eWPTX Preparation by Joas

API and Cloud Application Attacks

- https://techbeacon.com/enterprise-it/pen-testing-cloud-based-apps-step-step-guide
- https://kirkpatrickprice.com/blog/api-penetration-testing/
- https://securetriad.io/the-what-why-and-how-of-api-penetration-testing/
- https://secureideas.com/knowledge/what-is-the-difference-between-api-and-webapp-pentests
- https://www.breachlock.com/penetration-testing-of-apis-and-microservices/
- https://turingpoint.de/en/security-assessments/pentests/web-applications/
- https://www.sans.org/webcasts/pen-testing-api-security-web-cloud-119180
- https://thecyphere.com/services/web-application-penetration-testing/
- https://www.iarminfo.com/api-penetration-testing/
- https://www.securitycompassadvisory.com/blog/api-security-testing-best-practices-key-vulnerabilities/
- https://outpost24.com/blog/what-is-api-security-and-how-to-protect-them
- https://github.com/inonshk/31-days-of-API-Security-Tips
- https://github.com/0xbigshaq/firepwn-tool
- https://github.com/arainho/awesome-api-security
- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Cloud%20-%20Azure%20Pentest.md
- https://github.com/HSIS007/Useful_Websites_For_Pentester
- https://book.hacktricks.xyz/pentesting/pentesting-web/web-api-pentesting
- https://github.com/omkar-ukirde/api-pentesting
- https://github.com/BBVA/apicheck
- https://github.com/flipkart-incubator/Astra
- https://github.com/dsopas/MindAPI

Attacking Crypto

- https://www.hacker101.com/sessions/crypto_attacks.html
- https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html
- https://www.coindesk.com/crypto-attacks-bitcoin-ethereum-classic-open-source-value
- https://github.com/jvdsn/crypto-attacks
- https://www.coindesk.com/hackers-mined-crypto-on-githubs-servers-report
- https://heimdalsecurity.com/blog/github-infrastructure-used-to-mine-cryptocurrency/
- https://dev.to/thibaultduponchelle/the-github-action-mining-attack-through-pull-request-2lmc
- https://owasp.org/www-pdf-archive//Emil-gurevitch-practical-crypto-attacks-part-1.pdf
- https://auth0.com/blog/critical-vulnerabilities-in-json-web-token-libraries/
- https://www.sjoerdlangkemper.nl/2016/09/28/attacking-jwt-authentication/
- https://arstechnica.com/information-technology/2013/03/new-attacks-on-ssl-decrypt-authentication-cookies/
- https://attack.mitre.org/techniques/T1140/
- https://portswigger.net/bappstore/f923cbf91698420890354c1d8958fee6
- https://hackernoon.com/a-guide-to-hashing-how-to-keep-your-database-safe-4n1fq3lnz
- https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/
- https://auth0.com/blog/hashing-passwords-one-way-road-to-security/

Attacking Serialization

- https://www.reblaze.com/blog/serialization-attacks-what-they-are-and-how-to-prevent-them/#:~:text=A%20serialization%20attack%20happens%20when,into%20an%20in%2Dmemory%20structure.
- https://speakerdeck.com/pwntester/attacking-net-serialization
- https://www.youtube.com/watch?v=eDfGpu3iE4Q
- https://www.youtube.com/watch?v=qDoBlLwREYk
- https://www.youtube.com/watch?v=NqHsaVhlxAQ
- https://portswigger.net/web-security/deserialization
- https://owasp.org/www-community/vulnerabilities/Deserialization_of_untrusted_data
- https://cheatsheetseries.owasp.org/cheatsheets/Deserialization_Cheat_Sheet.html
- https://hdivsecurity.com/bornsecure/insecure-deserialization-attack-examples-mitigation/
- https://snyk.io/blog/serialization-and-deserialization-in-java/
- https://medium.com/gdg-vit/deserialization-attacks-d312fbe58e7d
- https://infosecwriteups.com/insecure-deserialization-5c64e9943f0e
- https://nickbloor.co.uk/2017/08/13/attacking-java-deserialization/
- https://www.cyberbit.com/blog/endpoint-security/serialization-vulnerabilities-explained/
- http://www.securitytube.net/video/1045
- https://www.cisecurity.org/blog/data-deserialization/
- https://blog.cobalt.io/the-anatomy-of-deserialization-attacks-b90b56328766
- https://www.immuniweb.com/blog/OWASP-insecure-deserialization.html
- https://securityboulevard.com/2018/06/deserialization-vulnerabilities-attacking-deserialization-in-js/
- https://portswigger.net/web-security/deserialization#:~:text=Insecure%20deserialization%20is%20when%20user,data%20into%20the%20application%20code.&text=For%20this%20reason%2C%20insecure%20deserialization,an%20%22object%20injection%22%20vulnerability.
- https://owasp.org/www-project-top-ten/2017/A8_2017-Insecure_Deserialization
- https://www.acunetix.com/blog/articles/what-is-insecure-deserialization/
- https://www.youtube.com/watch?v=nkTBwbnfesQ
- https://www.youtube.com/watch?v=jwzeJU_62lQ
- https://www.youtube.com/watch?v=EEHslhNbjeY
- https://thehackerish.com/insecure-deserialization-explained-with-examples/
- https://cyber.ithome.com.tw/2021/en/session-page/137
- https://s.itho.me/ccms_slides/2021/5/17/fdc541c0-5889-4f81-8f42-13fbb4ae5e60.pdf
- https://www.alluresec.com/2021/03/30/ewptxv2-review/
- https://www.alluresec.com/2021/02/03/polygot-phar-deserialization/

SQL Injections / Advanced SQL Injection and Bypass

- https://owasp.org/www-community/attacks/SQL_Injection
- https://www.devmedia.com.br/sql-injection/6102
- https://www.youtube.com/watch?v=ciNHn38EyRc
- https://www.youtube.com/watch?v=3Axp3VDnf0I
- https://portswigger.net/web-security/sql-injection
- https://www.acunetix.com/websitesecurity/sql-injection/
- https://www.imperva.com/learn/application-security/sql-injection-sqli/
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://www.programmersought.com/article/16352206542/
- https://owasp.org/www-community/attacks/SQL_Injection_Bypassing_WAF
- https://www.secjuice.com/advanced-sqli-waf-bypass/
- https://securityonline.info/sql-injection-9-ways-bypass-web-application-firewall/
- https://incogbyte.github.io/hacking/2020/12/12/sqli-bypass-techs.html
- https://www.ptsecurity.com/upload/corporate/ww-en/download/PT-devteev-CC-WAF-ENG.pdf
- https://www.exploit-db.com/papers/17934
- https://websec.files.wordpress.com/2010/11/sqli2.pdf
- https://gist.github.com/cyberheartmi9/b4a4ff0f691be6b5c866450563258e86
- https://isharaabeythissa.medium.com/sql-injection-waf-bypassing-b71cc373f6bf
- https://pentestit.medium.com/bypassing-waf-4cfa1aad16bf
- https://hydrasky.com/network-security/sql-injection-bypass-cheatsheet/
- https://learncybersec.blogspot.com/2020/03/bypassing-web-application-firewall-part_20.html
- https://securityreport.com/cloudflare-waf-xss-bypass-exploits-revealed/
- https://titanwolf.org/Network/Articles/Article?AID=a3861efd-d7bd-4150-8ede-8d46df68bb8f#gsc.tab=0
- http://spi.unob.cz/papers/2011/2011-11.pdf
- https://forum.bugcrowd.com/t/sqlmap-tamper-scripts-sql-injection-and-waf-bypass/423
- https://null-byte.wonderhowto.com/how-to/sql-injection-101-avoid-detection-bypass-defenses-0184918/
- https://security.stackexchange.com/questions/241149/sqli-filter-bypass-with-banned-table-column-names
- https://infosecwriteups.com/fun-sql-injection-mod-security-bypass-644b54b0c445
- https://book.hacktricks.xyz/pentesting-web/sql-injection
- https://websec.wordpress.com/2010/12/04/sqli-filter-evasion-cheat-sheet-mysql/
- https://www.youtube.com/watch?v=2Fn0WAyZV0E
- https://www.udemy.com/course/advanced-sql-tutorial/

Cross-Site Request Forgery

- https://owasp.org/www-community/attacks/csrf
- https://portswigger.net/web-security/csrf
- https://www.acunetix.com/websitesecurity/csrf-attacks/
- https://www.synopsys.com/glossary/what-is-csrf.html
- https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/
- https://www.netsparker.com/blog/web-security/csrf-cross-site-request-forgery/
- https://www.rapid7.com/fundamentals/cross-site-request-forgery/
- https://goteleport.com/blog/csrf-attacks/
- https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
- https://medium.com/@onehackman/cross-site-request-forgery-techniques-19270174ea4
- https://auth0.com/blog/cross-site-request-forgery-csrf/
- https://www.veracode.com/security/cross-site-request-forgery-guide-learn-all-about-csrf-attacks-and-csrf-protection
- https://www.neuralegion.com/blog/cross-site-request-forgery-csrf/
- https://blog.sessionstack.com/how-javascript-works-csrf-attacks-7-mitigation-strategies-757dfb08e7a6
- https://blog.qualys.com/vulnerabilities-threat-research/2015/01/14/do-your-anti-csrf-tokens-really-protect-your-applications-from-csrf-attack
- https://www.geeksforgeeks.org/cross-site-request-forgery-csrf-protection-methods-and-bypasses/
- https://www.barracuda.com/glossary/csrf
- https://seclab.stanford.edu/websec/csrf/
- https://book.hacktricks.xyz/pentesting-web/csrf-cross-site-request-forgery

Cross-Site Scripting and XSS Evasion

- https://github.com/payloadbox/xss-payload-list
- https://github.com/Learn-by-doing/xss
- https://github.com/s0md3v/XSStrike
- https://github.com/omurugur/XSS_Payload_List
- https://github.com/0xsobky/HackVault/wiki/Unleashing-an-Ultimate-XSS-Polyglot
- https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.md
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://owasp.org/www-community/attacks/xss/
- https://www.veracode.com/security/xss
- https://portswigger.net/web-security/cross-site-scripting
- https://www.acunetix.com/websitesecurity/xss/
- https://www.netsparker.com/blog/web-security/xss-filter-evasion/
- https://www.youtube.com/watch?v=O9vmnASdwZs
- https://www.youtube.com/watch?v=sq0jdhigKYM
- https://www.acunetix.com/blog/web-security-zone/xss-filter-evasion-basics/
- https://www.blackhat.com/presentations/bh-usa-09/VELANAVA/BHUSA09-VelaNava-FavoriteXSS-SLIDES.pdf
- https://portswigger.net/web-security/cross-site-scripting/cheat-sheet
- https://www.f5.com/pdf/white-papers/xss-evasion-wp.pdf
- https://null-byte.wonderhowto.com/how-to/advanced-techniques-bypass-defeat-xss-filters-part-1-0190257/

Review

- https://www.doyler.net/security-not-included/ewptx-review
- https://diesec.home.blog/2021/06/05/elearnsecurity-web-application-penetration-tester-extreme-ewptxv2/
- https://thomfre.dev/elearnsecurity-web-application-pentester
- https://infosecwriteups.com/ewptxv2-exam-review-2646dd145940
- https://blog.elearnsecurity.com/focus-on-the-web-application-penetration-testing-extreme-training-course-waptx.html
- https://medium.com/@klockw3rk/elearnsecurity-web-application-penetration-testing-course-wapt-ewpt-2f7480120b8e
- https://www.linkedin.com/pulse/como-se-tornar-um-engenheiro-e-mestre-em-offensive-dos-santos/?originalSubdomain=pt
- https://www.ethicalhacker.net/features/root/course-review-elearnsecurity-waptx-webapp-pentester-extreme/
- https://www.youtube.com/watch?v=ZaHt8KU3TBM
- https://stacktrac3.co/ewptx-review/
- https://community.infosecinstitute.com/discussion/129064/elearningsecurity-advanced-web-application-penetration-tester-ewptx-review
- https://osandamalith.com/2016/12/29/journey-into-ewptx/
- https://www.reddit.com/r/netsecstudents/comments/73728a/experience_with_elearnsecurity_web_application/

My Social Networks e ebooks

- https://twitter.com/C0d3Cr4zy
- https://www.linkedin.com/in/joas-antonio-dos-santos
- https://drive.google.com/drive/u/0/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU

LDAP Injection

- https://www.neuralegion.com/blog/ldap-injection/
- https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/LDAP%20Injection%20and%20Blind%20LDAP%20Injection.pdf
- https://www.researchgate.net/publication/220049933_Vulnerabilities_of_LDAP_As_An_Authentication_Service
- https://www.scirp.org/html/846.html
- http://www.redbooks.ibm.com/redbooks/pdfs/sg246193.pdf
- https://owasp.org/www-community/attacks/LDAP_Injection
- https://cheatsheetseries.owasp.org/cheatsheets/LDAP_Injection_Prevention_Cheat_Sheet.html
- https://www.synopsys.com/glossary/what-is-ldap-injection.html
- https://www.netsparker.com/blog/web-security/ldap-injection-how-to-prevent/
- https://book.hacktricks.xyz/pentesting-web/ldap-injection
- https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/LDAP%20Injection%20and%20Blind%20LDAP%20Injection.pdf
- https://www.calcomsoftware.com/preventing-ldap-reconnaissance/
- https://www.computerworld.com/article/3135727/attackers-abuse-exposed-ldap-servers-to-amplify-ddos-attacks.html
- https://portswigger.net/kb/issues/00100500_ldap-injection

Attacking Authentication & SSO

- https://www.youtube.com/watch?v=h7ViO5YUuFA
- https://www.youtube.com/watch?v=j9ALEIO3BSo
- https://portswigger.net/daily-swig/vulnerabilities-in-single-sign-on-services-could-be-abused-to-bypass-authentication-controls
- https://www.netspi.com/blog/technical/web-application-penetration-testing/attacking-sso-common-saml-vulnerabilities-ways-find/
- https://duo.com/resources/videos/identity-theft-attacks-on-sso-systems
- https://techbeacon.com/security/single-sign-still-open-attack-inside-look
- https://workos.com/blog/fun-with-saml-sso-vulnerabilities-and-footguns
- https://cheatsheetseries.owasp.org/cheatsheets/SAML_Security_Cheat_Sheet.html
- https://www.isdecisions.com/single-sign-on-active-directory-security-issues/
- https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
- https://securityboulevard.com/2018/02/some-sso-systems-vulnerable-to-authentication-bypass/
- https://dingelish.com/sso.pdf
- https://yangliang.github.io/pdf/inscrypt15.pdf
- https://www.researchgate.net/publication/257006846_An_authentication_flaw_in_browser-based_Single_Sign-On_protocols_Impact_and_remediations
- https://www.okta.com/resources/whitepaper/5-identity-attacks-that-exploit-your-broken-authentication/
- https://hdivsecurity.com/owasp-broken-authentication
- https://github.com/dogangcr/vulnerable-sso
- https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Authentication_Cheat_Sheet.md
- https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/SAML_Security_Cheat_Sheet.md
- https://github.com/kelbyludwig/saml-attack-surface

Server Side Attacks

- https://www.sciencedirect.com/topics/computer-science/server-side-attack#:~:text=Server%2Dside%20attacks%20(also%20called,client)%20to%20a%20listening%20service.&text=Patching%2C%20system%20hardening%2C%20firewalls%2C,depth%20mitigate%20server%2Dside%20attacks.
- https://www.javatpoint.com/server-side-attacks
- https://portswigger.net/web-security/ssrf
- https://owasp.org/www-community/attacks/Server-Side_Includes_(SSI)_Injection
- https://sidechannel.tempestsi.com/server-side-request-forgery-attack-and-defense-64474bac3b1e
- https://beaglesecurity.com/blog/article/server-side-request-forgery-attack.html
- https://security.stackexchange.com/questions/195496/attacks-on-server-side-web
  - Subtopic 1
- https://subscription.packtpub.com/book/networking_and_servers/9781785883149/6
- https://blog.convisoappsec.com/en/explaning_remote_code_execution/
- https://blog.sqreen.com/ssrf-explained/
- https://www.neuralegion.com/blog/ssrf-server-side-request-forgery/
- https://knowledge-base.secureflag.com/vulnerabilities/unvalidated_redirects_forwards/server_side_request_forgery_vulnerability.html
- https://github.com/OWASP/www-community/blob/master/pages/attacks/Server-Side_Includes_(SSI)_Injection.md
- https://github.com/esmog/nodexp
- https://github.com/epinna/tplmap
- https://github.com/payloadbox/ssti-payloads
- https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.md
- https://github.com/cujanovic/SSRF-Testing

Encoding and Filtering

- https://owasp.org/www-community/attacks/Unicode_Encoding
- https://owasp.org/www-community/Double_Encoding
- https://www.cgisecurity.com/lib/URLEmbeddedAttacks.html
- https://pt.slideshare.net/marco_morana/encoded-attacks-and-countermeasures-presentation
- https://owasp-top-10-proactive-controls-2018.readthedocs.io/en/latest/c4-encode-escape-data.html
- https://flylib.com/books/en/2.819.1.43/1/
- https://github.com/OWASP/www-community/blob/master/pages/xss-filter-evasion-cheatsheet.md
- https://github.com/OWASP/www-project-web-security-testing-guide/blob/master/latest/6-Appendix/D-Encoded_Injection.md
- https://github.com/OWASP/www-community/blob/master/pages/Double_Encoding.md
- https://github.com/OWASP/www-community/blob/master/pages/attacks/Unicode_Encoding.md
- https://github.com/OWASP/wstg/blob/master/document/4-Web_Application_Security_Testing/07-Input_Validation_Testing/01-Testing_for_Reflected_Cross_Site_Scripting.md

XML Attacks

- https://owasp.org/www-pdf-archive/XML_Based_Attacks_-_OWASP.pdf
- https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing
- https://gist.github.com/mgeeky/4f726d3b374f0a34267d4f19c9004870
- https://portswigger.net/web-security/xxe
- https://www.netsparker.com/blog/web-security/xxe-xml-external-entity-attacks/
- https://www.whitehatsec.com/glossary/content/xml-injection
- https://hdivsecurity.com/owasp-xml-external-entities-xxe
- https://www.acunetix.com/blog/articles/xml-external-entity-xxe-vulnerabilities/
- https://www.jigsawacademy.com/blogs/cyber-security/xml-external-entity/
- https://www.opswat.com/blog/depth-look-xml-document-attack-vectors
- https://www.appsecmonkey.com/blog/xxe
- https://www.hacksplaining.com/prevention/xml-external-entities
- https://we45.com/blog/xxe-injection-attack-3-ways-hit-hard/
- https://book.hacktricks.xyz/pentesting-web/xxe-xee-xml-external-entity
- https://ismailtasdelen.medium.com/xml-external-entity-xxe-injection-payload-list-937d33e5e116
- https://github.com/payloadbox/xxe-injection-payload-list
- https://hdivsecurity.com/bornsecure/prevention-of-xml-external-entity-xxe-attacks/
- https://cheatsheetseries.owasp.org/cheatsheets/XML_Security_Cheat_Sheet.html
- https://lab.wallarm.com/xxe-that-can-bypass-waf-protection-98f679452ce0/
- https://gosecure.github.io/xxe-workshop/#0
- https://www.synack.com/blog/a-deep-dive-into-xxe-injection/
- https://support.f5.com/csp/article/K50262217
- https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/top-level-protections/xml-entity-attack-protection.html
- https://resources.infosecinstitute.com/topic/guide-xml-file-structure-external-entity-xxe-attacks/

Evasion Basic

- https://github.com/EQuiw/2020-evasion-competition
- https://github.com/OWASP/www-community/blob/master/pages/xss-filter-evasion-cheatsheet.md
- https://github.com/0xInfection/Awesome-WAF
- https://owasp.org/www-community/attacks/SQL_Injection_Bypassing_WAF
- https://blog.isec.pl/waf-evasion-techniques/
- https://www.sciencedirect.com/topics/computer-science/evasion-technique
- https://medium.com/secjuice/waf-evasion-techniques-718026d693d8
- https://owasp.org/www-pdf-archive/OWASP_Stammtisch_Frankfurt_WAF_Profiling_and_Evasion.pdf
- https://blog.securelayer7.net/what-is-waf-how-web-application-firewall-evasion-techniques-work/
- https://www.secjuice.com/web-application-firewall-waf-evasion/
- https://www.exploit-db.com/docs/45366
- https://www.infoq.com/presentations/waf-scripting-techniques-autonomous-attacks/
- https://silo.tips/download/advanced-filter-evasion-and-web-application-firewall-bypassing
- https://silo.tips/download/advanced-filter-evasion-and-web-application-firewall-bypassing
- https://www.imperva.com/blog/score-sheet-testing-some-xss-evasion-techniques-against-our-waf/
- https://haiderm.com/10-methods-to-bypass-cross-site-request-forgery-csrf/