412-79V10$^{Q\&As}$

EC-Council Certified Security Analyst (ECSA) V10

Pass EC-COUNCIL 412-79V10 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

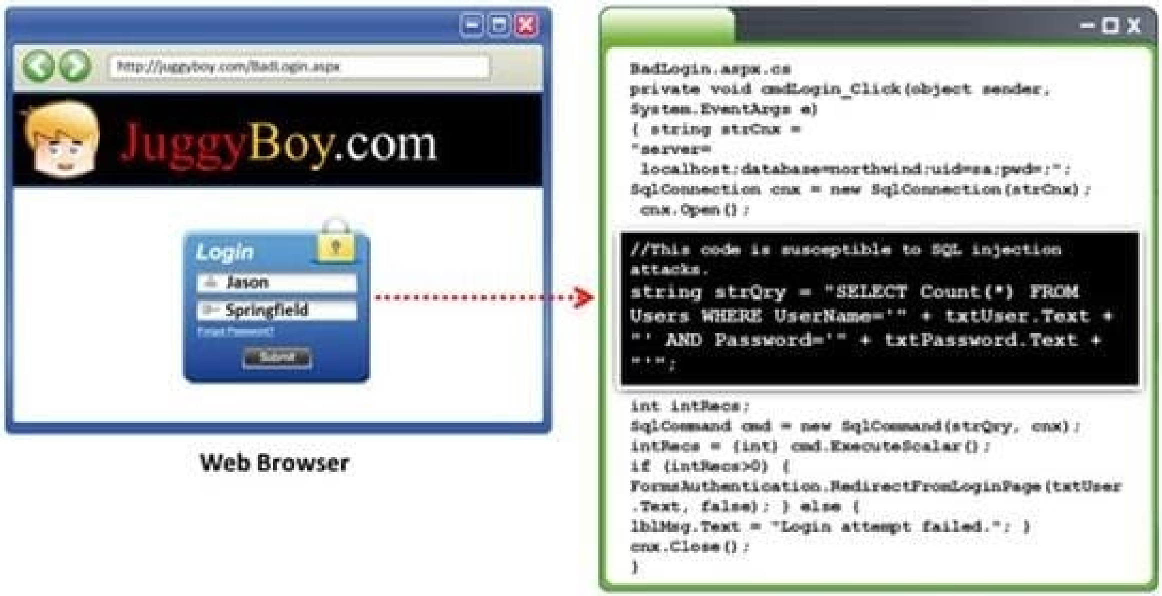
https://www.leads4pass.com/412-79v10.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings. Black-box testing is used to detect issues in SQL statements and to detect SQL injection vulnerabilities.



Web Browser

```
BadLogin.aspx.cs
private void cmdLogin_Click(object sender,
System.EventArgs e)
{ string strCnx =
"server=
 localhost;database=northwind;uid=sa;pwd=;";
SqlConnection cnx = new SqlConnection(strCnx);
 cnx.Open();
//This code is susceptible to SQL injection
attacks.
string strQry = "SELECT Count(*) FROM
Users WHERE UserName='" + txtUser.Text +
"' AND Password='" + txtPassword.Text +
"'";
int intRecs;
SqlCommand cmd = new SqlCommand(strQry, cnx);
intRecs = (int) cmd.ExecuteScalar();
if (intRecs>0) {
FormsAuthentication.RedirectFromLoginPage(txtUser
.Text, false); } else {
lblMsg.Text = "Login attempt failed."; }
cnx.Close();
}
```

Server Side Code (BadLogin.aspx)

Most commonly, SQL injection vulnerabilities are a result of coding vulnerabilities during the Implementation/Development phase and will likely require code changes.

Pen testers need to perform this testing during the development phase to find and fix the SQL injection vulnerability.

What can a pen tester do to detect input sanitization issues?

A. Send single quotes as the input data to catch instances where the user input is not sanitized

B. Send double quotes as the input data to catch instances where the user input is not sanitized

C. Send long strings of junk data, just as you would send strings to detect buffer overruns

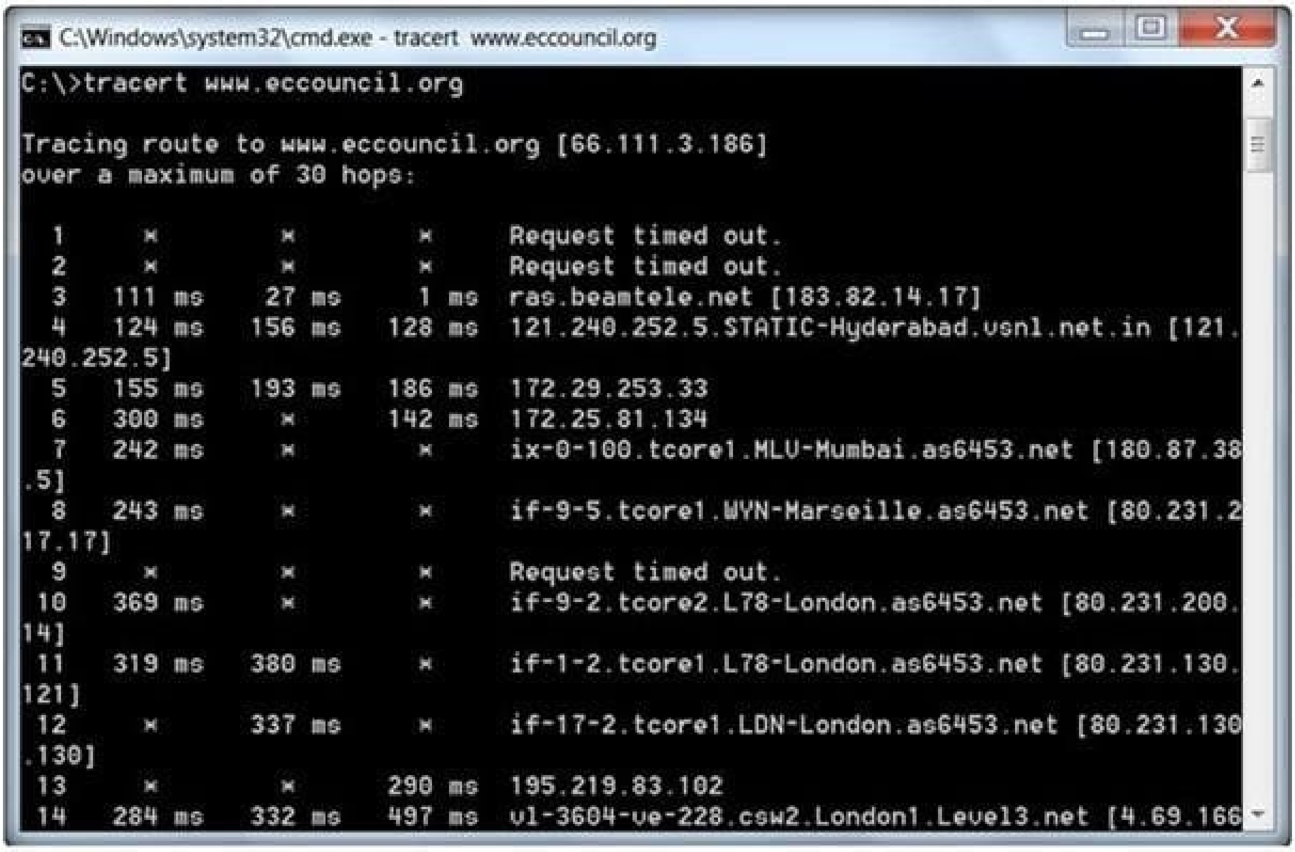
D. Use a right square bracket (the "]" character) as the input data to catch instances where the user input is used as part of a SQL identifier without any input sanitization

Correct Answer: D

QUESTION 2

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of three Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host.

The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.



```
C:\>tracert www.eccouncil.org

Tracing route to www.eccouncil.org [66.111.3.186]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     *        *        *     Request timed out.
  3   111 ms    27 ms     1 ms  ras.beamtele.net [183.82.14.17]
  4   124 ms   156 ms   128 ms  121.240.252.5.STATIC-Hyderabad.vsnl.net.in [121.
240.252.5]
  5   155 ms   193 ms   186 ms  172.29.253.33
  6   300 ms     *      142 ms  172.25.81.134
  7   242 ms     *        *     ix-0-100.tcore1.MLU-Mumbai.as6453.net [180.87.38
.5]
  8   243 ms     *        *     if-9-5.tcore1.WYN-Marseille.as6453.net [80.231.2
17.17]
  9     *        *        *     Request timed out.
 10   369 ms     *        *     if-9-2.tcore2.L78-London.as6453.net [80.231.200.
14]
 11   319 ms   380 ms     *     if-1-2.tcore1.L78-London.as6453.net [80.231.130.
121]
 12     *      337 ms     *     if-17-2.tcore1.LDN-London.as6453.net [80.231.130
.130]
 13     *        *      290 ms  195.219.83.102
 14   284 ms   332 ms   497 ms  vl-3604-ve-228.csw2.London1.Level3.net [4.69.166
```

During routing, each router reduces packets\\' TTL value by

B. 1

C. 4

D. 2

Correct Answer: B

Reference: http://www.packetu.com/2009/10/09/traceroute-through-the-asa/

QUESTION 3

Which of the following defines the details of services to be provided for the client\\'s organization and the list of services required for performing the test in the organization?

A. Draft

B. Report

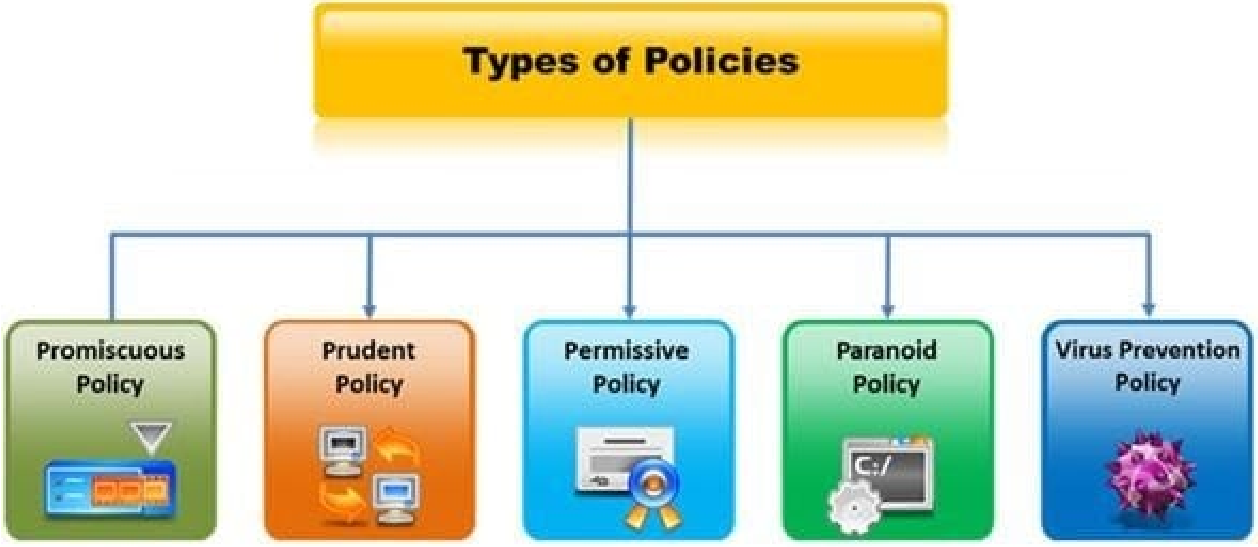
C. Requirement list

D. Quotation

Correct Answer: D

QUESTION 4

Which type of security policy applies to the below configuration? i)Provides maximum security while allowing known, but necessary, dangers ii)All services are blocked; nothing is allowed iii)Safe and necessary services are enabled individually iv)Non-essential services and procedures that cannot be made safe are NOT allowed v)Everything is logged



A. Paranoid Policy

B. Prudent Policy

C. Permissive Policy

D. Promiscuous Policy

Correct Answer: B

QUESTION 5

A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the table inside the database using the below query and finds the table:

http://juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype=\\'U\\')=3) WAITFOR DELAY \\'00:00:10\\'-

http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY \\'00:00:10\\'-

http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY \\'00:00:10\\'-

http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY \\'00:00:10\\'-

What is the table name?

A. CTS

B. QRT

C. EMP

D. ABC

Correct Answer: C