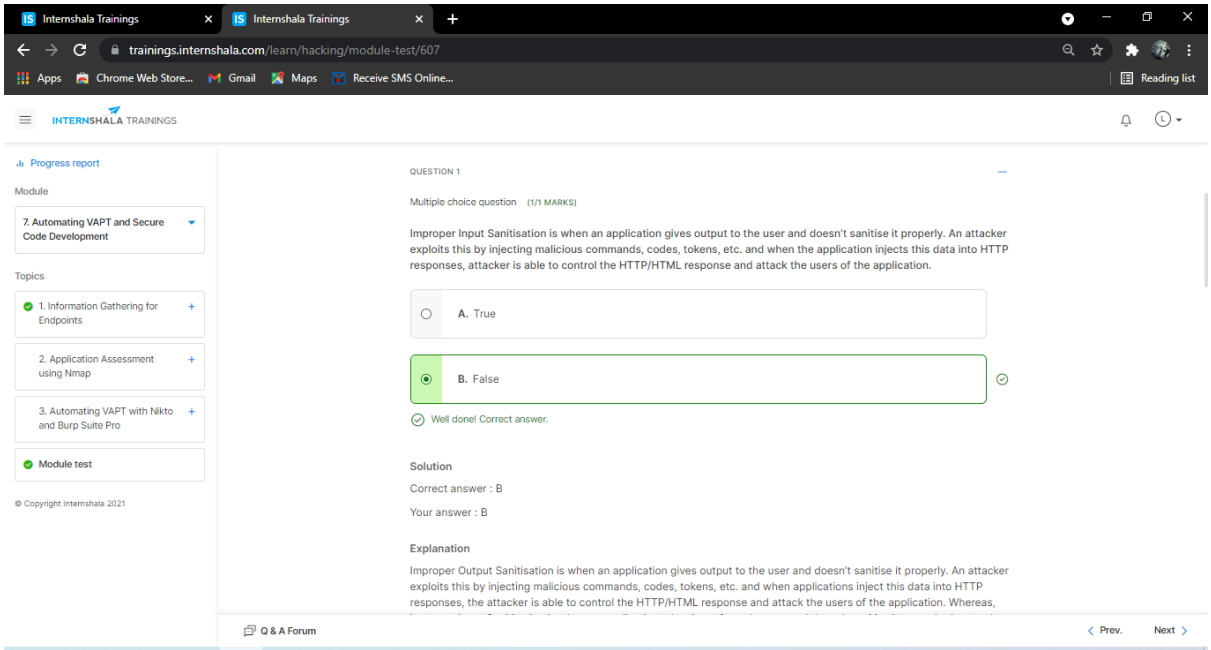
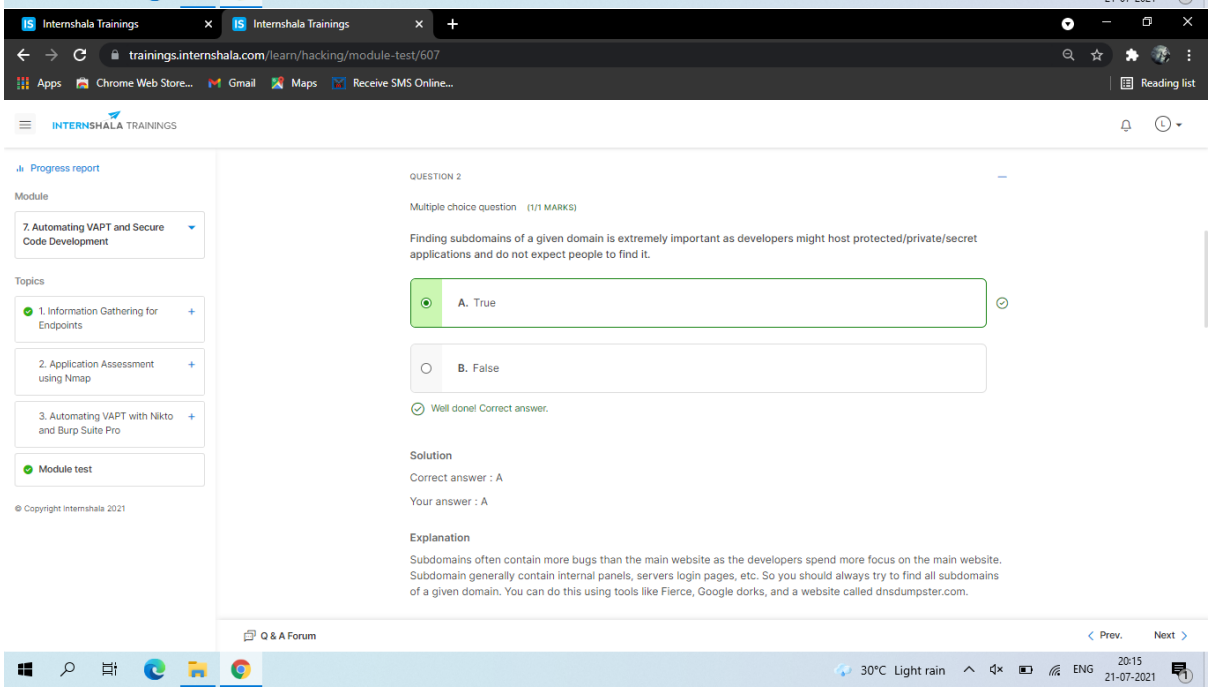
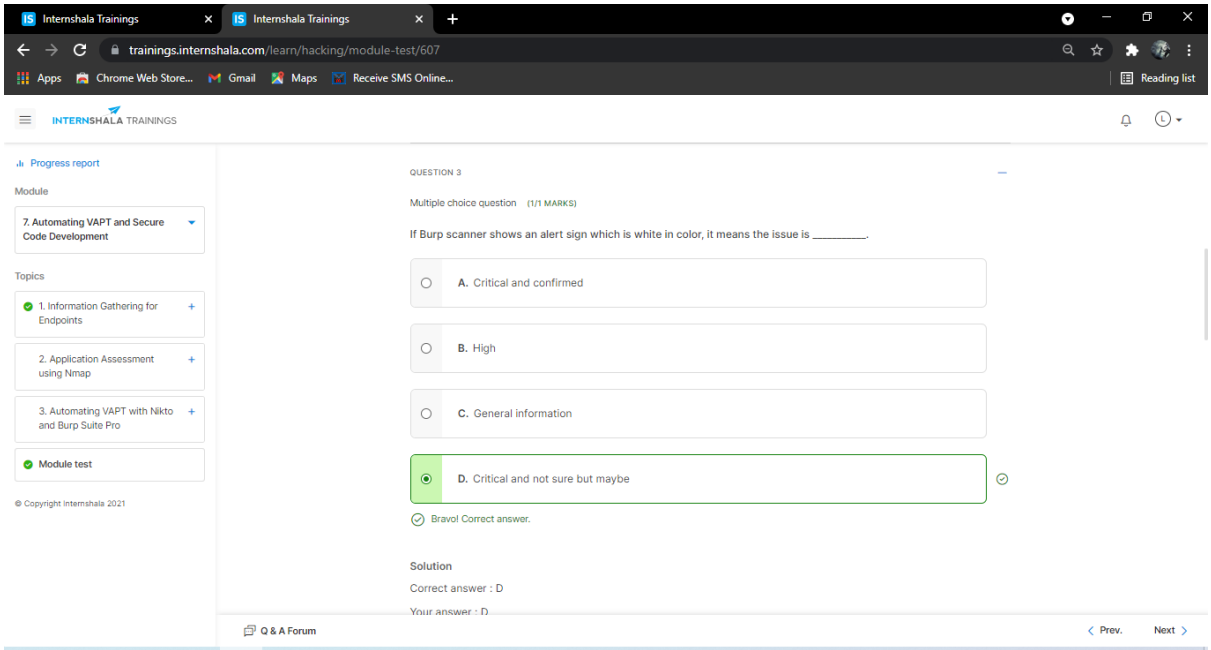
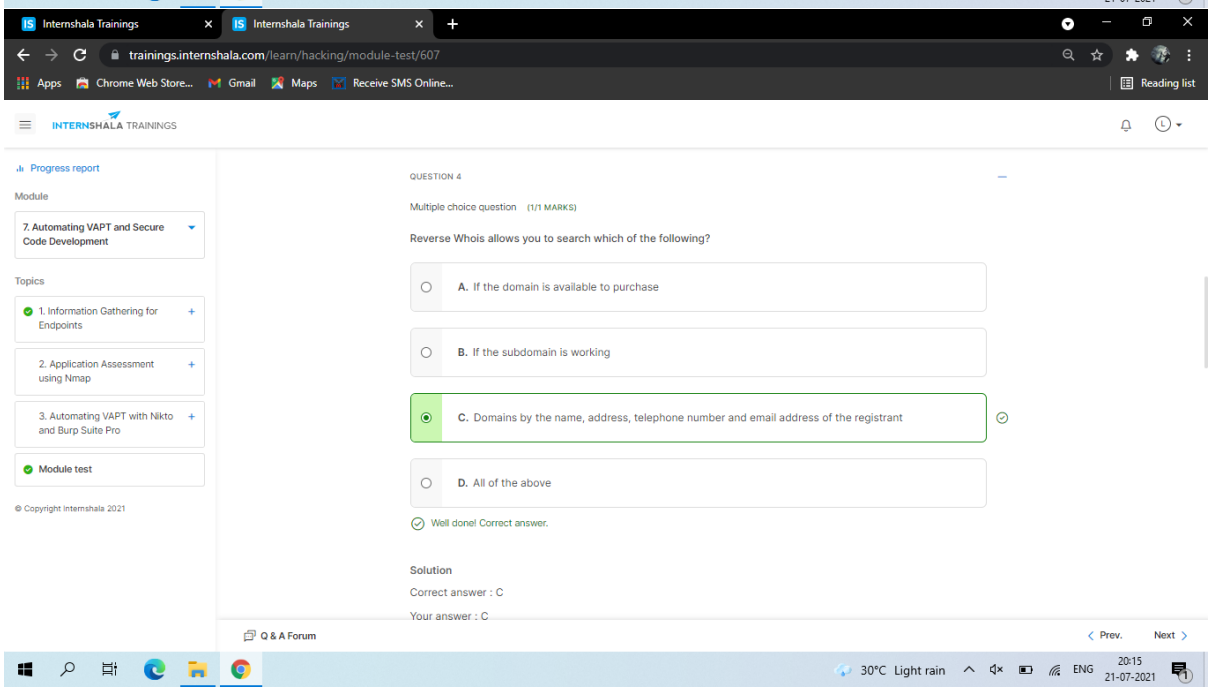
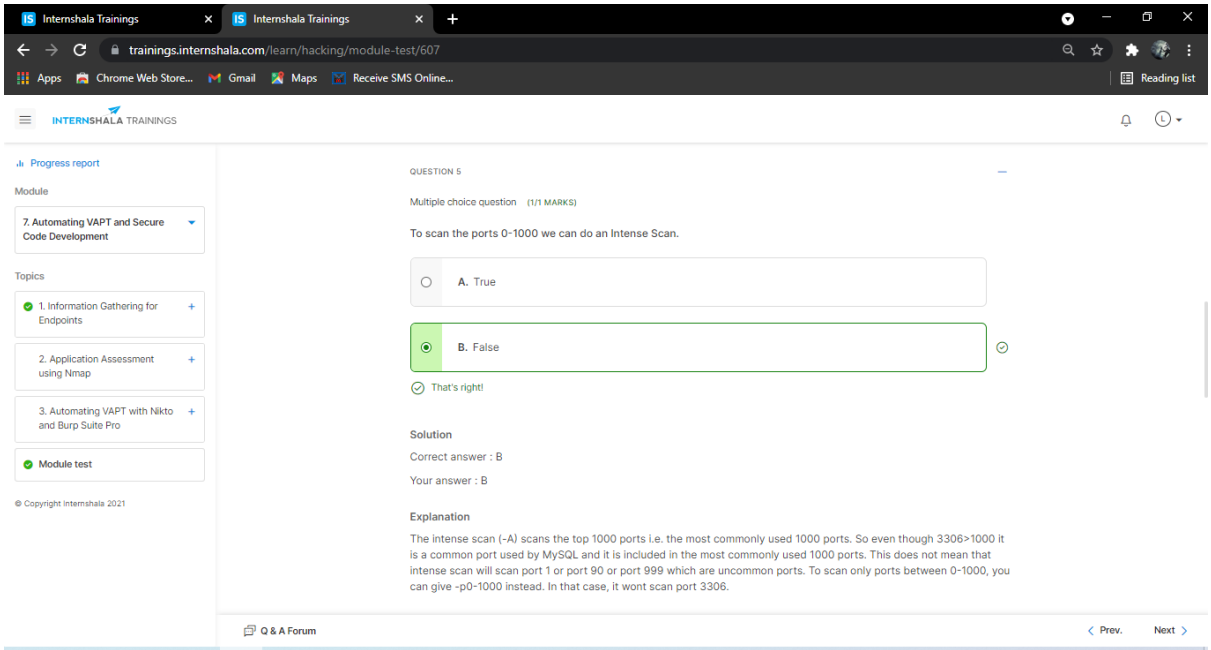
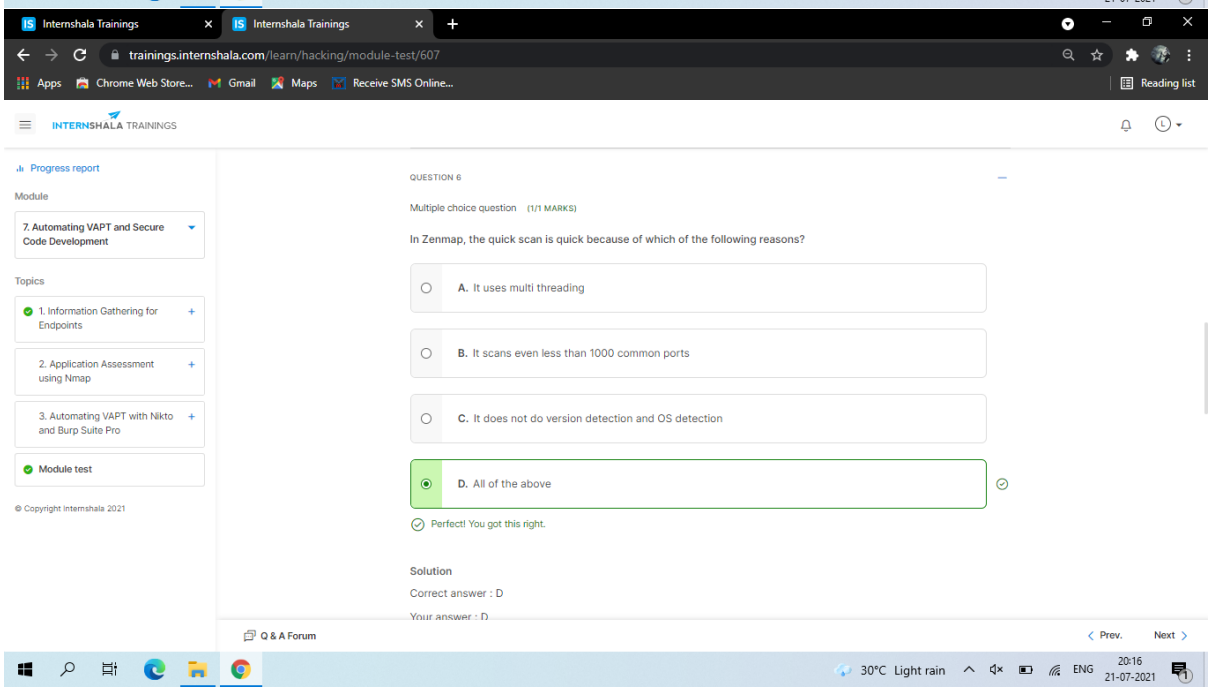

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/607
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
7. Automating VAPT and Secure Code Development
Topics
1. Information Gathering for Endpoints
2. Application Assessment using Nmap
3. Automating VAPT with Nikto and Burp Suite Pro
Module test
© Copyright Internshala 2021
QUESTION 1
Multiple choice question (1/1 MARKS)
Improper Input Sanitisation is when an application gives output to the user and doesn't sanitise it properly. An attacker exploits this by injecting malicious commands, codes, tokens, etc. and when the application injects this data into HTTP responses, attacker is able to control the HTTP/HTML response and attack the users of the application.
A. True
B. False
Well done! Correct answer.
Solution
Correct answer : B
Your answer : B
Explanation
Improper Output Sanitisation is when an application gives output to the user and doesn't sanitise it properly. An attacker exploits this by injecting malicious commands, codes, tokens, etc. and when applications inject this data into HTTP responses, the attacker is able to control the HTTP/HTML response and attack the users of the application. Whereas,
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:15
21-07-2021

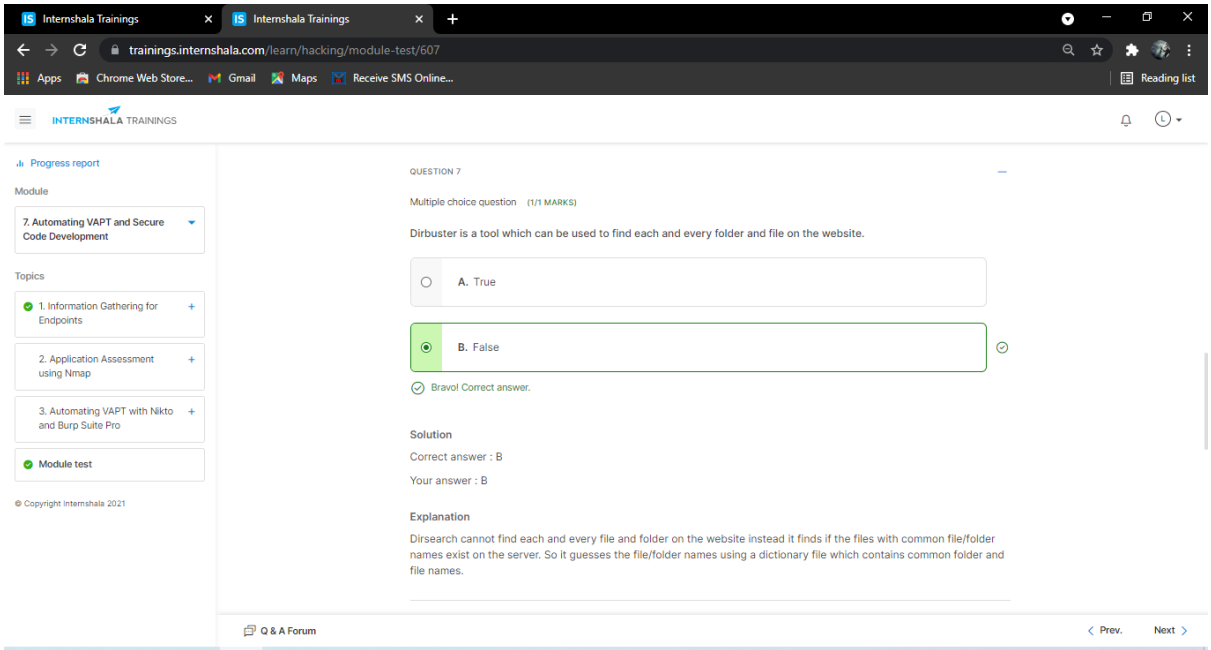

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/607
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
7. Automating VAPT and Secure Code Development
Topics
1. Information Gathering for Endpoints
2. Application Assessment using Nmap
3. Automating VAPT with Nikto and Burp Suite Pro
Module test
© Copyright Internshala 2021
QUESTION 2
Multiple choice question (1/1 MARKS)
Finding subdomains of a given domain is extremely important as developers might host protected/private/secret applications and do not expect people to find it.
A. True
B. False
Well done! Correct answer.
Solution
Correct answer : A
Your answer : A
Explanation
Subdomains often contain more bugs than the main website as the developers spend more focus on the main website. Subdomain generally contain internal panels, servers login pages, etc. So you should always try to find all subdomains of a given domain. You can do this using tools like Fierce, Google dorks, and a website called dnsdumpster.com.
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:15
21-07-2021

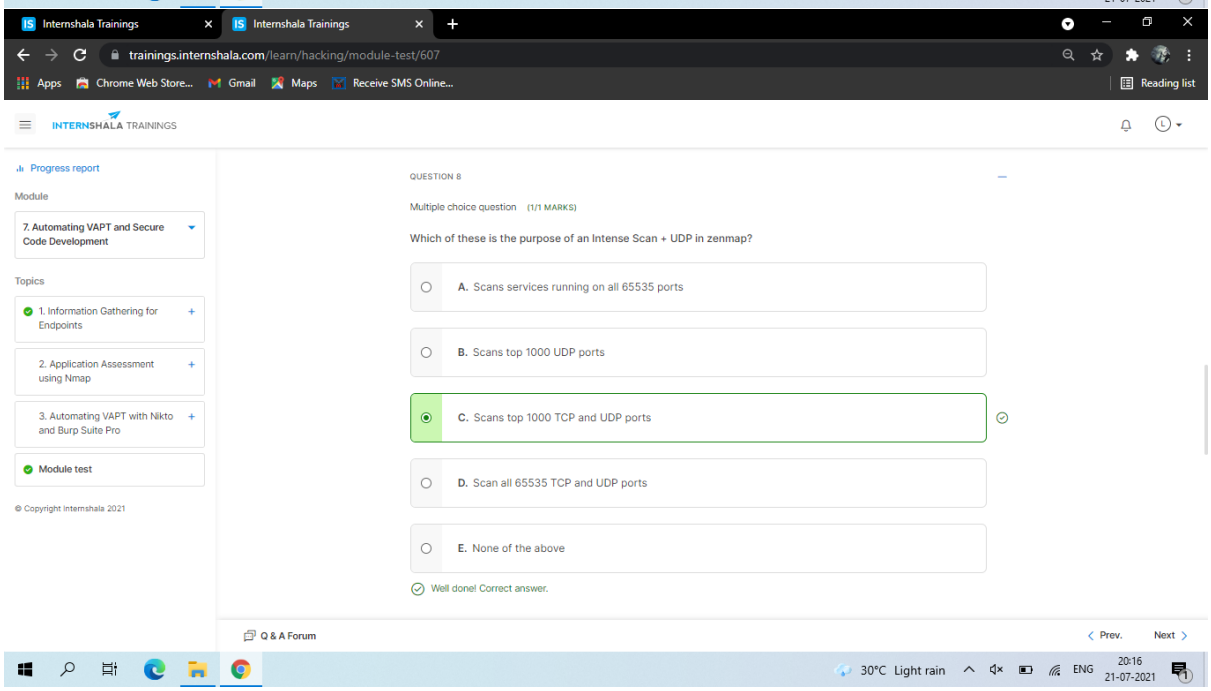

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/607
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
7. Automating VAPT and Secure Code Development
Topics
1. Information Gathering for Endpoints
2. Application Assessment using Nmap
3. Automating VAPT with Nikto and Burp Suite Pro
Module test
© Copyright Internshala 2021
QUESTION 3
Multiple choice question (1/1 MARKS)
If Burp scanner shows an alert sign which is white in color, it means the issue is _____.
A. Critical and confirmed
B. High
C. General information
D. Critical and not sure but maybe
Bravo! Correct answer.
Solution
Correct answer : D
Your answer : D
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:15
21-07-2021

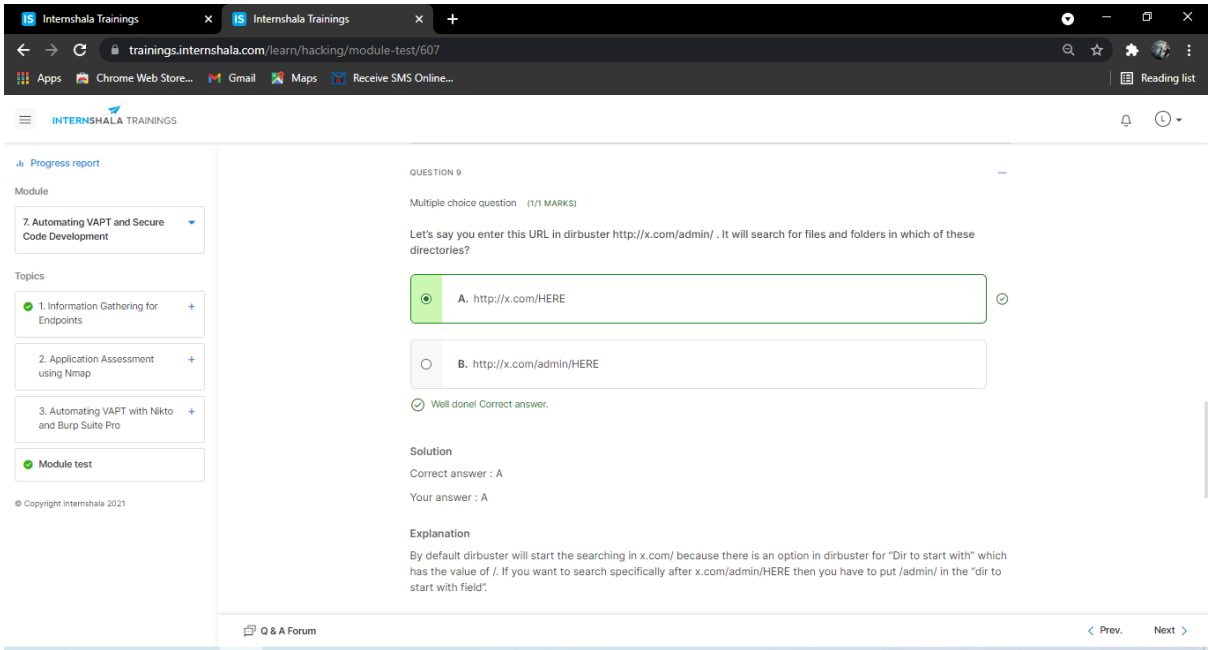

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/607
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
7. Automating VAPT and Secure Code Development
Topics
1. Information Gathering for Endpoints
2. Application Assessment using Nmap
3. Automating VAPT with Nikto and Burp Suite Pro
Module test
© Copyright Internshala 2021
QUESTION 4
Multiple choice question (1/1 MARKS)
Reverse Whois allows you to search which of the following?
A. If the domain is available to purchase
B. If the subdomain is working
C. Domains by the name, address, telephone number and email address of the registrant
D. All of the above
Well done! Correct answer.
Solution
Correct answer : C
Your answer : C
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:15
21-07-2021

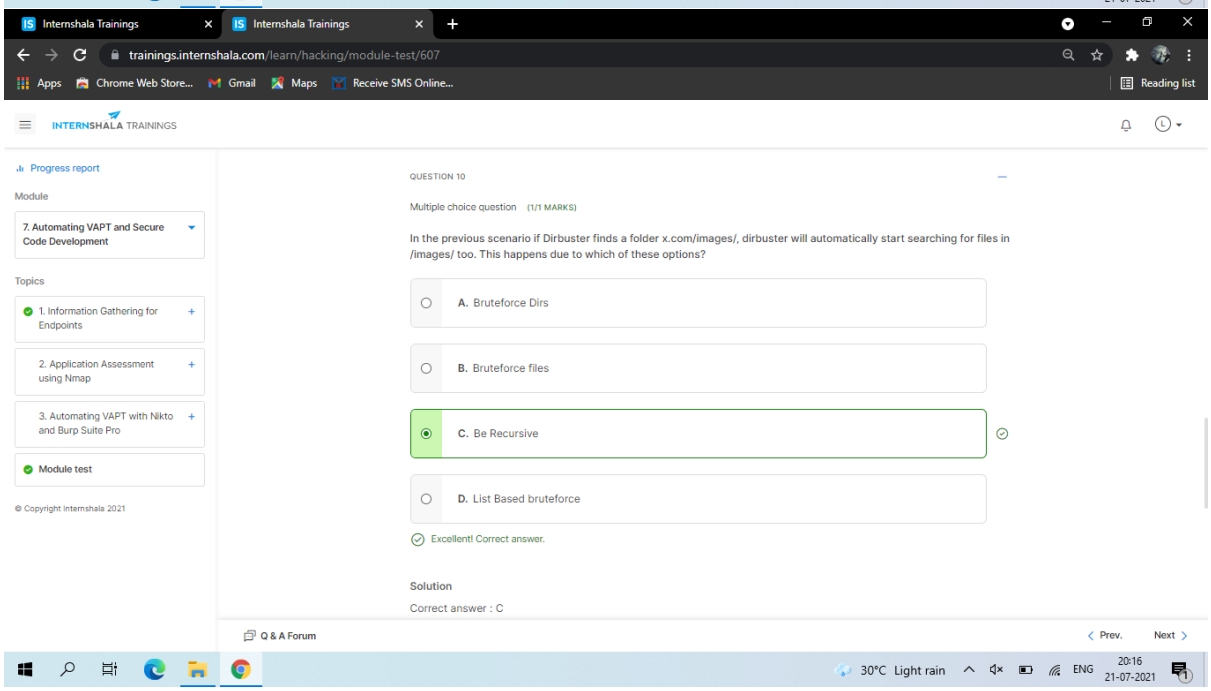

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/607
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
7. Automating VAPT and Secure Code Development
Topics
1. Information Gathering for Endpoints
2. Application Assessment using Nmap
3. Automating VAPT with Nikto and Burp Suite Pro
Module test
© Copyright Internshala 2021
QUESTION 5
Multiple choice question (1/1 MARKS)
To scan the ports 0-1000 we can do an Intense Scan.
A. True
B. False
That's right!
Solution
Correct answer : B
Your answer : B
Explanation
The intense scan (-A) scans the top 1000 ports i.e. the most commonly used 1000 ports. So even though 3306>1000 it is a common port used by MySQL and it is included in the most commonly used 1000 ports. This does not mean that intense scan will scan port 1 or port 90 or port 999 which are uncommon ports. To scan only ports between 0-1000, you can give -p0-1000 instead. In that case, it wont scan port 3306.
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:15
21-07-2021

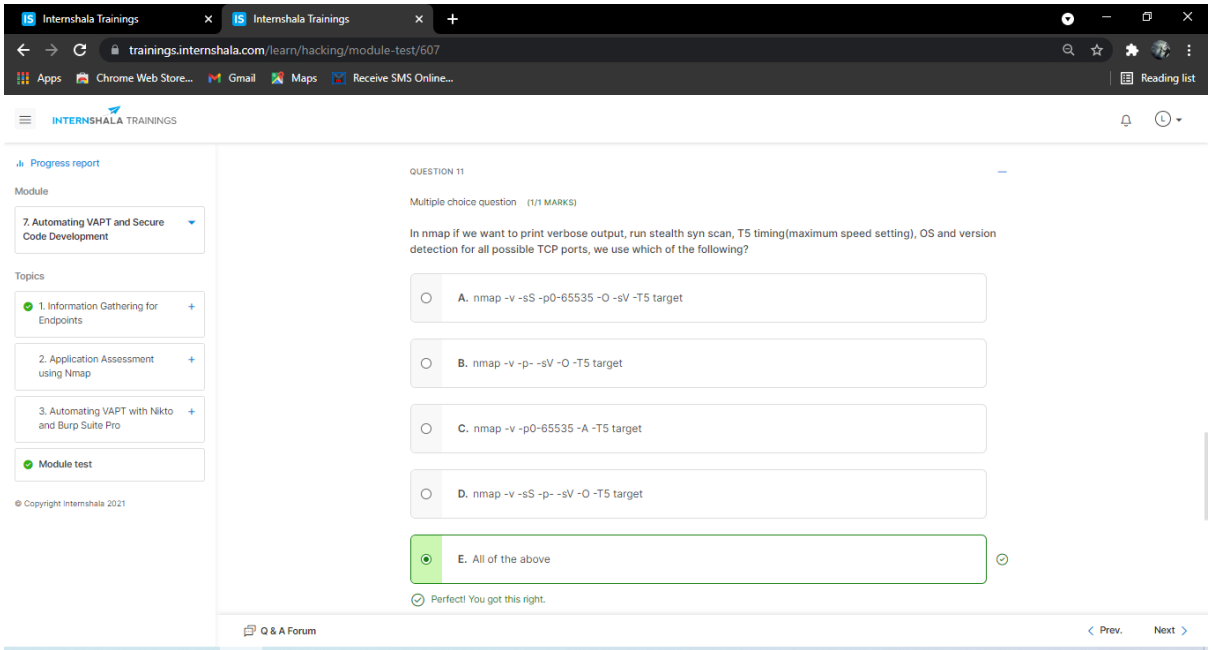

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/607
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
7. Automating VAPT and Secure Code Development
Topics
1. Information Gathering for Endpoints
2. Application Assessment using Nmap
3. Automating VAPT with Nikto and Burp Suite Pro
Module test
© Copyright Internshala 2021
QUESTION 6
Multiple choice question (1/1 MARKS)
In Zenmap, the quick scan is quick because of which of the following reasons?
A. It uses multi threading
B. It scans even less than 1000 common ports
C. It does not do version detection and OS detection
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
20:16
21-07-2021

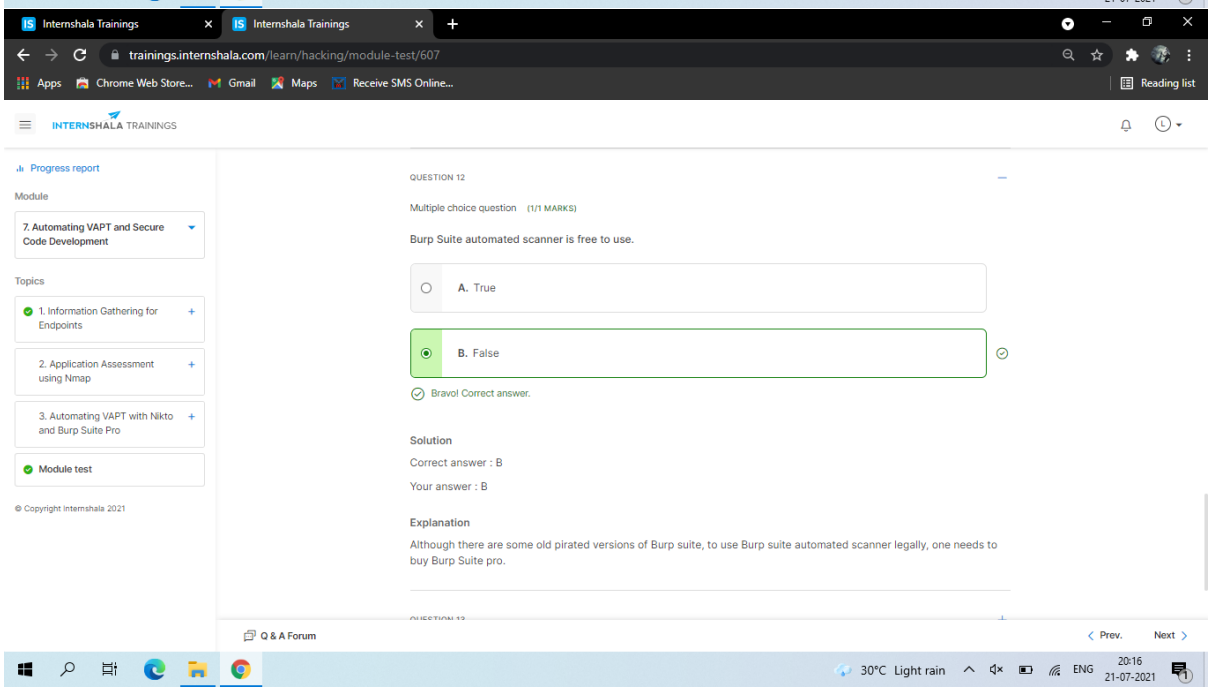

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/607
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
7. Automating VAPT and Secure Code Development
Topics
1. Information Gathering for Endpoints
2. Application Assessment using Nmap
3. Automating VAPT with Nikto and Burp Suite Pro
Module test
© Copyright Internshala 2021
QUESTION 7
Multiple choice question (1/1 MARKS)
Dirbuster is a tool which can be used to find each and every folder and file on the website.
A. True
B. False
Bravo! Correct answer.
Solution
Correct answer : B
Your answer : B
Explanation
Dirsearch cannot find each and every file and folder on the website instead it finds if the files with common file/folder names exist on the server. So it guesses the file/folder names using a dictionary file which contains common folder and file names.
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:16
21-07-2021

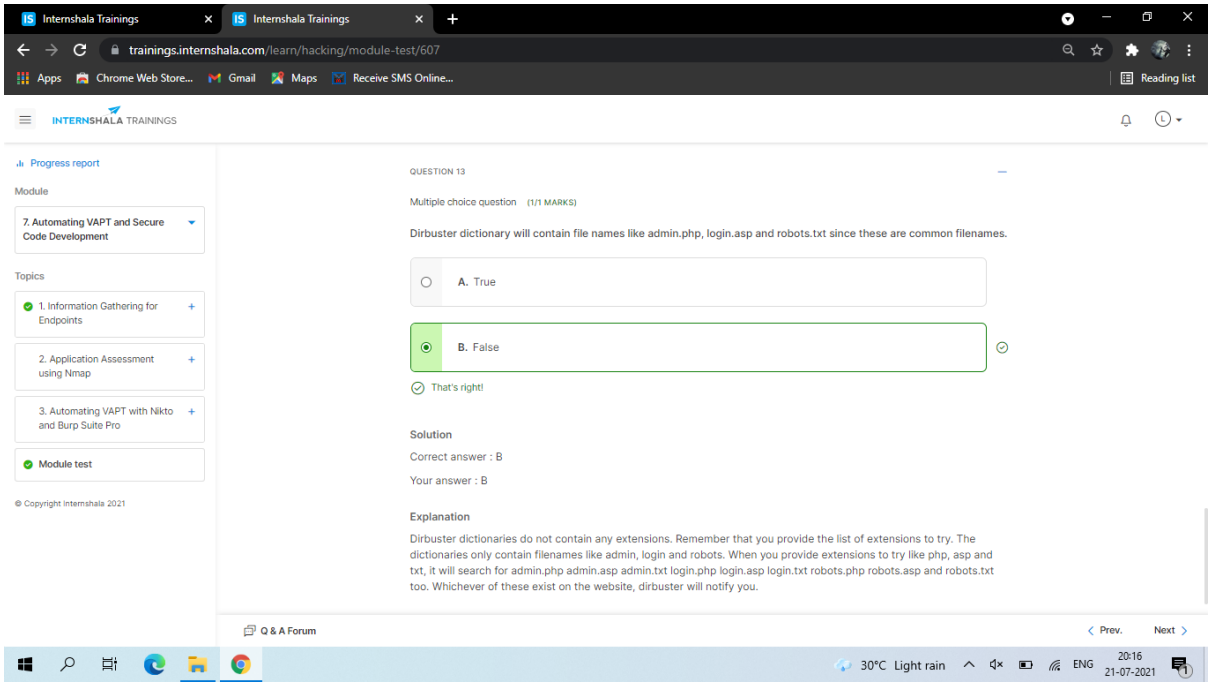

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/607
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
7. Automating VAPT and Secure Code Development
Topics
1. Information Gathering for Endpoints
2. Application Assessment using Nmap
3. Automating VAPT with Nikto and Burp Suite Pro
Module test
© Copyright Internshala 2021
QUESTION 8
Multiple choice question (1/1 MARKS)
Which of these is the purpose of an Intense Scan + UDP in zenmap?
A. Scans services running on all 65535 ports
B. Scans top 1000 UDP ports
C. Scans top 1000 TCP and UDP ports
D. Scan all 65535 TCP and UDP ports
E. None of the above
Well done! Correct answer.
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:16
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/607
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
7. Automating VAPT and Secure Code Development
Topics
1. Information Gathering for Endpoints
2. Application Assessment using Nmap
3. Automating VAPT with Nikto and Burp Suite Pro
Module test
© Copyright Internshala 2021
QUESTION 9
Multiple choice question (1/1 MARKS)
Let's say you enter this URL in dirbuster http://x.com/admin/ . It will search for files and folders in which of these directories?
A. http://x.com/HERE
B. http://x.com/admin/HERE
Well done! Correct answer.
Solution
Correct answer : A
Your answer : A
Explanation
By default dirbuster will start the searching in x.com/ because there is an option in dirbuster for "Dir to start with" which has the value of /. If you want to search specifically after x.com/admin/HERE then you have to put /admin/ in the "dir to start with field".
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:16
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/607
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
7. Automating VAPT and Secure Code Development
Topics
1. Information Gathering for Endpoints
2. Application Assessment using Nmap
3. Automating VAPT with Nikto and Burp Suite Pro
Module test
© Copyright Internshala 2021
QUESTION 10
Multiple choice question (1/1 MARKS)
In the previous scenario if Dirbuster finds a folder x.com/images/, dirbuster will automatically start searching for files in /images/ too. This happens due to which of these options?
A. Bruteforce Dirs
B. Bruteforce files
C. Be Recursive
D. List Based bruteforce
Excellent! Correct answer.
Solution
Correct answer : C
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:16
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/607
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
7. Automating VAPT and Secure Code Development
Topics
1. Information Gathering for Endpoints
2. Application Assessment using Nmap
3. Automating VAPT with Nikto and Burp Suite Pro
Module test
© Copyright Internshala 2021
QUESTION 11
Multiple choice question (1/1 MARKS)
In nmap if we want to print verbose output, run stealth syn scan, T5 timing(maximum speed setting), OS and version detection for all possible TCP ports, we use which of the following?
A. nmap -v -sS -p0-65535 -O -sV -T5 target
B. nmap -v -p- -sV -O -T5 target
C. nmap -v -p0-65535 -A -T5 target
D. nmap -v -sS -p- -sV -O -T5 target
E. All of the above
Perfect! You got this right.
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:16
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/607
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
7. Automating VAPT and Secure Code Development
Topics
1. Information Gathering for Endpoints
2. Application Assessment using Nmap
3. Automating VAPT with Nikto and Burp Suite Pro
Module test
© Copyright Internshala 2021
QUESTION 12
Multiple choice question (1/1 MARKS)
Burp Suite automated scanner is free to use.
A. True
B. False
Bravo! Correct answer.
Solution
Correct answer : B
Your answer : B
Explanation
Although there are some old pirated versions of Burp suite, to use Burp suite automated scanner legally, one needs to buy Burp Suite pro.
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:16
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/607
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
7. Automating VAPT and Secure Code Development
Topics
1. Information Gathering for Endpoints
2. Application Assessment using Nmap
3. Automating VAPT with Nikto and Burp Suite Pro
Module test
© Copyright Internshala 2021
QUESTION 13
Multiple choice question (1/1 MARKS)
Dirbuster dictionary will contain file names like admin.php, login.asp and robots.txt since these are common filenames.
A. True
B. False
That's right!
Solution
Correct answer : B
Your answer : B
Explanation
Dirbuster dictionaries do not contain any extensions. Remember that you provide the list of extensions to try. The dictionaries only contain filenames like admin, login and robots. When you provide extensions to try like php, asp and txt, it will search for admin.php admin.asp admin.txt login.php login.asp login.txt robots.php robots.asp and robots.txt too. Whichever of these exist on the website, dirbuster will notify you.
Q & A Forum
Prev.
Next
30°C Light rain
ENG
20:16
21-07-2021