CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

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

https://www.leads4pass.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

HOTSPOT

The developers recently deployed new code to three web servers. A daily automated external device scan report shows server vulnerabilities that are failing items according to PCI DSS.

If the vulnerability is not valid, the analyst must take the proper steps to get the scan clean.

If the vulnerability is valid, the analyst must remediate the finding.

After reviewing the information provided in the network diagram, select the STEP 2 tab to complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.

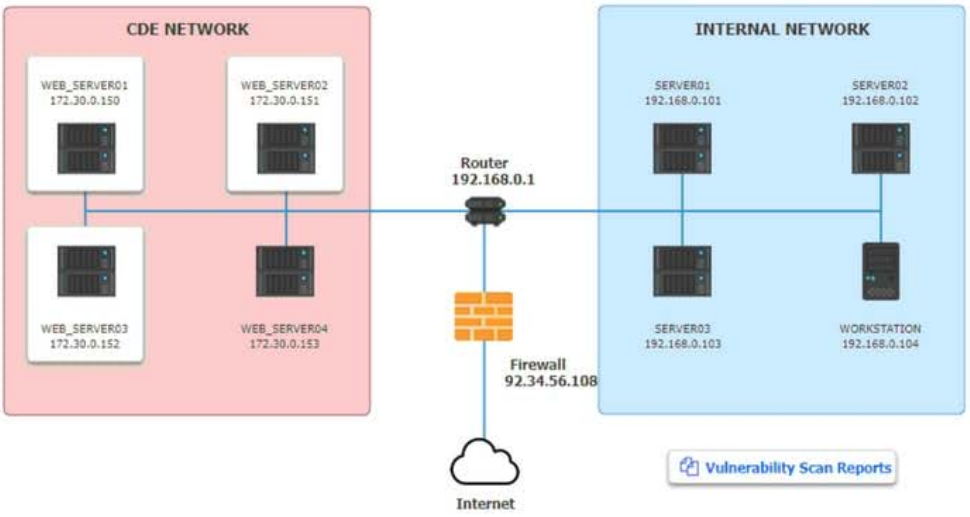
INSTRUCTIONS

STEP 1: Review the information provided in the network diagram.

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

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

Step 1



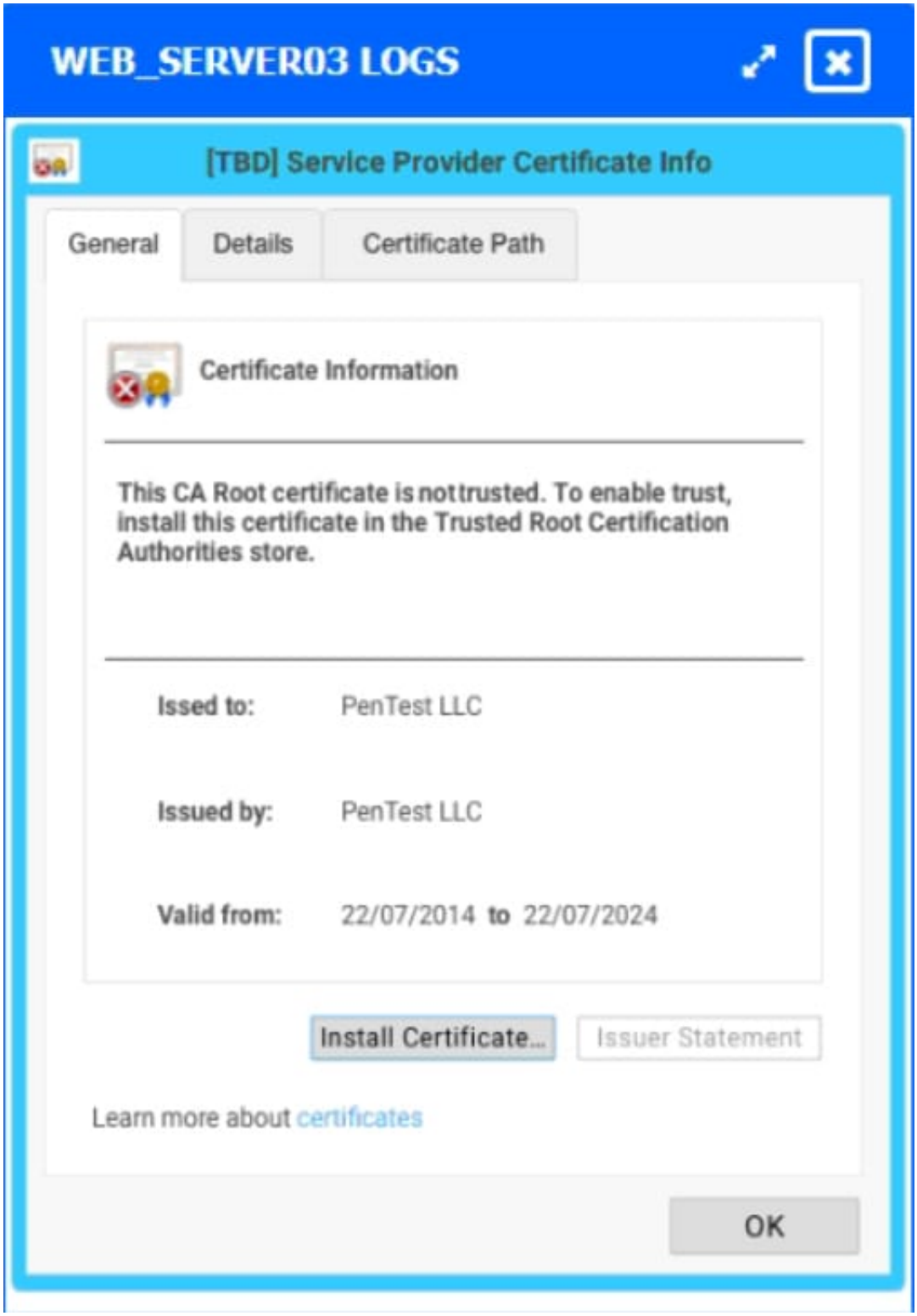
WEB_SERVER01 LOGS

```
While logged in to the web portal (172.30.0.150) from the workstation (192.168.0.104), perform an account
password change.  This process requires you to reenter the original password and enter a new password
twice.


192.168.0.104    172.30.0.151    TLSv1     733    Application Data
172.30.0.151     192.168.0.104   TLSv1    1107    Application Data
192.168.0.104    172.30.0.151    TCP        66    44088 > https   [ACK]  Seq=1510 Ack=12723  Win=42368
192.168.0.104    172.30.0.150    HTTP      608    GET  /verifpwd.learn?URL=AV5FPSHV2Ereal&SSL=83n28x
172.30.0.151     192.168.0.104   TCP        66    http > 60928  [ACK]  Seq=622  Ack=847  Win=5154  Len=…


Frame  4021:  114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src:  Vmware 00:03:22  (00:50:56:00:03:22),  Dst:  PaloAlto_39:1c:30  (00:1b:17:39:1c:30)
Internet Protocol Version 4, Src:  192.168.0.104 (192.168.0.104), Dst:  172.30.0.150 (172.30.0.150)
[2 Reassembled  TCP  Segments  (1496 bytes):  #4820(1448), #4821(48)]
Hypertext  Transfer  Protocol
    GET  /verifpwd.learn?URL=AV5FPSHV2Ereal&SSL=83n28x
    Host:  XXXXX
    User – Agent:  Mozilla/5.0  (x11;  Linux  x86_64;  rv:18.0)  Gecko/20100101  Firefox/18.0
Iceweasel/18.0.1
    Accept:  text/html, application/xhtml+xml,application/xml;q=0.9,*/*;q=0
    Accept-Language:  en=US,en;q=0.5
    Accept-Encoding:  gzip,  deflate
    Referer:  http:/XXXXX/Shared/Portal/CustomProfiles/A_Profile.real
    [truncated]  Cookie:  ASPSESSIONIDQABRBT BC=HEJCAHEDJPK08CEP; ZZZ; ECUSERPROPS=
    Connection:  keep alive
    Content-Type:  application/x-www-form-urlendcoded
    Content-Length:  121

    [Full  request  URI:  http//XXX/Shared/Portal/CustomProfiles/PostProfile.real?47=25378158]
Line-based   text  data:  application/x-www-form-urlencoded
    EMAIL=someone@cloud.org m&PASSold=PassWord1  m&PASSnew1=PassWord2  m&PASSnewv=PassWord2
```

WEB_SERVER02 LOGS

Cookies

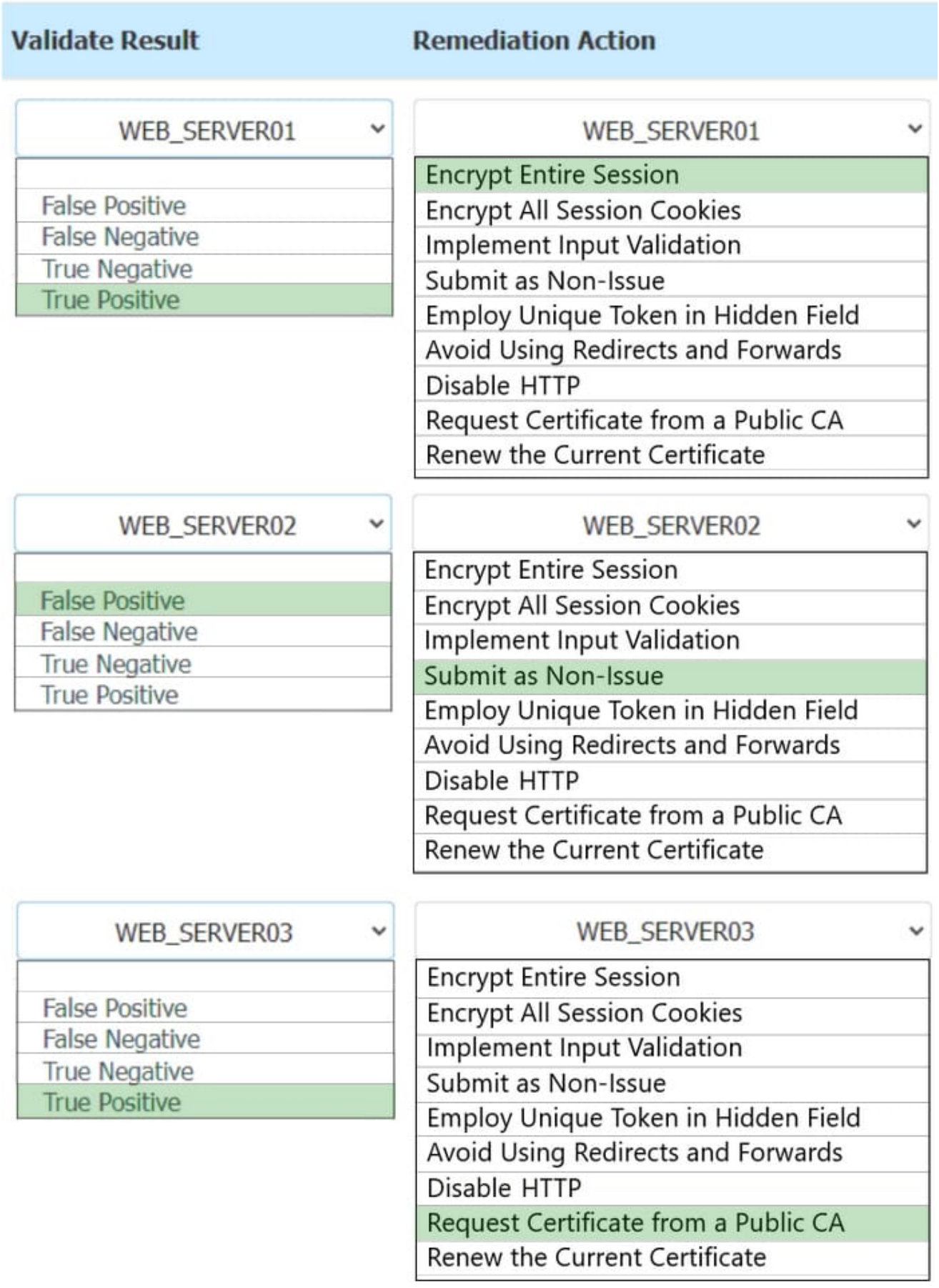
Name	Value	Domain	...	Expires / Max Age	...	Http	Secure
_utma	250288278.1028202552.1383963...	yourcompany.com	...	Thu, 05 Nov 2015 23:21:28 GMT	...		X
_utmb	250288278.2.10.1383693377	yourcompany.com	...	Tue, 05 Nov 2013 23:51:28 GMT	...		X
_utmc	250288278	yourcompany.com	...	Session	...		X
_utmz	250288278.1383693377.1.1.utmcs	yourcompany.com	...	Thu, 08 May 2014 11:21:28 GMT	...		X



Hot Area:

Correct Answer:

Validate Result	Remediation Action
WEB_SERVER01	WEB_SERVER01
False Positive	Encrypt Entire Session
False Negative	Encrypt All Session Cookies
True Negative	Implement Input Validation
True Positive	Submit as Non-Issue
	Employ Unique Token in Hidden Field
	Avoid Using Redirects and Forwards
	Disable HTTP
	Request Certificate from a Public CA
	Renew the Current Certificate
WEB_SERVER02	WEB_SERVER02
False Positive	Encrypt Entire Session
False Negative	Encrypt All Session Cookies
True Negative	Implement Input Validation
True Positive	Submit as Non-Issue
	Employ Unique Token in Hidden Field
	Avoid Using Redirects and Forwards
	Disable HTTP
	Request Certificate from a Public CA
	Renew the Current Certificate
WEB_SERVER03	WEB_SERVER03
False Positive	Encrypt Entire Session
False Negative	Encrypt All Session Cookies
True Negative	Implement Input Validation
True Positive	Submit as Non-Issue
	Employ Unique Token in Hidden Field
	Avoid Using Redirects and Forwards
	Disable HTTP
	Request Certificate from a Public CA
	Renew the Current Certificate


Validate Result
Remediation Action
WEB_SERVER01
False Positive
False Negative
True Negative
True Positive
WEB_SERVER01
Encrypt Entire Session
Encrypt All Session Cookies
Implement Input Validation
Submit as Non-Issue
Employ Unique Token in Hidden Field
Avoid Using Redirects and Forwards
Disable HTTP
Request Certificate from a Public CA
Renew the Current Certificate
WEB_SERVER02
False Positive
False Negative
True Negative
True Positive
WEB_SERVER02
Encrypt Entire Session
Encrypt All Session Cookies
Implement Input Validation
Submit as Non-Issue
Employ Unique Token in Hidden Field
Avoid Using Redirects and Forwards
Disable HTTP
Request Certificate from a Public CA
Renew the Current Certificate
WEB_SERVER03
False Positive
False Negative
True Negative
True Positive
WEB_SERVER03
Encrypt Entire Session
Encrypt All Session Cookies
Implement Input Validation
Submit as Non-Issue
Employ Unique Token in Hidden Field
Avoid Using Redirects and Forwards
Disable HTTP
Request Certificate from a Public CA
Renew the Current Certificate

QUESTION 2

A security analyst is writing a shell script to identify IP addresses from the same country. Which of the following functions would help the analyst achieve the objective?

A. function w() { info=$(pi" " }

B. function x() { info=$(geoipl" }

C. function y() { info=$(dig -x $1 | grep PTR | tail -n 1) andand " }

D. function z() { info=$(tracer""" }

Correct Answer: B

The function that would help the analyst identify IP addresses from the same country is:

function x() { info=$(geoiplookup $" }

This function takes an IP address as an argument and uses the geoiplookup command to get the geographic location information associated with the IP address, such as the country name, country code, region, city, or latitude and longitude.

The function then prints the IP address and the geographic location information, which can help identify any IP addresses that belong to the same country.

QUESTION 3

A security analyst is analyzing the following output from the Spider tab of OWASP ZAP after a vulnerability scan was completed: Which of the following options can the analyst conclude based on the provided output?

METHOD	URI	FLAG
GET	http://comptia.com	Seed
GET	http://comptia.com/robots.txt	Seed
GET	http://comptia.com/sitemap.xml	Seed
GET	http://localhost	Out of scope

A. The scanning vendor used robots to make the scanning job faster

B. The scanning job was successfully completed, and no vulnerabilities were detected

C. The scanning job did not successfully complete due to an out of scope error

D. The scanner executed a crawl process to discover pages to be assessed

Correct Answer: D

The output shows the result of usi"fter a vulnerability scan was completed. The Spider tab allows users to crawl web applications and discover pages and resources that can be assessed for vulnerabilities. The output shows that the

scanner

discovered various pages under different directories, such as /admin/, /blog/, /contact/, etc., as well as some parameters and forms that can be used for testing inputs and outputs. CompTIA Cybersecurity Analyst (CySA+) Certification Exam

Objectives (CS0-002), page 9;

https://www.zaproxy.org/docs/desktop/start/features/spider/

QUESTION 4

A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities:

Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerability research activity

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority. Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

A. InLoud: Cobain: Yes Grohl: No Novo: Yes Smear: Yes Channing: No

B. TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No

C. ENameless: Cobain: Yes Grohl: No

Novo: Yes

Smear: No

Channing: No

D. PBleach: Cobain: Yes Grohl: No Novo: No Smear: No Channing: Yes

Correct Answer: B

The vulnerability that should be patched first, given the above third-party scoring system, is:

TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear

and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

QUESTION 5

An analyst receives threat intelligence regarding potential attacks from an actor with seemingly unlimited time and resources. Which of the following best describes the threat actor attributed to the malicious activity?

A. Insider threat

B. Ransomware group

C. Nation-state

D. Organized crime

Correct Answer: C