



Free Questions for 350-201 by certsdeals

Shared by Barron on 12-12-2023

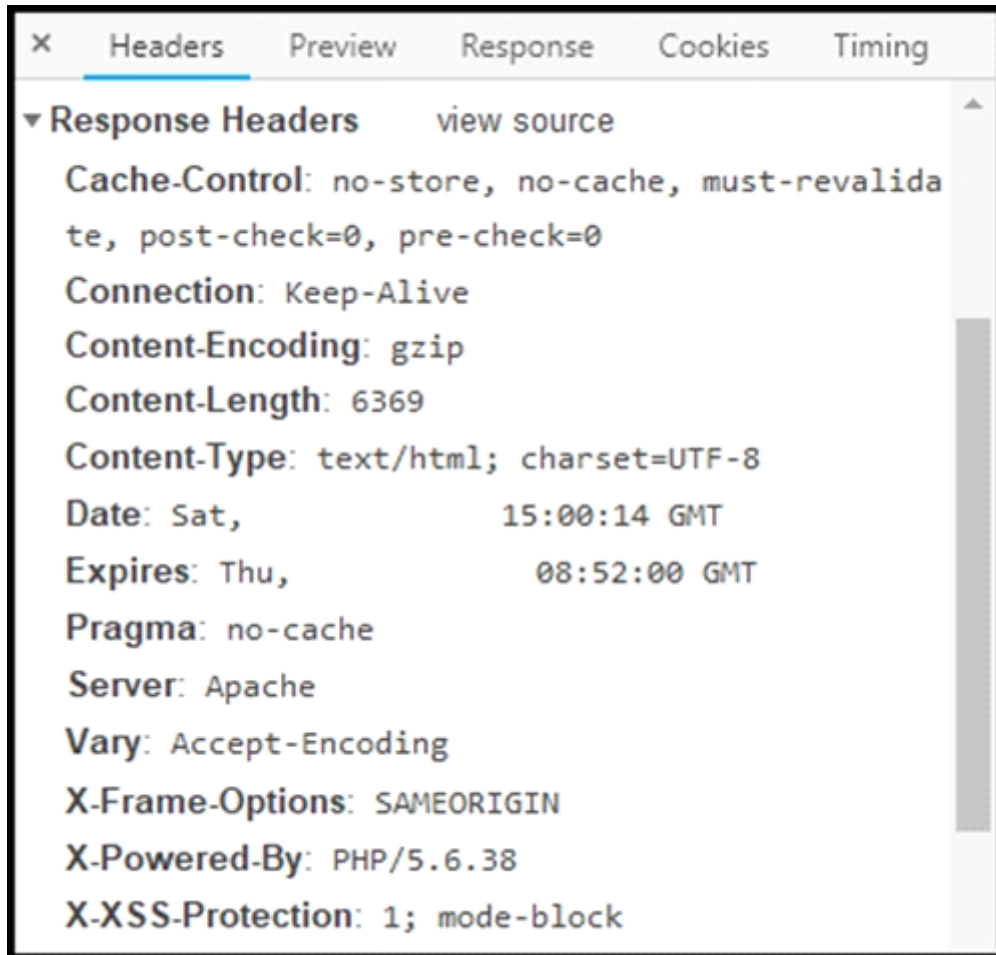
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



The image shows a browser's developer tools window with the 'Headers' tab selected. Under the 'Response Headers' section, the following headers are listed:

```
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 6369
Content-Type: text/html; charset=UTF-8
Date: Sat, 15:00:14 GMT
Expires: Thu, 08:52:00 GMT
Pragma: no-cache
Server: Apache
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
X-Powered-By: PHP/5.6.38
X-XSS-Protection: 1; mode-block
```

Where are the browser page rendering permissions displayed?

Options:

- A- X-Frame-Options
- B- X-XSS-Protection
- C- Content-Type
- D- Cache-Control

Answer:

C

Question 2

Question Type: MultipleChoice

What is idempotence?

Options:

- A- the assurance of system uniformity throughout the whole delivery process
- B- the ability to recover from failures while keeping critical services running
- C- the necessity of setting maintenance of individual deployment environments

D- the ability to set the target environment configuration regardless of the starting state

Answer:

A

Question 3

Question Type: MultipleChoice

A SOC team is investigating a recent, targeted social engineering attack on multiple employees. Cross-correlated log analysis revealed that two hours before the attack, multiple assets received requests on TCP port 79. Which action should be taken by the SOC team to mitigate this attack?

Options:

- A-** Disable BIND forwarding from the DNS server to avoid reconnaissance.
- B-** Disable affected assets and isolate them for further investigation.
- C-** Configure affected devices to disable NETRJS protocol.
- D-** Configure affected devices to disable the Finger service.

Answer:

D

Question 4

Question Type: MultipleChoice

Employees receive an email from an executive within the organization that summarizes a recent security breach and requests that employees verify their credentials through a provided link. Several employees report the email as suspicious, and a security analyst is investigating the reports. Which two steps should the analyst take to begin this investigation? (Choose two.)

Options:

- A-** Evaluate the intrusion detection system alerts to determine the threat source and attack surface.
- B-** Communicate with employees to determine who opened the link and isolate the affected assets.
- C-** Examine the firewall and HIPS configuration to identify the exploited vulnerabilities and apply recommended mitigation.
- D-** Review the mail server and proxy logs to identify the impact of a potential breach.
- E-** Check the email header to identify the sender and analyze the link in an isolated environment.

Section: (none)

Explanation

Answer:

C, E

Question 5

Question Type: MultipleChoice

Which action should be taken when the HTTP response code 301 is received from a web application?

Options:

- A-** Update the cached header metadata.
- B-** Confirm the resource's location.
- C-** Increase the allowed user limit.
- D-** Modify the session timeout setting.

Answer:

A

Question 6

Question Type: MultipleChoice

A SOC engineer discovers that the organization had three DDOS attacks overnight. Four servers are reported offline, even though the hardware seems to be working as expected. One of the offline servers is affecting the pay system reporting times. Three employees, including executive management, have reported ransomware on their laptops. Which steps help the engineer understand a comprehensive overview of the incident?

Options:

- A-** Run and evaluate a full packet capture on the workloads, review SIEM logs, and define a root cause.
- B-** Run and evaluate a full packet capture on the workloads, review SIEM logs, and plan mitigation steps.
- C-** Check SOAR to learn what the security systems are reporting about the overnight events, research the attacks, and plan mitigation step.
- D-** Check SOAR to know what the security systems are reporting about the overnight events, review the threat vectors, and define a root cause.

Answer:

D

Question 7

Question Type: MultipleChoice

The network operations center has identified malware, created a ticket within their ticketing system, and assigned the case to the SOC with high-level information. A SOC analyst was able to stop the malware from spreading and identified the attacking host. What is the next step in the incident response workflow?

Options:

- A- eradication and recovery
- B- post-incident activity
- C- containment
- D- detection and analysis

Answer:

A

Question 8

Question Type: MultipleChoice

An engineer detects an intrusion event inside an organization's network and becomes aware that files that contain personal data have been accessed. Which action must be taken to contain this attack?

Options:

- A- Disconnect the affected server from the network.
- B- Analyze the source.
- C- Access the affected server to confirm compromised files are encrypted.
- D- Determine the attack surface.

Answer:

C

To Get Premium Files for 350-201 Visit

<https://www.p2pexams.com/products/350-201>

For More Free Questions Visit

<https://www.p2pexams.com/cisco/pdf/350-201>

