

Introduction:

https://en.wikipedia.org/wiki/Web_application

<https://blog.stackpath.com/web-application/>

<https://www.guru99.com/difference-web-application-website.html>

<https://www.lifewire.com/what-is-a-web-application-3486637>

<https://stackify.com/web-application-architecture/>

<https://hackr.io/blog/web-application-architecture-definition-models-types-and-more>

<https://www.educative.io/blog/how-to-design-a-web-application-software-architecture-101>

<https://www.peerbits.com/blog/web-application-architecture.html>

<https://www.veracode.com/security/web-application-vulnerabilities>

<https://www.cypressdatadefense.com/blog/web-application-vulnerabilities/>

<https://exploitbyte.com/vulnerability-stack/>

<https://www.fullstackpython.com/web-application-security.html>

<https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/>

Pentesting resources:

<https://github.com/swisskyrepo/PayloadsAllTheThings>

<https://github.com/EnableSecurity/Webapp-Exploit-Payloads>

<https://github.com/0verpwn/Fuzzing>

SQL Injection:

<https://portswigger.net/web-security/sql-injection>

<http://leettime.net/sqlninja.com/>

http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Web/Web_SQL_Injection/

<https://hack.me/t/SQLi>
https://owasp.org/www-community/attacks/Blind_SQL_Injection
<https://portswigger.net/web-security/sql-injection/cheat-sheet>
<https://github.com/payloadbox/sql-injection-payload-list>
<https://github.com/trietptm/SQL-Injection-Payloads>
<https://github.com/AdmiralGaust/SQL-Injection-cheat-sheet>

Directory traversal:

<https://portswigger.net/web-security/file-path-traversal>
<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Directory%20Traversal>
https://owasp.org/www-community/attacks/Path_Traversal
<https://pentestlab.blog/2012/06/29/directory-traversal-cheat-sheet/>
<https://github.com/payloadbox/directory-payload-list>

Command Injection:

<https://hackersonlineclub.com/command-injection-cheatsheet/>
https://owasp.org/www-community/attacks/Command_Injection
<https://github.com/payloadbox/command-injection-payload-list>
<https://portswigger.net/web-security/os-command-injection>

Open Redirect:

https://portswigger.net/kb/issues/00500100_open-redirection-reflected
<https://github.com/payloadbox/open-redirect-payload-list>

<https://github.com/random-robbie/open-redirect>

https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html

<https://hackerone.com/reports/2731>

Broken Access Control:

https://owasp.org/www-community/Broken_Access_Control

<https://portswigger.net/web-security/access-control>

<https://www.contrastsecurity.com/knowledge-hub/glossary/broken-access-control>

<https://github.com/OWASP/Top10/blob/master/2017/en/0xa5-broken-access-control.md>

<https://portswigger.net/web-security/access-control/idor>

<https://github.com/gwen001/testidor>

<https://github.com/foospidy/payloads>

Information Disclosure:

<https://portswigger.net/web-security/information-disclosure>

<https://github.com/topics/information-disclosure>

<https://www.bugcrowd.com/resources/webinars/github-recon-and-sensitive-data-exposure/>

Improper Error Handling:

https://owasp.org/www-community/Improper_Error_Handling

Security Misconfiguration:

https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A6-Security_Misconfiguration

https://www.tutorialspoint.com/security_testing/testing_security_misconfiguration.htm

<https://bounty.github.com/classifications/security-misconfiguration.html>

Broken Authentication:

<https://portswigger.net/web-security/authentication>
<https://auth0.com/blog/what-is-broken-authentication/>
https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A2-Broken_Authentication
<https://www.contrastsecurity.com/knowledge-hub/glossary/broken-authentication>
<https://bounty.github.com/classifications/broken-authentication-or-session-management.html>
<https://github.com/rumkin/http-auth-payload>

Cross Site Scripting:

<https://portswigger.net/web-security/cross-site-scripting>
https://en.wikipedia.org/wiki/Cross-site_scripting
<https://owasp.org/www-community/attacks/xss/>
<https://github.com/s0md3v/XSSStrike>
<https://github.com/R0X4R/D4rkXSS>
<https://github.com/payloadbox/xss-payload-list>
<https://github.com/pgaijin66/XSS-Payloads>
<https://github.com/s0md3v/AwesomeXSS>

Cross Site Request Forgery:

<https://portswigger.net/web-security/csrf>
<https://owasp.org/www-community/attacks/csrf>
https://en.wikipedia.org/wiki/Cross-site_request_forgery
<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/CSRF%20Injection>

Malicious File Upload:

<https://www.acunetix.com/vulnerabilities/web/unrestricted-file-upload/>

Unrestricted_File_Upload <https://owasp.org/www-community/vulnerabilities/>

upload <https://book.hacktricks.xyz/pentesting-web/file->

<https://github.com/flozz/p0wny-shell>

<https://github.com/almandin/fuxploader>

<https://github.com/PortSwigger/upload-scanner>

<https://github.com/0xspade/XSS-Gif-Payload>

CORS Misconfiguration:

[https://portswigger.net/research/exploiting-cors-](https://portswigger.net/research/exploiting-cors-misconfigurations-for-bitcoins-and-bounties)
[misconfigurations-for-bitcoins-and-bounties](https://portswigger.net/research/exploiting-cors-misconfigurations-for-bitcoins-and-bounties)

<https://portswigger.net/web-security/cors>

<https://hackerone.com/reports/426147>

[https://blog.detectify.com/2018/04/26/cors-](https://blog.detectify.com/2018/04/26/cors-misconfigurations-explained/)
[misconfigurations-explained/](https://blog.detectify.com/2018/04/26/cors-misconfigurations-explained/)

[https://www.we45.com/blog/3-ways-to-exploit-](https://www.we45.com/blog/3-ways-to-exploit-misconfigured-cross-origin-resource-sharing-cors)
[misconfigured-cross-origin-resource-sharing-cors](https://www.we45.com/blog/3-ways-to-exploit-misconfigured-cross-origin-resource-sharing-cors)

<https://github.com/chenjji/CORScanner>

<https://github.com/RUB-NDS/CORStest>

<https://github.com/s0md3v/Corsy>

<https://github.com/incredibleindishell/CORS->
[vulnerable-Lab](https://github.com/incredibleindishell/CORS-)

Server Side Request Forgery:

<https://portswigger.net/web-security/ssrf>

<https://portswigger.net/web-security/ssrf/blind>

<https://portswigger.net/daily-swig/ssrf>

[https://www.acunetix.com/blog/articles/server-side-](https://www.acunetix.com/blog/articles/server-side-request-forgery-vulnerability/)
[request-forgery-vulnerability/](https://www.acunetix.com/blog/articles/server-side-request-forgery-vulnerability/)

<https://owasp.org/www-community/attacks/>
Server_Side_Request_Forgery

<https://github.com/swisskyrepo/SSRFmap>

<https://github.com/jdonsec/AllThingsSSRF>

<https://github.com/cujanovic/SSRF-Testing>

Clickjacking:

<https://en.wikipedia.org/wiki/Clickjacking>

Clickjacking

<https://owasp.org/www-community/attacks/>

<https://portswigger.net/web-security/clickjacking>

<https://github.com/D4Vinci/Clickjacking-Tester>

<https://github.com/clarkio/clickjacking>

Exploit

<https://github.com/thomaspatzke/Clickjacking-Exploit>

Server Side Template Injection:

<https://portswigger.net/research/server-side-template-injection>

<https://portswigger.net/web-security/server-side-template-injection>

<https://medium.com/server-side-template-injection/server-side-template-injection-faf88d0c7f34>

<https://www.we45.com/blog/server-side-template-injection-a-crash-course->

<https://github.com/epinna/tplmap>

<https://github.com/payloadbox/ssti-payloads>

<https://github.com/DiogoMRSilva/websitesVulnerableToSSTI>

Appication Level DOS:

<https://www.bugcrowd.com/resources/glossary/application-level-denial-of-service-dos/>

<https://github.com/shekyan/slowhttptest>

<https://github.com/Quitten/doser.py>

<https://github.com/tomasmichael995/DoSDroid>

<https://github.com/LaurentPerche/slowhttptest>

<https://tools.kali.org/stress-testing/slowhttptest>

XML External Entities:

<https://portswigger.net/web-security/xxe>

<https://portswigger.net/web-security/xxe/blind>

https://portswigger.net/kb/issues/00100700_xml-injection

<https://medium.com/@onehackman/exploiting-xml-external-entity-xxe-injections-b0e3eac388f9>

<https://github.com/payloadbox/xxe-injection-payload-list>

<https://gist.github.com/staaldraad/01415b990939494879b4>

<https://github.com/joernchen/xxeserve>

<https://github.com/RihaMaheshwari/XXE-Injection-Payloads>

Insecure Deserialization:

<https://portswigger.net/web-security/deserialization>

<https://portswigger.net/web-security/deserialization/exploiting>

<https://github.com/RihaMaheshwari/Insecure-Deserialization>

<https://github.com/raadfhaddad/Insecure-Deserialization>

<https://github.com/frohoff/ysoserial>

<https://securitylab.github.com/research/insecure-deserialization>

<https://github.com/indrefi/Insecure-Deserialization-.NET-RCE>

<https://github.com/sh4d3s/Insecure-Deserialization>

LFI/RFI:

<https://secf00tprint.github.io/blog/payload-tester/lfirfi/en>