**Web Vulnerabilities Methodology**

In every Web Pentest, there are **several hidden and obvious places that might be vulnerable**. This post is meant to be a checklist to confirm that you have searched for vulnerabilities in all the possible places.

## Proxies

Nowadays **web** **applications** usually **uses** some kind of **intermediary** **proxies**, those may be (ab)used to exploit vulnerabilities. These vulnerabilities need a vulnerable proxy to be in place, but they usually also need some extra vulnerability in the backend.

* [**Abusing hop-by-hop headers**](https://book.hacktricks.xyz/pentesting-web/abusing-hop-by-hop-headers)
* [**Cache Poisoning/Cache Deception**](https://book.hacktricks.xyz/pentesting-web/cache-deception)
* [**HTTP Request Smuggling**](https://book.hacktricks.xyz/pentesting-web/http-request-smuggling)
* [**H2C Smuggling**](https://book.hacktricks.xyz/pentesting-web/h2c-smuggling)
* [**Server Side Inclusion/Edge Side Inclusion**](https://book.hacktricks.xyz/pentesting-web/server-side-inclusion-edge-side-inclusion-injection)
* [**Uncovering Cloudflare**](https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/uncovering-cloudflare)
* [**XSLT Server Side Injection**](https://book.hacktricks.xyz/pentesting-web/xslt-server-side-injection-extensible-stylesheet-language-transformations)
* [**Proxy / WAF Protections Bypass**](https://book.hacktricks.xyz/pentesting-web/proxy-waf-protections-bypass)

## **User input**

Most of the web applications will **allow users to input some data that will be processed later.** Depending on the structure of the data the server is expecting some vulnerabilities may or may not apply.

### **Reflected Values**

If the introduced data may somehow be reflected in the response, the page might be vulnerable to several issues.

* [**Client Side Template Injection**](https://book.hacktricks.xyz/pentesting-web/client-side-template-injection-csti)
* [**Command Injection**](https://book.hacktricks.xyz/pentesting-web/command-injection)
* [**CRLF**](https://book.hacktricks.xyz/pentesting-web/crlf-0d-0a)
* [**Dangling Markup**](https://book.hacktricks.xyz/pentesting-web/dangling-markup-html-scriptless-injection)
* [**File Inclusion/Path Traversal**](https://book.hacktricks.xyz/pentesting-web/file-inclusion)
* [**Open Redirect**](https://book.hacktricks.xyz/pentesting-web/open-redirect)
* [**Prototype Pollution to XSS**](https://book.hacktricks.xyz/pentesting-web/deserialization/nodejs-proto-prototype-pollution#client-side-prototype-pollution-to-xss)
* [**Server Side Inclusion/Edge Side Inclusion**](https://book.hacktricks.xyz/pentesting-web/server-side-inclusion-edge-side-inclusion-injection)
* [**Server Side Request Forgery**](https://book.hacktricks.xyz/pentesting-web/ssrf-server-side-request-forgery)
* [**Server Side Template Injection**](https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection)
* [**Reverse Tab Nabbing**](https://book.hacktricks.xyz/pentesting-web/reverse-tab-nabbing)
* [**XSLT Server Side Injection**](https://book.hacktricks.xyz/pentesting-web/xslt-server-side-injection-extensible-stylesheet-language-transformations)
* [**XSS**](https://book.hacktricks.xyz/pentesting-web/xss-cross-site-scripting)
* [**XSSI**](https://book.hacktricks.xyz/pentesting-web/xssi-cross-site-script-inclusion)
* [**XS-Search**](https://book.hacktricks.xyz/pentesting-web/xs-search)

Some of the mentioned vulnerabilities require special conditions, others just require the content to be reflected. You can find some interesting polygloths to test quickly the vulnerabilities in:

[PAGEReflecting Techniques - PoCs and Polygloths CheatSheet](https://book.hacktricks.xyz/pentesting-web/pocs-and-polygloths-cheatsheet)

### **Search functionalities**

If the functionality may be used to search some kind of data inside the backend, maybe you can (ab)use it to search arbitrary data.

* [**File Inclusion/Path Traversal**](https://book.hacktricks.xyz/pentesting-web/file-inclusion)
* [**NoSQL Injection**](https://book.hacktricks.xyz/pentesting-web/nosql-injection)
* [**LDAP Injection**](https://book.hacktricks.xyz/pentesting-web/ldap-injection)
* [**ReDoS**](https://book.hacktricks.xyz/pentesting-web/regular-expression-denial-of-service-redos)
* [**SQL Injection**](https://book.hacktricks.xyz/pentesting-web/sql-injection)
* [**XPATH Injection**](https://book.hacktricks.xyz/pentesting-web/xpath-injection)

### **Forms, WebSockets and PostMsgs**

When a websocket posts a message or a form allowing users to perform actions vulnerabilities may arise.

* [**Cross Site Request Forgery**](https://book.hacktricks.xyz/pentesting-web/csrf-cross-site-request-forgery)
* [**Cross-site WebSocket hijacking (CSWSH)**](https://book.hacktricks.xyz/pentesting-web/websocket-attacks)
* [**PostMessage Vulnerabilities**](https://book.hacktricks.xyz/pentesting-web/postmessage-vulnerabilities)

### **HTTP Headers**

Depending on the HTTP headers given by the web server some vulnerabilities might be present.

* [**Clickjacking**](https://book.hacktricks.xyz/pentesting-web/clickjacking)
* [**Content Security Policy bypass**](https://book.hacktricks.xyz/pentesting-web/content-security-policy-csp-bypass)
* [**Cookies Hacking**](https://book.hacktricks.xyz/pentesting-web/hacking-with-cookies)
* [**CORS - Misconfigurations & Bypass**](https://book.hacktricks.xyz/pentesting-web/cors-bypass)

### **Bypasses**

There are several specific functionalities where some workarounds might be useful to bypass them

* [**2FA/OTP Bypass**](https://book.hacktricks.xyz/pentesting-web/2fa-bypass)
* [**Bypass Payment Process**](https://book.hacktricks.xyz/pentesting-web/bypass-payment-process)
* [**Captcha Bypass**](https://book.hacktricks.xyz/pentesting-web/captcha-bypass)
* [**Login Bypass**](https://book.hacktricks.xyz/pentesting-web/login-bypass)
* [**Race Condition**](https://book.hacktricks.xyz/pentesting-web/race-condition)
* [**Rate Limit Bypass**](https://book.hacktricks.xyz/pentesting-web/rate-limit-bypass)
* [**Reset Forgotten Password Bypass**](https://book.hacktricks.xyz/pentesting-web/reset-password)
* [**Registration Vulnerabilities**](https://book.hacktricks.xyz/pentesting-web/registration-vulnerabilities)

### **Structured objects / Specific functionalities**

Some functionalities will require the **data to be structured in a very specific format** (like a language serialized object or XML). Therefore, it's easier to identify if the application might be vulnerable as it needs to be processing that kind of data. Some **specific functionalities** may be also vulnerable if a **specific format of the input is used** (like Email Header Injections).

* [**Deserialization**](https://book.hacktricks.xyz/pentesting-web/deserialization)
* [**Email Header Injection**](https://book.hacktricks.xyz/pentesting-web/email-injections)
* [**JWT Vulnerabilities**](https://book.hacktricks.xyz/pentesting-web/hacking-jwt-json-web-tokens)
* [**XML External Entity**](https://book.hacktricks.xyz/pentesting-web/xxe-xee-xml-external-entity)

### Files

Functionalities that allow uploading files might be vulnerable to several issues. Functionalities that generate files including user input might execute unexpected code. Users that open files uploaded by users or automatically generated including user input might be compromised.

* [**File Upload**](https://book.hacktricks.xyz/pentesting-web/file-upload)
* [**Formula Injection**](https://book.hacktricks.xyz/pentesting-web/formula-csv-doc-latex-ghostscript-injection)
* [**PDF Injection**](https://book.hacktricks.xyz/pentesting-web/xss-cross-site-scripting/pdf-injection)
* [**Server Side XSS**](https://book.hacktricks.xyz/pentesting-web/xss-cross-site-scripting/server-side-xss-dynamic-pdf)

### **External Identity Management**

* [**OAUTH to Account takeover**](https://book.hacktricks.xyz/pentesting-web/oauth-to-account-takeover)
* [**SAML Attacks**](https://book.hacktricks.xyz/pentesting-web/saml-attacks)

### **Other Helpful Vulnerabilities**

These vulnerabilities might help to exploit other vulnerabilities.

* [**Domain/Subdomain takeover**](https://book.hacktricks.xyz/pentesting-web/domain-subdomain-takeover)
* [**IDOR**](https://book.hacktricks.xyz/pentesting-web/idor)
* [**Parameter Pollution**](https://book.hacktricks.xyz/pentesting-web/parameter-pollution)
* [**Unicode Normalization vulnerability**](https://book.hacktricks.xyz/pentesting-web/unicode-injection)