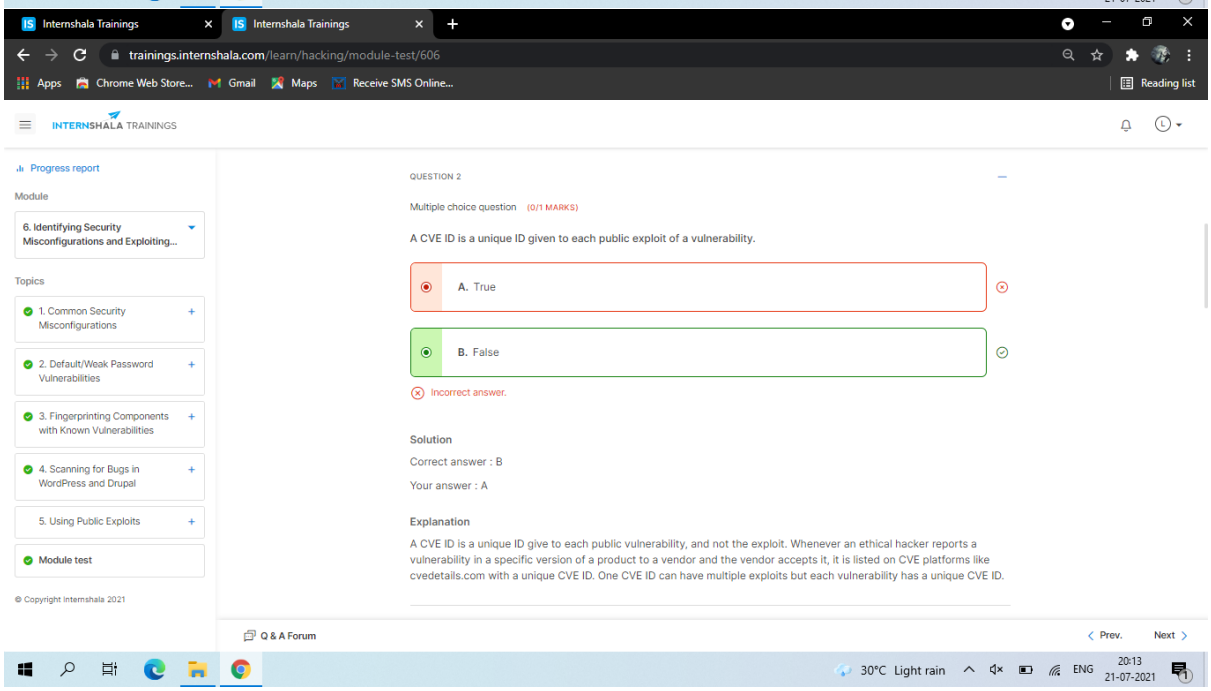
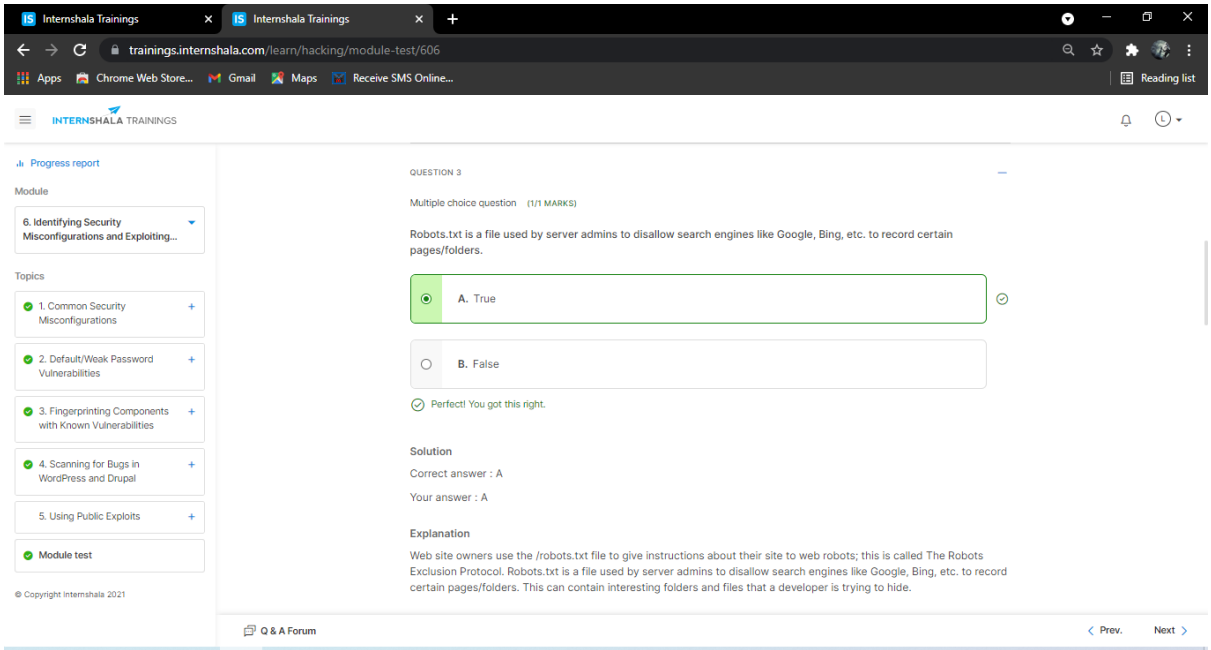
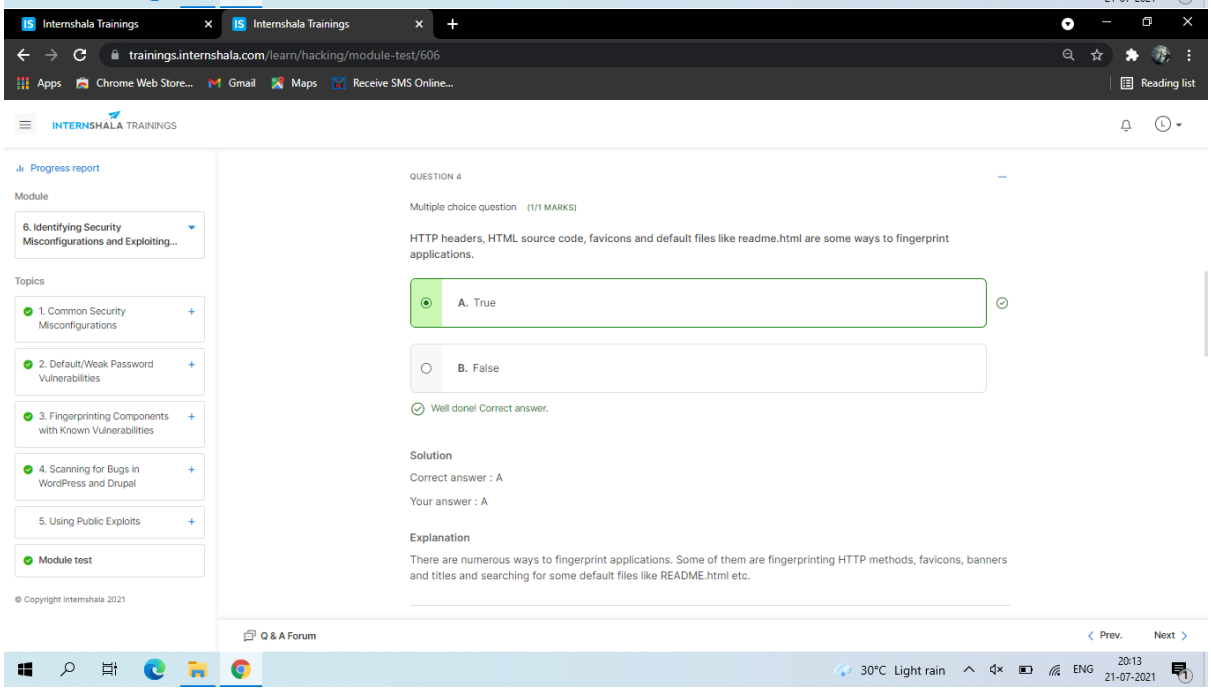
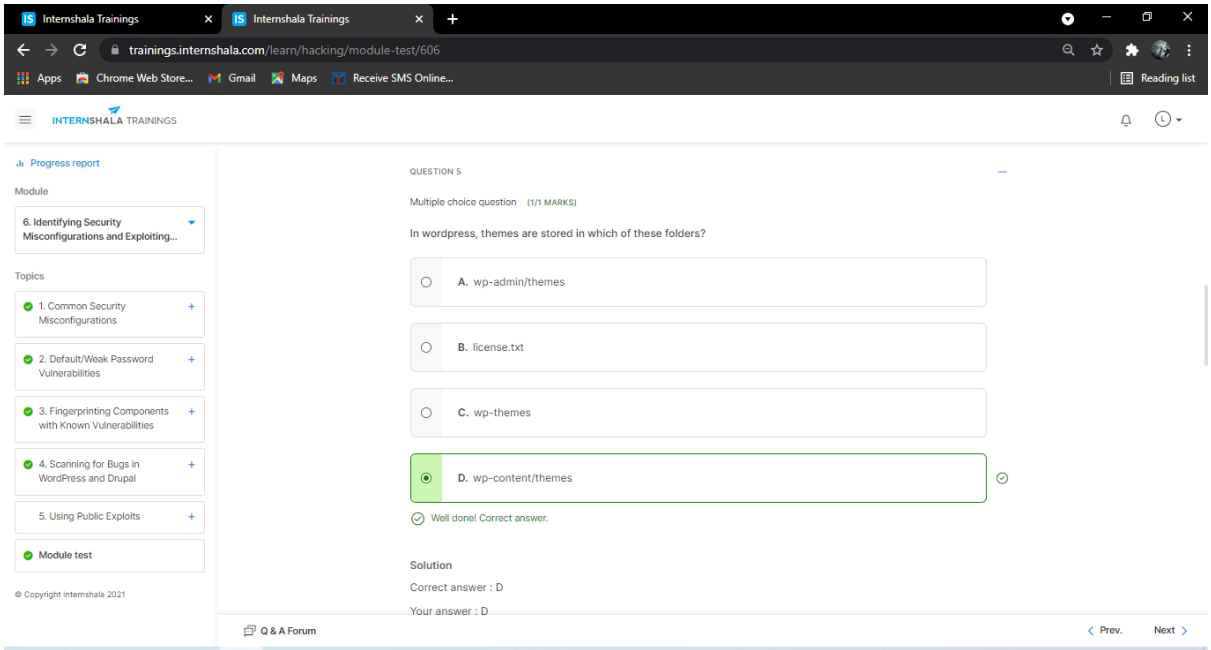
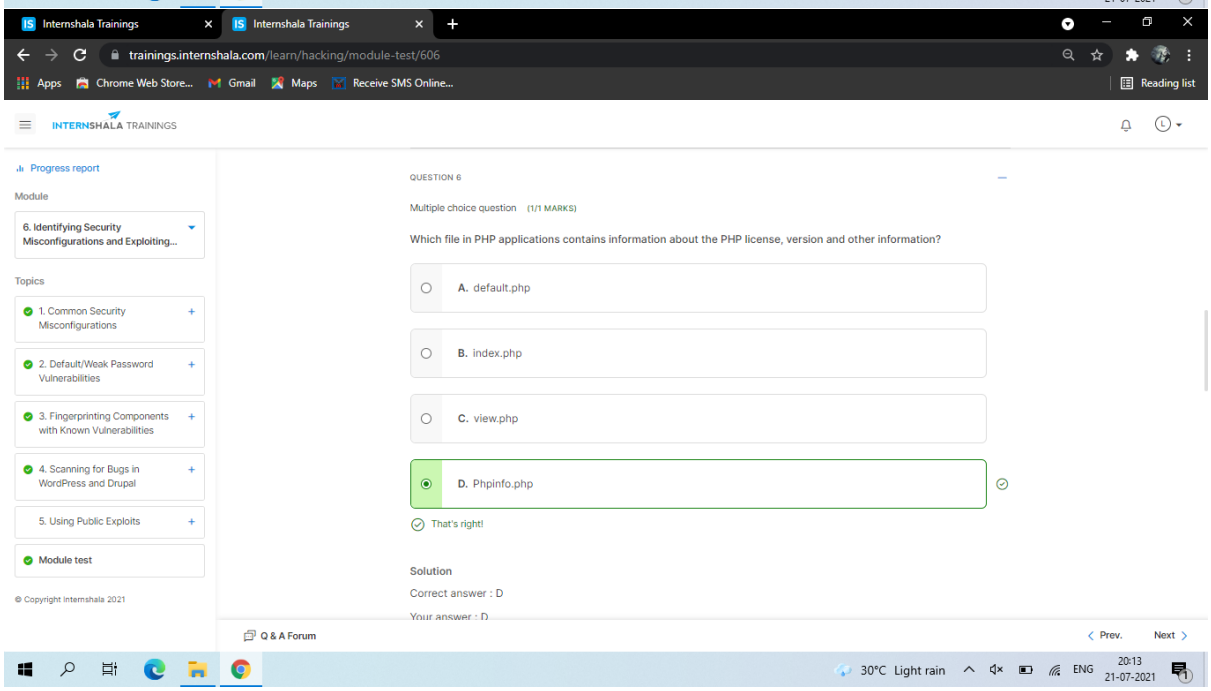

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 1
Multiple choice question (1/1 MARKS)
Vulnerabilities that occur due to the server admins keeping weak passwords on login pages and services or not changing/deleting the default accounts in applications that are created automatically during installation are known as _____ flaws.
A. Outdated software related vulnerabilities
B. Insecure Default configuration
C. Insecure Direct Object Reference
D. None of the above
That's right!
Solution
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:13
21-07-2021

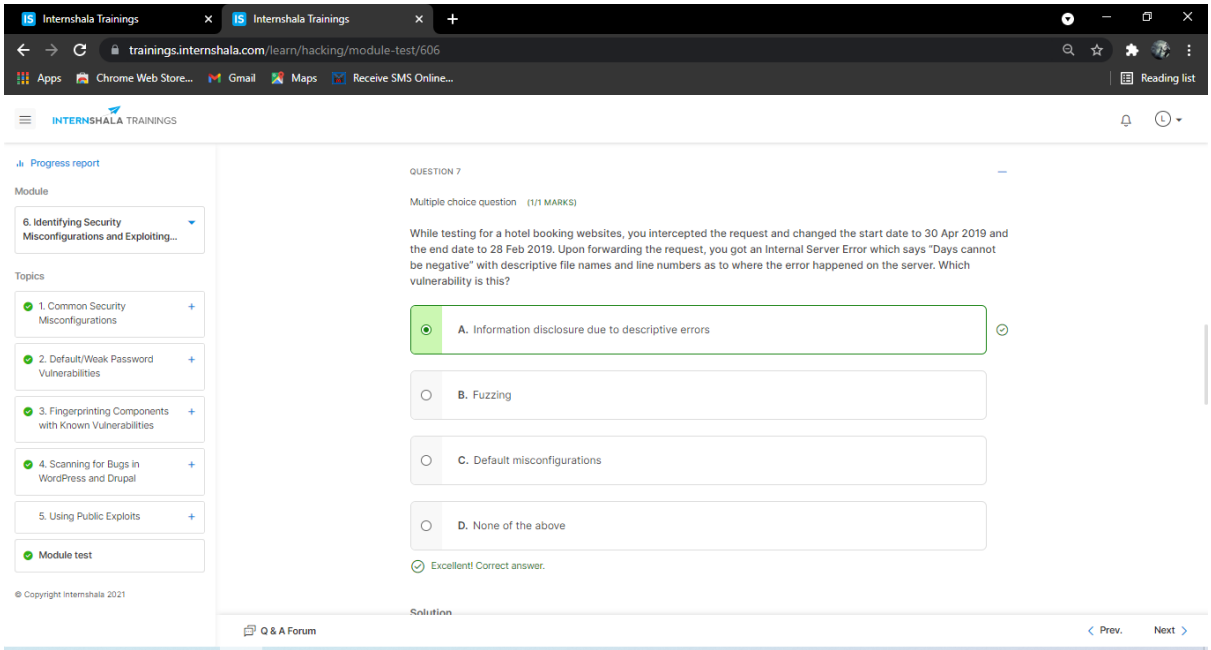

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 2
Multiple choice question (0/1 MARKS)
A CVE ID is a unique ID given to each public exploit of a vulnerability.
A. True
B. False
Incorrect answer.
Solution
Correct answer : B
Your answer : A
Explanation
A CVE ID is a unique ID give to each public vulnerability, and not the exploit. Whenever an ethical hacker reports a vulnerability in a specific version of a product to a vendor and the vendor accepts it, it is listed on CVE platforms like cvedetails.com with a unique CVE ID. One CVE ID can have multiple exploits but each vulnerability has a unique CVE ID.
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:13
21-07-2021

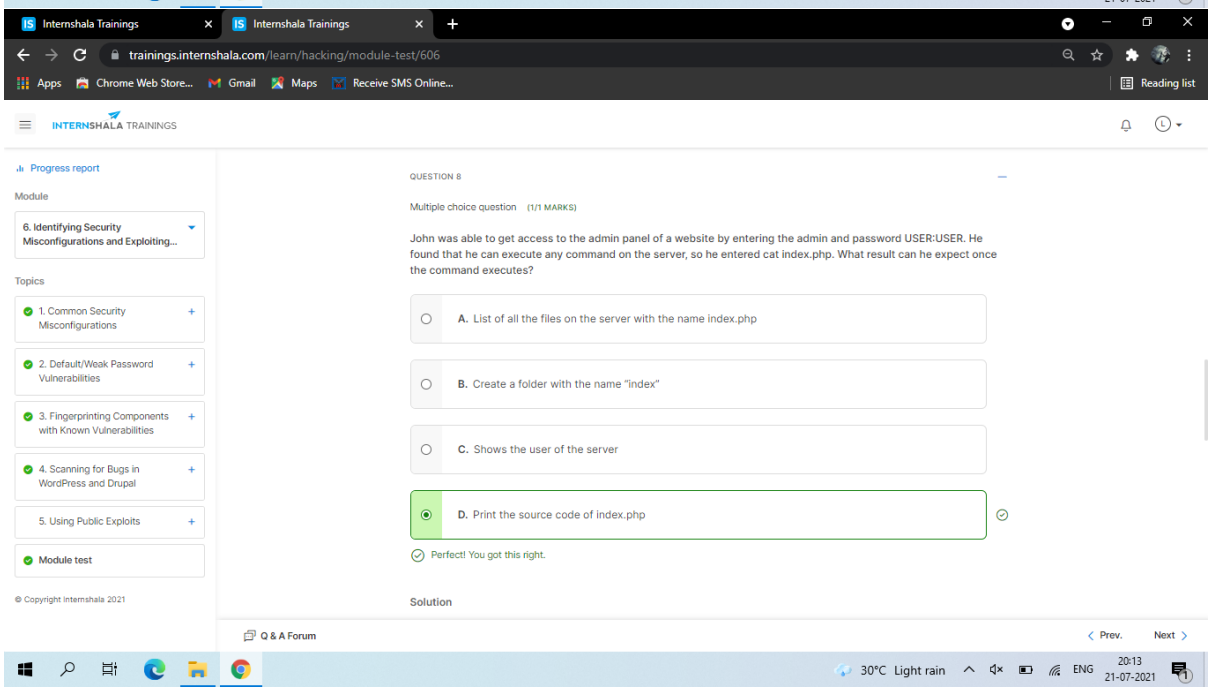

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 3
Multiple choice question (1/1 MARKS)
Robots.txt is a file used by server admins to disallow search engines like Google, Bing, etc. to record certain pages/folders.
A. True
B. False
Perfect! You got this right.
Solution
Correct answer : A
Your answer : A
Explanation
Web site owners use the /robots.txt file to give instructions about their site to web robots; this is called The Robots Exclusion Protocol. Robots.txt is a file used by server admins to disallow search engines like Google, Bing, etc. to record certain pages/folders. This can contain interesting folders and files that a developer is trying to hide.
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:13
21-07-2021

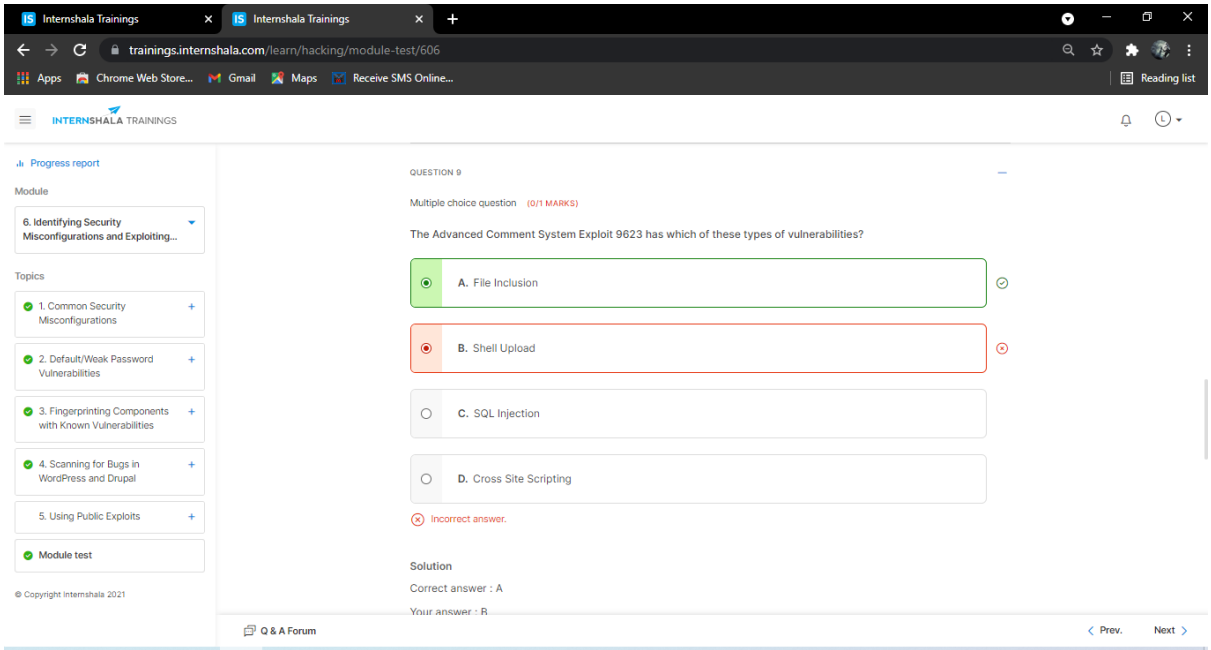

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 4
Multiple choice question (1/1 MARKS)
HTTP headers, HTML source code, favicons and default files like readme.html are some ways to fingerprint applications.
A. True
B. False
Well done! Correct answer.
Solution
Correct answer : A
Your answer : A
Explanation
There are numerous ways to fingerprint applications. Some of them are fingerprinting HTTP methods, favicons, banners and titles and searching for some default files like README.html etc.
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:13
21-07-2021

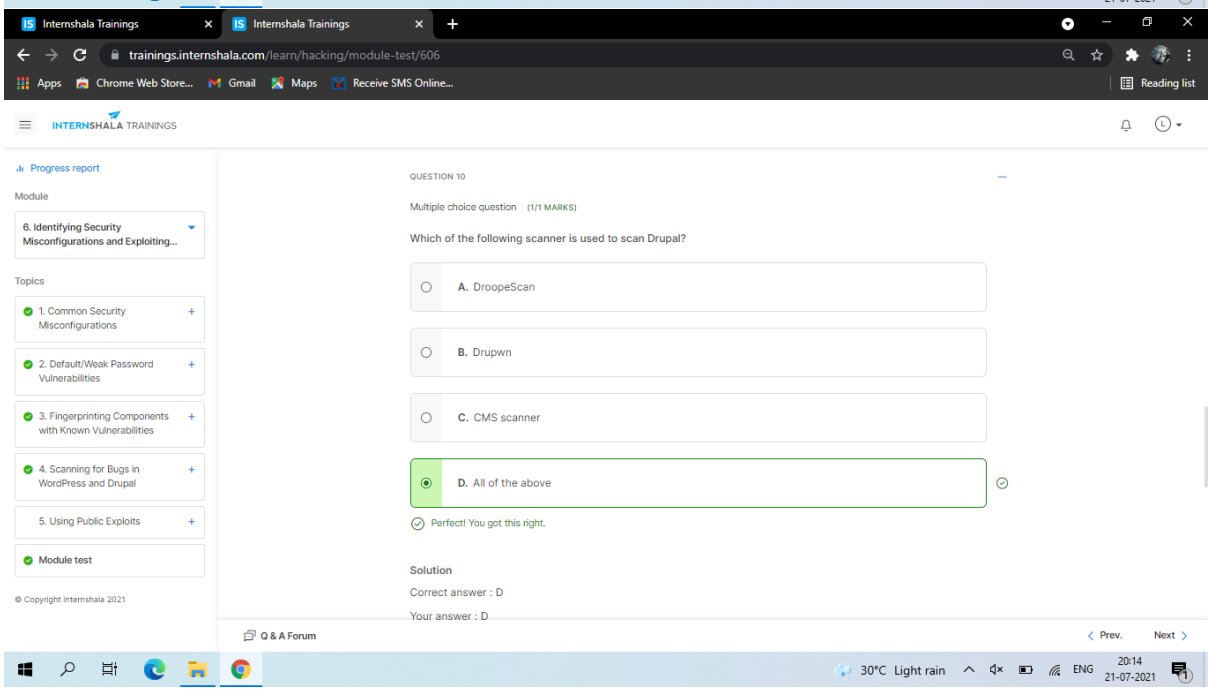

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 5
Multiple choice question (1/1 MARKS)
In wordpress, themes are stored in which of these folders?
A. wp-admin/themes
B. license.txt
C. wp-themes
D. wp-content/themes
Well done! Correct answer.
Solution
Correct answer : D
Your answer : D
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:13
21-07-2021

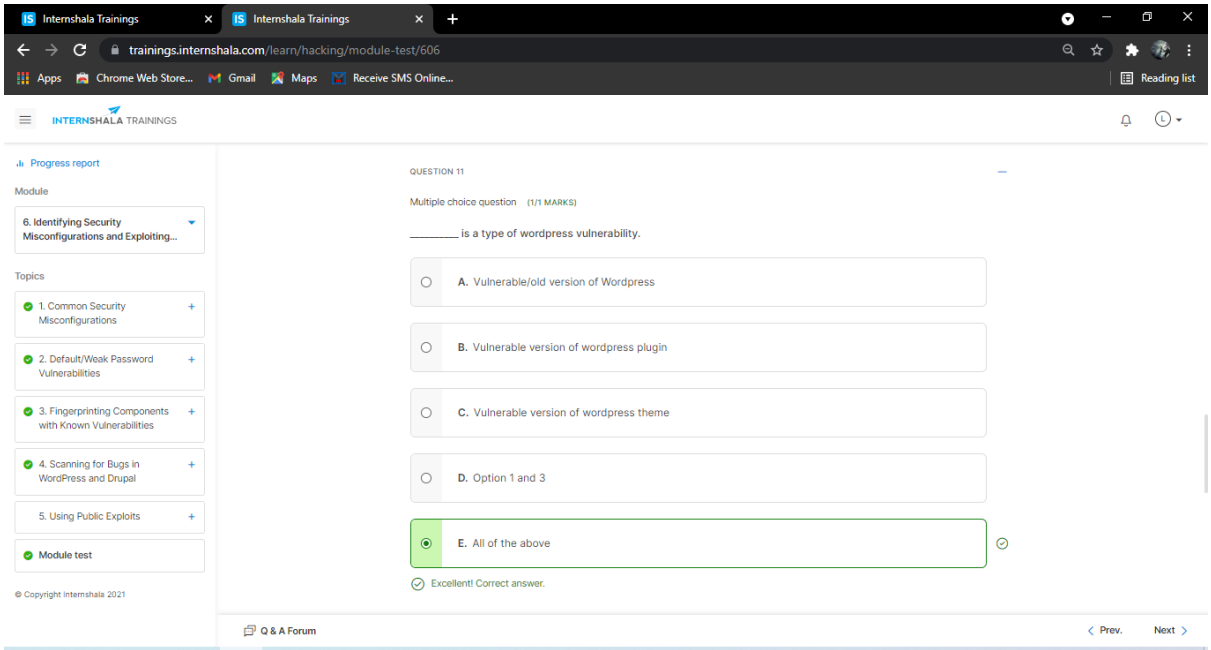

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 6
Multiple choice question (1/1 MARKS)
Which file in PHP applications contains information about the PHP license, version and other information?
A. default.php
B. index.php
C. view.php
D. Phpinfo.php
That's right!
Solution
Correct answer : D
Your answer : D
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:13
21-07-2021

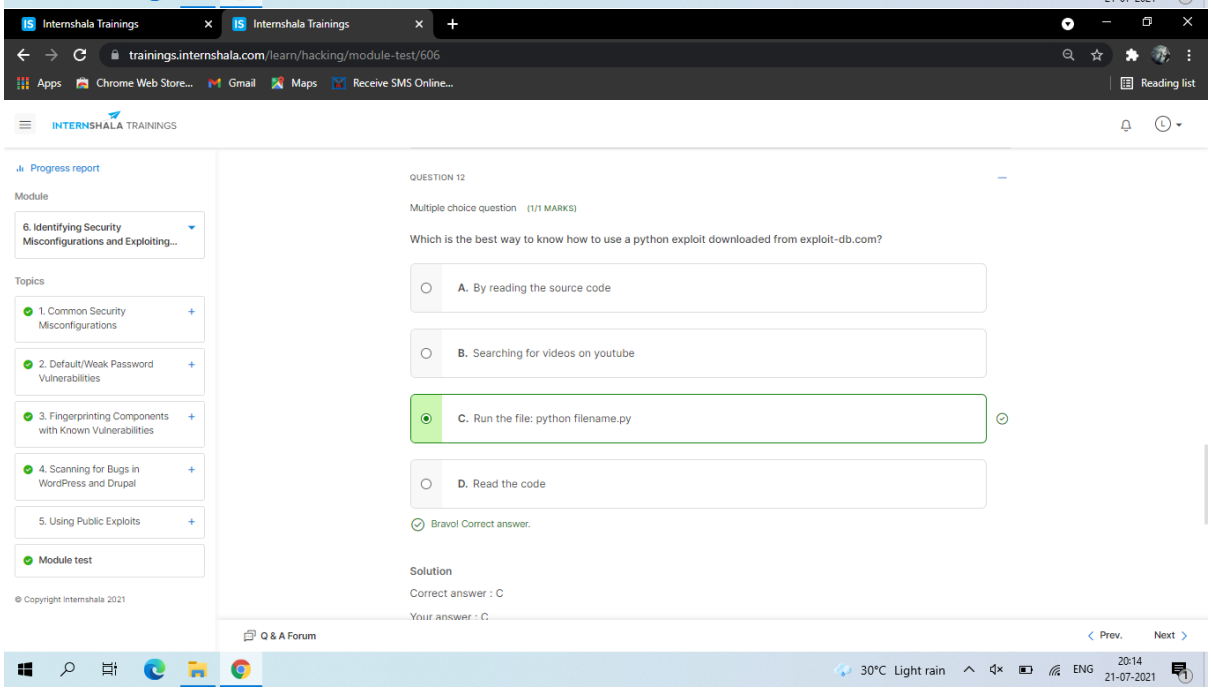

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 7
Multiple choice question (1/1 MARKS)
While testing for a hotel booking websites, you intercepted the request and changed the start date to 30 Apr 2019 and the end date to 28 Feb 2019. Upon forwarding the request, you got an Internal Server Error which says "Days cannot be negative" with descriptive file names and line numbers as to where the error happened on the server. Which vulnerability is this?
A. Information disclosure due to descriptive errors
B. Fuzzing
C. Default misconfigurations
D. None of the above
Excellent! Correct answer.
Solution
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:13
21-07-2021

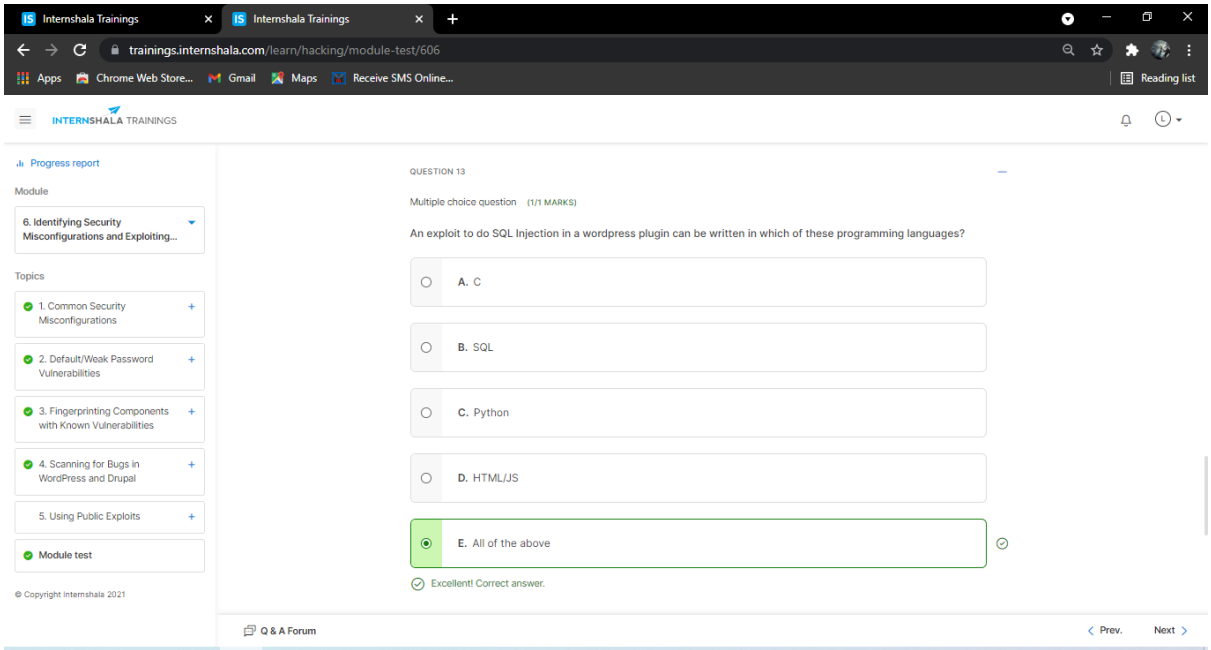

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 8
Multiple choice question (1/1 MARKS)
John was able to get access to the admin panel of a website by entering the admin and password USER:USER. He found that he can execute any command on the server, so he entered cat index.php. What result can he expect once the command executes?
A. List of all the files on the server with the name index.php
B. Create a folder with the name "index"
C. Shows the user of the server
D. Print the source code of index.php
Perfect! You got this right.
Solution
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:13
21-07-2021

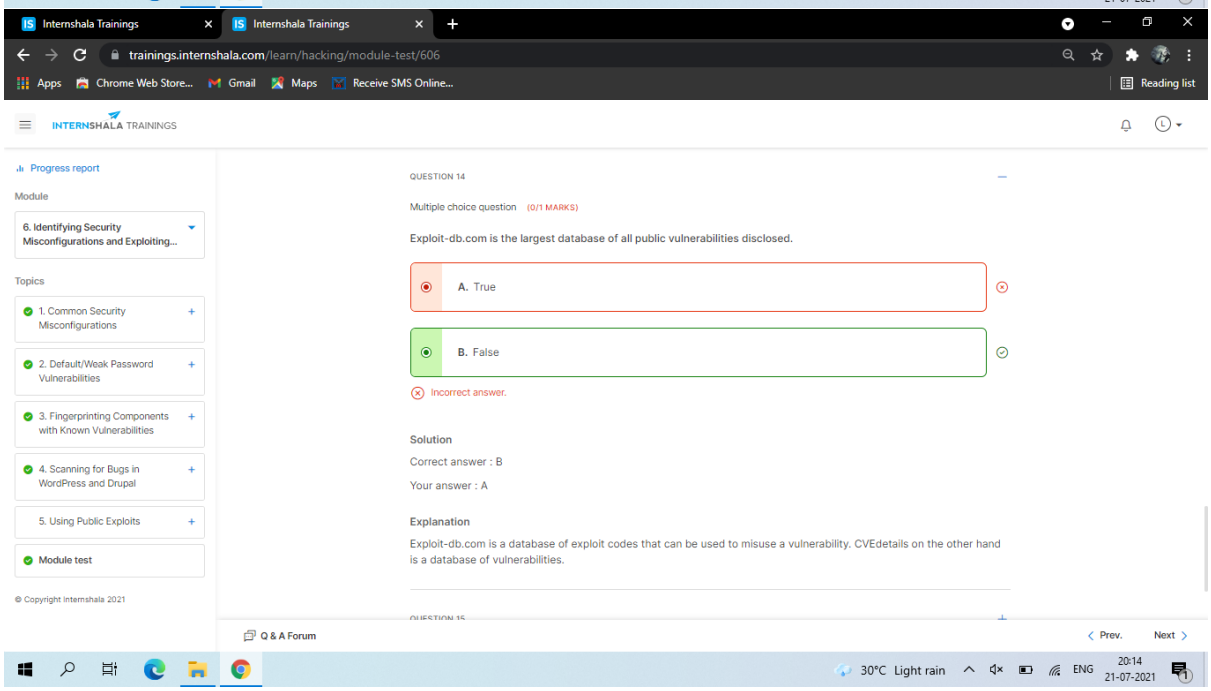

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 9
Multiple choice question (0/1 MARKS)
The Advanced Comment System Exploit 9623 has which of these types of vulnerabilities?
A. File Inclusion
B. Shell Upload
C. SQL Injection
D. Cross Site Scripting
Incorrect answer.
Solution
Correct answer : A
Your answer : B
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:14
21-07-2021

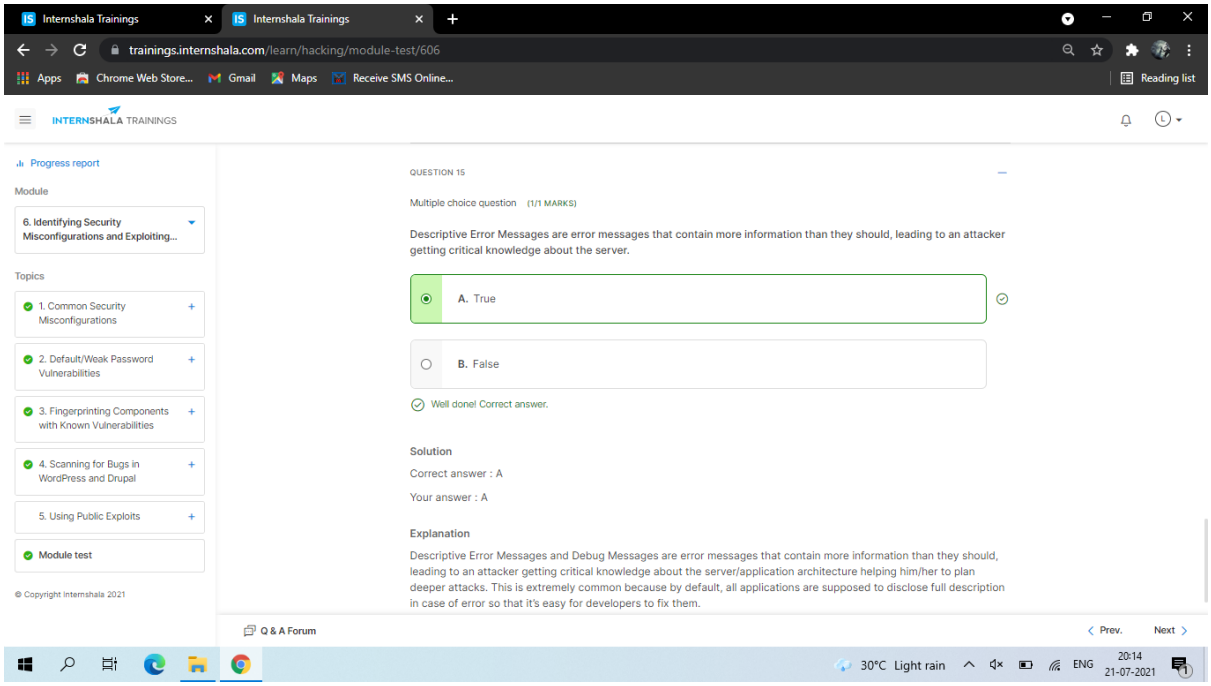

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 10
Multiple choice question (1/1 MARKS)
Which of the following scanner is used to scan Drupal?
A. DroopeScan
B. Drupwn
C. CMS scanner
D. All of the above
Perfect! You got this right.
Solution
Correct answer : D
Your answer : D
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:14
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 11
Multiple choice question (1/1 MARKS)
_____ is a type of wordpress vulnerability.
A. Vulnerable/old version of Wordpress
B. Vulnerable version of wordpress plugin
C. Vulnerable version of wordpress theme
D. Option 1 and 3
E. All of the above
Excellent! Correct answer.
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:14
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 12
Multiple choice question (1/1 MARKS)
Which is the best way to know how to use a python exploit downloaded from exploit-db.com?
A. By reading the source code
B. Searching for videos on youtube
C. Run the file: python filename.py
D. Read the code
Bravo! Correct answer.
Solution
Correct answer : C
Your answer : C
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:14
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 13
Multiple choice question (1/1 MARKS)
An exploit to do SQL Injection in a wordpress plugin can be written in which of these programming languages?
A. C
B. SQL
C. Python
D. HTML/JS
E. All of the above
Excellent! Correct answer.
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:14
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 14
Multiple choice question (0/1 MARKS)
Exploit-db.com is the largest database of all public vulnerabilities disclosed.
A. True
B. False
Incorrect answer.
Solution
Correct answer : B
Your answer : A
Explanation
Exploit-db.com is a database of exploit codes that can be used to misuse a vulnerability. CVEdetails on the other hand is a database of vulnerabilities.
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:14
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/606
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
6. Identifying Security Misconfigurations and Exploiting...
Topics
1. Common Security Misconfigurations
2. Default/Weak Password Vulnerabilities
3. Fingerprinting Components with Known Vulnerabilities
4. Scanning for Bugs in WordPress and Drupal
5. Using Public Exploits
Module test
© Copyright Internshala 2021
QUESTION 15
Multiple choice question (1/1 MARKS)
Descriptive Error Messages are error messages that contain more information than they should, leading to an attacker getting critical knowledge about the server.
A. True
B. False
Well done! Correct answer.
Solution
Correct answer : A
Your answer : A
Explanation
Descriptive Error Messages and Debug Messages are error messages that contain more information than they should, leading to an attacker getting critical knowledge about the server/application architecture helping him/her to plan deeper attacks. This is extremely common because by default, all applications are supposed to disclose full description in case of error so that it's easy for developers to fix them.
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:14
21-07-2021