

PHP Security Cheatsheet: PDO, XSS und CSRF

PRAXISLEITFADEN | Stand: 27. Oktober 2026 | Kostenlos

1. SQL-Injection verhindern

Vorgehen: Nutze PDO mit Prepared Statements und parametrisierten Werten; SQL-Bezeichner nicht ungeprüft übernehmen.

Beispiel: `$stmt = $pdo->prepare("SELECT * FROM users WHERE id = :id");
$stmt->execute(["id" => $id]);`

Prüfkriterium: Sonderzeichen im Parameter verändern nicht die Abfrage.

Vermeiden: SQL durch Escaping oder Stringverkettung zusammenbauen.

2. XSS vermeiden

Vorgehen: Escape dynamische HTML-Ausgaben kontextgerecht; für HTML-Text `htmlspecialchars` mit `ENT_QUOTES` und UTF-8.

Beispiel: `echo htmlspecialchars($name, ENT_QUOTES | ENT_SUBSTITUTE, "UTF-8");`

Prüfkriterium: Eingegebene Tags werden als Text angezeigt.

Vermeiden: HTML-Escaping für JavaScript- oder URL-Kontexte blind wiederverwenden.

3. CSRF-Schutz

Vorgehen: Nutze zufällige Session-Tokens für zustandsändernde Formulare und prüfe sie mit `hash_equals`.

Beispiel: `if (!hash_equals($_SESSION["csrf"], $_POST["csrf"] ?? "")) { http_response_code(403); exit; }`

Prüfkriterium: Formular ohne gültigen Token wird abgewiesen.

Vermeiden: Nur auf SameSite-Cookies als universellen Schutz vertrauen.

4. Sitzungen absichern

Vorgehen: Aktiviere `Secure/HttpOnly/SameSite`, erneuere Session-ID nach Login und setze angemessene Timeouts.

Beispiel: `session_regenerate_id(true);`

Prüfkriterium: Nach Login ist die Session-ID gewechselt und Cookies sind passend markiert.

Vermeiden: Session-IDs in URLs übertragen.

5. Uploads validieren

Vorgehen: Prüfe Größe, MIME-Typ serverseitig und Dateiinhalte; speichere mit zufälligem Namen außerhalb ausführbarer Pfade.

Beispiel: `finfo_file()` und `random_bytes()` für Dateinamen.

Prüfkriterium: Hochgeladene Dateien sind nicht als PHP ausführbar.

Vermeiden: Dateiendung oder Browser-MIME ungeprüft vertrauen.

Fachquellen

PHP: Security – <https://www.php.net/manual/en/security.php>

OWASP Cheat Sheets – <https://cheatsheetseries.owasp.org/>

Onlineversion: <https://www.cyberknecht.de/wissen/cheatsheets/php-security-cheatsheet.html>