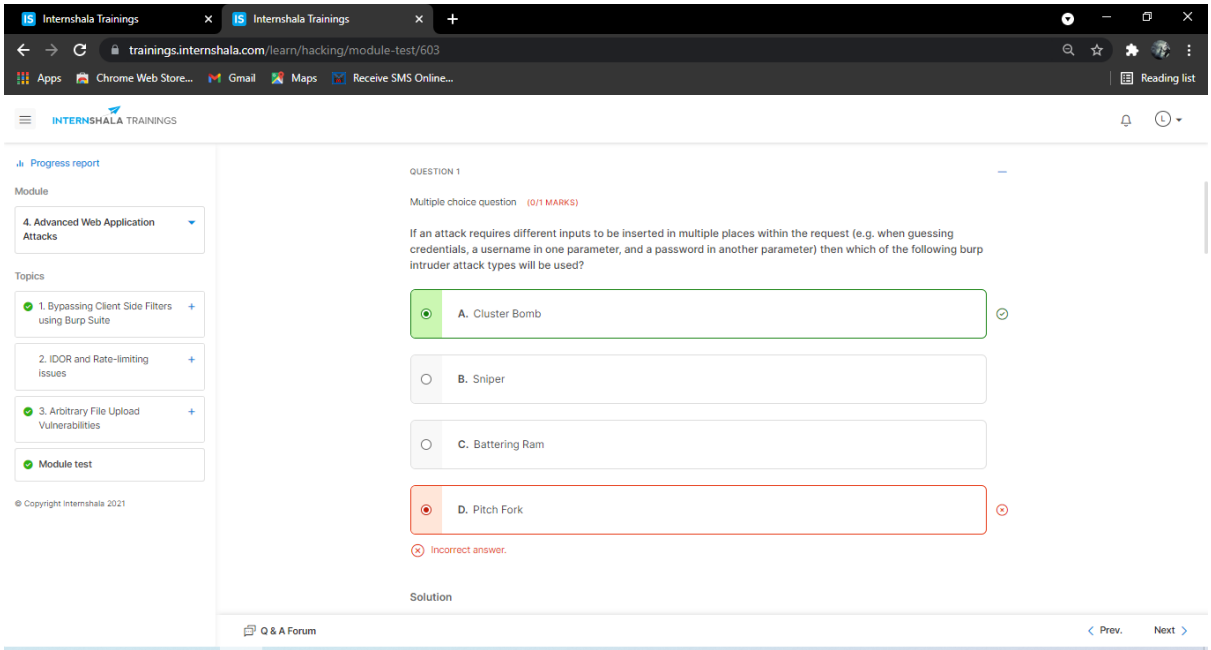
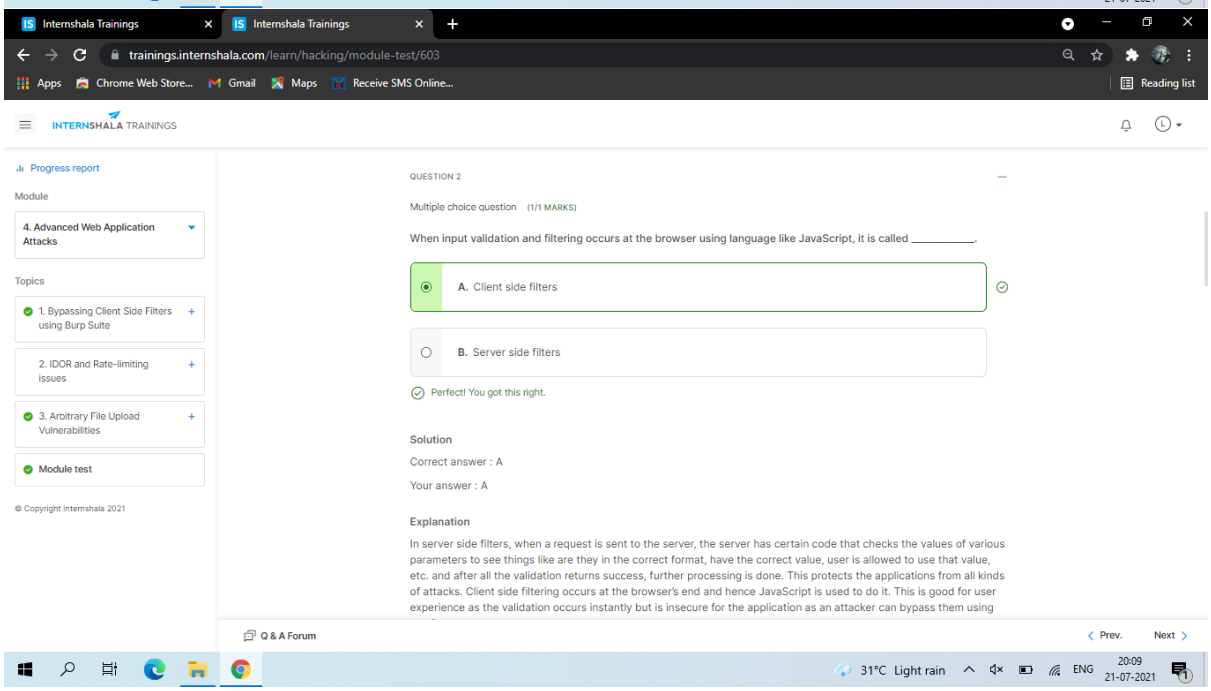
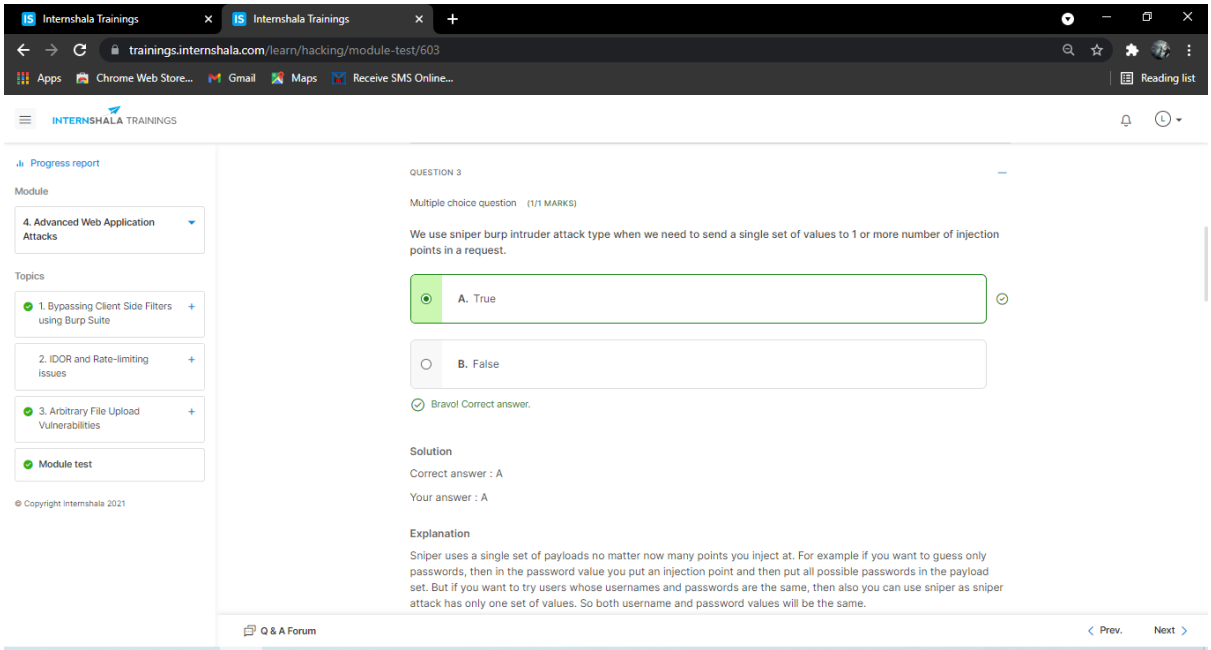
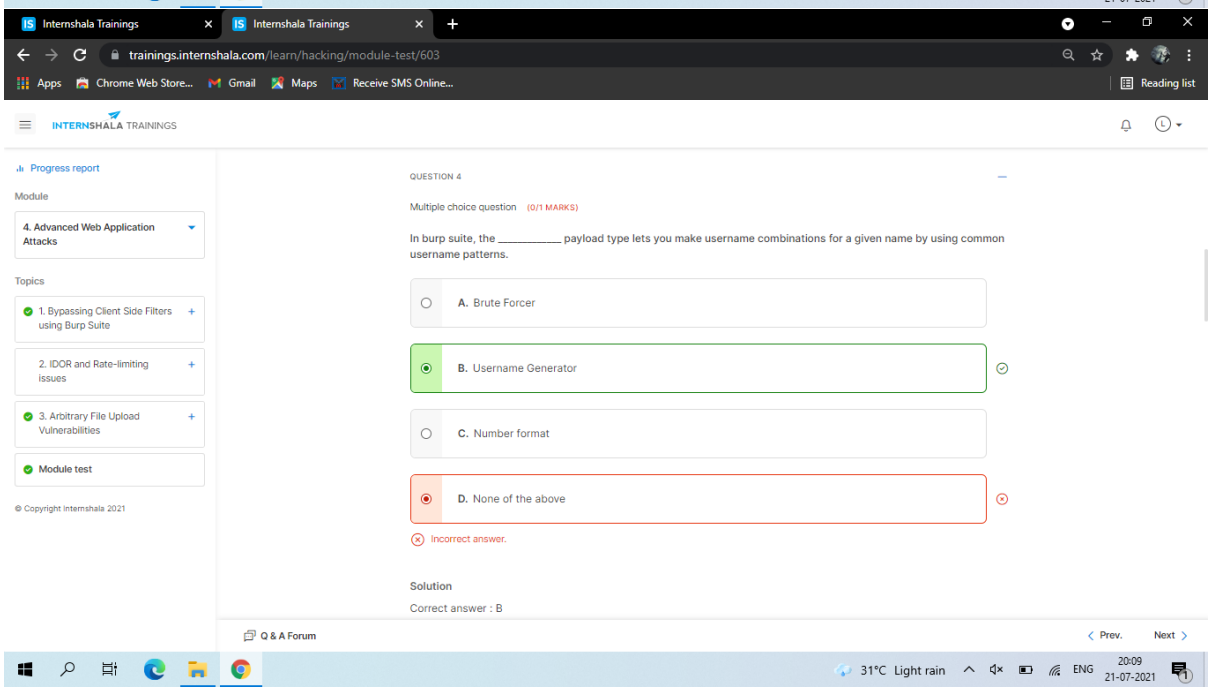
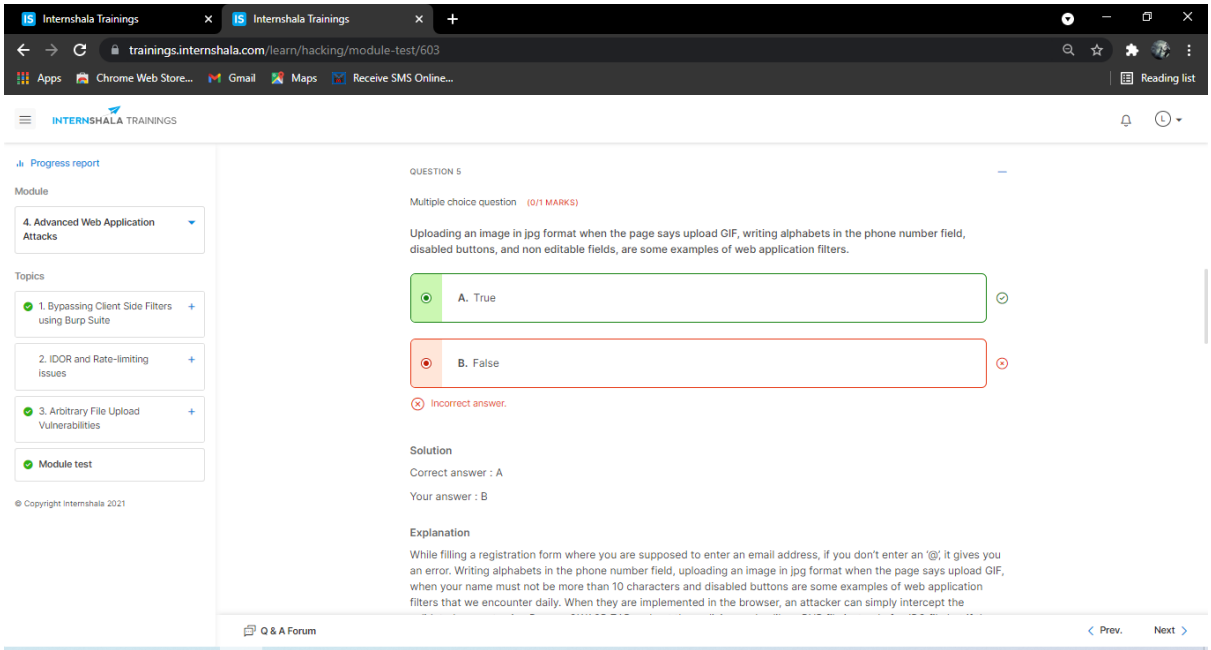
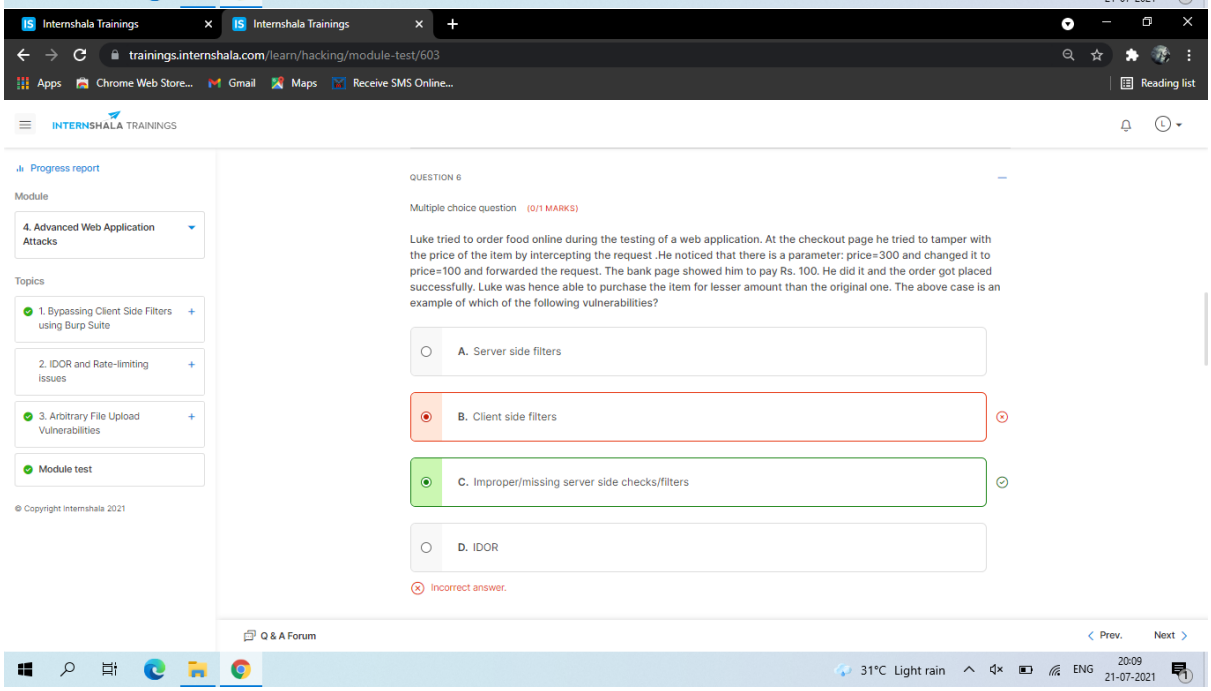

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 1
Multiple choice question (0/1 MARKS)
If an attack requires different inputs to be inserted in multiple places within the request (e.g. when guessing credentials, a username in one parameter, and a password in another parameter) then which of the following burp intruder attack types will be used?
A. Cluster Bomb
B. Sniper
C. Battering Ram
D. Pitch Fork
Incorrect answer.
Solution
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:08
21-07-2021

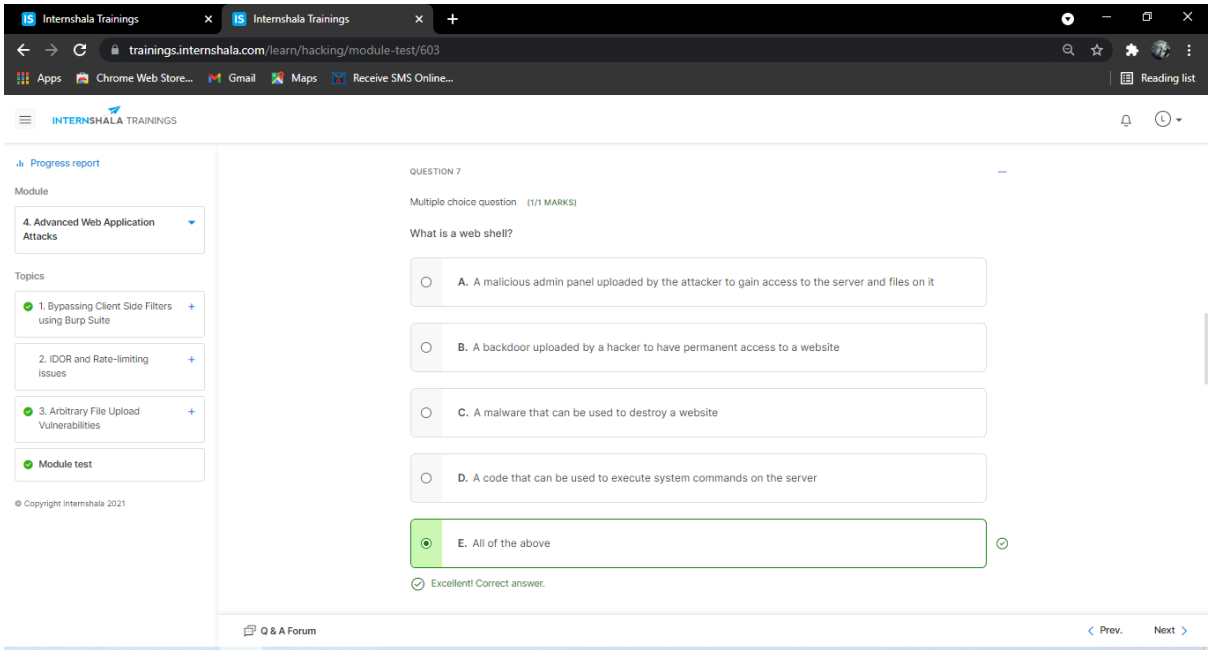

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 2
Multiple choice question (1/1 MARKS)
When input validation and filtering occurs at the browser using language like JavaScript, it is called _____.
A. Client side filters
B. Server side filters
Perfect! You got this right.
Solution
Correct answer : A
Your answer : A
Explanation
In server side filters, when a request is sent to the server, the server has certain code that checks the values of various parameters to see things like are they in the correct format, have the correct value, user is allowed to use that value, etc. and after all the validation returns success, further processing is done. This protects the applications from all kinds of attacks. Client side filtering occurs at the browser's end and hence JavaScript is used to do it. This is good for user experience as the validation occurs instantly but is insecure for the application as an attacker can bypass them using
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021

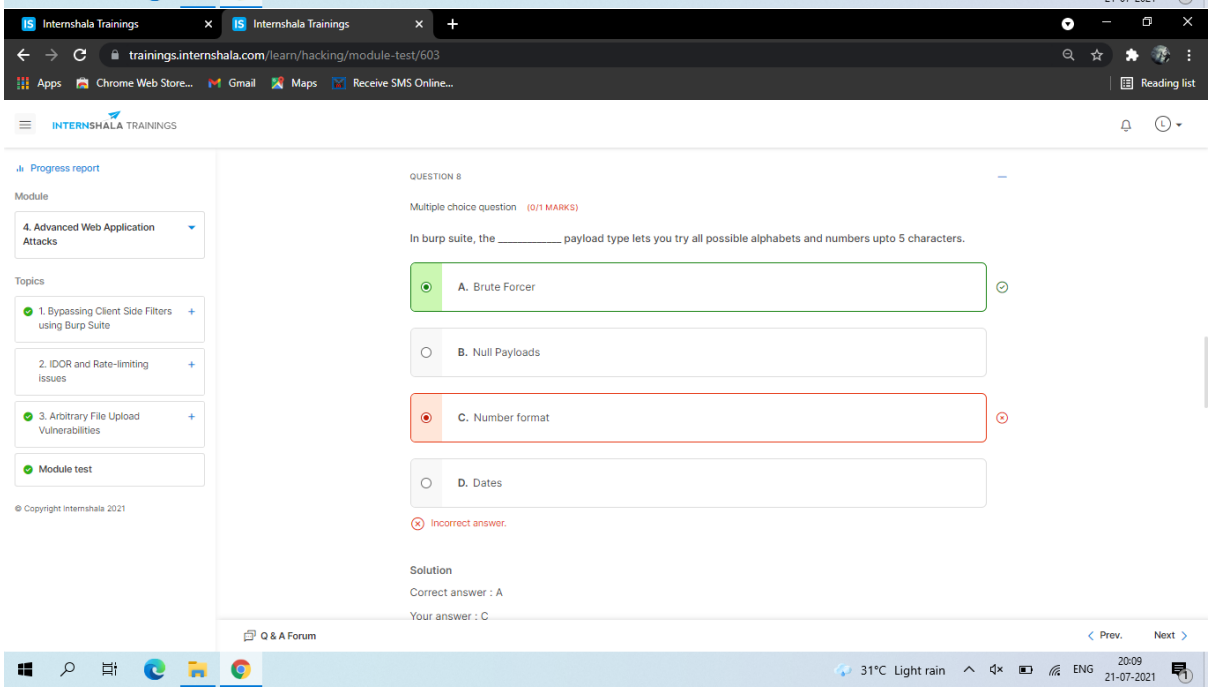

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 3
Multiple choice question (1/1 MARKS)
We use sniper burp intruder attack type when we need to send a single set of values to 1 or more number of injection points in a request.
A. True
B. False
Bravo! Correct answer.
Solution
Correct answer : A
Your answer : A
Explanation
Sniper uses a single set of payloads no matter now many points you inject at. For example if you want to guess only passwords, then in the password value you put an injection point and then put all possible passwords in the payload set. But if you want to try users whose usernames and passwords are the same, then also you can use sniper as sniper attack has only one set of values. So both username and password values will be the same.
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021

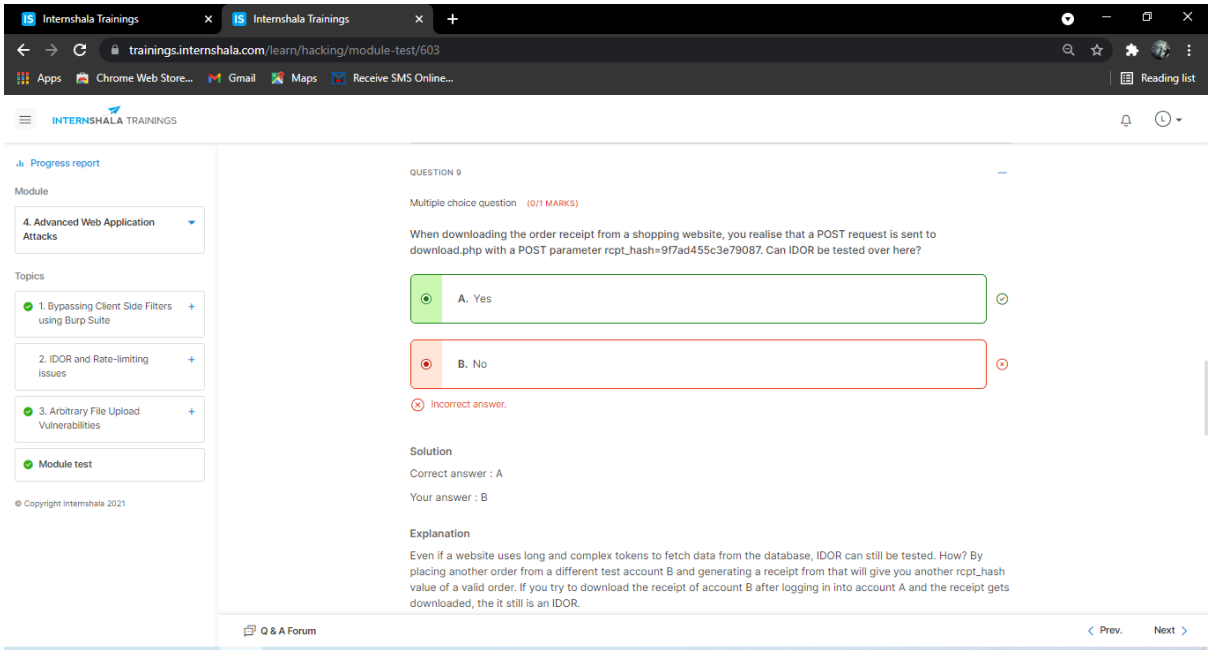

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 4
Multiple choice question (0/1 MARKS)
In burp suite, the _____ payload type lets you make username combinations for a given name by using common username patterns.
A. Brute Forcer
B. Username Generator
C. Number format
D. None of the above
Incorrect answer.
Solution
Correct answer : B
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021

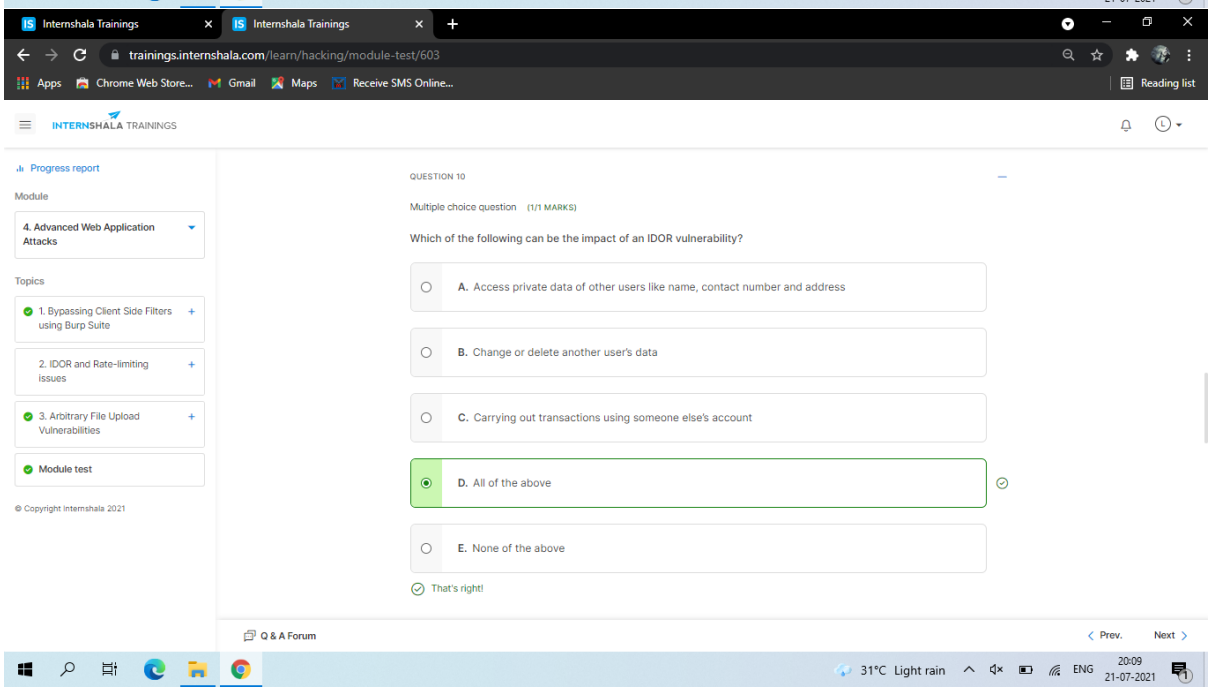

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 5
Multiple choice question (0/1 MARKS)
Uploading an image in jpg format when the page says upload GIF, writing alphabets in the phone number field, disabled buttons, and non editable fields, are some examples of web application filters.
A. True
B. False
Incorrect answer.
Solution
Correct answer : A
Your answer : B
Explanation
While filling a registration form where you are supposed to enter an email address, if you don't enter an '@', it gives you an error. Writing alphabets in the phone number field, uploading an image in jpg format when the page says upload GIF, when your name must not be more than 10 characters and disabled buttons are some examples of web application filters that we encounter daily. When they are implemented in the browser, an attacker can simply intercept the
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021

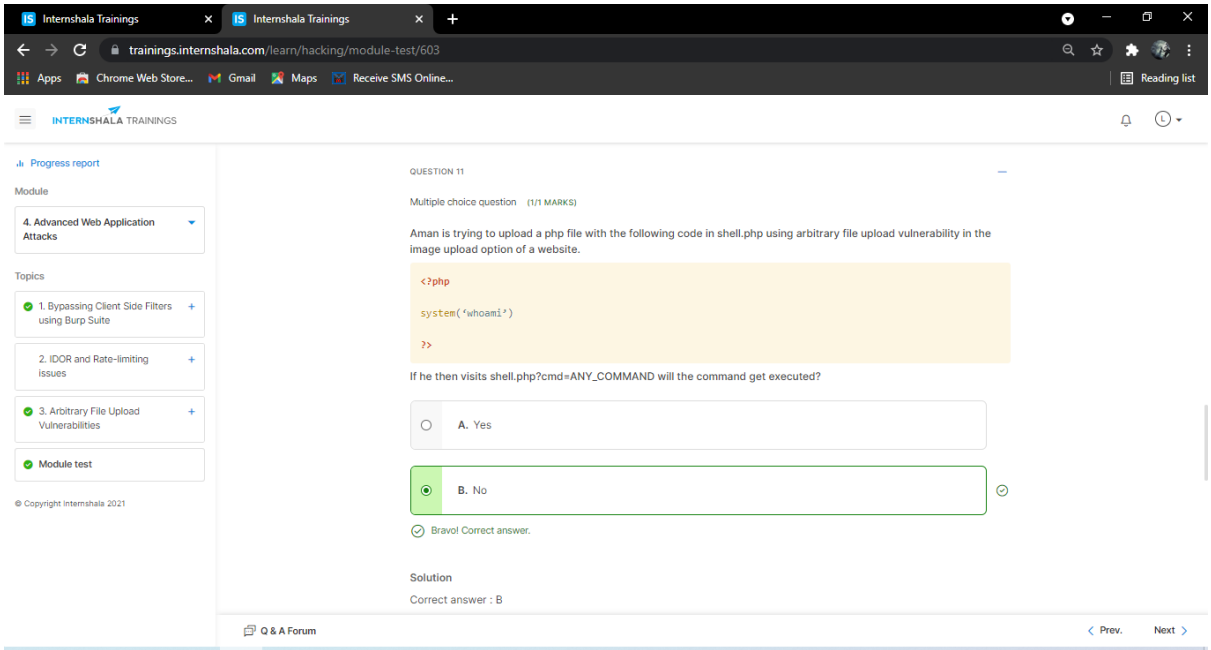

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 6
Multiple choice question (0/1 MARKS)
Luke tried to order food online during the testing of a web application. At the checkout page he tried to tamper with the price of the item by intercepting the request .He noticed that there is a parameter: price=300 and changed it to price=100 and forwarded the request. The bank page showed him to pay Rs. 100. He did it and the order got placed successfully. Luke was hence able to purchase the item for lesser amount than the original one. The above case is an example of which of the following vulnerabilities?
A. Server side filters
B. Client side filters
C. Improper/missing server side checks/filters
D. IDOR
Incorrect answer.
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021

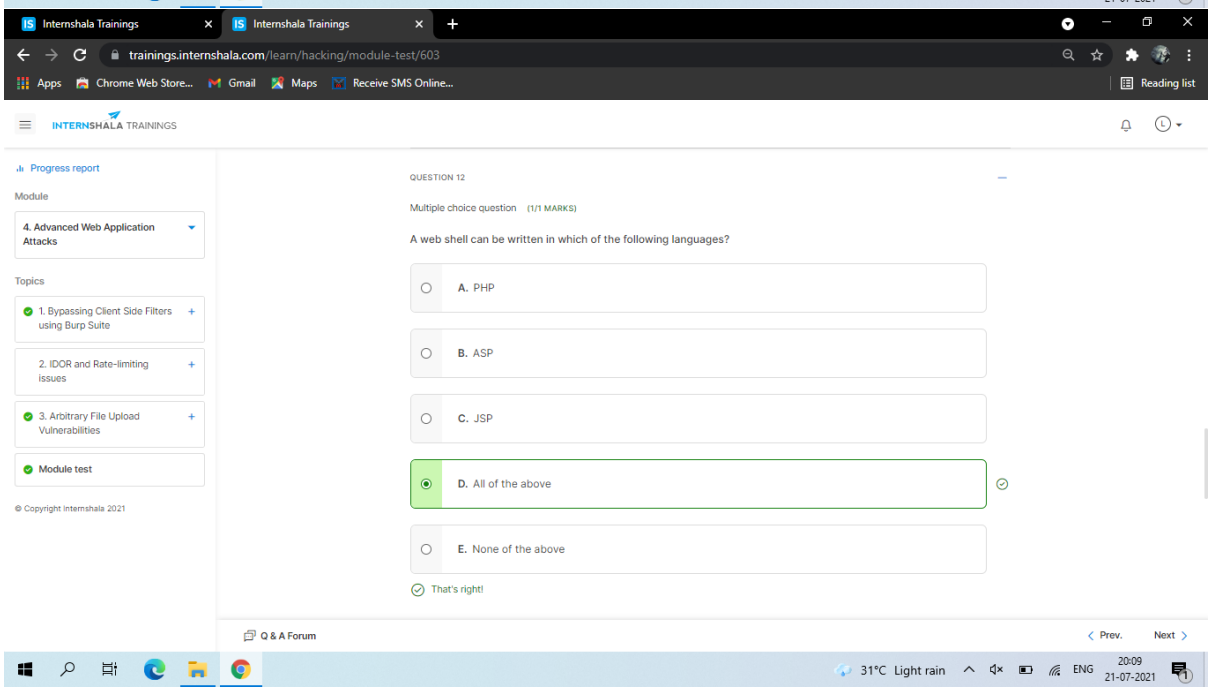

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 7
Multiple choice question (1/1 MARKS)
What is a web shell?
A. A malicious admin panel uploaded by the attacker to gain access to the server and files on it
B. A backdoor uploaded by a hacker to have permanent access to a website
C. A malware that can be used to destroy a website
D. A code that can be used to execute system commands on the server
E. All of the above
Excellent! Correct answer.
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021

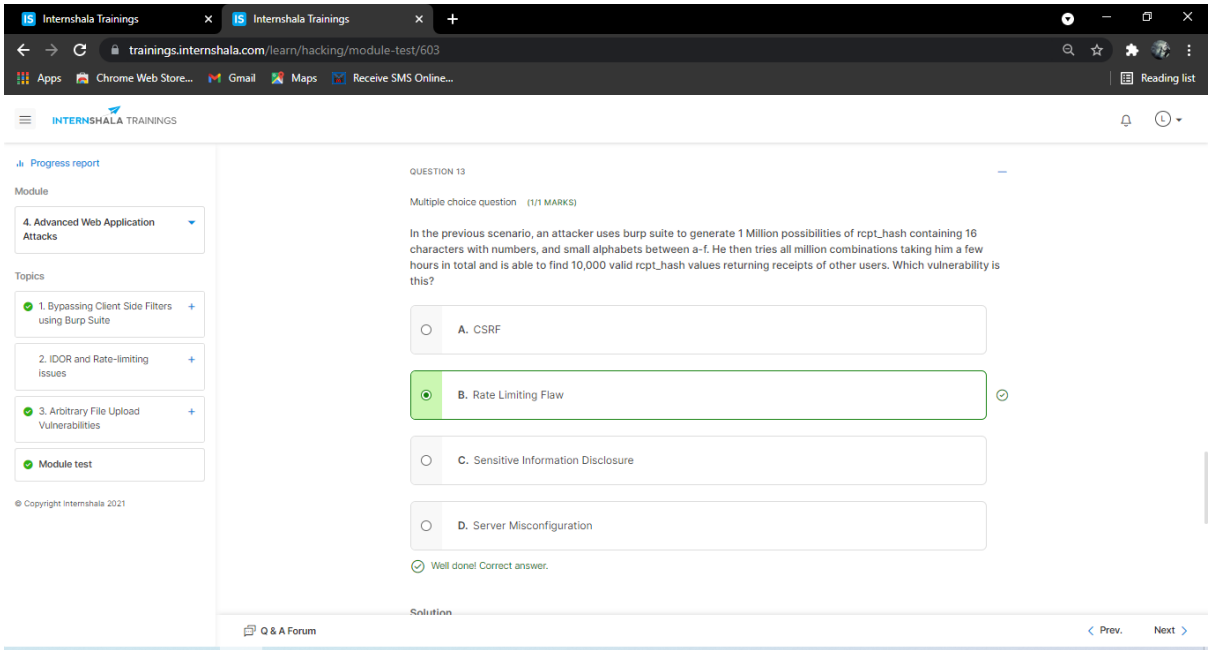

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 8
Multiple choice question (0/1 MARKS)
In burp suite, the _____ payload type lets you try all possible alphabets and numbers upto 5 characters.
A. Brute Forcer
B. Null Payloads
C. Number format
D. Dates
Incorrect answer.
Solution
Correct answer : A
Your answer : C
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021

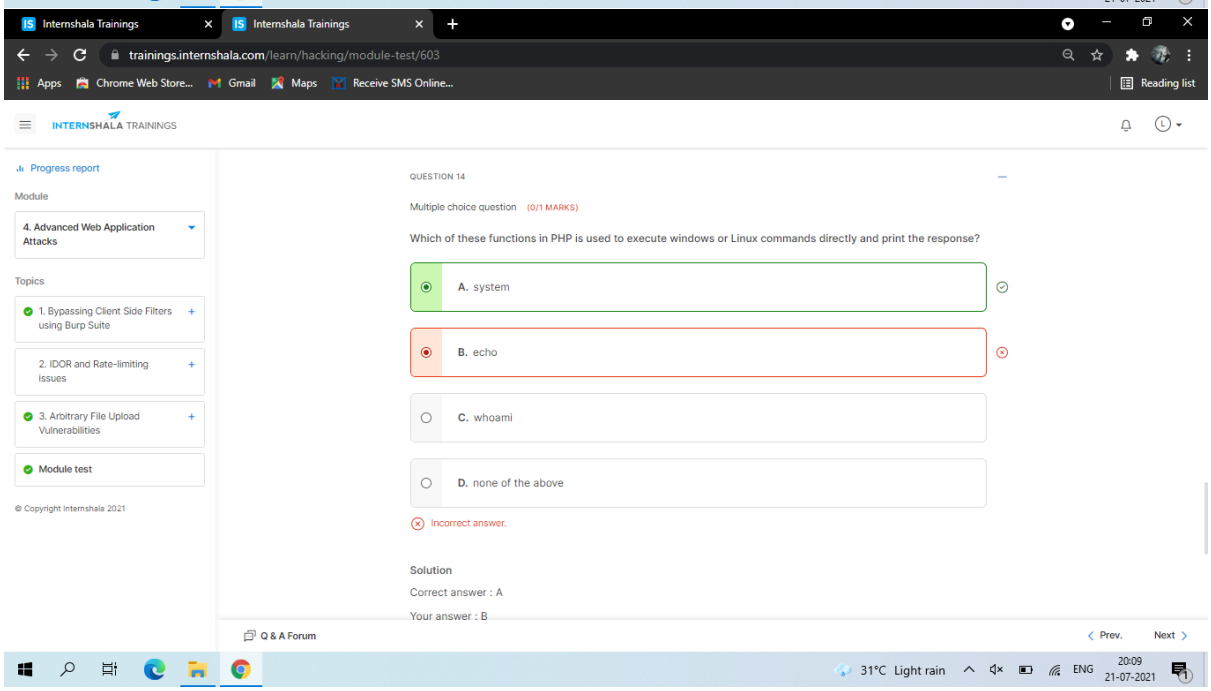

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 9
Multiple choice question (0/1 MARKS)
When downloading the order receipt from a shopping website, you realise that a POST request is sent to download.php with a POST parameter rcpt_hash=9f7ad455c3e79087. Can IDOR be tested over here?
A. Yes
B. No
Incorrect answer.
Solution
Correct answer : A
Your answer : B
Explanation
Even if a website uses long and complex tokens to fetch data from the database, IDOR can still be tested. How? By placing another order from a different test account B and generating a receipt from that will give you another rcpt_hash value of a valid order. If you try to download the receipt of account B after logging in into account A and the receipt gets downloaded, the it still is an IDOR.
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021

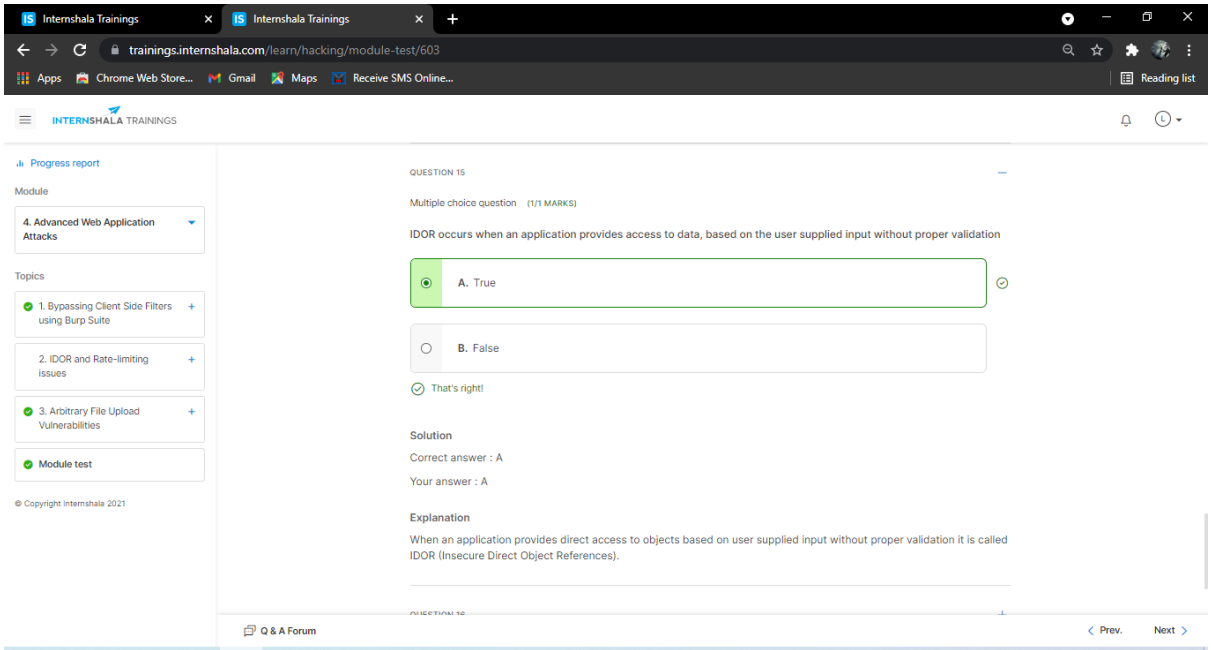

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 10
Multiple choice question (1/1 MARKS)
Which of the following can be the impact of an IDOR vulnerability?
A. Access private data of other users like name, contact number and address
B. Change or delete another user's data
C. Carrying out transactions using someone else's account
D. All of the above
E. None of the above
That's right!
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021

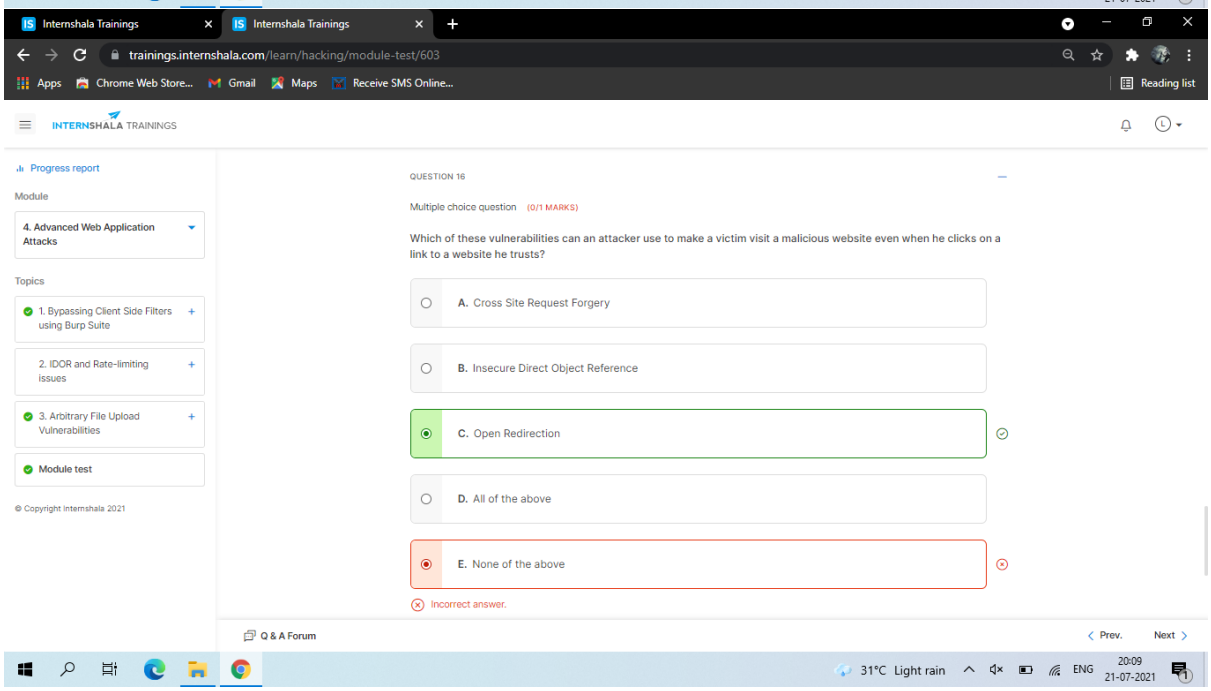

Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 11
Multiple choice question (1/1 MARKS)
Aman is trying to upload a php file with the following code in shell.php using arbitrary file upload vulnerability in the image upload option of a website.
<?php
system('whoami')
?>
If he then visits shell.php?cmd=ANY_COMMAND will the command get executed?
A. Yes
B. No
Bravo! Correct answer.
Solution
Correct answer : B
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 12
Multiple choice question (1/1 MARKS)
A web shell can be written in which of the following languages?
A. PHP
B. ASP
C. JSP
D. All of the above
E. None of the above
That's right!
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 13
Multiple choice question (1/1 MARKS)
In the previous scenario, an attacker uses burp suite to generate 1 Million possibilities of rcpt_hash containing 16 characters with numbers, and small alphabets between a-f. He then tries all million combinations taking him a few hours in total and is able to find 10,000 valid rcpt_hash values returning receipts of other users. Which vulnerability is this?
A. CSRF
B. Rate Limiting Flaw
C. Sensitive Information Disclosure
D. Server Misconfiguration
Well done! Correct answer.
Solution
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 14
Multiple choice question (0/1 MARKS)
Which of these functions in PHP is used to execute windows or Linux commands directly and print the response?
A. system
B. echo
C. whoami
D. none of the above
Incorrect answer.
Solution
Correct answer : A
Your answer : B
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 15
Multiple choice question (1/1 MARKS)
IDOR occurs when an application provides access to data, based on the user supplied input without proper validation
A. True
B. False
That's right!
Solution
Correct answer : A
Your answer : A
Explanation
When an application provides direct access to objects based on user supplied input without proper validation it is called IDOR (Insecure Direct Object References).
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021


Internshala Trainings
Internshala Trainings
trainings.internshala.com/learn/hacking/module-test/603
Apps
Chrome Web Store...
Gmail
Maps
Receive SMS Online...
Reading list
INTERNSHALA TRAININGS
Progress report
Module
4. Advanced Web Application Attacks
Topics
1. Bypassing Client Side Filters using Burp Suite
2. IDOR and Rate-limiting issues
3. Arbitrary File Upload Vulnerabilities
Module test
© Copyright Internshala 2021
QUESTION 16
Multiple choice question (0/1 MARKS)
Which of these vulnerabilities can an attacker use to make a victim visit a malicious website even when he clicks on a link to a website he trusts?
A. Cross Site Request Forgery
B. Insecure Direct Object Reference
C. Open Redirection
D. All of the above
E. None of the above
Incorrect answer.
Q & A Forum
Prev.
Next
31°C Light rain
ENG
20:09
21-07-2021