**Web Security**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| [**File upload vulnerabilities**](https://portswigger.net/web-security/file-upload) | | | | |
|  | [What are file upload vulnerabilities?](https://portswigger.net/web-security/file-upload#what-are-file-upload-vulnerabilities) | | | |
|  | [What is the impact of file upload vulnerabilities?](https://portswigger.net/web-security/file-upload#what-is-the-impact-of-file-upload-vulnerabilities) | | | |
|  | [How do file upload vulnerabilities arise?](https://portswigger.net/web-security/file-upload#how-do-file-upload-vulnerabilities-arise) | | | |
|  | [How do web servers handle requests for static files?](https://portswigger.net/web-security/file-upload#how-do-web-servers-handle-requests-for-static-files) | | | |
|  | [Exploiting unrestricted file uploads to deploy a web shell](https://portswigger.net/web-security/file-upload#exploiting-unrestricted-file-uploads-to-deploy-a-web-shell) | | | |
|  | [Exploiting flawed validation of file uploads](https://portswigger.net/web-security/file-upload#exploiting-flawed-validation-of-file-uploads) | | | |
|  |  | [Flawed file type validation](https://portswigger.net/web-security/file-upload#flawed-file-type-validation) | | |
|  |  | [Preventing file execution in user-accessible directories](https://portswigger.net/web-security/file-upload#preventing-file-execution-in-user-accessible-directories) | | |
|  |  | [Insufficient blacklisting of dangerous file types](https://portswigger.net/web-security/file-upload#insufficient-blacklisting-of-dangerous-file-types) | | |
|  | [Overriding the server configuration](https://portswigger.net/web-security/file-upload#overriding-the-server-configuration) | | | |
|  | [Obfuscating file extensions](https://portswigger.net/web-security/file-upload#obfuscating-file-extensions) | | | |
|  |  | [Flawed validation of the file's contents](https://portswigger.net/web-security/file-upload#flawed-validation-of-the-file-s-contents) | | |
|  |  | [Exploiting file upload race conditions](https://portswigger.net/web-security/file-upload#exploiting-file-upload-race-conditions) | | |
|  | [Race conditions in URL-based file uploads](https://portswigger.net/web-security/file-upload#race-conditions-in-url-based-file-uploads) | | | |
|  | [Exploiting file upload vulnerabilities without remote code execution](https://portswigger.net/web-security/file-upload#exploiting-file-upload-vulnerabilities-without-remote-code-execution) | | | |
|  |  | [Uploading malicious client-side scripts](https://portswigger.net/web-security/file-upload#uploading-malicious-client-side-scripts) | | |
|  |  | [Exploiting vulnerabilities in the parsing of uploaded files](https://portswigger.net/web-security/file-upload#exploiting-vulnerabilities-in-the-parsing-of-uploaded-files) | | |
|  | [Uploading files using PUT](https://portswigger.net/web-security/file-upload#uploading-files-using-put) | | | |
|  | [How to prevent file upload vulnerabilities](https://portswigger.net/web-security/file-upload#how-to-prevent-file-upload-vulnerabilities) | | | |
| [**OAuth 2.0 authentication vulnerabilities**](https://portswigger.net/web-security/oauth) | | | | |
|  | [What is OAuth?](https://portswigger.net/web-security/oauth#what-is-oauth) | | | |
|  | [How does OAuth 2.0 work?](https://portswigger.net/web-security/oauth#how-does-oauth-2-0-work) | | | |
|  |  | [OAuth authentication](https://portswigger.net/web-security/oauth#oauth-authentication) | | |
|  | [How do OAuth authentication vulnerabilities arise?](https://portswigger.net/web-security/oauth#how-do-oauth-authentication-vulnerabilities-arise) | | | |
|  | [Identifying OAuth authentication](https://portswigger.net/web-security/oauth#identifying-oauth-authentication) | | | |
|  | [Recon](https://portswigger.net/web-security/oauth#recon) | | | |
|  | [Exploiting OAuth authentication vulnerabilities](https://portswigger.net/web-security/oauth#exploiting-oauth-authentication-vulnerabilities) | | | |
|  |  | [Vulnerabilities in the OAuth client application](https://portswigger.net/web-security/oauth#vulnerabilities-in-the-oauth-client-application) | | |
|  | [Improper implementation of the implicit grant type](https://portswigger.net/web-security/oauth#improper-implementation-of-the-implicit-grant-type) | | | |
|  | [Flawed CSRF protection](https://portswigger.net/web-security/oauth#flawed-csrf-protection) | | | |
|  |  | [Leaking authorization codes and access tokens](https://portswigger.net/web-security/oauth#leaking-authorization-codes-and-access-tokens) | | |
|  |  | [Flawed scope validation](https://portswigger.net/web-security/oauth#flawed-scope-validation) | | |
|  |  | [Unverified user registration](https://portswigger.net/web-security/oauth#unverified-user-registration) | | |
|  | [Extending OAuth with OpenID Connect](https://portswigger.net/web-security/oauth#extending-oauth-with-openid-connect) | | | |
|  | [Preventing OAuth authentication vulnerabilities](https://portswigger.net/web-security/oauth#preventing-oauth-authentication-vulnerabilities) | | | |
|  | [How to prevent OAuth authentication vulnerabilities](https://portswigger.net/web-security/oauth/preventing) | | | |
|  |  | [For OAuth service providers](https://portswigger.net/web-security/oauth/preventing#for-oauth-service-providers) | | |
|  |  | [For OAuth client applications](https://portswigger.net/web-security/oauth/preventing#for-oauth-client-applications) | | |
|  | [OAuth grant types](https://portswigger.net/web-security/oauth/grant-types) | | | |
|  |  | [What is an OAuth grant type?](https://portswigger.net/web-security/oauth/grant-types#what-is-an-oauth-grant-type) | | |
|  |  | [OAuth scopes](https://portswigger.net/web-security/oauth/grant-types#oauth-scopes) | | |
|  |  | [Authorization code grant type](https://portswigger.net/web-security/oauth/grant-types#authorization-code-grant-type) | | |
|  |  | [Implicit grant type](https://portswigger.net/web-security/oauth/grant-types#implicit-grant-type) | | |
|  | [OpenID Connect](https://portswigger.net/web-security/oauth/openid) | | | |
|  |  | [What is OpenID Connect?](https://portswigger.net/web-security/oauth/openid#what-is-openid-connect) | | |
|  |  | [How does OpenID Connect work?](https://portswigger.net/web-security/oauth/openid#how-does-openid-connect-work) | | |
|  |  |  | [OpenID Connect roles](https://portswigger.net/web-security/oauth/openid#openid-connect-roles) | |
|  |  |  | [OpenID Connect claims and scopes](https://portswigger.net/web-security/oauth/openid#openid-connect-claims-and-scopes) | |
|  |  |  | [ID token](https://portswigger.net/web-security/oauth/openid#id-token) | |
|  |  | [Identifying OpenID Connect](https://portswigger.net/web-security/oauth/openid#identifying-openid-connect) | | |
|  |  | [OpenID Connect vulnerabilities](https://portswigger.net/web-security/oauth/openid#openid-connect-vulnerabilities) | | |
|  |  |  | [Unprotected dynamic client registration](https://portswigger.net/web-security/oauth/openid#unprotected-dynamic-client-registration) | |
|  |  |  | [Allowing authorization requests by reference](https://portswigger.net/web-security/oauth/openid#allowing-authorization-requests-by-reference) | |
| [**HTTP Host header attacks**](https://portswigger.net/web-security/host-header) | | | | |
|  | [What is the HTTP Host header?](https://portswigger.net/web-security/host-header#what-is-the-http-host-header) | | | |
|  | [What is the purpose of the HTTP Host header?](https://portswigger.net/web-security/host-header#what-is-the-purpose-of-the-http-host-header) | | | |
|  |  | [Virtual hosting](https://portswigger.net/web-security/host-header#virtual-hosting) | | |
|  |  | [Routing traffic via an intermediary](https://portswigger.net/web-security/host-header#routing-traffic-via-an-intermediary) | | |
|  |  | [How does the HTTP Host header solve this problem?](https://portswigger.net/web-security/host-header#how-does-the-http-host-header-solve-this-problem) | | |
|  | [What is an HTTP Host header attack?](https://portswigger.net/web-security/host-header#what-is-an-http-host-header-attack) | | | |
|  | [How do HTTP Host header vulnerabilities arise?](https://portswigger.net/web-security/host-header#how-do-http-host-header-vulnerabilities-arise) | | | |
|  | [Exploiting HTTP Host header vulnerabilities](https://portswigger.net/web-security/host-header#exploiting-http-host-header-vulnerabilities) | | | |
|  | [How to prevent HTTP Host header attacks](https://portswigger.net/web-security/host-header#how-to-prevent-http-host-header-attacks) | | | |
|  | [How to identify and exploit HTTP Host header vulnerabilities](https://portswigger.net/web-security/host-header/exploiting) | | | |
|  |  | [How to test for vulnerabilities using the HTTP Host header](https://portswigger.net/web-security/host-header/exploiting#how-to-test-for-vulnerabilities-using-the-http-host-header) | | |
|  |  |  | [Supply an arbitrary Host header](https://portswigger.net/web-security/host-header/exploiting#supply-an-arbitrary-host-header) | |
|  |  |  | [Check for flawed validation](https://portswigger.net/web-security/host-header/exploiting#check-for-flawed-validation) | |
|  |  |  | [Send ambiguous requests](https://portswigger.net/web-security/host-header/exploiting#send-ambiguous-requests) | |
|  |  |  | [Inject host override headers](https://portswigger.net/web-security/host-header/exploiting#inject-host-override-headers) | |
|  |  | [How to exploit the HTTP Host header](https://portswigger.net/web-security/host-header/exploiting#how-to-exploit-the-http-host-header) | | |
|  |  |  | [Password reset poisoning](https://portswigger.net/web-security/host-header/exploiting#password-reset-poisoning) | |
|  |  |  | [Web cache poisoning via the Host header](https://portswigger.net/web-security/host-header/exploiting#web-cache-poisoning-via-the-host-header) | |
|  |  |  | [Exploiting classic server-side vulnerabilities](https://portswigger.net/web-security/host-header/exploiting#exploiting-classic-server-side-vulnerabilities) | |
|  |  |  | [Accessing restricted functionality](https://portswigger.net/web-security/host-header/exploiting#accessing-restricted-functionality) | |
|  |  |  | [Accessing internal websites with virtual host brute-forcing](https://portswigger.net/web-security/host-header/exploiting#accessing-internal-websites-with-virtual-host-brute-forcing) | |
|  |  |  | [Routing-based SSRF](https://portswigger.net/web-security/host-header/exploiting#routing-based-ssrf) | |
|  |  | [Password reset poisoning](https://portswigger.net/web-security/host-header/exploiting/password-reset-poisoning) | | |
|  |  |  | [How does a password reset work?](https://portswigger.net/web-security/host-header/exploiting/password-reset-poisoning#how-does-a-password-reset-work) | |
|  |  |  | [How to construct a password reset poisoning attack](https://portswigger.net/web-security/host-header/exploiting/password-reset-poisoning#how-to-construct-a-password-reset-poisoning-attack) | |
| [**Business logic vulnerabilities**](https://portswigger.net/web-security/logic-flaws) | | | | |
|  | [What are business logic vulnerabilities?](https://portswigger.net/web-security/logic-flaws#what-are-business-logic-vulnerabilities) | | | |
|  | [How do business logic vulnerabilities arise?](https://portswigger.net/web-security/logic-flaws#how-do-business-logic-vulnerabilities-arise) | | | |
|  | [What is the impact of business logic vulnerabilities?](https://portswigger.net/web-security/logic-flaws#what-is-the-impact-of-business-logic-vulnerabilities) | | | |
|  | [What are some examples of business logic vulnerabilities?](https://portswigger.net/web-security/logic-flaws#what-are-some-examples-of-business-logic-vulnerabilities) | | | |
|  | [How to prevent business logic vulnerabilities](https://portswigger.net/web-security/logic-flaws#how-to-prevent-business-logic-vulnerabilities) | | | |
|  | [Examples of business logic vulnerabilities](https://portswigger.net/web-security/logic-flaws/examples) | | | |
|  |  | [Excessive trust in client-side controls](https://portswigger.net/web-security/logic-flaws/examples#excessive-trust-in-client-side-controls) | | |
|  |  | [Failing to handle unconventional input](https://portswigger.net/web-security/logic-flaws/examples#failing-to-handle-unconventional-input) | | |
|  |  | [Making flawed assumptions about user behavior](https://portswigger.net/web-security/logic-flaws/examples#making-flawed-assumptions-about-user-behavior) | | |
|  |  |  | [Trusted users won't always remain trustworthy](https://portswigger.net/web-security/logic-flaws/examples#trusted-users-won-t-always-remain-trustworthy) | |
|  |  |  | [Users won't always supply mandatory input](https://portswigger.net/web-security/logic-flaws/examples#users-won-t-always-supply-mandatory-input) | |
|  |  |  | [Users won't always follow the intended sequence](https://portswigger.net/web-security/logic-flaws/examples#users-won-t-always-follow-the-intended-sequence) | |
|  |  | [Domain-specific flaws](https://portswigger.net/web-security/logic-flaws/examples#domain-specific-flaws) | | |
|  |  | [Providing an encryption oracle](https://portswigger.net/web-security/logic-flaws/examples#providing-an-encryption-oracle) | | |
| [**SQL injection**](https://portswigger.net/web-security/sql-injection) | | | | |
|  | [What is SQL injection (SQLi)?](https://portswigger.net/web-security/sql-injection#what-is-sql-injection-sqli) | | | |
|  | [What is the impact of a successful SQL injection attack?](https://portswigger.net/web-security/sql-injection#what-is-the-impact-of-a-successful-sql-injection-attack) | | | |
|  | [SQL injection examples](https://portswigger.net/web-security/sql-injection#sql-injection-examples) | | | |
|  | [Retrieving hidden data](https://portswigger.net/web-security/sql-injection#retrieving-hidden-data) | | | |
|  | [Subverting application logic](https://portswigger.net/web-security/sql-injection#subverting-application-logic) | | | |
|  | [Retrieving data from other database tables](https://portswigger.net/web-security/sql-injection#retrieving-data-from-other-database-tables) | | | |
|  | [Examining the database](https://portswigger.net/web-security/sql-injection#examining-the-database) | | | |
|  | [Blind SQL injection vulnerabilities](https://portswigger.net/web-security/sql-injection#blind-sql-injection-vulnerabilities) | | | |
|  | [How to detect SQL injection vulnerabilities](https://portswigger.net/web-security/sql-injection#how-to-detect-sql-injection-vulnerabilities) | | | |
|  | [SQL injection in different parts of the query](https://portswigger.net/web-security/sql-injection#sql-injection-in-different-parts-of-the-query) | | | |
|  | [Second-order SQL injection](https://portswigger.net/web-security/sql-injection#second-order-sql-injection) | | | |
|  | [Database-specific factors](https://portswigger.net/web-security/sql-injection#database-specific-factors) | | | |
|  | [How to prevent SQL injection](https://portswigger.net/web-security/sql-injection#how-to-prevent-sql-injection) | | | |
|  | [SQL injection UNION attacks](https://portswigger.net/web-security/sql-injection/union-attacks) | | | |
|  |  | [Determining the number of columns required in an SQL injection UNION attack](https://portswigger.net/web-security/sql-injection/union-attacks#determining-the-number-of-columns-required-in-an-sql-injection-union-attack) | | |
|  |  | [Finding columns with a useful data type in an SQL injection UNION attack](https://portswigger.net/web-security/sql-injection/union-attacks#finding-columns-with-a-useful-data-type-in-an-sql-injection-union-attack) | | |
|  |  | [Using an SQL injection UNION attack to retrieve interesting data](https://portswigger.net/web-security/sql-injection/union-attacks#using-an-sql-injection-union-attack-to-retrieve-interesting-data) | | |
|  |  | [Retrieving multiple values within a single column](https://portswigger.net/web-security/sql-injection/union-attacks#retrieving-multiple-values-within-a-single-column) | | |
|  | [Examining the database in SQL injection attacks](https://portswigger.net/web-security/sql-injection/examining-the-database) | | | |
|  |  | [Querying the database type and version](https://portswigger.net/web-security/sql-injection/examining-the-database#querying-the-database-type-and-version) | | |
|  |  | [Listing the contents of the database](https://portswigger.net/web-security/sql-injection/examining-the-database#listing-the-contents-of-the-database) | | |
|  |  |  | [Equivalent to information schema on Oracle](https://portswigger.net/web-security/sql-injection/examining-the-database#equivalent-to-information-schema-on-oracle) | |
|  | [Blind SQL injection](https://portswigger.net/web-security/sql-injection/blind) | | | |
|  |  | [What is blind SQL injection?](https://portswigger.net/web-security/sql-injection/blind#what-is-blind-sql-injection) | | |
|  |  | [Exploiting blind SQL injection by triggering conditional responses](https://portswigger.net/web-security/sql-injection/blind#exploiting-blind-sql-injection-by-triggering-conditional-responses) | | |
|  |  | [Inducing conditional responses by triggering SQL errors](https://portswigger.net/web-security/sql-injection/blind#inducing-conditional-responses-by-triggering-sql-errors) | | |
|  |  | [Exploiting blind SQL injection by triggering time delays](https://portswigger.net/web-security/sql-injection/blind#exploiting-blind-sql-injection-by-triggering-time-delays) | | |
|  |  | [Exploiting blind SQL injection using out-of-band (OAST) techniques](https://portswigger.net/web-security/sql-injection/blind#exploiting-blind-sql-injection-using-out-of-band-oast-techniques) | | |
|  |  | [How to prevent blind SQL injection attacks?](https://portswigger.net/web-security/sql-injection/blind#how-to-prevent-blind-sql-injection-attacks) | | |
|  | [SQL injection cheat sheet](https://portswigger.net/web-security/sql-injection/cheat-sheet) | | | |
|  |  | [String concatenation](https://portswigger.net/web-security/sql-injection/cheat-sheet#string-concatenation) | | |
|  |  | [Substring](https://portswigger.net/web-security/sql-injection/cheat-sheet#substring) | | |
|  |  | [Comments](https://portswigger.net/web-security/sql-injection/cheat-sheet#comments) | | |
|  |  | [Database version](https://portswigger.net/web-security/sql-injection/cheat-sheet#database-version) | | |
|  |  | [Database contents](https://portswigger.net/web-security/sql-injection/cheat-sheet#database-contents) | | |
|  |  | [Conditional errors](https://portswigger.net/web-security/sql-injection/cheat-sheet#conditional-errors) | | |
|  |  | [Batched (or stacked) queries](https://portswigger.net/web-security/sql-injection/cheat-sheet#batched-or-stacked-queries) | | |
|  |  | [Time delays](https://portswigger.net/web-security/sql-injection/cheat-sheet#time-delays) | | |
|  |  | [Conditional time delays](https://portswigger.net/web-security/sql-injection/cheat-sheet#conditional-time-delays) | | |
|  |  | [DNS lookup](https://portswigger.net/web-security/sql-injection/cheat-sheet#dns-lookup) | | |
|  |  | [DNS lookup with data exfiltration](https://portswigger.net/web-security/sql-injection/cheat-sheet#dns-lookup-with-data-exfiltration) | | |
| [**Cross-site scripting**](https://portswigger.net/web-security/cross-site-scripting) | | | | |
|  | [What is cross-site scripting (XSS)?](https://portswigger.net/web-security/cross-site-scripting#what-is-cross-site-scripting-xss) | | | |
|  | [How does XSS work?](https://portswigger.net/web-security/cross-site-scripting#how-does-xss-work) | | | |
|  | [XSS proof of concept](https://portswigger.net/web-security/cross-site-scripting#xss-proof-of-concept) | | | |
|  | [What are the types of XSS attacks?](https://portswigger.net/web-security/cross-site-scripting#what-are-the-types-of-xss-attacks) | | | |
|  | [Reflected cross-site scripting](https://portswigger.net/web-security/cross-site-scripting#reflected-cross-site-scripting) | | | |
|  | [Stored cross-site scripting](https://portswigger.net/web-security/cross-site-scripting#stored-cross-site-scripting) | | | |
|  | [DOM-based cross-site scripting](https://portswigger.net/web-security/cross-site-scripting#dom-based-cross-site-scripting) | | | |
|  | [What can XSS be used for?](https://portswigger.net/web-security/cross-site-scripting#what-can-xss-be-used-for) | | | |
|  | [Impact of XSS vulnerabilities](https://portswigger.net/web-security/cross-site-scripting#impact-of-xss-vulnerabilities) | | | |
|  | [How to find and test for XSS vulnerabilities](https://portswigger.net/web-security/cross-site-scripting#how-to-find-and-test-for-xss-vulnerabilities) | | | |
|  | [Content security policy](https://portswigger.net/web-security/cross-site-scripting#content-security-policy) | | | |
|  | [Dangling markup injection](https://portswigger.net/web-security/cross-site-scripting#dangling-markup-injection) | | | |
|  | [How to prevent XSS attacks](https://portswigger.net/web-security/cross-site-scripting#how-to-prevent-xss-attacks) | | | |
|  | [Common questions about cross-site scripting](https://portswigger.net/web-security/cross-site-scripting#common-questions-about-cross-site-scripting) | | | |
|  | [Reflected XSS](https://portswigger.net/web-security/cross-site-scripting/reflected) | | | |
|  |  | [What is reflected cross-site scripting?](https://portswigger.net/web-security/cross-site-scripting/reflected#what-is-reflected-cross-site-scripting) | | |
|  |  | [Impact of reflected XSS attacks](https://portswigger.net/web-security/cross-site-scripting/reflected#impact-of-reflected-xss-attacks) | | |
|  |  | [Reflected XSS in different contexts](https://portswigger.net/web-security/cross-site-scripting/reflected#reflected-xss-in-different-contexts) | | |
|  |  | [How to find and test for reflected XSS vulnerabilities](https://portswigger.net/web-security/cross-site-scripting/reflected#how-to-find-and-test-for-reflected-xss-vulnerabilities) | | |
|  |  | [Common questions about reflected cross-site scripting](https://portswigger.net/web-security/cross-site-scripting/reflected#common-questions-about-reflected-cross-site-scripting) | | |
|  | [Cross-site scripting (XSS) cheat sheet](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet) | | | |
|  |  | [Event handlers](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#event-handlers) | | |
|  |  |  | [Event handlers that do not require user interaction](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#event-handlers-that-do-not-require-user-interaction) | |
|  |  |  | [Event handlers that do require user interaction](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#event-handlers-that-do-require-user-interaction) | |
|  |  | [Restricted characters](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#restricted-characters) | | |
|  |  | [Frameworks](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#frameworks) | | |
|  |  | [Protocols](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#protocols) | | |
|  |  | [Other useful attributes](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#other-useful-attributes) | | |
|  |  | [Special tags](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#special-tags) | | |
|  |  | [Encoding](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#encoding) | | |
|  |  | [Obfuscation](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#obfuscation) | | |
|  |  | [Client-side template injection](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#client-side-template-injection) | | |
|  |  |  | [VueJS reflected](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#vuejs-reflected) | |
|  |  |  | [AngularJS sandbox escapes reflected](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#angularjs-sandbox-escapes-reflected) | |
|  |  |  | [DOM based AngularJS sandbox escapes](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#dom-based-angularjs-sandbox-escapes) | |
|  |  |  | [AngularJS CSP bypasses](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#angularjs-csp-bypasses) | |
|  |  | [Scriptless attacks](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#scriptless-attacks) | | |
|  |  |  | [Dangling markup](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#dangling-markup) | |
|  |  | [Polyglots](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#polyglots) | | |
|  |  | [WAF bypass global objects](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#waf-bypass-global-objects) | | |
|  |  | [Content types](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#content-types) | | |
|  |  | [Response content types](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#response-content-types) | | |
|  |  | [Impossible labs](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#impossible-labs) | | |
|  |  | [Prototype pollution](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#prototype-pollution) | | |
|  |  | [Classic vectors (XSS crypt)](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#classic-vectors-xss-crypt) | | |
|  | [Stored XSS](https://portswigger.net/web-security/cross-site-scripting/stored) | | | |
|  |  | [What is stored cross-site scripting?](https://portswigger.net/web-security/cross-site-scripting/stored#what-is-stored-cross-site-scripting) | | |
|  |  | [Impact of stored XSS attacks](https://portswigger.net/web-security/cross-site-scripting/stored#impact-of-stored-xss-attacks) | | |
|  |  | [Stored XSS in different contexts](https://portswigger.net/web-security/cross-site-scripting/stored#stored-xss-in-different-contexts) | | |
|  |  | [How to find and test for stored XSS vulnerabilities](https://portswigger.net/web-security/cross-site-scripting/stored#how-to-find-and-test-for-stored-xss-vulnerabilities) | | |
|  | [DOM-based XSS](https://portswigger.net/web-security/cross-site-scripting/dom-based) | | | |
|  |  | [What is DOM-based cross-site scripting?](https://portswigger.net/web-security/cross-site-scripting/dom-based#what-is-dom-based-cross-site-scripting) | | |
|  |  | [How to test for DOM-based cross-site scripting](https://portswigger.net/web-security/cross-site-scripting/dom-based#how-to-test-for-dom-based-cross-site-scripting) | | |
|  |  |  | [Testing HTML sinks](https://portswigger.net/web-security/cross-site-scripting/dom-based#testing-html-sinks) | |
|  |  |  | [Testing JavaScript execution sinks](https://portswigger.net/web-security/cross-site-scripting/dom-based#testing-javascript-execution-sinks) | |
|  |  |  | [Testing for DOM XSS using DOM Invader](https://portswigger.net/web-security/cross-site-scripting/dom-based#testing-for-dom-xss-using-dom-invader) | |
|  |  | [Exploiting DOM XSS with different sources and sinks](https://portswigger.net/web-security/cross-site-scripting/dom-based#exploiting-dom-xss-with-different-sources-and-sinks) | | |
|  |  |  | [Sources and sinks in third-party dependencies](https://portswigger.net/web-security/cross-site-scripting/dom-based#sources-and-sinks-in-third-party-dependencies) | |
|  |  | [DOM XSS in jQuery](https://portswigger.net/web-security/cross-site-scripting/dom-based#dom-xss-in-jquery) | | |
|  |  | [DOM XSS in AngularJS](https://portswigger.net/web-security/cross-site-scripting/dom-based#dom-xss-in-angularjs) | | |
|  |  | [DOM XSS combined with reflected and stored data](https://portswigger.net/web-security/cross-site-scripting/dom-based#dom-xss-combined-with-reflected-and-stored-data) | | |
|  |  | [Which sinks can lead to DOM-XSS vulnerabilities?](https://portswigger.net/web-security/cross-site-scripting/dom-based#which-sinks-can-lead-to-dom-xss-vulnerabilities) | | |
|  |  | [How to prevent DOM-XSS vulnerabilities](https://portswigger.net/web-security/cross-site-scripting/dom-based#how-to-prevent-dom-xss-vulnerabilities) | | |
|  | [Exploiting cross-site scripting vulnerabilities](https://portswigger.net/web-security/cross-site-scripting/exploiting) | | | |
|  |  | [Exploiting cross-site scripting to steal cookies](https://portswigger.net/web-security/cross-site-scripting/exploiting#exploiting-cross-site-scripting-to-steal-cookies) | | |
|  |  | [Exploiting cross-site scripting to capture passwords](https://portswigger.net/web-security/cross-site-scripting/exploiting#exploiting-cross-site-scripting-to-capture-passwords) | | |
|  |  | [Exploiting cross-site scripting to perform CSRF](https://portswigger.net/web-security/cross-site-scripting/exploiting#exploiting-cross-site-scripting-to-perform-csrf) | | |
|  | [Cross-site scripting contexts](https://portswigger.net/web-security/cross-site-scripting/contexts) | | | |
|  |  | [XSS between HTML tags](https://portswigger.net/web-security/cross-site-scripting/contexts#xss-between-html-tags) | | |
|  |  | [XSS in HTML tag attributes](https://portswigger.net/web-security/cross-site-scripting/contexts#xss-in-html-tag-attributes) | | |
|  |  | [XSS into JavaScript](https://portswigger.net/web-security/cross-site-scripting/contexts#xss-into-javascript) | | |
|  |  |  | [Terminating the existing script](https://portswigger.net/web-security/cross-site-scripting/contexts#terminating-the-existing-script) | |
|  |  |  | [Breaking out of a JavaScript string](https://portswigger.net/web-security/cross-site-scripting/contexts#breaking-out-of-a-javascript-string) | |
|  |  |  | [Making use of HTML-encoding](https://portswigger.net/web-security/cross-site-scripting/contexts#making-use-of-html-encoding) | |
|  |  |  | [XSS in JavaScript template literals](https://portswigger.net/web-security/cross-site-scripting/contexts#xss-in-javascript-template-literals) | |
|  |  | [XSS in the context of the AngularJS sandbox](https://portswigger.net/web-security/cross-site-scripting/contexts#xss-in-the-context-of-the-angularjs-sandbox) | | |
|  |  | [AngularJS sandbox](https://portswigger.net/web-security/cross-site-scripting/contexts/angularjs-sandbox) | | |
|  |  |  | [What is the AngularJS sandbox?](https://portswigger.net/web-security/cross-site-scripting/contexts/angularjs-sandbox#what-is-the-angularjs-sandbox) | |
|  |  |  | [How does the AngularJS sandbox work?](https://portswigger.net/web-security/cross-site-scripting/contexts/angularjs-sandbox#how-does-the-angularjs-sandbox-work) | |
|  |  |  | [How does an AngularJS sandbox escape work?](https://portswigger.net/web-security/cross-site-scripting/contexts/angularjs-sandbox#how-does-an-angularjs-sandbox-escape-work) | |
|  |  |  | [How does an AngularJS CSP bypass work?](https://portswigger.net/web-security/cross-site-scripting/contexts/angularjs-sandbox#how-does-an-angularjs-csp-bypass-work) | |
|  |  |  | [How to prevent AngularJS injection](https://portswigger.net/web-security/cross-site-scripting/contexts/angularjs-sandbox#how-to-prevent-angularjs-injection) | |
|  | [Content security policy](https://portswigger.net/web-security/cross-site-scripting/content-security-policy) | | | |
|  |  | [What is CSP (content security policy)?](https://portswigger.net/web-security/cross-site-scripting/content-security-policy#what-is-csp-content-security-policy) | | |
|  |  | [Mitigating XSS attacks using CSP](https://portswigger.net/web-security/cross-site-scripting/content-security-policy#mitigating-xss-attacks-using-csp) | | |
|  |  | [Mitigating dangling markup attacks using CSP](https://portswigger.net/web-security/cross-site-scripting/content-security-policy#mitigating-dangling-markup-attacks-using-csp) | | |
|  |  | [Bypassing CSP with policy injection](https://portswigger.net/web-security/cross-site-scripting/content-security-policy#bypassing-csp-with-policy-injection) | | |
|  |  | [Protecting against clickjacking using CSP](https://portswigger.net/web-security/cross-site-scripting/content-security-policy#protecting-against-clickjacking-using-csp) | | |
|  | [Dangling markup injection](https://portswigger.net/web-security/cross-site-scripting/dangling-markup) | | | |
|  |  | [What is dangling markup injection?](https://portswigger.net/web-security/cross-site-scripting/dangling-markup#what-is-dangling-markup-injection) | | |
|  |  | [How to prevent dangling markup attacks](https://portswigger.net/web-security/cross-site-scripting/dangling-markup#how-to-prevent-dangling-markup-attacks) | | |
|  | [How to prevent XSS](https://portswigger.net/web-security/cross-site-scripting/preventing) | | | |
|  |  | [Encode data on output](https://portswigger.net/web-security/cross-site-scripting/preventing#encode-data-on-output) | | |
|  |  | [Validate input on arrival](https://portswigger.net/web-security/cross-site-scripting/preventing#validate-input-on-arrival) | | |
|  |  |  | [Whitelisting vs blacklisting](https://portswigger.net/web-security/cross-site-scripting/preventing#whitelisting-vs-blacklisting) | |
|  |  | [Allowing "safe" HTML](https://portswigger.net/web-security/cross-site-scripting/preventing#allowing-safe-html) | | |
|  |  | [How to prevent XSS using a template engine](https://portswigger.net/web-security/cross-site-scripting/preventing#how-to-prevent-xss-using-a-template-engine) | | |
|  |  | [How to prevent XSS in PHP](https://portswigger.net/web-security/cross-site-scripting/preventing#how-to-prevent-xss-in-php) | | |
|  |  | [How to prevent XSS client-side in JavaScript](https://portswigger.net/web-security/cross-site-scripting/preventing#how-to-prevent-xss-client-side-in-javascript) | | |
|  |  | [How to prevent XSS in jQuery](https://portswigger.net/web-security/cross-site-scripting/preventing#how-to-prevent-xss-in-jquery) | | |
|  |  | [Mitigating XSS using content security policy (CSP)](https://portswigger.net/web-security/cross-site-scripting/preventing#mitigating-xss-using-content-security-policy-csp) | | |
| [**Cross-site request forgery (CSRF)**](https://portswigger.net/web-security/csrf) | | | | |
|  | [What is CSRF?](https://portswigger.net/web-security/csrf#what-is-csrf) | | | |
|  | [What is the impact of a CSRF attack?](https://portswigger.net/web-security/csrf#what-is-the-impact-of-a-csrf-attack) | | | |
|  | [How does CSRF work?](https://portswigger.net/web-security/csrf#how-does-csrf-work) | | | |
|  | [How to construct a CSRF attack](https://portswigger.net/web-security/csrf#how-to-construct-a-csrf-attack) | | | |
|  | [How to deliver a CSRF exploit](https://portswigger.net/web-security/csrf#how-to-deliver-a-csrf-exploit) | | | |
|  | [Preventing CSRF attacks](https://portswigger.net/web-security/csrf#preventing-csrf-attacks) | | | |
|  | [Common CSRF vulnerabilities](https://portswigger.net/web-security/csrf#common-csrf-vulnerabilities) | | | |
|  |  | [Validation of CSRF token depends on request method](https://portswigger.net/web-security/csrf#validation-of-csrf-token-depends-on-request-method) | | |
|  |  | [Validation of CSRF token depends on token being present](https://portswigger.net/web-security/csrf#validation-of-csrf-token-depends-on-token-being-present) | | |
|  |  | [CSRF token is not tied to the user session](https://portswigger.net/web-security/csrf#csrf-token-is-not-tied-to-the-user-session) | | |
|  |  | [CSRF token is tied to a non-session cookie](https://portswigger.net/web-security/csrf#csrf-token-is-tied-to-a-non-session-cookie) | | |
|  |  | [CSRF token is simply duplicated in a cookie](https://portswigger.net/web-security/csrf#csrf-token-is-simply-duplicated-in-a-cookie) | | |
|  | [Referer-based defenses against CSRF](https://portswigger.net/web-security/csrf#referer-based-defenses-against-csrf) | | | |
|  |  | [Validation of Referer depends on header being present](https://portswigger.net/web-security/csrf#validation-of-referer-depends-on-header-being-present) | | |
|  |  | [Validation of Referer can be circumvented](https://portswigger.net/web-security/csrf#validation-of-referer-can-be-circumvented) | | |
|  | [Defending against CSRF with SameSite cookies](https://portswigger.net/web-security/csrf/samesite-cookies) | | | |
|  | [XSS vs CSRF](https://portswigger.net/web-security/csrf/xss-vs-csrf) | | | |
|  |  | [What is the difference between XSS and CSRF?](https://portswigger.net/web-security/csrf/xss-vs-csrf#what-is-the-difference-between-xss-and-csrf) | | |
|  |  | [Can CSRF tokens prevent XSS attacks?](https://portswigger.net/web-security/csrf/xss-vs-csrf#can-csrf-tokens-prevent-xss-attacks) | | |
|  | [CSRF tokens](https://portswigger.net/web-security/csrf/tokens) | | | |
|  |  | [What are CSRF tokens?](https://portswigger.net/web-security/csrf/tokens#what-are-csrf-tokens) | | |
|  |  | [How should CSRF tokens be generated?](https://portswigger.net/web-security/csrf/tokens#how-should-csrf-tokens-be-generated) | | |
|  |  | [How should CSRF tokens be transmitted?](https://portswigger.net/web-security/csrf/tokens#how-should-csrf-tokens-be-transmitted) | | |
|  |  | [How should CSRF tokens be validated?](https://portswigger.net/web-security/csrf/tokens#how-should-csrf-tokens-be-validated) | | |
| [**XML external entity (XXE) injection**](https://portswigger.net/web-security/xxe) | | | | |
|  | [What is XML external entity injection?](https://portswigger.net/web-security/xxe#what-is-xml-external-entity-injection) | | | |
|  | [How do XXE vulnerabilities arise?](https://portswigger.net/web-security/xxe#how-do-xxe-vulnerabilities-arise) | | | |
|  | [What are the types of XXE attacks?](https://portswigger.net/web-security/xxe#what-are-the-types-of-xxe-attacks) | | | |
|  | [Exploiting XXE to retrieve files](https://portswigger.net/web-security/xxe#exploiting-xxe-to-retrieve-files) | | | |
|  | [Exploiting XXE to perform SSRF attacks](https://portswigger.net/web-security/xxe#exploiting-xxe-to-perform-ssrf-attacks) | | | |
|  | [Blind XXE vulnerabilities](https://portswigger.net/web-security/xxe#blind-xxe-vulnerabilities) | | | |
|  | [Finding hidden attack surface for XXE injection](https://portswigger.net/web-security/xxe#finding-hidden-attack-surface-for-xxe-injection) | | | |
|  |  | [XInclude attacks](https://portswigger.net/web-security/xxe#xinclude-attacks) | | |
|  |  | [XXE attacks via file upload](https://portswigger.net/web-security/xxe#xxe-attacks-via-file-upload) | | |
|  |  | [XXE attacks via modified content type](https://portswigger.net/web-security/xxe#xxe-attacks-via-modified-content-type) | | |
|  | [How to find and test for XXE vulnerabilities](https://portswigger.net/web-security/xxe#how-to-find-and-test-for-xxe-vulnerabilities) | | | |
|  | [How to prevent XXE vulnerabilities](https://portswigger.net/web-security/xxe#how-to-prevent-xxe-vulnerabilities) | | | |
|  | [XML entities](https://portswigger.net/web-security/xxe/xml-entities) | | | |
|  |  | [What is XML?](https://portswigger.net/web-security/xxe/xml-entities#what-is-xml) | | |
|  |  | [What are XML entities?](https://portswigger.net/web-security/xxe/xml-entities#what-are-xml-entities) | | |
|  |  | [What is document type definition?](https://portswigger.net/web-security/xxe/xml-entities#what-is-document-type-definition) | | |
|  |  | [What are XML custom entities?](https://portswigger.net/web-security/xxe/xml-entities#what-are-xml-custom-entities) | | |
|  |  | [What are XML external entities?](https://portswigger.net/web-security/xxe/xml-entities#what-are-xml-external-entities) | | |
|  | [Finding and exploiting blind XXE vulnerabilities](https://portswigger.net/web-security/xxe/blind) | | | |
|  |  | [What is blind XXE?](https://portswigger.net/web-security/xxe/blind#what-is-blind-xxe) | | |
|  |  | [Detecting blind XXE using out-of-band (OAST) techniques](https://portswigger.net/web-security/xxe/blind#detecting-blind-xxe-using-out-of-band-oast-techniques) | | |
|  |  | [Exploiting blind XXE to exfiltrate data out-of-band](https://portswigger.net/web-security/xxe/blind#exploiting-blind-xxe-to-exfiltrate-data-out-of-band) | | |
|  |  | [Exploiting blind XXE to retrieve data via error messages](https://portswigger.net/web-security/xxe/blind#exploiting-blind-xxe-to-retrieve-data-via-error-messages) | | |
|  |  | [Exploiting blind XXE by repurposing a local DTD](https://portswigger.net/web-security/xxe/blind#exploiting-blind-xxe-by-repurposing-a-local-dtd) | | |
|  |  |  | [Locating an existing DTD file to repurpose](https://portswigger.net/web-security/xxe/blind#locating-an-existing-dtd-file-to-repurpose) | |
| [**Clickjacking (UI redressing)**](https://portswigger.net/web-security/clickjacking) | | | | |
|  | [What is clickjacking?](https://portswigger.net/web-security/clickjacking#what-is-clickjacking) | | | |
|  | [How to construct a basic clickjacking attack](https://portswigger.net/web-security/clickjacking#how-to-construct-a-basic-clickjacking-attack) | | | |
|  | [Clickjacking with prefilled form input](https://portswigger.net/web-security/clickjacking#clickjacking-with-prefilled-form-input) | | | |
|  | [Frame busting scripts](https://portswigger.net/web-security/clickjacking#frame-busting-scripts) | | | |
|  | [Combining clickjacking with a DOM XSS attack](https://portswigger.net/web-security/clickjacking#combining-clickjacking-with-a-dom-xss-attack) | | | |
|  | [Multistep clickjacking](https://portswigger.net/web-security/clickjacking#multistep-clickjacking) | | | |
|  | [How to prevent clickjacking attacks](https://portswigger.net/web-security/clickjacking#how-to-prevent-clickjacking-attacks) | | | |
|  |  | [X-Frame-Options](https://portswigger.net/web-security/clickjacking#x-frame-options) | | |
|  |  | [Content Security Policy (CSP)](https://portswigger.net/web-security/clickjacking#content-security-policy-csp) | | |
| [**Cross-origin resource sharing (CORS)**](https://portswigger.net/web-security/cors) | | | | |
|  | [What is CORS (cross-origin resource sharing)?](https://portswigger.net/web-security/cors#what-is-cors-cross-origin-resource-sharing) | | | |
|  | [Same-origin policy](https://portswigger.net/web-security/cors#same-origin-policy) | | | |
|  | [Relaxation of the same-origin policy](https://portswigger.net/web-security/cors#relaxation-of-the-same-origin-policy) | | | |
|  | [Vulnerabilities arising from CORS configuration issues](https://portswigger.net/web-security/cors#vulnerabilities-arising-from-cors-configuration-issues) | | | |
|  |  | [Server-generated ACAO header from client-specified Origin header](https://portswigger.net/web-security/cors#server-generated-acao-header-from-client-specified-origin-header) | | |
|  |  | [Errors parsing Origin headers](https://portswigger.net/web-security/cors#errors-parsing-origin-headers) | | |
|  |  | [Whitelisted null origin value](https://portswigger.net/web-security/cors#whitelisted-null-origin-value) | | |
|  |  | [Exploiting XSS via CORS trust relationships](https://portswigger.net/web-security/cors#exploiting-xss-via-cors-trust-relationships) | | |
|  |  | [Breaking TLS with poorly configured CORS](https://portswigger.net/web-security/cors#breaking-tls-with-poorly-configured-cors) | | |
|  |  | [Intranets and CORS without credentials](https://portswigger.net/web-security/cors#intranets-and-cors-without-credentials) | | |
|  | [How to prevent CORS-based attacks](https://portswigger.net/web-security/cors#how-to-prevent-cors-based-attacks) | | | |
|  |  | [Proper configuration of cross-origin requests](https://portswigger.net/web-security/cors#proper-configuration-of-cross-origin-requests) | | |
|  |  | [Only allow trusted sites](https://portswigger.net/web-security/cors#only-allow-trusted-sites) | | |
|  |  | [Avoid whitelisting null](https://portswigger.net/web-security/cors#avoid-whitelisting-null) | | |
|  |  | [Avoid wildcards in internal networks](https://portswigger.net/web-security/cors#avoid-wildcards-in-internal-networks) | | |
|  |  | [CORS is not a substitute for server-side security policies](https://portswigger.net/web-security/cors#cors-is-not-a-substitute-for-server-side-security-policies) | | |
|  | [Same-origin policy (SOP)](https://portswigger.net/web-security/cors/same-origin-policy) | | | |
|  |  | [What is the same-origin policy?](https://portswigger.net/web-security/cors/same-origin-policy#what-is-the-same-origin-policy) | | |
|  |  | [Why is the same-origin policy necessary?](https://portswigger.net/web-security/cors/same-origin-policy#why-is-the-same-origin-policy-necessary) | | |
|  |  | [How is the same-origin policy implemented?](https://portswigger.net/web-security/cors/same-origin-policy#how-is-the-same-origin-policy-implemented) | | |
|  | [CORS and the Access-Control-Allow-Origin response header](https://portswigger.net/web-security/cors/access-control-allow-origin) | | | |
|  |  | [What is the Access-Control-Allow-Origin response header?](https://portswigger.net/web-security/cors/access-control-allow-origin#what-is-the-access-control-allow-origin-response-header) | | |
|  |  | [Implementing simple cross-origin resource sharing](https://portswigger.net/web-security/cors/access-control-allow-origin#implementing-simple-cross-origin-resource-sharing) | | |
|  |  | [Handling cross-origin resource requests with credentials](https://portswigger.net/web-security/cors/access-control-allow-origin#handling-cross-origin-resource-requests-with-credentials) | | |
|  |  | [Relaxation of CORS specifications with wildcards](https://portswigger.net/web-security/cors/access-control-allow-origin#relaxation-of-cors-specifications-with-wildcards) | | |
|  |  | [Pre-flight checks](https://portswigger.net/web-security/cors/access-control-allow-origin#pre-flight-checks) | | |
|  |  | [Does CORS protect against CSRF?](https://portswigger.net/web-security/cors/access-control-allow-origin#does-cors-protect-against-csrf) | | |
| [**Server-side request forgery (SSRF)**](https://portswigger.net/web-security/ssrf) | | | | |
|  | [What is SSRF?](https://portswigger.net/web-security/ssrf#what-is-ssrf) | | | |
|  | [What is the impact of SSRF attacks?](https://portswigger.net/web-security/ssrf#what-is-the-impact-of-ssrf-attacks) | | | |
|  | [Common SSRF attacks](https://portswigger.net/web-security/ssrf#common-ssrf-attacks) | | | |
|  |  | [SSRF attacks against the server itself](https://portswigger.net/web-security/ssrf#ssrf-attacks-against-the-server-itself) | | |
|  |  | [SSRF attacks against other back-end systems](https://portswigger.net/web-security/ssrf#ssrf-attacks-against-other-back-end-systems) | | |
|  | [Circumventing common SSRF defenses](https://portswigger.net/web-security/ssrf#circumventing-common-ssrf-defenses) | | | |
|  |  | [SSRF with blacklist-based input filters](https://portswigger.net/web-security/ssrf#ssrf-with-blacklist-based-input-filters) | | |
|  |  | [SSRF with whitelist-based input filters](https://portswigger.net/web-security/ssrf#ssrf-with-whitelist-based-input-filters) | | |
|  |  | [Bypassing SSRF filters via open redirection](https://portswigger.net/web-security/ssrf#bypassing-ssrf-filters-via-open-redirection) | | |
|  | [Blind SSRF vulnerabilities](https://portswigger.net/web-security/ssrf#blind-ssrf-vulnerabilities) | | | |
|  | [Finding hidden attack surface for SSRF vulnerabilities](https://portswigger.net/web-security/ssrf#finding-hidden-attack-surface-for-ssrf-vulnerabilities) | | | |
|  |  | [Partial URLs in requests](https://portswigger.net/web-security/ssrf#partial-urls-in-requests) | | |
|  |  | [URLs within data formats](https://portswigger.net/web-security/ssrf#urls-within-data-formats) | | |
|  |  | [SSRF via the Referer header](https://portswigger.net/web-security/ssrf#ssrf-via-the-referer-header) | | |
|  | [Blind SSRF vulnerabilities](https://portswigger.net/web-security/ssrf/blind) | | | |
|  |  | [What is blind SSRF?](https://portswigger.net/web-security/ssrf/blind#what-is-blind-ssrf) | | |
|  |  | [What is the impact of blind SSRF vulnerabilities?](https://portswigger.net/web-security/ssrf/blind#what-is-the-impact-of-blind-ssrf-vulnerabilities) | | |
|  |  | [How to find and exploit blind SSRF vulnerabilities](https://portswigger.net/web-security/ssrf/blind#how-to-find-and-exploit-blind-ssrf-vulnerabilities) | | |
| [**HTTP request smuggling**](https://portswigger.net/web-security/request-smuggling) | | | | |
|  | [What is HTTP request smuggling?](https://portswigger.net/web-security/request-smuggling#what-is-http-request-smuggling) | | | |
|  | [What happens in an HTTP request smuggling attack?](https://portswigger.net/web-security/request-smuggling#what-happens-in-an-http-request-smuggling-attack) | | | |
|  | [How do HTTP request smuggling vulnerabilities arise?](https://portswigger.net/web-security/request-smuggling#how-do-http-request-smuggling-vulnerabilities-arise) | | | |
|  | [How to perform an HTTP request smuggling attack](https://portswigger.net/web-security/request-smuggling#how-to-perform-an-http-request-smuggling-attack) | | | |
|  |  | [CL.TE vulnerabilities](https://portswigger.net/web-security/request-smuggling#cl-te-vulnerabilities) | | |
|  |  | [TE.CL vulnerabilities](https://portswigger.net/web-security/request-smuggling#te-cl-vulnerabilities) | | |
|  |  | [TE.TE behavior: obfuscating the TE header](https://portswigger.net/web-security/request-smuggling#te-te-behavior-obfuscating-the-te-header) | | |
|  | [How to identify HTTP request smuggling vulnerabilities](https://portswigger.net/web-security/request-smuggling#how-to-identify-http-request-smuggling-vulnerabilities) | | | |
|  | [How to exploit HTTP request smuggling vulnerabilities](https://portswigger.net/web-security/request-smuggling#how-to-exploit-http-request-smuggling-vulnerabilities) | | | |
|  | [Advanced HTTP request smuggling](https://portswigger.net/web-security/request-smuggling#advanced-http-request-smuggling) | | | |
|  | [How to prevent HTTP request smuggling vulnerabilities](https://portswigger.net/web-security/request-smuggling#how-to-prevent-http-request-smuggling-vulnerabilities) | | | |
|  | [Finding HTTP request smuggling vulnerabilities](https://portswigger.net/web-security/request-smuggling/finding) | | | |
|  |  | [Finding HTTP request smuggling vulnerabilities using timing techniques](https://portswigger.net/web-security/request-smuggling/finding#finding-http-request-smuggling-vulnerabilities-using-timing-techniques) | | |
|  |  |  | [Finding CL.TE vulnerabilities using timing techniques](https://portswigger.net/web-security/request-smuggling/finding#finding-cl-te-vulnerabilities-using-timing-techniques) | |
|  |  |  | [Finding TE.CL vulnerabilities using timing techniques](https://portswigger.net/web-security/request-smuggling/finding#finding-te-cl-vulnerabilities-using-timing-techniques) | |
|  |  | [Confirming HTTP request smuggling vulnerabilities using differential responses](https://portswigger.net/web-security/request-smuggling/finding#confirming-http-request-smuggling-vulnerabilities-using-differential-responses) | | |
|  |  |  | [Confirming CL.TE vulnerabilities using differential responses](https://portswigger.net/web-security/request-smuggling/finding#confirming-cl-te-vulnerabilities-using-differential-responses) | |
|  |  |  | [Confirming TE.CL vulnerabilities using differential responses](https://portswigger.net/web-security/request-smuggling/finding#confirming-te-cl-vulnerabilities-using-differential-responses) | |
|  | [Exploiting HTTP request smuggling vulnerabilities](https://portswigger.net/web-security/request-smuggling/exploiting) | | | |
|  |  | [Using HTTP request smuggling to bypass front-end security controls](https://portswigger.net/web-security/request-smuggling/exploiting#using-http-request-smuggling-to-bypass-front-end-security-controls) | | |
|  |  | [Revealing front-end request rewriting](https://portswigger.net/web-security/request-smuggling/exploiting#revealing-front-end-request-rewriting) | | |
|  |  | [Bypassing client authentication](https://portswigger.net/web-security/request-smuggling/exploiting#bypassing-client-authentication) | | |
|  |  | [Capturing other users' requests](https://portswigger.net/web-security/request-smuggling/exploiting#capturing-other-users-requests) | | |
|  |  | [Using HTTP request smuggling to exploit reflected XSS](https://portswigger.net/web-security/request-smuggling/exploiting#using-http-request-smuggling-to-exploit-reflected-xss) | | |
|  |  | [Using HTTP request smuggling to turn an on-site redirect into an open redirect](https://portswigger.net/web-security/request-smuggling/exploiting#using-http-request-smuggling-to-turn-an-on-site-redirect-into-an-open-redirect) | | |
|  |  | [Using HTTP request smuggling to perform web cache poisoning](https://portswigger.net/web-security/request-smuggling/exploiting#using-http-request-smuggling-to-perform-web-cache-poisoning) | | |
|  |  | [Using HTTP request smuggling to perform web cache deception](https://portswigger.net/web-security/request-smuggling/exploiting#using-http-request-smuggling-to-perform-web-cache-deception) | | |
|  | [Advanced request smuggling](https://portswigger.net/web-security/request-smuggling/advanced) | | | |
|  |  | [HTTP/2 request smuggling](https://portswigger.net/web-security/request-smuggling/advanced#http-2-request-smuggling) | | |
|  |  |  | [HTTP/2 message length](https://portswigger.net/web-security/request-smuggling/advanced#http-2-message-length) | |
|  |  |  | [HTTP/2 downgrading](https://portswigger.net/web-security/request-smuggling/advanced#http-2-downgrading) | |
|  |  |  | [H2.CL vulnerabilities](https://portswigger.net/web-security/request-smuggling/advanced#h2-cl-vulnerabilities) | |
|  |  |  | [H2.TE vulnerabilities](https://portswigger.net/web-security/request-smuggling/advanced#h2-te-vulnerabilities) | |
|  |  | [Response queue poisoning](https://portswigger.net/web-security/request-smuggling/advanced#response-queue-poisoning) | | |
|  |  | [Request smuggling via CRLF injection](https://portswigger.net/web-security/request-smuggling/advanced#request-smuggling-via-crlf-injection) | | |
|  |  | [HTTP/2 request splitting](https://portswigger.net/web-security/request-smuggling/advanced#http-2-request-splitting) | | |
|  |  |  | [Accounting for front-end rewriting](https://portswigger.net/web-security/request-smuggling/advanced#accounting-for-front-end-rewriting) | |
|  |  | [HTTP request tunnelling](https://portswigger.net/web-security/request-smuggling/advanced#http-request-tunnelling) | | |
|  |  | [Response queue poisoning](https://portswigger.net/web-security/request-smuggling/advanced/response-queue-poisoning) | | |
|  |  |  | [What is the impact of response queue poisoning?](https://portswigger.net/web-security/request-smuggling/advanced/response-queue-poisoning#what-is-the-impact-of-response-queue-poisoning) | |
|  |  |  | [How to construct a response queue poisoning attack](https://portswigger.net/web-security/request-smuggling/advanced/response-queue-poisoning#how-to-construct-a-response-queue-poisoning-attack) | |
|  |  |  |  | [Understanding the aftermath of request smuggling](https://portswigger.net/web-security/request-smuggling/advanced/response-queue-poisoning#understanding-the-aftermath-of-request-smuggling) |
|  |  |  |  | [Smuggling a complete request](https://portswigger.net/web-security/request-smuggling/advanced/response-queue-poisoning#smuggling-a-complete-request) |
|  |  |  |  | [Desynchronizing the response queue](https://portswigger.net/web-security/request-smuggling/advanced/response-queue-poisoning#desynchronizing-the-response-queue) |
|  |  |  |  | [Stealing other users' responses](https://portswigger.net/web-security/request-smuggling/advanced/response-queue-poisoning#stealing-other-users-responses) |
|  |  | [HTTP request tunnelling](https://portswigger.net/web-security/request-smuggling/advanced/request-tunnelling) | | |
|  |  |  | [Request tunnelling with HTTP/2](https://portswigger.net/web-security/request-smuggling/advanced/request-tunnelling#request-tunnelling-with-http-2) | |
|  |  |  | [Leaking internal headers via HTTP/2 request tunnelling](https://portswigger.net/web-security/request-smuggling/advanced/request-tunnelling#leaking-internal-headers-via-http-2-request-tunnelling) | |
|  |  |  | [Blind request tunnelling](https://portswigger.net/web-security/request-smuggling/advanced/request-tunnelling#blind-request-tunnelling) | |
|  |  |  | [Non-blind request tunnelling using HEAD](https://portswigger.net/web-security/request-smuggling/advanced/request-tunnelling#non-blind-request-tunnelling-using-head) | |
|  |  |  | [Web cache poisoning via HTTP/2 request tunnelling](https://portswigger.net/web-security/request-smuggling/advanced/request-tunnelling#web-cache-poisoning-via-http-2-request-tunnelling) | |
|  |  | [HTTP/2 downgrading](https://portswigger.net/web-security/request-smuggling/advanced/http2-downgrading) | | |
|  |  |  | [What risks are associated with HTTP/2 downgrading?](https://portswigger.net/web-security/request-smuggling/advanced/http2-downgrading#what-risks-are-associated-with-http-2-downgrading) | |
|  |  | [HTTP/2-exclusive vectors](https://portswigger.net/web-security/request-smuggling/advanced/http2-exclusive-vectors) | | |
|  |  |  | [Injecting via header names](https://portswigger.net/web-security/request-smuggling/advanced/http2-exclusive-vectors#injecting-via-header-names) | |
|  |  |  | [Injecting via pseudo-headers](https://portswigger.net/web-security/request-smuggling/advanced/http2-exclusive-vectors#injecting-via-pseudo-headers) | |
|  |  |  |  | [Supplying an ambiguous host](https://portswigger.net/web-security/request-smuggling/advanced/http2-exclusive-vectors#supplying-an-ambiguous-host) |
|  |  |  |  | [Supplying an ambiguous path](https://portswigger.net/web-security/request-smuggling/advanced/http2-exclusive-vectors#supplying-an-ambiguous-path) |
|  |  |  |  | [Injecting a full request line](https://portswigger.net/web-security/request-smuggling/advanced/http2-exclusive-vectors#injecting-a-full-request-line) |
|  |  |  |  | [Injecting a URL prefix](https://portswigger.net/web-security/request-smuggling/advanced/http2-exclusive-vectors#injecting-a-url-prefix) |
|  |  |  |  | [Injecting newlines into pseudo-headers](https://portswigger.net/web-security/request-smuggling/advanced/http2-exclusive-vectors#injecting-newlines-into-pseudo-headers) |
| [**OS command injection**](https://portswigger.net/web-security/os-command-injection) | | | | |
|  | [What is OS command injection?](https://portswigger.net/web-security/os-command-injection#what-is-os-command-injection) | | | |
|  | [Executing arbitrary commands](https://portswigger.net/web-security/os-command-injection#executing-arbitrary-commands) | | | |
|  | [Useful commands](https://portswigger.net/web-security/os-command-injection#useful-commands) | | | |
|  | [Blind OS command injection vulnerabilities](https://portswigger.net/web-security/os-command-injection#blind-os-command-injection-vulnerabilities) | | | |
|  |  | [Detecting blind OS command injection using time delays](https://portswigger.net/web-security/os-command-injection#detecting-blind-os-command-injection-using-time-delays) | | |
|  |  | [Exploiting blind OS command injection by redirecting output](https://portswigger.net/web-security/os-command-injection#exploiting-blind-os-command-injection-by-redirecting-output) | | |
|  |  | [Exploiting blind OS command injection using out-of-band (OAST) techniques](https://portswigger.net/web-security/os-command-injection#exploiting-blind-os-command-injection-using-out-of-band-oast-techniques) | | |
|  | [Ways of injecting OS commands](https://portswigger.net/web-security/os-command-injection#ways-of-injecting-os-commands) | | | |
|  | [How to prevent OS command injection attacks](https://portswigger.net/web-security/os-command-injection#how-to-prevent-os-command-injection-attacks) | | | |
| [**Server-side template injection**](https://portswigger.net/web-security/server-side-template-injection) | | | | |
|  | [What is server-side template injection?](https://portswigger.net/web-security/server-side-template-injection#what-is-server-side-template-injection) | | | |
|  | [What is the impact of server-side template injection?](https://portswigger.net/web-security/server-side-template-injection#what-is-the-impact-of-server-side-template-injection) | | | |
|  | [How do server-side template injection vulnerabilities arise?](https://portswigger.net/web-security/server-side-template-injection#how-do-server-side-template-injection-vulnerabilities-arise) | | | |
|  | [Constructing a server-side template injection attack](https://portswigger.net/web-security/server-side-template-injection#constructing-a-server-side-template-injection-attack) | | | |
|  |  | [Detect](https://portswigger.net/web-security/server-side-template-injection#detect) | | |
|  |  | [Identify](https://portswigger.net/web-security/server-side-template-injection#identify) | | |
|  |  | [Exploit](https://portswigger.net/web-security/server-side-template-injection#exploit) | | |
|  | [How to prevent server-side template injection vulnerabilities](https://portswigger.net/web-security/server-side-template-injection#how-to-prevent-server-side-template-injection-vulnerabilities) | | | |
|  | [Exploiting server-side template injection vulnerabilities](https://portswigger.net/web-security/server-side-template-injection/exploiting) | | | |
|  |  | [Read](https://portswigger.net/web-security/server-side-template-injection/exploiting#read) | | |
|  |  |  | [Learn the basic template syntax](https://portswigger.net/web-security/server-side-template-injection/exploiting#learn-the-basic-template-syntax) | |
|  |  |  | [Read about the security implications](https://portswigger.net/web-security/server-side-template-injection/exploiting#read-about-the-security-implications) | |
|  |  |  | [Look for known exploits](https://portswigger.net/web-security/server-side-template-injection/exploiting#look-for-known-exploits) | |
|  |  | [Explore](https://portswigger.net/web-security/server-side-template-injection/exploiting#explore) | | |
|  |  |  | [Developer-supplied objects](https://portswigger.net/web-security/server-side-template-injection/exploiting#developer-supplied-objects) | |
|  |  | [Create a custom attack](https://portswigger.net/web-security/server-side-template-injection/exploiting#create-a-custom-attack) | | |
|  |  |  | [Constructing a custom exploit using an object chain](https://portswigger.net/web-security/server-side-template-injection/exploiting#constructing-a-custom-exploit-using-an-object-chain) | |
|  |  |  | [Constructing a custom exploit using developer-supplied objects](https://portswigger.net/web-security/server-side-template-injection/exploiting#constructing-a-custom-exploit-using-developer-supplied-objects) | |
| [**Insecure deserialization**](https://portswigger.net/web-security/deserialization) | | | | |
|  | [What is serialization?](https://portswigger.net/web-security/deserialization#what-is-serialization) | | | |
|  |  | [Serialization vs deserialization](https://portswigger.net/web-security/deserialization#serialization-vs-deserialization) | | |
|  | [What is insecure deserialization?](https://portswigger.net/web-security/deserialization#what-is-insecure-deserialization) | | | |
|  | [How do insecure deserialization vulnerabilities arise?](https://portswigger.net/web-security/deserialization#how-do-insecure-deserialization-vulnerabilities-arise) | | | |
|  | [What is the impact of insecure deserialization?](https://portswigger.net/web-security/deserialization#what-is-the-impact-of-insecure-deserialization) | | | |
|  | [How to exploit insecure deserialization vulnerabilities](https://portswigger.net/web-security/deserialization#how-to-exploit-insecure-deserialization-vulnerabilities) | | | |
|  | [How to prevent insecure deserialization vulnerabilities](https://portswigger.net/web-security/deserialization#how-to-prevent-insecure-deserialization-vulnerabilities) | | | |
|  | [Exploiting insecure deserialization vulnerabilities](https://portswigger.net/web-security/deserialization/exploiting) | | | |
|  |  | [How to identify insecure deserialization](https://portswigger.net/web-security/deserialization/exploiting#how-to-identify-insecure-deserialization) | | |
|  |  |  | [PHP serialization format](https://portswigger.net/web-security/deserialization/exploiting#php-serialization-format) | |
|  |  |  | [Java serialization format](https://portswigger.net/web-security/deserialization/exploiting#java-serialization-format) | |
|  |  | [Manipulating serialized objects](https://portswigger.net/web-security/deserialization/exploiting#manipulating-serialized-objects) | | |
|  |  |  | [Modifying object attributes](https://portswigger.net/web-security/deserialization/exploiting#modifying-object-attributes) | |
|  |  |  | [Modifying data types](https://portswigger.net/web-security/deserialization/exploiting#modifying-data-types) | |
|  |  | [Using application functionality](https://portswigger.net/web-security/deserialization/exploiting#using-application-functionality) | | |
|  |  | [Magic methods](https://portswigger.net/web-security/deserialization/exploiting#magic-methods) | | |
|  |  | [Injecting arbitrary objects](https://portswigger.net/web-security/deserialization/exploiting#injecting-arbitrary-objects) | | |
|  |  | [Gadget chains](https://portswigger.net/web-security/deserialization/exploiting#gadget-chains) | | |
|  |  |  | [Working with pre-built gadget chains](https://portswigger.net/web-security/deserialization/exploiting#working-with-pre-built-gadget-chains) | |
|  |  |  | [Working with documented gadget chains](https://portswigger.net/web-security/deserialization/exploiting#working-with-documented-gadget-chains) | |
|  |  | [Creating your own exploit](https://portswigger.net/web-security/deserialization/exploiting#creating-your-own-exploit) | | |
|  |  | [PHAR deserialization](https://portswigger.net/web-security/deserialization/exploiting#phar-deserialization) | | |
|  |  | [Exploiting deserialization using memory corruption](https://portswigger.net/web-security/deserialization/exploiting#exploiting-deserialization-using-memory-corruption) | | |
| [**Directory traversal**](https://portswigger.net/web-security/file-path-traversal) | | | | |
|  | [What is directory traversal?](https://portswigger.net/web-security/file-path-traversal#what-is-directory-traversal) | | | |
|  | [Reading arbitrary files via directory traversal](https://portswigger.net/web-security/file-path-traversal#reading-arbitrary-files-via-directory-traversal) | | | |
|  | [Common obstacles to exploiting file path traversal vulnerabilities](https://portswigger.net/web-security/file-path-traversal#common-obstacles-to-exploiting-file-path-traversal-vulnerabilities) | | | |
|  | [How to prevent a directory traversal attack](https://portswigger.net/web-security/file-path-traversal#how-to-prevent-a-directory-traversal-attack) | | | |
| [**Access control vulnerabilities and privilege escalation**](https://portswigger.net/web-security/access-control) | | | | |
|  | [What is access control?](https://portswigger.net/web-security/access-control#what-is-access-control) | | | |
|  |  | [Vertical access controls](https://portswigger.net/web-security/access-control#vertical-access-controls) | | |
|  |  | [Horizontal access controls](https://portswigger.net/web-security/access-control#horizontal-access-controls) | | |
|  |  | [Context-dependent access controls](https://portswigger.net/web-security/access-control#context-dependent-access-controls) | | |
|  | [Examples of broken access controls](https://portswigger.net/web-security/access-control#examples-of-broken-access-controls) | | | |
|  |  | [Vertical privilege escalation](https://portswigger.net/web-security/access-control#vertical-privilege-escalation) | | |
|  |  | [Horizontal privilege escalation](https://portswigger.net/web-security/access-control#horizontal-privilege-escalation) | | |
|  |  | [Horizontal to vertical privilege escalation](https://portswigger.net/web-security/access-control#horizontal-to-vertical-privilege-escalation) | | |
|  |  | [Insecure direct object references](https://portswigger.net/web-security/access-control#insecure-direct-object-references) | | |
|  |  | [Access control vulnerabilities in multi-step processes](https://portswigger.net/web-security/access-control#access-control-vulnerabilities-in-multi-step-processes) | | |
|  |  | [Referer-based access control](https://portswigger.net/web-security/access-control#referer-based-access-control) | | |
|  |  | [Location-based access control](https://portswigger.net/web-security/access-control#location-based-access-control) | | |
|  | [How to prevent access control vulnerabilities](https://portswigger.net/web-security/access-control#how-to-prevent-access-control-vulnerabilities) | | | |
|  | [Access control security models](https://portswigger.net/web-security/access-control/security-models) | | | |
|  |  | [What are access control security models?](https://portswigger.net/web-security/access-control/security-models#what-are-access-control-security-models) | | |
|  |  | [Programmatic access control](https://portswigger.net/web-security/access-control/security-models#programmatic-access-control) | | |
|  |  | [Discretionary access control (DAC)](https://portswigger.net/web-security/access-control/security-models#discretionary-access-control-dac) | | |
|  |  | [Mandatory access control (MAC)](https://portswigger.net/web-security/access-control/security-models#mandatory-access-control-mac) | | |
|  |  | [Role-based access control (RBAC)](https://portswigger.net/web-security/access-control/security-models#role-based-access-control-rbac) | | |
|  | [Insecure direct object references (IDOR)](https://portswigger.net/web-security/access-control/idor) | | | |
|  |  | [What are insecure direct object references (IDOR)?](https://portswigger.net/web-security/access-control/idor#what-are-insecure-direct-object-references-idor) | | |
|  |  | [IDOR examples](https://portswigger.net/web-security/access-control/idor#idor-examples) | | |
|  |  |  | [IDOR vulnerability with direct reference to database objects](https://portswigger.net/web-security/access-control/idor#idor-vulnerability-with-direct-reference-to-database-objects) | |
|  |  |  | [IDOR vulnerability with direct reference to static files](https://portswigger.net/web-security/access-control/idor#idor-vulnerability-with-direct-reference-to-static-files) | |
| [**Authentication vulnerabilities**](https://portswigger.net/web-security/authentication) | | | | |
|  | [What is authentication?](https://portswigger.net/web-security/authentication#what-is-authentication) | | | |
|  |  | [What is the difference between authentication and authorization?](https://portswigger.net/web-security/authentication#what-is-the-difference-between-authentication-and-authorization) | | |
|  | [How do authentication vulnerabilities arise?](https://portswigger.net/web-security/authentication#how-do-authentication-vulnerabilities-arise) | | | |
|  | [What is the impact of vulnerable authentication?](https://portswigger.net/web-security/authentication#what-is-the-impact-of-vulnerable-authentication) | | | |
|  | [Vulnerabilities in authentication mechanisms](https://portswigger.net/web-security/authentication#vulnerabilities-in-authentication-mechanisms) | | | |
|  |  | [Vulnerabilities in third-party authentication mechanisms](https://portswigger.net/web-security/authentication#vulnerabilities-in-third-party-authentication-mechanisms) | | |
|  | [Preventing attacks on your own authentication mechanisms](https://portswigger.net/web-security/authentication#preventing-attacks-on-your-own-authentication-mechanisms) | | | |
|  | [Vulnerabilities in password-based login](https://portswigger.net/web-security/authentication/password-based) | | | |
|  |  | [Brute-force attacks](https://portswigger.net/web-security/authentication/password-based#brute-force-attacks) | | |
|  |  |  | [Brute-forcing usernames](https://portswigger.net/web-security/authentication/password-based#brute-forcing-usernames) | |
|  |  |  | [Brute-forcing passwords](https://portswigger.net/web-security/authentication/password-based#brute-forcing-passwords) | |
|  |  |  | [Username enumeration](https://portswigger.net/web-security/authentication/password-based#username-enumeration) | |
|  |  | [Flawed brute-force protection](https://portswigger.net/web-security/authentication/password-based#flawed-brute-force-protection) | | |
|  |  |  | [Account locking](https://portswigger.net/web-security/authentication/password-based#account-locking) | |
|  |  |  | [User rate limiting](https://portswigger.net/web-security/authentication/password-based#user-rate-limiting) | |
|  |  | [HTTP basic authentication](https://portswigger.net/web-security/authentication/password-based#http-basic-authentication) | | |
|  | [Vulnerabilities in multi-factor authentication](https://portswigger.net/web-security/authentication/multi-factor) | | | |
|  |  | [Two-factor authentication tokens](https://portswigger.net/web-security/authentication/multi-factor#two-factor-authentication-tokens) | | |
|  |  | [Bypassing two-factor authentication](https://portswigger.net/web-security/authentication/multi-factor#bypassing-two-factor-authentication) | | |
|  |  | [Flawed two-factor verification logic](https://portswigger.net/web-security/authentication/multi-factor#flawed-two-factor-verification-logic) | | |
|  |  | [Brute-forcing 2FA verification codes](https://portswigger.net/web-security/authentication/multi-factor#brute-forcing-2fa-verification-codes) | | |
|  | [Vulnerabilities in other authentication mechanisms](https://portswigger.net/web-security/authentication/other-mechanisms) | | | |
|  |  | [Keeping users logged in](https://portswigger.net/web-security/authentication/other-mechanisms#keeping-users-logged-in) | | |
|  |  | [Resetting user passwords](https://portswigger.net/web-security/authentication/other-mechanisms#resetting-user-passwords) | | |
|  |  |  | [Sending passwords by email](https://portswigger.net/web-security/authentication/other-mechanisms#sending-passwords-by-email) | |
|  |  |  | [Resetting passwords using a URL](https://portswigger.net/web-security/authentication/other-mechanisms#resetting-passwords-using-a-url) | |
|  |  | [Changing user passwords](https://portswigger.net/web-security/authentication/other-mechanisms#changing-user-passwords) | | |
|  | [Authentication lab usernames](https://portswigger.net/web-security/authentication/auth-lab-usernames) | | | |
|  | [Authentication lab passwords](https://portswigger.net/web-security/authentication/auth-lab-passwords) | | | |
|  | [How to secure your authentication mechanisms](https://portswigger.net/web-security/authentication/securing) | | | |
|  |  | [Take care with user credentials](https://portswigger.net/web-security/authentication/securing#take-care-with-user-credentials) | | |
|  |  | [Don't count on users for security](https://portswigger.net/web-security/authentication/securing#don-t-count-on-users-for-security) | | |
|  |  | [Prevent username enumeration](https://portswigger.net/web-security/authentication/securing#prevent-username-enumeration) | | |
|  |  | [Implement robust brute-force protection](https://portswigger.net/web-security/authentication/securing#implement-robust-brute-force-protection) | | |
|  |  | [Triple-check your verification logic](https://portswigger.net/web-security/authentication/securing#triple-check-your-verification-logic) | | |
|  |  | [Don't forget supplementary functionality](https://portswigger.net/web-security/authentication/securing#don-t-forget-supplementary-functionality) | | |
|  |  | [Implement proper multi-factor authentication](https://portswigger.net/web-security/authentication/securing#implement-proper-multi-factor-authentication) | | |
| [**Testing for WebSockets security vulnerabilities**](https://portswigger.net/web-security/websockets) | | | | |
|  | [WebSockets](https://portswigger.net/web-security/websockets#websockets) | | | |
|  | [Manipulating WebSocket traffic](https://portswigger.net/web-security/websockets#manipulating-websocket-traffic) | | | |
|  |  | [Intercepting and modifying WebSocket messages](https://portswigger.net/web-security/websockets#intercepting-and-modifying-websocket-messages) | | |
|  |  | [Replaying and generating new WebSocket messages](https://portswigger.net/web-security/websockets#replaying-and-generating-new-websocket-messages) | | |
|  |  | [Manipulating WebSocket connections](https://portswigger.net/web-security/websockets#manipulating-websocket-connections) | | |
|  | [WebSockets security vulnerabilities](https://portswigger.net/web-security/websockets#websockets-security-vulnerabilities) | | | |
|  |  | [Manipulating WebSocket messages to exploit vulnerabilities](https://portswigger.net/web-security/websockets#manipulating-websocket-messages-to-exploit-vulnerabilities) | | |
|  |  | [Manipulating the WebSocket handshake to exploit vulnerabilities](https://portswigger.net/web-security/websockets#manipulating-the-websocket-handshake-to-exploit-vulnerabilities) | | |
|  |  | [Using cross-site WebSockets to exploit vulnerabilities](https://portswigger.net/web-security/websockets#using-cross-site-websockets-to-exploit-vulnerabilities) | | |
|  | [How to secure a WebSocket connection](https://portswigger.net/web-security/websockets#how-to-secure-a-websocket-connection) | | | |
|  | [What are WebSockets?](https://portswigger.net/web-security/websockets/what-are-websockets) | | | |
|  |  | [What is the difference between HTTP and WebSockets?](https://portswigger.net/web-security/websockets/what-are-websockets#what-is-the-difference-between-http-and-websockets) | | |
|  |  | [How are WebSocket connections established?](https://portswigger.net/web-security/websockets/what-are-websockets#how-are-websocket-connections-established) | | |
|  |  | [What do WebSocket messages look like?](https://portswigger.net/web-security/websockets/what-are-websockets#what-do-websocket-messages-look-like) | | |
|  | [Cross-site WebSocket hijacking](https://portswigger.net/web-security/websockets/cross-site-websocket-hijacking) | | | |
|  |  | [What is cross-site WebSocket hijacking?](https://portswigger.net/web-security/websockets/cross-site-websocket-hijacking#what-is-cross-site-websocket-hijacking) | | |
|  |  | [What is the impact of cross-site WebSocket hijacking?](https://portswigger.net/web-security/websockets/cross-site-websocket-hijacking#what-is-the-impact-of-cross-site-websocket-hijacking) | | |
|  |  | [Performing a cross-site WebSocket hijacking attack](https://portswigger.net/web-security/websockets/cross-site-websocket-hijacking#performing-a-cross-site-websocket-hijacking-attack) | | |
| [**DOM-based vulnerabilities**](https://portswigger.net/web-security/dom-based) | | | | |
|  | [What is the DOM?](https://portswigger.net/web-security/dom-based#what-is-the-dom) | | | |
|  | [Taint-flow vulnerabilities](https://portswigger.net/web-security/dom-based#taint-flow-vulnerabilities) | | | |
|  |  | [What is taint flow?](https://portswigger.net/web-security/dom-based#what-is-taint-flow) | | |
|  |  | [Common sources](https://portswigger.net/web-security/dom-based#common-sources) | | |
|  |  | [Which sinks can lead to DOM-based vulnerabilities?](https://portswigger.net/web-security/dom-based#which-sinks-can-lead-to-dom-based-vulnerabilities) | | |
|  |  | [How to prevent DOM-based taint-flow vulnerabilities](https://portswigger.net/web-security/dom-based#how-to-prevent-dom-based-taint-flow-vulnerabilities) | | |
|  | [DOM clobbering](https://portswigger.net/web-security/dom-based#dom-clobbering) | | | |
|  | [Controlling the web message source](https://portswigger.net/web-security/dom-based/controlling-the-web-message-source) | | | |
|  |  | [What is the impact of DOM-based web message vulnerabilities?](https://portswigger.net/web-security/dom-based/controlling-the-web-message-source#what-is-the-impact-of-dom-based-web-message-vulnerabilities) | | |
|  |  | [How to construct an attack using web messages as the source](https://portswigger.net/web-security/dom-based/controlling-the-web-message-source#how-to-construct-an-attack-using-web-messages-as-the-source) | | |
|  |  | [Origin verification](https://portswigger.net/web-security/dom-based/controlling-the-web-message-source#origin-verification) | | |
|  |  | [Which sinks can lead to DOM-based web message vulnerabilities?](https://portswigger.net/web-security/dom-based/controlling-the-web-message-source#which-sinks-can-lead-to-dom-based-web-message-vulnerabilities) | | |
|  | [DOM-based open redirection](https://portswigger.net/web-security/dom-based/open-redirection) | | | |
|  |  | [What is DOM-based open redirection?](https://portswigger.net/web-security/dom-based/open-redirection#what-is-dom-based-open-redirection) | | |
|  |  | [What is the impact of DOM-based open redirection?](https://portswigger.net/web-security/dom-based/open-redirection#what-is-the-impact-of-dom-based-open-redirection) | | |
|  |  | [Which sinks can lead to DOM-based open-redirection vulnerabilities?](https://portswigger.net/web-security/dom-based/open-redirection#which-sinks-can-lead-to-dom-based-open-redirection-vulnerabilities) | | |
|  |  | [How to prevent DOM-based open-redirection vulnerabilities](https://portswigger.net/web-security/dom-based/open-redirection#how-to-prevent-dom-based-open-redirection-vulnerabilities) | | |
|  | [DOM-based cookie manipulation](https://portswigger.net/web-security/dom-based/cookie-manipulation) | | | |
|  |  | [What is DOM-based cookie manipulation?](https://portswigger.net/web-security/dom-based/cookie-manipulation#what-is-dom-based-cookie-manipulation) | | |
|  |  | [What is the impact of a DOM-based cookie-manipulation attack?](https://portswigger.net/web-security/dom-based/cookie-manipulation#what-is-the-impact-of-a-dom-based-cookie-manipulation-attack) | | |
|  |  | [Which sinks can lead to DOM-based cookie-manipulation vulnerabilities?](https://portswigger.net/web-security/dom-based/cookie-manipulation#which-sinks-can-lead-to-dom-based-cookie-manipulation-vulnerabilities) | | |
|  |  | [How to prevent DOM-based cookie-manipulation vulnerabilities](https://portswigger.net/web-security/dom-based/cookie-manipulation#how-to-prevent-dom-based-cookie-manipulation-vulnerabilities) | | |
|  | [DOM-based JavaScript injection](https://portswigger.net/web-security/dom-based/javascript-injection) | | | |
|  |  | [What is DOM-based JavaScript injection?](https://portswigger.net/web-security/dom-based/javascript-injection#what-is-dom-based-javascript-injection) | | |
|  |  | [What is the impact of a DOM-based JavaScript-injection attack?](https://portswigger.net/web-security/dom-based/javascript-injection#what-is-the-impact-of-a-dom-based-javascript-injection-attack) | | |
|  |  | [Which sinks can lead to DOM-based JavaScript-injection vulnerabilities?](https://portswigger.net/web-security/dom-based/javascript-injection#which-sinks-can-lead-to-dom-based-javascript-injection-vulnerabilities) | | |
|  |  | [How to prevent DOM-based JavaScript-injection vulnerabilities](https://portswigger.net/web-security/dom-based/javascript-injection#how-to-prevent-dom-based-javascript-injection-vulnerabilities) | | |
|  | [DOM-based document-domain manipulation](https://portswigger.net/web-security/dom-based/document-domain-manipulation) | | | |
|  |  | [What is DOM-based document-domain manipulation?](https://portswigger.net/web-security/dom-based/document-domain-manipulation#what-is-dom-based-document-domain-manipulation) | | |
|  |  | [Which sinks can lead to DOM-based document-domain manipulation vulnerabilities?](https://portswigger.net/web-security/dom-based/document-domain-manipulation#which-sinks-can-lead-to-dom-based-document-domain-manipulation-vulnerabilities) | | |
|  |  | [How to prevent DOM-based document-domain manipulation vulnerabilities](https://portswigger.net/web-security/dom-based/document-domain-manipulation#how-to-prevent-dom-based-document-domain-manipulation-vulnerabilities) | | |
|  | [DOM-based WebSocket-URL poisoning](https://portswigger.net/web-security/dom-based/websocket-url-poisoning) | | | |
|  |  | [What is DOM-based WebSocket-URL poisoning?](https://portswigger.net/web-security/dom-based/websocket-url-poisoning#what-is-dom-based-websocket-url-poisoning) | | |
|  |  | [What is the impact of WebSocket-URL poisoning?](https://portswigger.net/web-security/dom-based/websocket-url-poisoning#what-is-the-impact-of-websocket-url-poisoning) | | |
|  |  | [Which sinks can lead to WebSocket-URL poisoning vulnerabilities?](https://portswigger.net/web-security/dom-based/websocket-url-poisoning#which-sinks-can-lead-to-websocket-url-poisoning-vulnerabilities) | | |
|  |  | [How to prevent DOM-based WebSocket-URL poisoning vulnerabilities](https://portswigger.net/web-security/dom-based/websocket-url-poisoning#how-to-prevent-dom-based-websocket-url-poisoning-vulnerabilities) | | |
|  | [DOM-based link manipulation](https://portswigger.net/web-security/dom-based/link-manipulation) | | | |
|  |  | [What is DOM-based link manipulation?](https://portswigger.net/web-security/dom-based/link-manipulation#what-is-dom-based-link-manipulation) | | |
|  |  | [What is the impact of a DOM-based link-manipulation attack?](https://portswigger.net/web-security/dom-based/link-manipulation#what-is-the-impact-of-a-dom-based-link-manipulation-attack) | | |
|  |  | [Which sinks can lead to DOM-based link-manipulation vulnerabilities?](https://portswigger.net/web-security/dom-based/link-manipulation#which-sinks-can-lead-to-dom-based-link-manipulation-vulnerabilities) | | |
|  |  | [How to prevent DOM-based link-manipulation vulnerabilities](https://portswigger.net/web-security/dom-based/link-manipulation#how-to-prevent-dom-based-link-manipulation-vulnerabilities) | | |
|  | [Web message manipulation](https://portswigger.net/web-security/dom-based/web-message-manipulation) | | | |
|  |  | [What is DOM-based web message manipulation?](https://portswigger.net/web-security/dom-based/web-message-manipulation#what-is-dom-based-web-message-manipulation) | | |
|  |  | [Which sinks can lead to DOM-based web-message manipulation vulnerabilities?](https://portswigger.net/web-security/dom-based/web-message-manipulation#which-sinks-can-lead-to-dom-based-web-message-manipulation-vulnerabilities) | | |
|  |  | [How to prevent DOM-based web message manipulation](https://portswigger.net/web-security/dom-based/web-message-manipulation#how-to-prevent-dom-based-web-message-manipulation) | | |
|  | [DOM-based Ajax request-header manipulation](https://portswigger.net/web-security/dom-based/ajax-request-header-manipulation) | | | |
|  |  | [What is DOM-based Ajax request-header manipulation?](https://portswigger.net/web-security/dom-based/ajax-request-header-manipulation#what-is-dom-based-ajax-request-header-manipulation) | | |
|  |  | [What is the impact of DOM-based Ajax request-header manipulation?](https://portswigger.net/web-security/dom-based/ajax-request-header-manipulation#what-is-the-impact-of-dom-based-ajax-request-header-manipulation) | | |
|  |  | [Which sinks can lead to DOM-based Ajax request-header manipulation vulnerabilities?](https://portswigger.net/web-security/dom-based/ajax-request-header-manipulation#which-sinks-can-lead-to-dom-based-ajax-request-header-manipulation-vulnerabilities) | | |
|  |  | [How to prevent DOM-based Ajax request-header manipulation](https://portswigger.net/web-security/dom-based/ajax-request-header-manipulation#how-to-prevent-dom-based-ajax-request-header-manipulation) | | |
|  | [DOM-based local file-path manipulation](https://portswigger.net/web-security/dom-based/local-file-path-manipulation) | | | |
|  |  | [What is DOM-based local file-path manipulation?](https://portswigger.net/web-security/dom-based/local-file-path-manipulation#what-is-dom-based-local-file-path-manipulation) | | |
|  |  | [What is the impact of DOM-based local file-path manipulation?](https://portswigger.net/web-security/dom-based/local-file-path-manipulation#what-is-the-impact-of-dom-based-local-file-path-manipulation) | | |
|  |  | [Which sinks can lead to DOM-based local file-path manipulation vulnerabilities?](https://portswigger.net/web-security/dom-based/local-file-path-manipulation#which-sinks-can-lead-to-dom-based-local-file-path-manipulation-vulnerabilities) | | |
|  |  | [How to prevent DOM-based local file-path manipulation vulnerabilities](https://portswigger.net/web-security/dom-based/local-file-path-manipulation#how-to-prevent-dom-based-local-file-path-manipulation-vulnerabilities) | | |
|  | [DOM-based client-side SQL injection](https://portswigger.net/web-security/dom-based/client-side-sql-injection) | | | |
|  |  | [What is DOM-based client-side SQL injection?](https://portswigger.net/web-security/dom-based/client-side-sql-injection#what-is-dom-based-client-side-sql-injection) | | |
|  |  | [What is the impact of DOM-based client-side SQL injection?](https://portswigger.net/web-security/dom-based/client-side-sql-injection#what-is-the-impact-of-dom-based-client-side-sql-injection) | | |
|  |  | [Which sinks can lead to DOM-based client-side SQL-injection vulnerabilities?](https://portswigger.net/web-security/dom-based/client-side-sql-injection#which-sinks-can-lead-to-dom-based-client-side-sql-injection-vulnerabilities) | | |
|  |  | [How to prevent DOM-based client-side SQL-injection vulnerabilities](https://portswigger.net/web-security/dom-based/client-side-sql-injection#how-to-prevent-dom-based-client-side-sql-injection-vulnerabilities) | | |
|  | [DOM-based HTML5-storage manipulation](https://portswigger.net/web-security/dom-based/html5-storage-manipulation) | | | |
|  |  | [What is DOM-based HTML5-storage manipulation?](https://portswigger.net/web-security/dom-based/html5-storage-manipulation#what-is-dom-based-html5-storage-manipulation) | | |
|  |  | [Which sinks can lead to DOM-based HTML5-storage manipulation vulnerabilities?](https://portswigger.net/web-security/dom-based/html5-storage-manipulation#which-sinks-can-lead-to-dom-based-html5-storage-manipulation-vulnerabilities) | | |
|  |  | [How to prevent DOM-based HTML5-storage manipulation vulnerabilities](https://portswigger.net/web-security/dom-based/html5-storage-manipulation#how-to-prevent-dom-based-html5-storage-manipulation-vulnerabilities) | | |
|  | [DOM-based client-side XPath injection](https://portswigger.net/web-security/dom-based/client-side-xpath-injection) | | | |
|  |  | [What is DOM-based XPath injection?](https://portswigger.net/web-security/dom-based/client-side-xpath-injection#what-is-dom-based-xpath-injection) | | |
|  |  | [What is the impact of DOM-based XPath injection?](https://portswigger.net/web-security/dom-based/client-side-xpath-injection#what-is-the-impact-of-dom-based-xpath-injection) | | |
|  |  | [Which sinks can lead to XPath-injection vulnerabilities?](https://portswigger.net/web-security/dom-based/client-side-xpath-injection#which-sinks-can-lead-to-xpath-injection-vulnerabilities) | | |
|  |  | [How to prevent DOM-based XPath-injection vulnerabilities](https://portswigger.net/web-security/dom-based/client-side-xpath-injection#how-to-prevent-dom-based-xpath-injection-vulnerabilities) | | |
|  | [DOM-based client-side JSON injection](https://portswigger.net/web-security/dom-based/client-side-json-injection) | | | |
|  |  | [What is DOM-based JSON injection?](https://portswigger.net/web-security/dom-based/client-side-json-injection#what-is-dom-based-json-injection) | | |
|  |  | [What is the impact of a DOM-based JSON-injection attack?](https://portswigger.net/web-security/dom-based/client-side-json-injection#what-is-the-impact-of-a-dom-based-json-injection-attack) | | |
|  |  | [Which sinks can lead to DOM-based JSON-injection vulnerabilities?](https://portswigger.net/web-security/dom-based/client-side-json-injection#which-sinks-can-lead-to-dom-based-json-injection-vulnerabilities) | | |
|  |  | [How to prevent client-side JSON-injection vulnerabilities?](https://portswigger.net/web-security/dom-based/client-side-json-injection#how-to-prevent-client-side-json-injection-vulnerabilities) | | |
|  | [DOM-data manipulation](https://portswigger.net/web-security/dom-based/dom-data-manipulation) | | | |
|  |  | [What is DOM-data manipulation?](https://portswigger.net/web-security/dom-based/dom-data-manipulation#what-is-dom-data-manipulation) | | |
|  |  | [What is the impact of DOM-data manipulation?](https://portswigger.net/web-security/dom-based/dom-data-manipulation#what-is-the-impact-of-dom-data-manipulation) | | |
|  |  | [Which sinks can lead to DOM-data manipulation vulnerabilities?](https://portswigger.net/web-security/dom-based/dom-data-manipulation#which-sinks-can-lead-to-dom-data-manipulation-vulnerabilities) | | |
|  |  | [How to prevent DOM-data manipulation vulnerabilities](https://portswigger.net/web-security/dom-based/dom-data-manipulation#how-to-prevent-dom-data-manipulation-vulnerabilities) | | |
|  | [DOM-based denial of service](https://portswigger.net/web-security/dom-based/denial-of-service) | | | |
|  |  | [What is DOM-based denial of service?](https://portswigger.net/web-security/dom-based/denial-of-service#what-is-dom-based-denial-of-service) | | |
|  |  | [Which sinks can lead to DOM-based denial-of-service vulnerabilities?](https://portswigger.net/web-security/dom-based/denial-of-service#which-sinks-can-lead-to-dom-based-denial-of-service-vulnerabilities) | | |
|  |  | [How to prevent DOM-based denial-of-service vulnerabilities](https://portswigger.net/web-security/dom-based/denial-of-service#how-to-prevent-dom-based-denial-of-service-vulnerabilities) | | |
|  | [DOM clobbering](https://portswigger.net/web-security/dom-based/dom-clobbering) | | | |
|  |  | [What is DOM clobbering?](https://portswigger.net/web-security/dom-based/dom-clobbering#what-is-dom-clobbering) | | |
|  |  | [How to exploit DOM-clobbering vulnerabilities](https://portswigger.net/web-security/dom-based/dom-clobbering#how-to-exploit-dom-clobbering-vulnerabilities) | | |
|  |  | [How to prevent DOM-clobbering attacks](https://portswigger.net/web-security/dom-based/dom-clobbering#how-to-prevent-dom-clobbering-attacks) | | |
| [**Web cache poisoning**](https://portswigger.net/web-security/web-cache-poisoning) | | | | |
|  | [What is web cache poisoning?](https://portswigger.net/web-security/web-cache-poisoning#what-is-web-cache-poisoning) | | | |
|  |  | [Web cache poisoning research](https://portswigger.net/web-security/web-cache-poisoning#web-cache-poisoning-research) | | |
|  |  | [How does a web cache work?](https://portswigger.net/web-security/web-cache-poisoning#how-does-a-web-cache-work) | | |
|  | [What is the impact of a web cache poisoning attack?](https://portswigger.net/web-security/web-cache-poisoning#what-is-the-impact-of-a-web-cache-poisoning-attack) | | | |
|  | [Constructing a web cache poisoning attack](https://portswigger.net/web-security/web-cache-poisoning#constructing-a-web-cache-poisoning-attack) | | | |
|  |  | [Identify and evaluate unkeyed inputs](https://portswigger.net/web-security/web-cache-poisoning#identify-and-evaluate-unkeyed-inputs) | | |
|  | [Param Miner](https://portswigger.net/web-security/web-cache-poisoning#param-miner) | | | |
|  |  | [Elicit a harmful response from the back-end server](https://portswigger.net/web-security/web-cache-poisoning#elicit-a-harmful-response-from-the-back-end-server) | | |
|  |  | [Get the response cached](https://portswigger.net/web-security/web-cache-poisoning#get-the-response-cached) | | |
|  | [Exploiting web cache poisoning vulnerabilities](https://portswigger.net/web-security/web-cache-poisoning#exploiting-web-cache-poisoning-vulnerabilities) | | | |
|  | [How to prevent web cache poisoning vulnerabilities](https://portswigger.net/web-security/web-cache-poisoning#how-to-prevent-web-cache-poisoning-vulnerabilities) | | | |
|  | [Exploiting cache design flaws](https://portswigger.net/web-security/web-cache-poisoning/exploiting-design-flaws) | | | |
|  |  | [Using web cache poisoning to deliver an XSS attack](https://portswigger.net/web-security/web-cache-poisoning/exploiting-design-flaws#using-web-cache-poisoning-to-deliver-an-xss-attack) | | |
|  |  | [Using web cache poisoning to exploit unsafe handling of resource imports](https://portswigger.net/web-security/web-cache-poisoning/exploiting-design-flaws#using-web-cache-poisoning-to-exploit-unsafe-handling-of-resource-imports) | | |
|  |  | [Using web cache poisoning to exploit cookie-handling vulnerabilities](https://portswigger.net/web-security/web-cache-poisoning/exploiting-design-flaws#using-web-cache-poisoning-to-exploit-cookie-handling-vulnerabilities) | | |
|  |  | [Using multiple headers to exploit web cache poisoning vulnerabilities](https://portswigger.net/web-security/web-cache-poisoning/exploiting-design-flaws#using-multiple-headers-to-exploit-web-cache-poisoning-vulnerabilities) | | |
|  |  | [Exploiting responses that expose too much information](https://portswigger.net/web-security/web-cache-poisoning/exploiting-design-flaws#exploiting-responses-that-expose-too-much-information) | | |
|  |  |  | [Cache-control directives](https://portswigger.net/web-security/web-cache-poisoning/exploiting-design-flaws#cache-control-directives) | |
|  |  |  | [Vary header](https://portswigger.net/web-security/web-cache-poisoning/exploiting-design-flaws#vary-header) | |
|  |  | [Using web cache poisoning to exploit DOM-based vulnerabilities](https://portswigger.net/web-security/web-cache-poisoning/exploiting-design-flaws#using-web-cache-poisoning-to-exploit-dom-based-vulnerabilities) | | |
|  |  | [Chaining web cache poisoning vulnerabilities](https://portswigger.net/web-security/web-cache-poisoning/exploiting-design-flaws#chaining-web-cache-poisoning-vulnerabilities) | | |
|  | [Exploiting cache implementation flaws](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws) | | | |
|  |  | [Cache key flaws](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#cache-key-flaws) | | |
|  |  | [Cache probing methodology](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#cache-probing-methodology) | | |
|  |  |  | [Identify a suitable cache oracle](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#identify-a-suitable-cache-oracle) | |
|  |  |  | [Probe key handling](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#probe-key-handling) | |
|  |  |  | [Identify an exploitable gadget](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#identify-an-exploitable-gadget) | |
|  |  | [Exploiting cache key flaws](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#exploiting-cache-key-flaws) | | |
|  |  |  | [Unkeyed port](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#unkeyed-port) | |
|  |  |  | [Unkeyed query string](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#unkeyed-query-string) | |
|  |  |  | [Unkeyed query parameters](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#unkeyed-query-parameters) | |
|  |  |  | [Cache parameter cloaking](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#cache-parameter-cloaking) | |
|  |  |  | [Normalized cache keys](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#normalized-cache-keys) | |
|  |  |  | [Cache key injection](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#cache-key-injection) | |
|  |  | [Poisoning internal caches](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#poisoning-internal-caches) | | |
|  |  |  | [How to identify internal caches](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#how-to-identify-internal-caches) | |
|  |  |  | [Testing internal caches safely](https://portswigger.net/web-security/web-cache-poisoning/exploiting-implementation-flaws#testing-internal-caches-safely) | |
| [**Information disclosure vulnerabilities**](https://portswigger.net/web-security/information-disclosure) | | | | |
|  | [What is information disclosure?](https://portswigger.net/web-security/information-disclosure#what-is-information-disclosure) | | | |
|  | [How do information disclosure vulnerabilities arise?](https://portswigger.net/web-security/information-disclosure#how-do-information-disclosure-vulnerabilities-arise) | | | |
|  | [What is the impact of information disclosure vulnerabilities?](https://portswigger.net/web-security/information-disclosure#what-is-the-impact-of-information-disclosure-vulnerabilities) | | | |
|  |  | [How to assess the severity of information disclosure vulnerabilities](https://portswigger.net/web-security/information-disclosure#how-to-assess-the-severity-of-information-disclosure-vulnerabilities) | | |
|  | [Exploiting information disclosure](https://portswigger.net/web-security/information-disclosure#exploiting-information-disclosure) | | | |
|  | [How to prevent information disclosure vulnerabilities](https://portswigger.net/web-security/information-disclosure#how-to-prevent-information-disclosure-vulnerabilities) | | | |
|  | [How to find and exploit information disclosure vulnerabilities](https://portswigger.net/web-security/information-disclosure/exploiting) | | | |
|  |  | [How to test for information disclosure vulnerabilities](https://portswigger.net/web-security/information-disclosure/exploiting#how-to-test-for-information-disclosure-vulnerabilities) | | |
|  |  |  | [Fuzzing](https://portswigger.net/web-security/information-disclosure/exploiting#fuzzing) | |
|  |  |  | [Using Burp Scanner](https://portswigger.net/web-security/information-disclosure/exploiting#using-burp-scanner) | |
|  |  |  | [Using Burp's engagement tools](https://portswigger.net/web-security/information-disclosure/exploiting#using-burp-s-engagement-tools) | |
|  |  |  | [Engineering informative responses](https://portswigger.net/web-security/information-disclosure/exploiting#engineering-informative-responses) | |
|  |  | [Common sources of information disclosure](https://portswigger.net/web-security/information-disclosure/exploiting#common-sources-of-information-disclosure) | | |
|  |  |  | [Files for web crawlers](https://portswigger.net/web-security/information-disclosure/exploiting#files-for-web-crawlers) | |
|  |  |  | [Directory listings](https://portswigger.net/web-security/information-disclosure/exploiting#directory-listings) | |
|  |  |  | [Developer comments](https://portswigger.net/web-security/information-disclosure/exploiting#developer-comments) | |
|  |  |  | [Error messages](https://portswigger.net/web-security/information-disclosure/exploiting#error-messages) | |
|  |  |  | [Debugging data](https://portswigger.net/web-security/information-disclosure/exploiting#debugging-data) | |
|  |  |  | [User account pages](https://portswigger.net/web-security/information-disclosure/exploiting#user-account-pages) | |
|  |  |  | [Source code disclosure via backup files](https://portswigger.net/web-security/information-disclosure/exploiting#source-code-disclosure-via-backup-files) | |
|  |  |  | [Information disclosure due to insecure configuration](https://portswigger.net/web-security/information-disclosure/exploiting#information-disclosure-due-to-insecure-configuration) | |
|  |  |  | [Version control history](https://portswigger.net/web-security/information-disclosure/exploiting#version-control-history) | |
| [**Reference**](https://portswigger.net/web-security/reference) | | | | |
|  | [Augmenting your manual testing with Burp Scanner](https://portswigger.net/web-security/reference/augmenting-your-manual-testing-with-burp-scanner) | | | |
|  |  | [Scanning a specific request](https://portswigger.net/web-security/reference/augmenting-your-manual-testing-with-burp-scanner#scanning-a-specific-request) | | |
|  |  | [Scanning custom insertion points](https://portswigger.net/web-security/reference/augmenting-your-manual-testing-with-burp-scanner#scanning-custom-insertion-points) | | |
|  |  | [Scanning non-standard data structures](https://portswigger.net/web-security/reference/augmenting-your-manual-testing-with-burp-scanner#scanning-non-standard-data-structures) | | |
|  | [Obfuscating attacks using encodings](https://portswigger.net/web-security/reference/obfuscating-attacks-using-encodings) | | | |
|  |  | [Context-specific decoding](https://portswigger.net/web-security/reference/obfuscating-attacks-using-encodings#context-specific-decoding) | | |
|  |  | [Decoding discrepancies](https://portswigger.net/web-security/reference/obfuscating-attacks-using-encodings#decoding-discrepancies) | | |
|  |  | [Obfuscation via URL encoding](https://portswigger.net/web-security/reference/obfuscating-attacks-using-encodings#obfuscation-via-url-encoding) | | |
|  |  | [Obfuscation via double URL encoding](https://portswigger.net/web-security/reference/obfuscating-attacks-using-encodings#obfuscation-via-double-url-encoding) | | |
|  |  | [Obfuscation via HTML encoding](https://portswigger.net/web-security/reference/obfuscating-attacks-using-encodings#obfuscation-via-html-encoding) | | |
|  |  |  | [Leading zeros](https://portswigger.net/web-security/reference/obfuscating-attacks-using-encodings#leading-zeros) | |
|  |  | [Obfuscation via unicode escaping](https://portswigger.net/web-security/reference/obfuscating-attacks-using-encodings#obfuscation-via-unicode-escaping) | | |
|  |  | [Obfuscation via hex escaping](https://portswigger.net/web-security/reference/obfuscating-attacks-using-encodings#obfuscation-via-hex-escaping) | | |
|  |  | [Obfuscation via octal escaping](https://portswigger.net/web-security/reference/obfuscating-attacks-using-encodings#obfuscation-via-octal-escaping) | | |
|  |  | [Obfuscation via multiple encodings](https://portswigger.net/web-security/reference/obfuscating-attacks-using-encodings#obfuscation-via-multiple-encodings) | | |
|  |  | [Obfuscation via the SQL CHAR() function](https://portswigger.net/web-security/reference/obfuscating-attacks-using-encodings#obfuscation-via-the-sql-char-function) | | |