



**Progress report**

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

QUESTION 1

Multiple choice question (0/1 MARKS)

A pentester found a vulnerability on a website where he can get all the sensitive information of a user by just changing the alphanumeric user ID in the URL. What kind of attack is this?

☒ A. Injection

☐ B. Cross Site Request Forgery (CSRF)

☒ C. Insecure Direct Object References (IDOR)

☐ D. Open Redirection

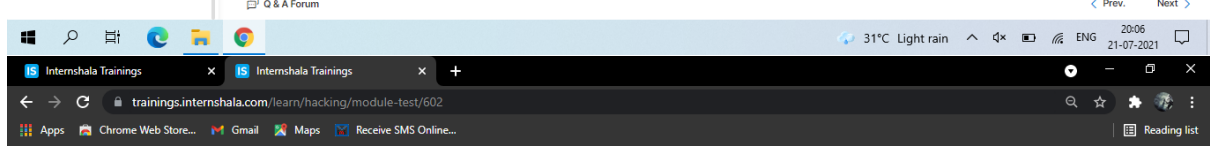
Incorrect answer.

Solution

Correct answer : C

Q & A Forum

Prev. Next >



**Progress report**

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

QUESTION 2

Multiple choice question (1/1 MARKS)

Which of the following is not a valid HTTP method?

☐ A. GET

☐ B. POST

☐ C. PUT

☐ D. DELETE

☒ E. None of the above

That's right!

Q & A Forum

Prev. Next >





INTERNSHALA TRAININGS

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

© Copyright Internshala 2021

QUESTION 3

Multiple choice question (1/1 MARKS)

Broken Authentication and Session Management flaws are the ones which allow the hacker to inject his own code/commands on the web server.

☐ A. True

☒ B. False

Excellent! Correct answer.

Solution

Correct answer : B

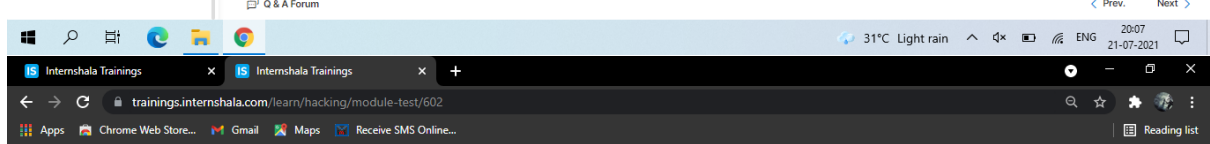
Your answer : B

Explanation

Broken Authentication and Session Management flaws are the ones which allow attackers to bypass authentication mechanisms like Logins and Sessions whereas Injection flaws are the ones that may allow a hacker to inject his own code/commands right on the web server.

Q & A Forum

< Prev. Next >



INTERNSHALA TRAININGS

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

© Copyright Internshala 2021

QUESTION 4

Multiple choice question (1/1 MARKS)

In Burp Suite if we want to see the GUI view of the response, which of the following tabs will be used?

☐ A. HTML

☐ B. HEX

☐ C. History

☒ D. Render

Bravo! Correct answer.

Solution

Correct answer : D

Your answer : D

Q & A Forum

< Prev. Next >

Internshala Trainings

trainings.internshala.com/learn/hacking/module-test/602

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

QUESTION 5

Multiple choice question (1/1 MARKS)

Cookies are basically text files that a website puts in the browser to uniquely identify us.

☒ A. True

☐ B. False

Perfect! You got this right.

Solution

Correct answer : A

Your answer : A

Explanation

Cookies are basically text files that a website puts in the browser to uniquely identify us, maintain our login states and show relevant content. Cookies contain a key-value pair which we can use along with --cookie switch in SQLmap. These cookies can be found in the Cookie Header of the HTTP request.

Q & A Forum

Prev. Next >

31°C Light rain 20:07 21-07-2021

Internshala Trainings

trainings.internshala.com/learn/hacking/module-test/602

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

QUESTION 6

Multiple choice question (0/1 MARKS)

To test SQL injection in a shopping application, you apply a single quote in the "catid" parameter in the URL: x.com/products.php?catid=1&prodid=9 The page throws a PHP error saying there is an issue at line 27. Which of the following injections you CANNOT do?

☒ A. Union Based injection

☐ B. Boolean Based Injection

☒ C. Error Based Injection

☐ D. Time Based Injection

Incorrect answer.

Solution

Prev. Next >

31°C Light rain 20:07 21-07-2021

INTERNSHALA TRAININGS

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

QUESTION 7

Multiple choice question (1/1 MARKS)

In order to do UNION based injections, which of the following conditions should be true?

☐ A. Number of columns selected in the first select query should be same as number of tables selected in the second query

☐ B. Number of tables selected in the first select query should be same as number of columns selected in the second query

☐ C. Number of tables selected in the first select query should be same as number of tables selected in the second query

☒ D. Number of columns selected in the first select query should be same as number of columns selected in the second query

Excellent! Correct answer.

Q & A Forum

Prev. Next >

31°C Light rain 20:07 21-07-2021

INTERNSHALA TRAININGS

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

QUESTION 8

Multiple choice question (1/1 MARKS)

The Content-Type Header in an HTTP request tells about which of the following?

☐ A. The length of the data we are sending

☒ B. The type of information we are sending to the server

☐ C. The type of information we are expecting back from the server

☐ D. The type of encoding in which we are sending the data

That's right!

Solution

Correct answer : B

Your answer : B

Q & A Forum

Prev. Next >

31°C Light rain 20:07 21-07-2021

INTERNSHALA TRAININGS

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

QUESTION 9

Multiple choice question (0/1 MARKS)

Given below is the sql query which is vulnerable to sql injection: SELECT \* FROM students where Id=("\$sid") order by id; The URL is x.com/student.php?sid=1 The sid parameter is sent to the query as shown above. Which of the following payloads will show the student information for all the students?

☐ A. ' or '1'=1

☐ B. \* or "0"=0

☒ C. or 0=0--+

☒ D. None of the above

☐ E. All of the above

Q & A Forum

Prev. Next >

INTERNSHALA TRAININGS

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

QUESTION 10

Multiple choice question (0/1 MARKS)

In SQLmap, to get the column names in the "transactions" table in the "banking\_db" database, which of the following switches will be used?

☐ A. -C -T "transactions" -D "banking\_db"

☒ B. -C --tables "transactions" -dbs "banking\_db"

☒ C. --columns -T "transactions" -D "banking\_db"

☐ D. --columns -T "transactions" -D "banking\_db" --dump

Incorrect answer.

Solution

Correct answer : C

Q & A Forum

Prev. Next >

INTERNSHALA TRAININGS

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

QUESTION 11

Multiple choice question (0/1 MARKS)

Which of the following places should you test an SQL injection for?

☒ A. GET parameters like a,b,c in x.php?a=123&b=bulia&c=u8hqI9

☐ B. HTTP headers like User-Agent: Mozilla Firefox 30.0, windows NT 10.0....

☐ C. Cookies like login in Cookie:PHPSESSID=9128371209jsaiuc89b;login=admin

☐ D. In the URL even if there are no parameters like http://securesite.com/user/bulia

☒ E. All of the above

Incorrect answer.

Q & A Forum

Prev. Next >

INTERNSHALA TRAININGS

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

QUESTION 12

Multiple choice question (1/1 MARKS)

Which of the following HTTP response codes correspond to the "Page Moved to a different location" category?

☐ A. 200

☒ B. 300

☐ C. 400

☐ D. 500

Perfect! You got this right.

Solution

Correct answer : B

Your answer : B

Q & A Forum

Prev. Next >

INTERNSHALA TRAININGS

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

Q & A Forum

QUESTION 13

Multiple choice question (1/1 MARKS)

Vulnerability Assessment is where a hacker or a security expert exploits a vulnerability and tests the damage caused by it.

☐ A. True

☒ B. False

Well done! Correct answer.

Solution

Correct answer : B

Your answer : B

Explanation

Vulnerability Assessment is a phase where a hacker or a security expert tries to find all the vulnerabilities in a system. Whereas, Penetration Testing is where a hacker or a security expert exploits a vulnerability and tests how much damage he can cause using that vulnerability.

Prev. Next >

INTERNSHALA TRAININGS

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

Q & A Forum

QUESTION 14

Multiple choice question (1/1 MARKS)

There is a flaw where an application doesn't handle sensitive data such as passwords, credit card numbers and other personal information securely enough and allows the attacker to steal them while they are being used. What is the name used for this vulnerability?

☐ A. Insecure Direct Object References (IDOR)

☐ B. Broken Authentication and Session Management

☐ C. Missing Function-Level Access Controls

☒ D. Sensitive Data Exposure

Bravo! Correct answer.

Solution

Prev. Next >

INTERNSHALA TRAININGS

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

QUESTION 15

Multiple choice question (1/1 MARKS)

select name from products where id=15 AND (if the 1st character of the password = 'a' then sleep for 10 seconds)---+. This is a syntax for which of the following injections?

☐ A. Error based injections

☒ B. Time based injections

☐ C. Boolean based injections

☐ D. Union based injections

Well done! Correct answer.

Solution

Correct answer : B

Q & A Forum

Prev. Next >

INTERNSHALA TRAININGS

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

QUESTION 16

Multiple choice question (1/1 MARKS)

In SQL map if we want to keep changing the user agent, which of the following switches will we use?

☐ A. --flush

☐ B. --session

☒ C. --random-agent

☐ D. None of the above

Bravo! Correct answer.

Solution

Correct answer : C

Your answer : C

Q & A Forum

Prev. Next >





**Progress report**

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

© Copyright Internshala 2021

**QUESTION 17**

Multiple choice question (0/1 MARKS)

If a hacker finds a website where he can inject code like HTML, JS, directly into the web pages allowing him to control how the website looks to a user, which one of the OWASP top 10 web vulnerability is this?

☒ A. Injection

☐ B. Insecure Direct Object Reference (IDOR)

☐ C. Cross Site Request Forgery (CSRF)

☒ D. Cross Site Scripting (XSS)

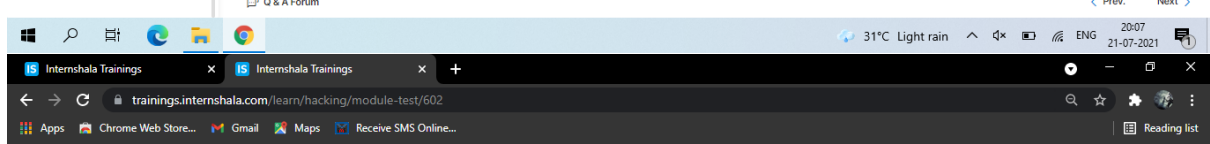
Incorrect answer.

Solution

Correct answer : D

Q & A Forum

Prev. Next >



**Progress report**

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

© Copyright Internshala 2021

**QUESTION 18**

Multiple choice question (0/1 MARKS)

You are using SQLmap to dump the columns "username" and "password" from the "users\_tbl" table in the "main\_db" database. What command will be used for doing this?

☐ A. Sqlmap.py -u "url..." -p "parameter..." --tables="users\_tbl" --columns="username" --column="password" --database="main\_db"

☐ B. Sqlmap.py -u "url..." -p "parameter..." -T "users\_tbl" -C "username" -C "password" -D "main\_db"

☐ C. Sqlmap.py -u "url..." -p "parameter..." -T "users\_tbl" -C "username,password" --dbs "main\_db"

☒ D. Sqlmap.py -u "url..." -p "parameter..." -T "users\_tbl" -C "username,password" --dbs "main\_db" --dump

☒ E. None of the above

Q & A Forum

Prev. Next >



INTERNSHALA TRAININGS

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

© Copyright Internshala 2021

QUESTION 19

Multiple choice question (0/1 MARKS)

To test for \_\_\_\_\_ sql injection we first ask the website to evaluate a true condition (and 1=1) and then a false condition (and 1=0). If the website responds differently to true and false with respect to the response length being 10000 when we ask a true question and 259 when we ask a false question, we can then use that information to ask things we don't know about like if the length of the database name is 6 (and length(database())=6). If the response length is 10000, we would know that the length is indeed 6 else we can try a different length.

☐ A. Union Based injection

☒ B. Boolean Based Injection

☐ C. Error Based Injection

☐ D. Time Based Injection

Incorrect answer.

Q & A Forum

Prev. Next >

INTERNSHALA TRAININGS

Progress report

Module

3. Introduction to Web VAPT, OWASP and SQL Injections

Topics

Part 1

5. GET based SQL Injection- Part 2

6. POST based SQL Injection- Part 1

7. POST based SQL Injection- Part 2

8. Advanced SQL Injections

9. Automating SQL Injections- SQL Map

Module test

© Copyright Internshala 2021

QUESTION 20

Multiple choice question (1/1 MARKS)

In SQLmap we want to check if the DBMS current user is the Administrator of the database. Which of the the following switched will be used for this?

☒ A. --is-dba

☐ B. --current-user

☐ C. --dbs

☐ D. None of the above

That's right!

Solution

Correct answer : A

Q & A Forum

Prev. Next >