Web Security Fundamentals

Examination Scope: 25 Questions | 25 Minutes | Passing Standard: 80%

1. EXECUTIVE OVERVIEW & CREDENTIAL STANDARDS

Foundational certification proving practical understanding of web encryption, core HTTP security headers, DNS security, and defen

2. KEY TOPICS & SYLLABUS

* SSL/TLS encryption handshakes and certificates
* HTTP Strict Transport Security (HSTS) mechanics
* Fundamental security headers (X-Frame-Options, X-Content-Type-Options)
* Cookie security flags (HttpOnly, Secure, SameSite)
* Basic DNS security: CAA and SPF introduction
* Exposed server files and dangerous public ports

Examination Integrity & Anti-Cheat Protocols:

* Correct answer keys are evaluated strictly server-side and never sent to client devices.
* Questions and multiple-choice options are dynamically shuffled per individual session.
* Time limits are strictly enforced on the server; background blur/tab switches are audited.

CHAPTER 1: SSL/TLS & Transport Layer Security

How transport encryption protects data in transit and why certificates expire.

Transport Layer Security (TLS) encrypts the communication channel between web browsers and servers. Modern web security mandates TLS 1.3 or TLS 1.2 with strong ephemeral ciphers (ECDHE). Without TLS, network intermediaries (ISPs, public Wi-Fi operators) can intercept credentials, session tokens, and tamper with page content (Man-in-the-Middle attacks). SSL certificates must be issued by a trusted Certificate Authority (CA) and renewed regularly. Certificates expired even by a single minute cause browsers to display fatal full-page security warnings.

```
# Nginx SSL Configuration
ssl_protocols TLSv1.2 TLSv1.3;
ssl_prefer_server_ciphers off;
ssl_ciphers "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256";
```

CHAPTER 2: HTTP Strict Transport Security (HSTS)

Enforcing HTTPS connections and preventing SSL-stripping attacks.

Even if a site supports HTTPS, users often type http:// or click plaintext links. Attackers can execute SSL-stripping to downgrade connections to plaintext HTTP. The Strict-Transport-Security header instructs browsers to never make an unencrypted HTTP connection to the host for a specified duration (max-age). To score A+ on SurfaceScan, max-age must be at least 31,536,000 seconds (1 year) and include the includeSubDomains directive.

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

CHAPTER 3: Fundamental HTTP Security Headers

X-Frame-Options, X-Content-Type-Options, and Referrer-Policy.

Security headers are lightweight directives sent in server HTTP responses to enable browser-level security defenses:
1. X-Frame-Options: Set to DENY or SAMEORIGIN to prevent Clickjacking (embedding your site in hidden iframes to hijack clicks).
2. X-Content-Type-Options: Set to nosniff to stop browsers from MIME-sniffing files (e.g. executing an image upload as JavaScript).
3. Referrer-Policy: Set to strict-origin-when-cross-origin to protect sensitive query parameters and URL tokens from leaking to external analytics or third-party links.

```
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin-when-cross-origin
```

© 2026 SurfaceScan · CWSF Certification Curriculum

CHAPTER 4: Cookie Hardening: HttpOnly, Secure & SameSite

Preventing session hijacking via XSS and CSRF attacks.

Session cookies are the keys to user accounts. If stolen, attackers gain full access without needing passwords:

- HttpOnly: Disallows client-side JavaScript (document.cookie) from accessing the cookie, blocking token exfiltration via Cross-Site Scripting (XSS).
- Secure: Guarantees the browser will only transmit the cookie over encrypted TLS/HTTPS connections.
- SameSite=Lax or SameSite=Strict: Prevents the cookie from being sent along with cross-site requests, mitigating Cross-Site Request Forgery (CSRF).

```
Set-Cookie: session_id=xyz789; Path=/; Secure; HttpOnly; SameSite=Lax
```

CHAPTER 5: Exposed Files, Git Repositories & Open Ports

Recognizing reconnaissance vulnerabilities before attackers exploit them.

Attackers continuously run automated scans looking for exposed environment files (/.env) and source control metadata (/.git/HEAD). An exposed .env file immediately leaks database passwords, Stripe keys, and JWT secrets. An exposed .git repository allows complete source code reconstruction. Furthermore, database ports (MySQL 3306, PostgreSQL 5432, Redis 6379, MongoDB 27017) and remote administration ports (RDP 3389, Telnet 23) should never be exposed to the public Internet; they must be bound to 127.0.0.1 or guarded by private VPNs.

```
# Apache .htaccess: Deny access to hidden files and .env
<FilesMatch "^(\.git|\.env|\.yml|composer\.json)">
  Order allow,deny
  Deny from all
</FilesMatch>
```

© 2026 SurfaceScan · CWSF Certification Curriculum