Question - 1

SCORE: **5 points**

Red team engagement

Application Security | Cybersecurity | Open Source Intelligence | Google Dork | Easy

For a red-team engagement, a security analyst has been given a task to hack into a SaaS-based application. The goal is to gain information about their users. The analyst discovers a major vulnerability in one of their assets that has vBulletin 3.6.1 with request.php as the vulnerable file. Which tool will be used to exploit it?

○ Commix

○ SSRFMap

○ xcat

● SQLMap

Question - 2

SCORE: **5 points**

SQL Injection Attack

Application Security | SQL Injection | Cybersecurity | Easy

While testing a web application, you came across a URL https://xyz.com?id=1. You thought it would a good idea to test the *id* parameter for SQL injection. You fuzz the *id* with various payloads and do not find any anomalous behavior. That is, unless you use the payload WAITFOR DELAY '00:00:1337'-- which caused a delay of 1337 seconds in the application response. Which type of SQL injection does this involve?

○ In-Band SQL injection

● Inferential SQL Injection

○ Out of Band

○ None of the above

Question - 3

SCORE: **5 points**

Bypass File Extension

Application Security | Cybersecurity | Easy

You want to exploit a potential LFI in an application running on a Unix host. Your goal is to read **/etc/passwd** as a POC, but the application has a defense in place. It appends the php extension to the requested file. If you request **/etc/passwd** the application uses the filename to **/etc/passwd.php** which does not exist.

Given this limited information, which is the most suitable payload to bypass this defense?

○ /etc/passwd%0A

○ /etc/passwd%0F

● /etc/passwd%00

○ /etc/passwd%FF

Question - 4
Data leak

SCORE: **5 points**

Cybersecurity | Application Security | Easy

An attacker was able to download a database that was leaked from a recent data breach of an eye clinic in Singapore. The attacker was able to get into many Gmail IDs.

What attack did they perform?

● credential stuffing

○ SQL injection

○ remote code injection

○ XXE

Question - 5
eGift URL

SCORE: **5 points**

Application Security | Cybersecurity | Easy

Your friend sent you an eGift that can be redeemed using this URL: https://www.secureegfit.com/b59c67bf196a4758191e42f76670ceba. Considering there is no other defense in place for this feature, what is the potential vulnerability that might allow an attacker to redeem an eGift of another user, if vulnerable?

○ Cross-site scripting

● Insecure Direct Object Reference

○ SQL injection

○ The eGift link seems secure.

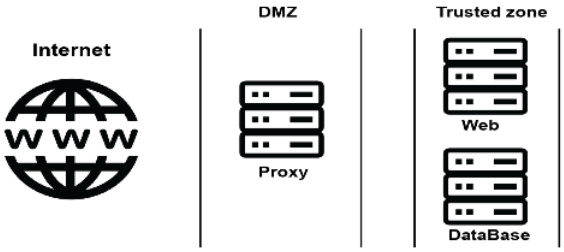
Question - 6
Secure Architechure

SCORE: **5 points**

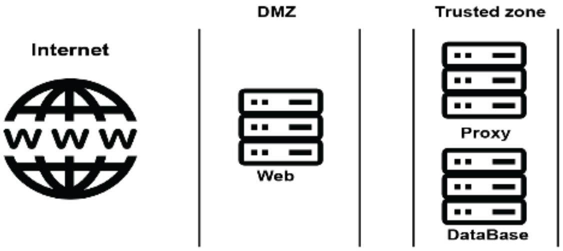
Application Security | Cybersecurity | Easy

Which of the following architectures is most secure?

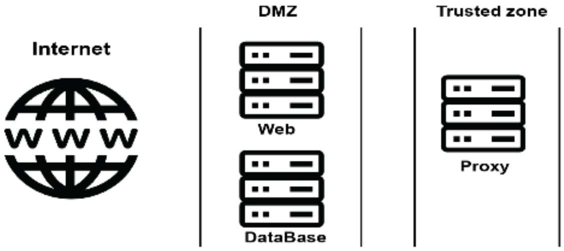
(A)



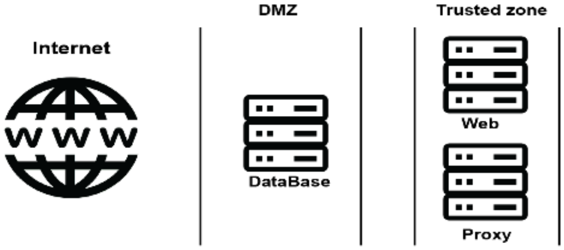
(B)



(C)



(D)



● A

○ B

○ C

○ D

Question - 7

Security Orchestration

SCORE: **5 points**

Hard | Application security | Security Operations and Incident Response

A cloud-based *ERP* (Enterprise Resource Planning) system was infiltrated by an advanced threat actor. The attacker exploited a series of interconnected vulnerabilities:

- a timing attack on the encryption protocol
- a subtle *XXE* (XML External Entity) injection within the data exchange interface
- exploitation of improper session management in the user access control module

The ERP system architecture comprises a *client access portal, a secure data exchange gateway*, an *encrypted database storage system*, and a comprehensive *event logging* and anomaly detection subsystem. The attack was characterized by its multi-stage execution and the use of polymorphic malware to evade conventional detection techniques.

What comprehensive security upgrade should be prioritized to fortify the cloud-based ERP system against similar sophisticated attacks?

○

Implement a next-generation firewall with DPI (Deep Packet Inspection) capabilities and AI-based heuristic analysis, focusing on encrypted traffic and advanced malware detection.

○

Develop a hybrid encryption framework combining post-quantum algorithms with existing encryption methods to address the timing attack vulnerability and enhance overall data security.

○

Establish an integrated security orchestration, automation, and response (SOAR) platform, focusing on real-time threat intelligence, automated incident response, and cross-system security coordination.

● Reinforce the user access control module with continuous adaptive risk assessment that utilizes behavioral biometrics and context-aware session management to detect and prevent improper access and session exploits.

Question - 8
Secure channel communication

SCORE: **5 points**

Cryptography | Cybersecurity | Application Security | Hard

Alice and Bob want to communicate securely over an insecure channel. Which of the following technologies can help them achieve this? Select all correct options.

○ Public Key Encryption

● Public Key Encryption w/ Digital Signatures

○ Symmetric Key Encryption

○ Symmetric Key Encryption w/ Digital Signatures

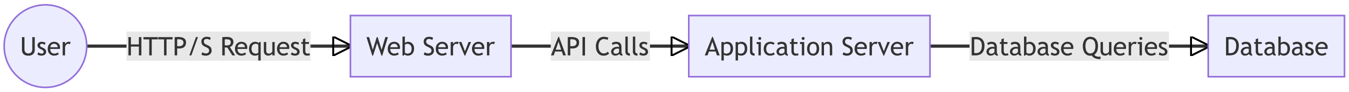
Question - 9
Secure layer

SCORE: **5 points**

Easy | Application security | Security Operations and Incident Response

A new web application in a company is under frequent attack. The company wants to add a security layer without major architecture changes.

Which security solution best protects against these attacks?



○ Add another database with replicated data for load balancing.

● Integrate a security layer between the user and the web server.

○ Implement an additional application server for redundancy.

○ Increase the capacity of the existing web server.

Question - 10
Security Assessment

SCORE: **5 points**

Medium | Security Assessment and Testing | Security Architecture

Suspicious traffic in a financial firm's network suggests a potential breach. Early analysis points to unpatched software and open ports on critical servers. The network team needs a fast and efficient way to assess the network's security posture and identify vulnerable areas for immediate patching.

Which command combination effectively identifies unpatched software and open ports on each server?

●

Run nmap -sV <network_range> to identify open ports and service versions, and yum check-update on each Linux server to list pending software updates.

○ Use traceroute <network_range> to trace network paths, and apt list --upgradable on each Linux server to find software needing upgrades.

○ Execute netstat -tuln on each server to list open ports, and wmic qfe list on Windows servers to check for installed updates.

○ Implement ping -a to resolve hostnames and IP addresses, and dpkg --list | grep -v 'ii' on each Linux server to check for non-installed packages.

Question - 11
Security Focus

SCORE: **5 points**

Easy | Application security | Security Testing

An online banking platform update added data encryption and user input validation. A security review found a critical flaw that allows attackers to bypass authentication. This issue is not related to data storage or validation.

What is the immediate priority to fix this vulnerability?

○ Introduce more complex encryption methods for user data.

● Strengthen the protocol for user identity verification.

○ Enhance the algorithm for input data validation.

○ Implement additional layers in the web application firewall.

Question - 12
Web Infrastructure Security

SCORE: **5 points**

Application Security | Cloud Security | Cybersecurity | Cloud Penetration Testing | Medium

A bank is hosting its entire web infrastructure on Firebase and has no registration functionality. The analyst tries to intercept requests via proxy, but there is always some issue in doing so. After a lot of enumeration, the attacker finds that there is a JS file having an implementation of Firebase SDK, with a constant variable for the apiKey, database URL, and project ID.

What are the possibilities to create the highest impact?

○ The attacker can achieve read, write, delete, and update access to the database.

● The attacker can register any user, gain read, write, delete, and update access.

○ Still, an API secret key is required to create impact.

○ The attacker can gain access to all the user data.

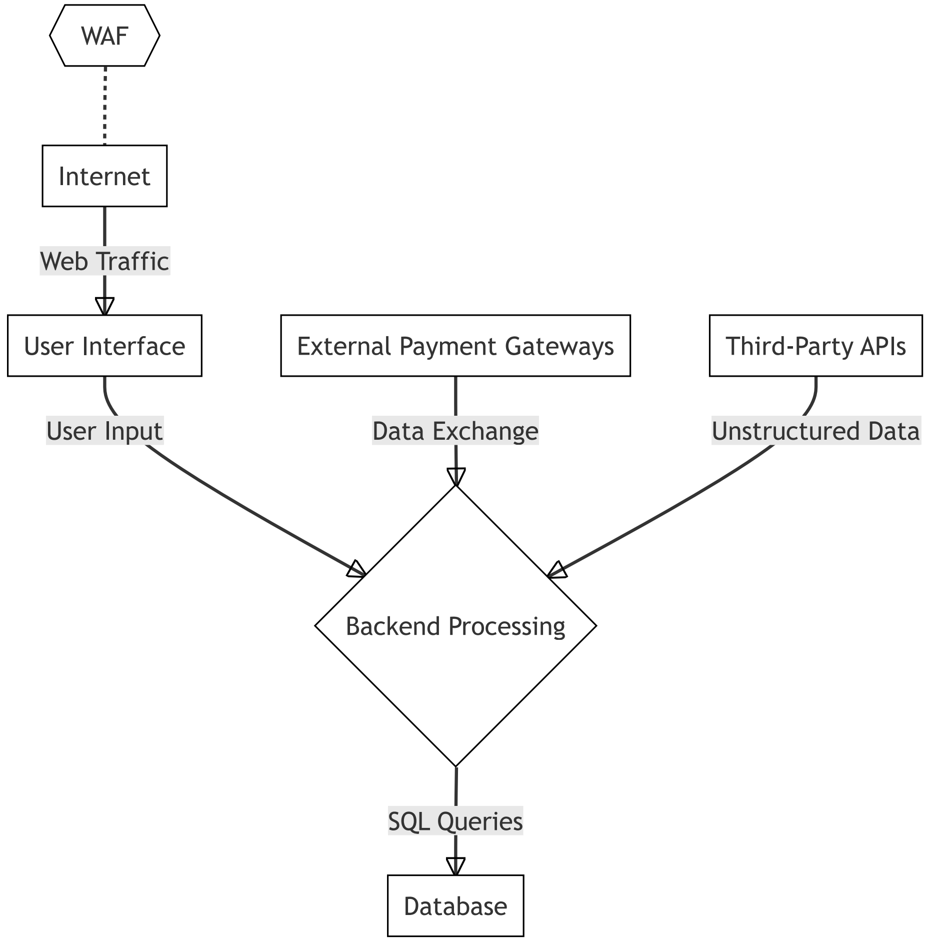
Question - 13
Query Security

SCORE: **5 points**

Medium | Application security | Secure Coding Practices

Following a security audit in an e-commerce platform, it was discovered that the SQL injection vulnerability originated from dynamically generated queries within the payment processing system. The platform's architecture, as depicted in the diagram, includes user interface components, a backend processing system, a database for transaction storage, and integrations with external payment gateways. The audit also highlighted potential weaknesses in handling unstructured data received from third-party APIs. The company needs to address these specific vulnerabilities to strengthen its overall security posture.

Which action should be prioritized to address the identified vulnerabilities?



● Implement parameterized queries and enhanced input sanitization in the backend processing system.

○ Apply stricter output encoding rules at the user interface level to prevent cross-site scripting.

○ Introduce an additional layer of data validation for information received from external payment gateways.

○ Reinforce the database security with additional access control mechanisms.

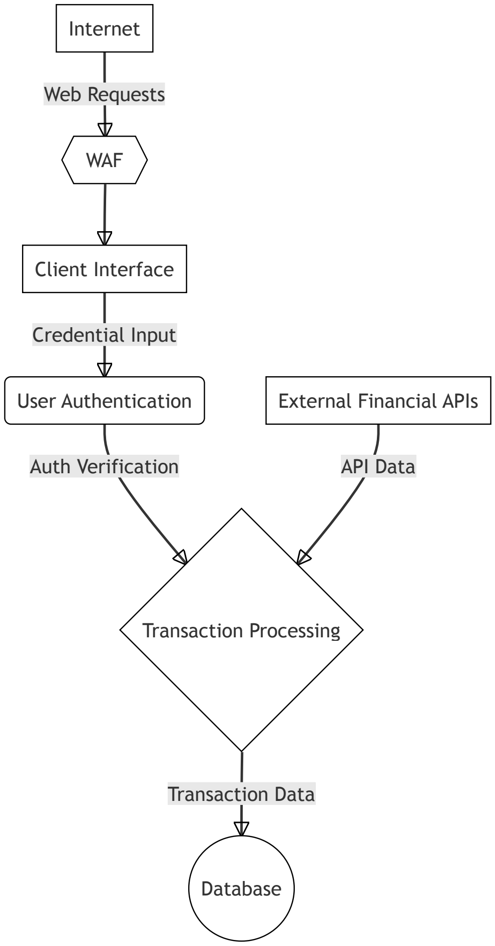
Question - 14
Security Reinforcement

SCORE: **5 points**

Hard | Application security | Data Protection and Privacy

After a targeted cyber attack on a financial institution's online system, it was discovered that attackers exploited a subtle flaw in the transaction initiation process despite robust security measures. The system architecture includes layered components: a client-facing interface, a sophisticated authentication module, an intricate transaction processing mechanism, and a highly secure database. Additionally, the system has complex integrations with external financial APIs. The current security setup includes an advanced WAF between the client-facing interface and the Internet, and stringent encryption protocols for data transfer. A detailed analysis highlighted potential security gaps in the handoff points between these components.

Referring to the diagram, which corrective action should the institution prioritize to address this specific security lapse?



○ Revise the WAF configuration to include deep packet inspection at the client interface ingress point.

● Implement an advanced monitoring and intrusion detection system at the API integration points to detect and prevent anomalous data patterns and security threats.

○ Introduce additional security layers between the authentication module and transaction processing, such as tokenization and enhanced logging for improved traceability and auditing.

○ Enhance the interface between the authentication module and transaction processing to include dynamic behavioral analysis.

Question - 15

Security Priorities

SCORE: **5 points**

Easy | Security Assessment and Testing | Security Operations

A medium-sized company suffers a data breach after a recent network upgrade. Analysis reveals:

- Weak user credentials were compromised, granting initial access.
- The intruder moved freely across network segments, accessing multiple systems.

Which action should the company prioritize to prevent future breaches?

○ Implement a strong password policy and conduct regular security awareness training for all employees.

○ Install an advanced intrusion detection/prevention system to monitor network traffic for suspicious activities.

● Redesign network architecture to include more stringent network segmentation and enforce access controls on each segment.

○ Focus on regular patching of all network devices and systems without altering the existing network structure or policies.

Question - 16
Encrypt Financial Data

SCORE: **5 points**

Cybersecurity | Application Security | Easy

You are assigned to create a 2nd layer of defense for a banking application by encrypting the sensitive data in the database. Which of the following standards is the best choice if security is your first priority, irrespective of the computing power required?

○ SHA

○ DES

○ Triple DES

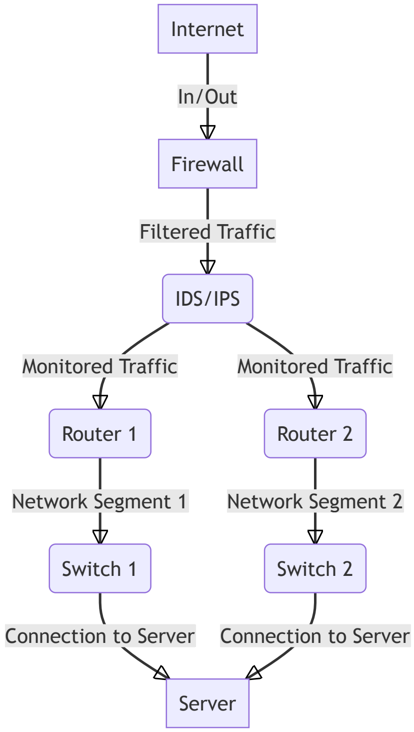
● AES

Question - 17
Attack Mitigation

SCORE: **5 points**

Hard | Security Architecture | Security Assessment and Testing

A cyber-attack occurred In a global finance corporation's network, depicted in the diagram.



The attackers exploited a zero-day vulnerability in the firewall, gained access through weak credentials on Router 2, and then installed malware on Switch 2, compromising the server. The IT security team needs to execute a series of command-based operations to mitigate the breach and fortify the network against future attacks, considering the interconnected nature of the network components.

Operations performed:

1. Disable unused services on router 2.

```
router2> enable
router2# configure terminal
router2(config)# no service tcp-small-servers
router2(config)# no service udp-small-servers
```

2. Disable Cisco Discovery Protocol on Switch 2 to prevent network topology disclosure.

```
switch2> enable
switch2# configure terminal
switch2(config)# no cdp run
```

3. Update the firewall firmware to patch the zero-day vulnerability.

```
firewall> enable
firewall# update firmware
```

4. Apply a new access control list to the server.

```
server> enable
server# configure terminal
server(config)# ip access-group 105 in
```

5. Create a new VLAN on Switch 1 for critical financial data.

```
switch1> enable
switch1# configure terminal
switch1(config)# vlan 3
switch1(config)# exit
```

6. Update the signature definitions on the IDS/IPS.

```
ids_ips> enable
ids_ips# configure terminal
ids_ips(config)# signature-definition update
```

What is the correct sequence of priority of operations, higher to lower, to fortify security?

● 3 -> 1 -> 6 -> 2 -> 4 -> 5

○ 1 -> 2 -> 3 -> 4 -> 5 -> 6

○ 3 -> 1 -> 5 -> 2 -> 4 -> 6

○ 3 -> 5 -> 4 -> 6 -> 2 -> 1

Question - 18

SCORE: 5 points

Unreachable ATMs

Networking | Troubleshooting | System Administration | Easy

You are using SNMP protocol for collecting data from an ATM network. The network consists of 730 ATMs across the city. Suddenly, you receive an alert that 10 ATMs are not reachable anymore. What would be the likely reason for that?

○ The monitoring server is down.

● The network switch servicing that ATM segment is down.

○ The DNS Server is down.

○ The SNMP server's gateway is down.

○ It seems like someone is trying to hack your network.

Question - 19
Extra Risks

SCORE: 5 points

Network Security | SSH | Telnet | Encryption | Remote Access | Risk Evaluation | Easy

You are working in a large telecom company. You need to change the settings on a remote legacy device that is used for historical reasons. It does not support SSH. Instead, it supports Telnet. What extra risks (if any) are you taking by connecting to this device?

○ You are susceptible to the SSL HeartBleed attack.

○ Port 23 is more dangerous than port 22 in general.

● You are susceptible to a MITM attack.

○ You are susceptible to a BruteForce attack.

○ You are susceptible to DNS poisoning.

○ There are no additional risks if the device is not reachable from the WAN.

Question - 20
Intrusion Prevention

SCORE: 5 points

Easy | Security Architecture | Security Assessment and Testing

A company's network administrator configures the firewall to bolster the organization's defense against external threats. They are focusing on protecting the internal network. SQL injection attacks have recently targeted the company's website. The network setup includes a DMZ (Demilitarized Zone) hosting their public-facing web server.

Which firewall rule might the administrator use to enhance network security against this threat?

○ iptables -A INPUT -p tcp --dport 80 -j DROP

○ iptables -A FORWARD -p tcp --dport 443 -s 192.168.1.0/24 -j ACCEPT

● iptables -A INPUT -p tcp --dport 80 -m string --string 'select' --algo bm -j DROP

○ iptables -A OUTPUT -p tcp --dport 22 -d 10.10.10.0/24 -j ACCEPT

Question - 21
URL Miscategorization

SCORE: 5 points

Easy | URL categorization | Content Filtering

In a corporate environment where URL filtering is implemented, employees have reported issues accessing legitimate websites related to their work. An investigation found that certain URLs are being incorrectly categorized as malicious by the URL filtering system, leading to unnecessary blocks.

How should the issue be addressed?

- ○ Conduct a network-wide security audit to identify any malicious activities triggering the URL filtering system, and resolve those issues.
- ○ Disable the URL filtering system temporarily until the issue is resolved to ensure uninterrupted access for employees.
- ● Add the affected URLs to a whitelist, allowing access without URL filtering, and report the misclassification to the vendor for correction.
- ○ Increase the strictness level of the URL filtering system to ensure comprehensive security coverage, even if it leads to some false positives.

Question - 22

SCORE: 5 points

DDoS Protection

Easy | DDoS attack | Network Security Monitoring

In a scenario where an organization's network is under a Distributed Denial of Service (DDoS) attack, they observe that the firewall is struggling to handle the high volume of incoming traffic, impacting legitimate user access. What is the most effective approach to mitigate the impact of the DDoS attack using firewall capabilities?

- ● Implement rate limiting on the firewall to restrict the number of connections per second from individual source IPs.
- ○ Increase the maximum connection limit on the firewall to accommodate the surge in incoming connections during the DDoS attack.
- ○ Configure the firewall to automatically block all incoming traffic, allowing only whitelisted IP addresses during the DDoS attack.
- ○ Deploy additional firewalls in parallel to distribute the load and enhance the network's capacity to handle the DDoS traffic.