Free Questions for CPEH-001 by certsdeals

Shared by Eaton on 07-06-2022

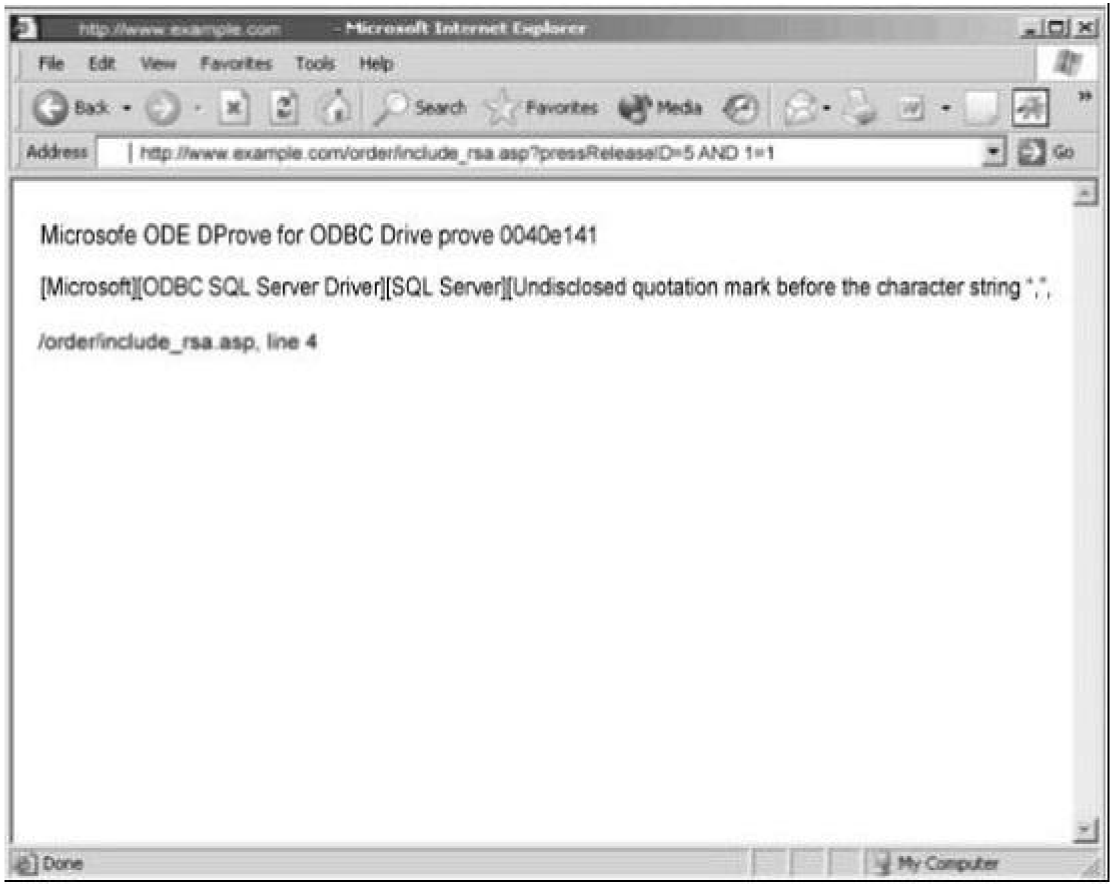
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Exhibit:



http://www.example.com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Done
My Computer

http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND 1=1

Microsofe ODE DProve for ODBC Drive prove 0040e141

[Microsoft][ODBC SQL Server Driver][SQL Server][Undisclosed quotation mark before the character string ',',

/order/include_rsa.asp, line 4

You are conducting pen-test against a company's website using SQL Injection techniques. You enter "anuthing or 1=1-" in the username filed of an authentication form. This is the output returned from the server. What is the next step you should do?

Options:

A) Identify the user context of the web application by running_
http://www.example.com/order/include_rsa_asp?pressReleaseID=5
AND
USER_NAME() = 'dbo'

B) Identify the database and table name by running:
http://www.example.com/order/include_rsa.asp?pressReleaseID=5
AND
ascii(lower(substring((SELECT TOP 1 name FROM sysobjects WHERE
xtype='U'), 1))) > 109

C) Format the C: drive and delete the database by running:
http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND
xp_cmdshell 'format c: /q /yes '; drop database myDB; --

D) Reboot the web server by running:
http://www.example.com/order/include_rsa.asp?pressReleaseID=5
AND xp_cmdshell 'iisreset --reboot'; --

Answer:

A

Question 2

Question Type: **MultipleChoice**

Exhibit:

ettercap --NCLzs --quiet

What does the command in the exhibit do in "Ettercap"?

Options:

A) This command will provide you the entire list of hosts in the LAN

B) This command will check if someone is poisoning you and will report its IP.

C) This command will detach from console and log all the collected passwords from the network to a file.

D) This command broadcasts ping to scan the LAN instead of ARP request of all the subnet IPs.

Answer:

C

Explanation:

-N = NON interactive mode (without ncurses)

-C = collect all users and passwords

-L = if used with -C (collector) it creates a file with all the password sniffed in the session in the form 'YYYYMMDD-collected-pass.log'

-z = start in silent mode (no arp storm on start up)

-s = IP BASED sniffing

--quiet = 'demonize' ettercap. Useful if you want to log all data in background.

Question 3

Question Type: **MultipleChoice**

What file system vulnerability does the following command take advantage of?

type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.exe

Options:

A) HFS

B) ADS

C) NTFS

D) Backdoor access

Answer:

B

Explanation:

ADS (or Alternate Data Streams) is a "feature" in the NTFS file system that makes it possible to hide information in alternate data streams in existing files. The file can have multiple data streams and the data streams are accessed by filename:stream.

Question 4

Question Type: MultipleChoice

Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use * \\10.1.2.3\c$ /user:"Administrator" %%a
```

What is Eve trying to do?

Options:

A) Eve is trying to connect as an user with Administrator privileges

B) Eve is trying to enumerate all users with Administrative privileges

C) Eve is trying to carry out a password crack for user Administrator

D) Eve is trying to escalate privilege of the null user to that of Administrator

Answer:

C

Explanation:

Eve tries to get a successful login using the username Administrator and passwords from the file hackfile.txt.

Question 5

Question Type: MultipleChoice

To what does "message repudiation" refer to what concept in the realm of email security?

Options:

A) Message repudiation means a user can validate which mail server or servers a message was passed through.

B) Message repudiation means a user can claim damages for a mail message that damaged their reputation.

C) Message repudiation means a recipient can be sure that a message was sent from a particular person.

D) Message repudiation means a recipient can be sure that a message was sent from a certain host.

E) Message repudiation means a sender can claim they did not actually send a particular message.

Answer:

E

Explanation:

A quality that prevents a third party from being able to prove that a communication between two other parties ever took place. This is a desirable quality if you do not want your communications to be traceable.

Non-repudiation is the opposite quality---a third party can prove that a communication between two other parties took place. Non-repudiation is desirable if you want to be able to trace your communications and prove that they occurred. Repudiation -- Denial of message submission or delivery.

Question 6

Question Type: **MultipleChoice**

What does the term ''Ethical Hacking'' mean?

Options:

A) Someone who is hacking for ethical reasons.

B) Someone who is using his/her skills for ethical reasons.

C) Someone who is using his/her skills for defensive purposes.

D) Someone who is using his/her skills for offensive purposes.

Answer:

C

Explanation:

Ethical hacking is only about defending yourself or your employer against malicious persons by using the same techniques and skills.

Question 7

Question Type: MultipleChoice

What is the main difference between a "Normal" SQL Injection and a "Blind" SQL Injection vulnerability?

Options:

A) The request to the web server is not visible to the administrator of the vulnerable application.

B) The attack is called "Blind" because, although the application properly filters user input, it is still vulnerable to code injection.

C) The successful attack does not show an error message to the administrator of the affected application.

D) The vulnerable application does not display errors with information about the injection results to the attacker.

Answer:

D

Question 8

Question Type: **MultipleChoice**

What is the outcome of the comm"nc -l -p 2222 | nc 10.1.0.43 1234"?

Options:

A) Netcat will listen on the 10.1.0.43 interface for 1234 secondson port 2222.

B) Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43port 1234.

C) Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.

D) Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43.

Answer:

B

Question 9

Question Type: MultipleChoice

What will the following command produce on a website's login page if executed successfully? SELECT email, passwd, login_id, full_name FROM members WHERE email = 'someone@somewhere.com'; DROP TABLE members; --'

Options:

A) This code will insert the someone@somewhere.com email address into the members table.

B) This command will delete the entire members table.

C) It retrieves the password for the first user in the members table.

D) This command will not produce anything since the syntax is incorrect.

Answer:

B

Question 10

Question Type: **MultipleChoice**

Choose one of the following pseudo codes to describe this statement:

"If we have written 200 characters to the buffer variable, the stack should stop because it cannot hold any more data."

Options:

A) If (I > 200) then exit (1)

B) If (I < 200) then exit (1)

C) If (I <= 200) then exit (1)

D) If (I >= 200) then exit (1)

Answer:

D

20%
DISCOUNT