# Information Security

## MOCK OBJECTIVE PRACTICE PAPER

1. A sudden spike in inbound ICMP Echo Replies overwhelms a server even though the server did not initiate requests. Which attack is MOST likely occurring?
   a) Ping of Death
   b) Smurf Attack
   c) UDP Flood
   d) ARP Poisoning
2. Which characteristic BEST differentiates a DDoS attack from a DoS attack?
   a) Use of malformed packets
   b) Involvement of multiple compromised systems
   c) Targeting application layer services
   d) Exploitation of ICMP only
3. In a botnet-based DDoS attack, the primary role of the Command and Control (C2) server is to:
   a) Generate spoofed IP addresses
   b) Encrypt attack traffic
   c) Coordinate and control compromised hosts
   d) Bypass firewall rules
4. A volumetric attack primarily aims to:
   a) Exhaust server memory
   b) Consume bandwidth and network capacity
   c) Exploit application logic
   d) Corrupt routing tables
5. Which protocol is MOST commonly abused in amplification-based DDoS attacks due to its connectionless nature?
   a) TCP
   b) ICMP
   c) UDP
   d) ARP
6. A UDP flood is particularly effective because:
   a) UDP packets require authentication
   b) UDP establishes a session before data transfer
   c) The victim must respond with ICMP messages
   d) UDP lacks connection state and validation
7. Which attack causes system failure by sending oversized ICMP packets exceeding allowed limits?
   a) Smurf Attack
   b) Ping of Death
   c) ICMP Flood
   d) UDP Flood
8. In a Smurf attack, the amplification effect is achieved by:
   a) Spoofing the victim’s IP address
   b) Sending packets to a broadcast address

c) Exploiting TCP retransmissions
d) Using malformed ARP replies

9. ARP poisoning can indirectly assist DDoS attacks by:
   a) Increasing packet size
   b) Redirecting traffic through the attacker
   c) Exhausting UDP ports
   d) Spoofing DNS records
10. Which layer is the PRIMARY target of HTTP floods and Slowloris attacks?
   a) Network Layer
   b) Transport Layer
   c) Application Layer
   d) Data Link Layer
11. Application-layer attacks are harder to detect because they:
   a) Use encrypted payloads only
   b) Appear similar to legitimate user traffic
   c) Do not consume bandwidth
   d) Operate only on UDP
12. Which defensive technique prevents packets with spoofed source IP addresses from entering a network?
   a) Egress filtering
   b) Ingress filtering
   c) Load balancing
   d) Rate limiting
13. Egress filtering is MOST effective in preventing:
   a) Incoming volumetric attacks
   b) Internal hosts launching spoofed attacks
   c) Application-layer DDoS attacks
   d) Botnet command communication
14. Throttling as a mitigation strategy focuses on:
   a) Blocking all traffic
   b) Reducing packet size
   c) Limiting traffic flow to manageable levels
   d) Redirecting traffic to honeypots
15. A network device configured to “drop requests” during high load is primarily protecting against:
   a) ARP Poisoning
   b) Resource exhaustion
   c) Session hijacking
   d) DNS spoofing
16. TCP Intercept is used to mitigate SYN flood attacks by:
   a) Encrypting TCP sessions
   b) Acting as a proxy for TCP handshakes
   c) Blocking all TCP traffic
   d) Reducing RTT
17. Which mechanism distributes incoming traffic across multiple servers to improve availability during attacks?

a) Rate limiting
b) Load balancing
c) Ingress filtering
d) Throttling

18. Rate limiting is MOST effective against:
    a) Low-volume, stealthy attacks
    b) ARP spoofing
    c) High-frequency request floods
    d) Insider threats
19. Which attack exploits trust in local network address resolution rather than bandwidth exhaustion?
    a) UDP Flood
    b) Smurf Attack
    c) ARP Poisoning
    d) ICMP Flood
20. Combining ingress filtering, rate limiting, and load balancing is most effective because it:
    a) Eliminates all attack traffic
    b) Addresses attacks at multiple network layers
    c) Works only for ICMP-based attacks
    d) Prevents malware installation
21. Which access control concept answers the question: *"Who are you?"*
    a) Authentication
    b) Identification
    c) Authorization
    d) Accountability
22. Which mechanism ensures that a user cannot deny having performed an action?
    a) Auditing
    b) Accountability
    c) Non-repudiation
    d) Authorization
23. Logging and periodic review of user activities primarily enforce:
    a) Authentication
    b) Auditing
    c) Identification
    d) Authorization
24. Holding a user responsible for actions performed using their credentials is known as:
    a) Accountability
    b) Non-repudiation
    c) Auditing
    d) Authorization
25. Authorization is best defined as:
    a) Verifying identity
    b) Granting permissions after authentication
    c) Logging system activity
    d) Identifying a user

26. Storing fingerprint templates of all citizens for matching at arrival/departure represents which biometric operation?
    a) Verification
    b) Identification
    c) Authentication
    d) Authorization
27. A 1:N biometric comparison is associated with:
    a) Verification
    b) Identification
    c) Authentication token
    d) Authorization list
28. Checking a traveler's fingerprint against their passport-linked record is an example of:
    a) Identification
    b) Verification
    c) Auditing
    d) Accountability
29. A false acceptance in biometric systems means:
    a) Legitimate user is rejected
    b) Illegitimate user is accepted
    c) Fingerprint template is corrupted
    d) System timeout occurs
30. A false rejection occurs when:
    a) An attacker gains access
    b) A valid user is denied access
    c) The database fails completely
    d) A blacklist is updated
31. The probability of false acceptance per match is 0.0001%. The database contains 500,000 citizens. What is the approximate false acceptance probability during one full identification attempt (1:N)?
    a) 0.0001%
    b) 0.05%
    c) 50%
    d) Approximately 0.5%
32. The increased risk of false acceptance in a large biometric database is mainly due to:
    a) Poor fingerprint quality
    b) Increased number of comparisons
    c) Network latency
    d) Database encryption
33. Biometric false acceptance probability increases most significantly in which scenario?
    a) Verification mode
    b) Identification mode
    c) Auditing mode
    d) Logging mode
34. A false acceptance at a national airport most directly impacts:
    a) Confidentiality
    b) Integrity

c) Availability
d) Authorization

35. A criminal falsely accepted as a legitimate traveler creates a risk to:
    a) System availability
    b) National security
    c) Database performance
    d) Biometric accuracy only
36. False rejection of a legitimate citizen most directly results in:
    a) Security breach
    b) User inconvenience and delays
    c) System compromise
    d) Credential theft
37. Matching travelers against a blacklist of 50 criminals is best classified as:
    a) Identification system
    b) Verification system
    c) Authorization control
    d) Auditing control
38. False acceptance in a blacklist scenario means:
    a) A criminal is blocked
    b) A criminal is allowed to leave
    c) A citizen is delayed
    d) Logs are incomplete
39. A whitelist of 100 high-ranking officials used for preferential treatment primarily implements:
    a) Accountability
    b) Authentication
    c) Authorization
    d) Identification
40. False rejection in the whitelist system would MOST likely lead to:
    a) Security compromise
    b) Delay or denial of privileges to authorized officials
    c) Increased false acceptance rate
    d) Database corruption
41. Which scenario is MOST tolerant of false rejection but NOT false acceptance?
    a) Office attendance system
    b) Airport immigration control
    c) Library access system
    d) Parking gate system
42. Which access control objective is violated if biometric logs are deleted?
    a) Authentication
    b) Identification
    c) Auditing
    d) Authorization
43. Combining biometrics with audit logs most strongly enforces:
    a) Authentication only
    b) Accountability

c) Confidentiality
d) Availability

44. Which statement BEST explains why biometrics strengthen non-repudiation?
    a) Biometrics are secret
    b) Biometrics are difficult to share
    c) Biometrics encrypt credentials
    d) Biometrics guarantee availability
45. Increasing biometric system sensitivity will generally:
    a) Increase false acceptance and false rejection
    b) Decrease both FAR and FRR
    c) Decrease FAR but increase FRR
    d) Eliminate both errors
46. A biometric system has a False Acceptance Rate (FAR) of 0.001% per match. If an identification system performs 10,000 comparisons, what is the approximate probability of at least one false acceptance?
    a) 0.001%
    b) 0.01%
    c) 0.1%
    d) ~10%
47. A fingerprint system has FAR = 0.0001 per attempt. If a criminal attempts access 1,000 times, what is the expected number of false acceptances?
    a) 0
    b) 0.1
    c) 1
    d) 10
48. A biometric system supports 1:1 verification and 1:N identification. FAR is constant per comparison. Which mode has a higher overall false acceptance probability and why?
    a) Verification – because data is encrypted
    b) Identification – due to multiple comparisons
    c) Verification – due to reduced accuracy
    d) Both are equal
49. A biometric database contains 200,000 identities. FAR per match = 0.00001 ($1\times10^{-5}$). What is the approximate FAR for a single identification attempt (1:N)?
    a) 0.001%
    b) 0.01%
    c) 0.2%
    d) 2%
50. If FAR is reduced by tightening the matching threshold, what is the MOST likely effect?
    a) FRR decreases
    b) FRR increases
    c) Both FAR and FRR decrease
    d) No impact on FRR
51. A system administrator reduces FRR aggressively. What does this unintentionally increase?

a) Availability
b) False Acceptance Rate
c) Audit accuracy
d) Non-repudiation

52. In a high-security airport, which biometric error is more dangerous?
a) False rejection
b) False acceptance
c) Equal risk
d) Neither

53. A biometric system has FRR = 2%. If 5,000 legitimate passengers use the system, how many are expected to face rejection?
a) 5
b) 50
c) 100
d) 1,000

54. In Mandatory Access Control (MAC), access decisions are based on:
a) User discretion
b) Owner permission
c) System-enforced security labels
d) Group membership

55. Which entity determines access in a DAC model?
a) Security administrator
b) Operating system kernel
c) Data owner
d) Policy server

56. Which model is MOST resistant to insider privilege abuse?
a) DAC
b) MAC
c) RBAC
d) ABAC

57. In a military system using MAC, a user with “Secret” clearance tries to access “Top Secret” data. What happens?
a) Access allowed if owner permits
b) Access denied by policy
c) Access logged but allowed
d) Depends on DAC settings

58. Which access control model allows users to pass access rights to others?
a) MAC
b) DAC
c) RBAC
d) Rule-based access

59. Which access control model enforces centralized policy enforcement?
a) DAC
b) MAC
c) Access Control Lists
d) Capability lists

60. Principle of Least Privilege means:
    a) Users get maximum access
    b) Users get temporary access only
    c) Users get only required access
    d) All users get equal access
61. A developer is given database-admin rights for debugging a UI bug. This violates:
    a) Authentication
    b) Authorization
    c) Least Privilege
    d) Accountability
62. Which access model BEST supports Least Privilege?
    a) DAC
    b) MAC
    c) RBAC
    d) Open access
63. A service account that runs continuously with administrator privileges presents risk mainly because it:
    a) Breaks availability
    b) Violates least privilege
    c) Prevents auditing
    d) Increases FRR
64. Applying POLP primarily reduces the impact of:
    a) External DDoS attacks
    b) Insider threats
    c) Physical theft
    d) Network congestion
65. In malware containment, Least Privilege helps because it:
    a) Stops network traffic
    b) Limits damage post-compromise
    c) Prevents phishing
    d) Encrypts credentials
66. A biometric system switches from verification to identification without changing FAR. What happens to system risk?
    a) Decreases
    b) Remains same
    c) Increases exponentially
    d) Eliminated
67. A whitelist biometric system has 100 users. FAR = 0.001. Compared to a blacklist of 50,000 criminals, which has higher FAR risk?
    a) Whitelist
    b) Blacklist
    c) Same risk
    d) Depends on FRR
68. Which combination best minimizes FAR without significantly hurting usability?
    a) Low threshold, identification mode
    b) High threshold, verification mode

c) No threshold tuning
d) Remove auditing

69. Which of the following is NOT a primary goal of web security?
    a) Confidentiality
    b) Integrity
    c) Availability
    d) Data redundancy
70. Ensuring that a web page is not altered during transit primarily supports:
    a) Confidentiality
    b) Integrity
    c) Authentication
    d) Authorization
71. Preventing unauthorized users from accessing a web application mainly ensures:
    a) Availability
    b) Authentication
    c) Authorization
    d) Integrity
72. Which security goal is compromised if a website becomes unreachable due to heavy traffic?
    a) Confidentiality
    b) Integrity
    c) Availability
    d) Authentication
73. The fundamental security weakness of HTTP is that it:
    a) Does not support cookies
    b) Sends data in plaintext
    c) Uses complex headers
    d) Is slower than HTTPS
74. HTTPS provides security primarily by using:
    a) Firewalls
    b) Encryption and certificates
    c) Hash functions only
    d) IP filtering
75. Which protocol is used to secure HTTP traffic?
    a) SSL only
    b) TLS only
    c) SSL/TLS
    d) IPsec
76. What happens if a user accesses an HTTPS site using HTTP instead?
    a) Automatic TLS encryption is enforced
    b) Data is always encrypted
    c) The connection may be vulnerable to attacks
    d) The browser blocks the site
77. Which HTTP method appends parameters directly in the URL?
    a) POST
    b) GET

c) PUT
d) DELETE

78. Sensitive data should NOT be sent using GET requests because:
a) GET is slower
b) URLs can be logged and cached
c) GET does not support headers
d) GET does not support encryption
79. The primary difference between GET and POST is that POST:
a) Is always encrypted
b) Sends data in the request body
c) Cannot be intercepted
d) Does not use headers
80. Which HTTP method is more suitable for submitting login credentials?
a) GET
b) POST
c) OPTIONS
d) HEAD
81. Which HTTP header specifies the domain name of the server being requested?
a) User-Agent
b) Host
c) Referer
d) Accept
82. The User-Agent header is mainly used to:
a) Authenticate users
b) Identify client software
c) Encrypt data
d) Specify content length
83. Which header reveals the web page from which a request originated?
a) Origin
b) Referer
c) Cookie
d) Cache-Control
84. Cookies sent from client to server are carried in which header?
a) Set-Cookie
b) Cookie
c) Authorization
d) Accept-Encoding
85. An SSL Strip attack primarily works by:
a) Breaking TLS encryption mathematically
b) Forcing HTTPS connections to downgrade to HTTP
c) Injecting malware into the browser
d) Exploiting weak passwords
86. In SSL stripping, which party is typically positioned between the user and server?
a) Web server
b) Firewall

c) Man-in-the-middle
d) Certificate Authority

87. The attack succeeds mainly because users:
    a) Ignore browser warnings
    b) Do not check the URL scheme
    c) Use weak passwords
    d) Disable cookies
88. A TLS downgrade attack forces a connection to:
    a) Use a faster protocol
    b) Use older, weaker encryption
    c) Disable cookies
    d) Switch IP addresses
89. Which protocol versions are commonly targeted in downgrade attacks?
    a) TLS 1.3 only
    b) TLS 1.2 only
    c) SSL 2.0 / SSL 3.0
    d) DNS
90. Which mechanism helps prevent TLS downgrade attacks?
    a) Cookies
    b) HSTS
    c) URL encoding
    d) CAPTCHA
91. Mixed content occurs when:
    a) HTTP and HTTPS are used on different domains
    b) An HTTPS page loads HTTP resources
    c) Multiple cookies exist in the browser
    d) POST and GET are mixed
92. Which type of mixed content is most dangerous?
    a) Passive (images, videos)
    b) Active (scripts, iframes)
    c) Cached content
    d) Encrypted content
93. Mixed content vulnerabilities mainly compromise:
    a) Availability
    b) Confidentiality and Integrity
    c) Authorization
    d) Accountability
94. A login page is served over HTTPS but submits credentials using HTTP. This is an example of:
    a) TLS downgrade
    b) Mixed content
    c) SSL strip
    d) Cross-site scripting
95. Which defense MOST effectively prevents SSL stripping attacks?
    a) Strong passwords
    b) HSTS
    c) GET to POST conversion
    d) Encryption at database level

96. Which HTTP header is crucial for token-based authentication (e.g., Bearer tokens)?
    a) Cookie
    b) Authorization
    c) Accept
    d) Host
97. Which scenario BEST illustrates loss of confidentiality in web security?
    a) Website downtime
    b) SQL query modification
    c) Credentials visible in URL logs
    d) User denied access
98. Using HTTPS alone does NOT fully protect a website if:
    a) Strong certificates are used
    b) Mixed content exists
    c) TLS 1.3 is enabled
    d) HSTS is configured
99. SQL Injection mainly exploits which application weakness?
    a) Weak cryptography
    b) Improper input handling
    c) Missing firewall
    d) Lack of SSL
100. Which query is MOST vulnerable to SQL injection?
    a) SELECT * FROM users WHERE id = ?
    b) SELECT * FROM users WHERE id = '$id'
    c) SELECT username FROM users
    d) SELECT NOW()
101. The payload ' OR '1'='1'-- exploits:
    a) Authentication logic
    b) Authorization tables
    c) Database indexing
    d) Encryption algorithms
102. Which parameter location is MOST commonly abused in SQL injection?
    a) HTTP headers
    b) URL query strings
    c) DNS records
    d) Cookies only
103. Google dorking assists attackers primarily during:
    a) Exploitation phase
    b) Vulnerability discovery phase
    c) Post-exploitation phase
    d) Payload encoding
104. Which Google search query helps find SQL-vulnerable pages?
    a) site:example.com "login success"
    b) inurl:php?id=
    c) filetype:jpg user
    d) intitle:secure
105. Why do attackers use ORDER BY n in SQL injection?
    a) To sort database records
    b) To insert new data
    c) To discover column count
    d) To trigger authentication failure

106. If ORDER BY 6 returns an error but ORDER BY 5 does not, the query likely has:
    a) 6 columns
    b) 5 columns
    c) Unlimited columns
    d) Hidden columns
107. Which condition MUST be satisfied for UNION-based SQL injection to work?
    a) Same data types in selected columns
    b) Database must be MySQL
    c) Error messages must be shown
    d) Table names must be known
108. Which payload attempts to extract database version using UNION?
    a) UNION SELECT user()
    b) UNION SELECT version()
    c) OR 1=1

    d) ORDER BY 1

109. UNION-based SQL injection mainly violates:
    a) Availability
    b) Confidentiality
    c) Authentication
    d) Accountability
110. Error-based SQL injection is effective when:
    a) Errors are suppressed
    b) Detailed DB errors are displayed
    c) Only POST requests exist
    d) TLS is enabled
111. Which DB behavior enables error-based SQL injection?
    a) Debug mode disabled
    b) Verbose exception handling
    c) Stored procedures
    d) Token authentication
112. Blind SQL injection is used when attackers:
    a) Can see database errors
    b) Can retrieve query output directly
    c) Receive limited application responses
    d) Have database credentials
113. Which observation MOST helps in blind SQL injection?
    a) SQL syntax errors
    b) Page layout differences
    c) Code comments
    d) Table names
114. Boolean-based SQL injection relies on:
    a) Time delays
    b) True/false response behavior
    c) Error messages
    d) Stack traces
115. A page showing different content when condition is true indicates:
    a) Error-based SQL injection
    b) Boolean blind SQL injection

c) UNION SQL injection
d) Second-order SQL injection

116. Which payload is an example of time-based blind SQL injection?
a) ' OR 1=1--
b) UNION SELECT NULL
c) IF(1=1,SLEEP(5),0)
d) ORDER BY 3

117. Time-based SQL injection is identified by:
a) HTTP 403 errors
b) Database crash
c) Response delay
d) Invalid URL

118. Second-order SQL injection differs because payloads are:
a) Executed immediately
b) Stored and triggered later
c) Always error-based
d) Network-based

119. Which example BEST fits second-order SQL injection?
a) Login bypass using OR 1=1
b) Malicious input stored in profile and later used in SQL query
c) UNION extraction from URL
d) Time delay in login

120. Why is blacklisting unreliable against SQL injection?
a) Too slow
b) Limited patterns can be bypassed
c) Requires encryption
d) Stops only GET requests

121. Which defense is MOST effective against SQL injection?
a) Client-side validation
b) Input escaping only
c) Prepared statements
d) Hiding error messages

122. Whitelisting improves security by:
a) Blocking known bad inputs
b) Allowing only approved input formats
c) Encoding dangerous characters
d) Increasing database speed

123. Which step parses SQL structure in prepared statements?
a) Parameter binding
b) Query execution
c) Parsing/precompilation
d) Result fetching

124. Prepared statements stop SQL injection because user input is:
a) Executed as code
b) Treated as literal data
c) Parsed separately
d) Encrypted

125. SQL injection can STILL occur with prepared statements when:
a) Placeholders are used properly
b) Dynamic SQL builds table names

c) Stored procedures are avoided
d) TLS is enabled

126. Which SQL injection type is the MOST difficult to detect automatically?
a) Error-based
b) UNION-based
c) Blind SQL injection
d) Login bypass

127. A website returns identical pages but slower responses after payloads. The MOST likely attack is:
a) Error-based SQL injection
b) Boolean blind SQL injection
c) Time-based blind SQL injection
d) Second-order SQL injection

128. Proper use of prepared statements mainly enforces which security goal?
a) Integrity of SQL syntax
b) Availability of database
c) Confidentiality of encryption keys
d) Non-repudiation

129. HTTP is considered stateless because it:
a) Encrypts each request
b) Does not retain client state between requests
c) Uses cookies automatically
d) Prevents sessions

130. Which mechanism is MOST commonly used to maintain user state in HTTP?
a) IP address
b) MAC address
c) Session ID
d) Port number

131. A session ID stored in a cookie mainly supports:
a) Confidentiality
b) Integrity
c) User session continuity
d) Data encryption

132. Personalization on websites mainly relies on:
a) Stateless HTTP
b) Cookies and session data
c) DNS records
d) TLS certificates

133. Hidden fields are primarily used to:
a) Encrypt form data
b) Store session data client-side
c) Pass state information between requests
d) Prevent CSRF

134. Which is a key limitation of hidden form fields?
a) They are automatically encrypted
b) They cannot be modified by users
c) They can be viewed and altered by the client
d) They expire automatically

135. Which header is used by a server to set a cookie?
a) Cookie

b) Set-Cookie
c) Authorization
d) Host

136. Which cookie attribute ensures the cookie is sent ONLY over HTTPS?
a) Domain
b) Path
c) Secure
d) HttpOnly

137. The HttpOnly attribute primarily protects against:
a) CSRF attacks
b) XSS-based cookie theft
c) Packet sniffing
d) Session fixation

138. Which cookie attribute restricts where the cookie is sent within a site?
a) Path
b) Expires
c) Secure
d) Domain

139. A major downside of cookies is that they:
a) Are always encrypted
b) Can be used to track users
c) Cannot store identifiers
d) Expire immediately

140. Tracking users across different websites is MOST commonly done using:
a) First-party cookies
b) Session cookies
c) Third-party cookies
d) Secure cookies

141. Browser fingerprinting differs from cookies because it:
a) Requires user consent
b) Stores data on the server
c) Tracks users without storing data on the client
d) Uses encrypted cookies

142. Which factor is commonly used in browser fingerprinting?
a) User password
b) Screen resolution and fonts
c) Session ID only
d) TLS private key

143. Session hijacking occurs when an attacker:
a) Breaks encryption
b) Steals or predicts a session identifier
c) Modifies database tables
d) Performs brute-force login

144. Which attack MOST directly enables session hijacking?
a) SQL Injection
b) Cookie theft
c) DNS poisoning
d) CAPTCHA bypass

145. A session ID exposed in a URL is dangerous because it:
a) Improves performance

b) Can be cached, logged, or leaked
c) Encrypts the session
d) Prevents replay

146. Which defense MOST effectively reduces cookie theft via network sniffing?
a) Long cookie expiration
b) Using HTTPS with Secure flag
c) Client-side validation
d) Browser cache control

147. Regenerating session IDs after login primarily prevents:
a) XSS
b) CSRF
c) Session fixation
d) SQL injection

148. Which combination provides STRONGEST protection for session cookies?
a) Large cookie size only
b) Secure + HttpOnly + HTTPS
c) Short session timeout only
d) Hidden fields and cookies

149. The Same-Origin Policy (SOP) primarily restricts:
a) Network access between servers
b) Script access across different origins
c) HTTPS connections only
d) Cookie creation

150. An “origin” in web security is defined by:
a) Domain name only
b) Protocol, host, and port
c) IP address and port
d) URL path

151. Two URLs differ only in port number. According to SOP, they are:
a) Same origin
b) Trusted origins
c) Different origin
d) Conditionally allowed

152. Frame isolation mainly prevents:
a) SQL injection
b) Clickjacking attacks
c) One frame accessing another frame’s DOM
d) CSRF attacks

153. Which SOP violation enables many XSS attacks?
a) Allowing cookies
b) Allowing script execution
c) Allowing injected scripts to run with page origin
d) Allowing HTTPS connections

154. XSS is particularly dangerous because injected scripts execute:
a) With attacker privileges
b) With browser privileges
c) With victim user’s origin and privileges
d) In isolated sandboxes

155. Which type of XSS stores malicious code on the server?
a) Reflected

b) DOM-based
c) Stored (Persistent)
d) Blind

156. Stored XSS is especially dangerous because it:
a) Requires user interaction
b) Affects all users automatically
c) Cannot bypass SOP
d) Occurs only in URLs

157. Reflected XSS typically occurs when:
a) Malicious input is stored in database
b) Server immediately reflects user input in response
c) JavaScript reads cookies directly
d) CSP blocks scripts

158. Which situation best represents reflected XSS?
a) Malicious comment stored in forum
b) Script injected via URL parameter and echoed
c) Script injected into database report
d) Script from third-party CDN

159. XSS subverts the Same-Origin Policy by:
a) Disabling cookies
b) Injecting scripts that inherit the page's origin
c) Using HTTPS downgrade
d) Breaking TLS encryption

160. Which defense BEST prevents XSS at the browser level?
a) Blacklisting tags
b) Input validation alone
c) Content Security Policy (CSP)
d) Cookie expiration

161. CSP primarily defends against XSS by:
a) Encrypting JavaScript
b) Blocking inline and untrusted scripts
c) Preventing form submission
d) Hiding error messages

162. Which CSP directive restricts where scripts can load from?
a) default-src
b) script-src
c) frame-src
d) object-src

163. Input validation fails against XSS primarily because:
a) JavaScript is encrypted
b) Filters can be bypassed
c) Browsers block scripts
d) HTTPS stops injection

164. Cross-Site Request Forgery (CSRF) exploits the fact that:
a) Browsers allow cross-origin scripts
b) Browsers automatically include credentials
c) Cookies are encrypted
d) SOP blocks requests

165. CSRF attacks succeed even though SOP exists because:
a) SOP blocks reading responses, not sending requests

b) SOP is disabled in HTTPS
c) SOP applies only to scripts
d) SOP allows cookie theft

166. Which CSRF attack scenario is MOST realistic?
a) Attacker steals session cookie via XSS
b) Victim clicks a link transferring funds
c) Attacker queries database
d) Victim downloads malware
167. Referer validation works by:
a) Blocking all external requests
b) Checking source domain of requests
c) Encrypting request headers
d) Changing session Ids
168. Referer-based CSRF protection is unreliable because:
a) Referer headers are encrypted
b) Browsers may omit Referer
c) TLS disables Referer
d) Cookies override Referer
169. The Synchronizer Token Pattern defends against CSRF by:
a) Using predictable tokens
b) Including secret tokens in each request
c) Storing token only in cookies
d) Encrypting request body
170. CSRF tokens must be:
a) Static and reusable
b) Guessable
c) Unique and unpredictable
d) Stored in URLs always
171. Double Submit Cookie defense works by:
a) Storing token only server-side
b) Comparing cookie token with request token
c) Disabling cookies
d) Using CSP
172. Double Submit Cookie does NOT require:
a) Server-side token storage
b) Cookies
c) Client-side scripting
d) HTTPS
173. SameSite=Lax cookies:
a) Are never sent cross-site
b) Are sent on top-level navigation
c) Are less secure than None always
d) Block all POST requests
174. SameSite=Strict provides stronger CSRF protection because:
a) Cookies are encrypted
b) Cookies are never sent on cross-site requests
c) It disables JavaScript
d) It blocks XSS
175. Which SameSite option provides the HIGHEST CSRF protection but lowest usability?

a) None
b) Lax
c) Strict
d) HttpOnly

176. Which combination BEST defends against CSRF in modern browsers?
a) Referer only
b) SameSite cookies only
c) CSRF tokens + SameSite cookies
d) HTTPS only