CompTIA

CS0-003 Exam

CompTIA CyberSecurity Analyst CySA+ Certification Exam

Questions & Answers
Demo

Version: 9.6

Question: 1

A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

A. CVSS: 31/AV: N/AC: L/PR: N/UI: N/S: U/C: H/1: K/A: L
B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L
C. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H
D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H

Answer: A

Explanation:

This answer matches the description of the zero-day threat. The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L). Official Reference: https://nvd.nist.gov/vuln-metrics/cvss

Question: 2

Which of the following tools would work best to prevent the exposure of PII outside of an organization?

A. PAM
B. IDS
C. PKI
D. DLP

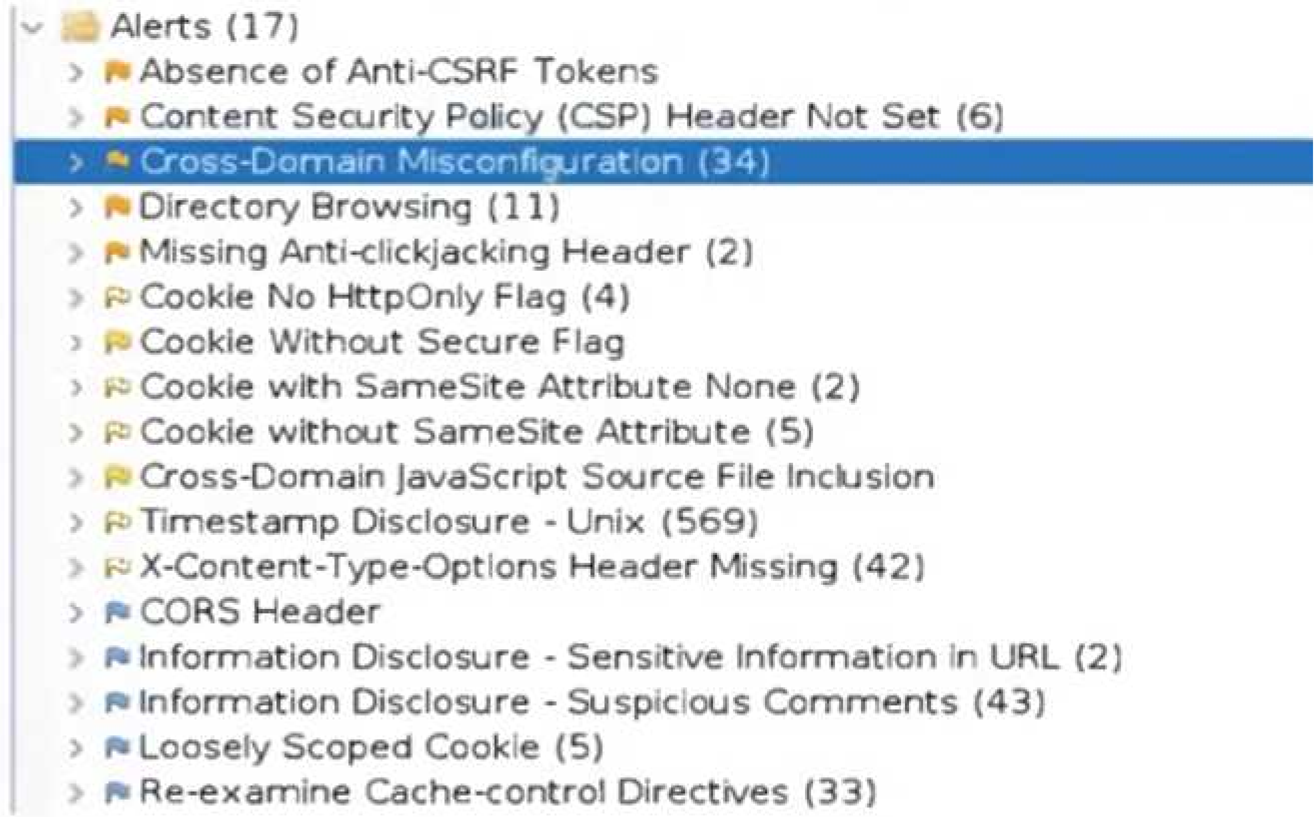
Answer: D

Explanation:

Data loss prevention (DLP) is a tool that can prevent the exposure of PII outside of an organization by monitoring, detecting, and blocking sensitive data in motion, in use, or at rest.

Question: 3

An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:



```
Alerts (17)
  Absence of Anti-CSRF Tokens
  Content Security Policy (CSP) Header Not Set (6)
  Cross-Domain Misconfiguration (34)
  Directory Browsing (11)
  Missing Anti-clickjacking Header (2)
  Cookie No HttpOnly Flag (4)
  Cookie Without Secure Flag
  Cookie with SameSite Attribute None (2)
  Cookie without SameSite Attribute (5)
  Cross-Domain JavaScript Source File Inclusion
  Timestamp Disclosure - Unix (569)
  X-Content-Type-Options Header Missing (42)
  CORS Header
  Information Disclosure - Sensitive Information in URL (2)
  Information Disclosure - Suspicious Comments (43)
  Loosely Scoped Cookie (5)
  Re-examine Cache-control Directives (33)
```

Which of the following tuning recommendations should the security analyst share?

A. Set an HttpOnlvflaq to force communication by HTTPS
B. Block requests without an X-Frame-Options header
C. Configure an Access-Control-Allow-Origin header to authorized domains
D. Disable the cross-origin resource sharing header

Answer: B

Explanation:

The output shows that the web application is vulnerable to clickjacking attacks, which allow an attacker to overlay a hidden frame on top of a legitimate page and trick users into clicking on malicious links. Blocking requests without an X-Frame-Options header can prevent this attack by instructing the browser to not display the page within a frame.

Question: 4

Which of the following items should be included in a vulnerability scan report? (Choose two.)

A. Lessons learned
B. Service-level agreement

C. Playbook
D. Affected hosts
E. Risk score
F. Education plan

Answer: D, E

Explanation:

A vulnerability scan report should include information about the affected hosts, such as their IP addresses, hostnames, operating systems, and services. It should also include a risk score for each vulnerability, which indicates the severity and potential impact of the vulnerability on the host and the organization. Official Reference: https://www.first.org/cvss/

Question: 5

The Chief Executive Officer of an organization recently heard that exploitation of new attacks in the industry was happening approximately 45 days after a patch was released. Which of the following would best protect this organization?

A. A mean time to remediate of 30 days
B. A mean time to detect of 45 days
C. A mean time to respond of 15 days
D. Third-party application testing

Answer: A

Explanation:

A mean time to remediate (MTTR) is a metric that measures how long it takes to fix a vulnerability after it is discovered. A MTTR of 30 days would best protect the organization from the new attacks that are exploited 45 days after a patch is released, as it would ensure that the vulnerabilities are fixed before they are exploited