CodeNinja a.k.a. Aakash Choudhary

Home About Vulnerability Newsletter Welcome to my website

Bug-Bounty-Bookmarks

Jun 18, 2019

First Stage Testing [Recon]

1. https://medium.com/bugbountywriteup/guide-to-basic-recon-bug-bounties-recon-728c5242a115
2. https://www.hackerone.com/blog/how-to-recon-and-content-discovery
3. https://github.com/EdOverflow/bugbounty-cheatsheet/blob/master/cheatsheets/recon.md
4. https://gauravnarwani.com/a-1000-bounty/
5. https://medium.com/@ehsahil/recon-my-way-82b7e5f62e21
6. https://pentester.land/conference-notes/2018/08/02/levelup-2018-the-bug-hunters-methodology-v3.html
7. https://pentester.land/conference-notes/2018/04/26/levelup-2017-doing-recon-like-a-boss-disobey-2018-its-the-little-things.html
8. https://pentester.land/conference-notes/2018/04/25/levelup-2017-Esoteric-subdomain-enumeration-techniques.html
9. https://appsecco.com/books/subdomain-enumeration/
10. https://edoverflow.com/2017/broken-link-hijacking/
11. https://blog.appsecco.com/static-analysis-of-client-side-javascript-for-pen-testers-and-bug-bounty-hunters-f1cb1a5d5288
12. https://blog.appsecco.com/open-source-intelligence-gathering-201-covering-12-additional-techniques-b7
13. https://blog.usejournal.com/bug-hunting-methodology-part-1-91295b2d2066
14. https://blog.usejournal.com/bug-hunting-methodology-part-2-5579dac06150

Domain Enumeration

1. https://medium.com/@arbazhussain/gathering-domains-subdomains-with-ipranges-of-organization-49362d8a1271
2. https://blog.appsecco.com/certificate-transparency-part-3-the-dark-side-9d401809b025
3. https://blog.appsecco.com/a-penetration-testers-guide-to-sub-domain-enumeration-7d842d5570f6
4. https://blog.appsecco.com/a-penetration-testers-guide-to-sub-domain-enumeration-7d842d5570f6
5. https://info.menandmice.com/blog/bid/73645/Take-your-DNSSEC-with-a-grain-of-salt

password Reset

1. https://medium.com/bugbountywriteup/bugbounty-how-i-was-able-to-compromise-any-user-account-via-reset-password-functionality-a11bb5f863b3
2. https://medium.com/bugbountywriteup/bugbounty-i-dont-need-your-current-password-to-login-into-your-account-how-could-i-e51a945b083d
3. https://medium.com/@khaled.hassan/full-account-takeover-via-reset-password-function-8b6ef15f346f
4. https://medium.com/@BgxDoc/bugbounty-how-i-was-able-to-hack-any-user-account-via-password-reset-9009d84d94ff
5. https://medium.com/@Alpha66/reset-password-token-lead-to-account-takeover-8cfce2554b70

Current Password | Security Bypass

1. https://medium.com/@YoKoKho/bypassing-the-current-password-protection-at-techsupport-portal-b9005ee17e64
2. https://medium.com/@ciph3r7r0ll/simple-login-brute-force-current-password-requirement-bypass-e8f58931e257

gitleaks

1. https://lambda.grofers.com/credentials-leaked-in-public-heres-what-grofers-implemented-to-prevent-such-mishaps-66a40b5743af

DNS Misconfiguratons

1. https://www.cybrary.it/0p3n/find-dns-zone-transfer-misconfiguration/
2. https://medium.com/@valeriyshevchenko/dns-vulnerability-for-axfr-queries-58a51972fc4d

Subdomain Takeover

1. https://medium.com/@valeriyshevchenko/subdomain-takeover-with-shopify-heroku-and-something-more-6e9504da34a1
2. https://medium.com/bugbountywriteup/subdomain-takeover-new-level-43f88b55e0b2
3. https://labs.detectify.com/2014/10/21/hostile-subdomain-takeover-using-herokugithubdesk-more/
4. https://medium.com/@hakluke/how-to-setup-an-automated-sub-domain-takeover-scanner-for-all-bug-bounty-programs-in-5-minutes-3562eb621db3

Information Gathering

1. https://medium.com/@dhiraj_mishra/hi-internet-fbb72c3e6990

CSRF

1. https://medium.com/bugbountywriteup/content-negotiation-with-csrf-969e639d6a1a
2. https://shahmeeramir.com/methods-to-bypass-csrf-protection-on-a-web-application-3198093f6599
3. https://medium.com/bugbountywriteup/account-take-over-vulnerability-in-google-acquisition-famebit-e93b1a0a7af9
4. http://yasserali.com/hacking-paypal-accounts-with-one-click/
5. https://philippeharewood.com/facebookmarketingdevelopers-com-proxies-csrf-quandry-and-api-fun/

Idor

1. https://medium.com/@logicbomb_1/bugbounty-how-naaptol-indias-popular-home-shopping-company-kept-their-millions-of-user-data-e414cd4151c
2. https://medium.com/@logicbomb_1/bugbounty-paytm-customer-information-is-at-risk-indias-largest-digital-wallet-company-6f7116d4b2d5
3. https://medium.com/bugbountywriteup/bugbounty-how-i-was-able-to-read-chat-of-users-in-an-online-travel-portal-c55a1787f999
4. https://medium.com/bugbountywriteup/bugbounty-how-i-was-able-to-delete-anyones-account-in-an-online-car-rental-company-8a4022cc611
5. https://medium.com/@logicbomb_1/bugbounty-your-details-are-saved-into-my-account-user-info-disclosure-vulnerability-in-practo-fe36930a1246

6. https://medium.com/@YoKoKho/ribose-idor-with-simple-csrf-bypass-unrestricted-changes-and-deletion-to-other-photo-profile-e4393305274e
7. https://medium.com/@YoKoKho/idor-at-private-bug-bounty-program-that-could-leads-to-personal-data-leaks-d2536d026bf5
8. https://medium.com/@alt3kx/ektron-content-management-system-cms-9-20-sp2-remote-re-enabling-users-cve-2018-12596-bdf1e3a05158
9. https://medium.com/@alt3kx/idors-insecure-direct-object-reference-over-fortify-software-security-center-ssc-17-10-8c7916ca98bc
10. https://medium.com/@Skylinearafat/idor-that-calls-me-you-cant-delete-but-i-can-idor-to-delete-admin-annonations-by-any-user-72c64e8989d1
11. https://medium.com/@arbazhussain/idor-while-connecting-social-account-in-hackster-io-2296b316b7a7
12. https://medium.com/@injector.pca_87232/idor-account-takeover-1ff5a2d03b8b
13. https://medium.com/intigriti/how-spending-our-saturday-hacking-earned-us-20k-60990c4678d4
14. https://medium.com/bugbountywriteup/account-takeover-using-idor-and-the-misleading-case-of-error-403-cb42c96ea310

CORS

1. https://medium.com/bugbountywriteup/pre-domain-wildcard-cors-exploitation-2d6ac1d4bd30
2. https://medium.com/@arbazhussain/exploiting-misconfigured-cors-on-popular-btc-site-2aedfff906f6
3. https://medium.com/@sandh0t/think-outside-the-scope-advanced-cors-exploitation-techniques-dad019c68397
4. https://medium.com/bedefended/implement-secure-cors-tomcat-f813e308b67c
5. https://www.exploit-db.com/docs/english/45906-cors-attacks.pdf
6. https://medium.com/@osamaavvan/cors-to-csrf-attack-c33a595d441

Host Header Injection

1. https://blog.usejournal.com/bugbounty-database-hacked-of-indias-popular-sports-company-bypassing-host-header-to-sql-7b9af997c610
2. https://medium.com/@arbazhussain/auto-web-cache-deception-tool-2b995c1d1ab2

RCE

1. https://medium.com/@logicbomb_1/bugbounty-how-i-was-able-to-bypass-firewall-to-get-rce-and-then-went-from-server-shell-to-get-783f71131b94
2. https://medium.com/bugbountywriteup/bugbounty-journey-from-lfi-to-rce-how-a69afe5a0899
3. https://parsiya.net/blog/2019-06-18-chaining-three-bugs-to-get-rce-in-microsoft-attacksurfaceanalyzer/

Cloud Storage

1. https://medium.com/bugbountywriteup/bugbounty-aws-s3-added-to-my-bucket-list-f68dd7d0d1ce
2. https://medium.com/@mahitman1/i-own-your-customers-22e965761abd
3. https://medium.com/@jonathanbouman/how-i-hacked-apple-com-unrestricted-file-upload-bcda047e27e3
4. https://medium.com/@valeriyshevchenko/how-to-delete-all-company-progress-by-one-rm-command-in-aws-s3-bucket-df9c44727d7b
5. https://blog.appsecco.com/hunting-publicly-accessible-digitalocean-spaces-for-pentesters-9516a4cd3c87
6. https://medium.com/@arbazhussain/improper-storage-of-protected-projects-files-9ece8e9a4743

Account Takeover

1. https://medium.com/@injector.pca_87232/account-takeover-worth-900-cacbe10de58e
2. https://medium.com/@y.shahinzadeh/1-click-account-takeover-in-virgool-io-a-nice-case-study-6bfc3cb98ef2

Header Injection

1. https://medium.com/bugbountywriteup/bugbounty-exploiting-crlf-injection-can-lands-into-a-nice-bounty-159525a9cb62

Open Rediraction

1. https://medium.com/bugbountywriteup/bugbounty-linkedln-how-i-was-able-to-bypass-open-redirection-protection-2e143eb36941
2. https://medium.com/@**rishabh**/open-redirect-to-account-takeover-e939006a9f24

Rate Limit

1. https://medium.com/@arbazhussain/bypassing-rate-limit-protection-by-spoofing-originating-ip-ff06adf34157
2. https://medium.com/@valeriyshevchenko/how-to-check-race-conditions-in-web-applications-338f73937992
3. https://medium.com/@ciph3r7r0ll/race-condition-bug-in-web-app-a-use-case-21fd4df71f0e
4. https://medium.com/@samm0uda/bruteforcing-instagram-accounts-passwords-without-limit-7eaeda606ea
5. https://medium.com/@valeriyshevchenko/gone-in-60-seconds-using-carsharing-service-bf5bbd06815b
6. https://medium.com/@arbazhussain/race-condition-bypassing-team-limit-b162e777ca3b

Path Travesal

1. https://medium.com/bugbountywriteup/bugbounty-api-keys-leakage-source-code-disclosure-in-indias-largest-e-commerce-health-care-c75967392c7e
2. https://medium.com/@jonathanbouman/local-file-inclusion-at-ikea-com-e695ed64d82f

Upload

1. https://medium.com/@jonathanbouman/how-i-hacked-apple-com-unrestricted-file-upload-bcda047e27e3
2. https://medium.com/@injector.pca_87232/complete-web-server-access-46d19279a2b
3. https://medium.com/@mr_hacker/a-5000-idor-f4268fffcd2e
4. https://anotherhackerblog.com/exploiting-file-uploads-pt1/
5. https://github.com/modzero/mod0BurpUploadScanner
6. https://medium.com/@satboy.fb/art-of-unrestricted-file-upload-exploitation-92ed28796d0

oAuth

1. https://medium.com/@arbazhussain/stealing-0auth-token-mitm-3eeab46e96cf
2. https://medium.com/@arbazhussain/stealing-access-token-of-one-drive-integration-by-chaining-csrf-vulnerability-779f999624a7

XXE

1. https://medium.com/@jonathanbouman/xxe-at-bol-com-7d331186de54
2. https://medium.com/@mrnikhilsri/oob-xxe-in-prizmdoc-cve-2018-15805-dfb1e474345c

3. https://medium.com/@canavaroxum/xxe-on-windows-system-then-what-76d571d66745
4. https://medium.com/@zain.sabahat/an-interesting-xxe-in-sap-8b35fec6ef33
5. https://medium.com/@mrnikhilsri/soap-based-unauthenticated-out-of-band-xml-external-entity-oob-xxe-in-a-help-desk-software-c27a6abf182a
6. https://medium.com/@valeriyshevchenko/my-first-xml-external-entity-xxe-attack-with-gpx-file-5ca78da9ae98
7. https://medium.com/@kevinlpd/matesctf-final-2018-web-1-ex50-ph%E1%BA%A7n-2-xxe-6a34542ef496
8. https://lab.wallarm.com/critical-linkedin-vulnerability-proactively-resolved-by-wallarm-xxe-in-application-server-239bba28e415
9. https://medium.com/@iraklis/an-unlikely-xxe-in-hikvisions-remote-access-camera-cloud-d57faf99620f
10. https://medium.com/@alt3kx/out-of-band-xml-external-entity-oob-xxe-exploitation-over-fortify-software-security-center-ssc-1d5c7169b561

SSRF

1. https://hackerone.com/reports/115748
2. https://medium.com/@zain.sabahat/exploiting-ssrf-like-a-boss-c090dc63d326
3. https://medium.com/@alyssa.o.herrera/wappalyzer-ssrf-write-up-2dab4df064ae
4. https://medium.com/bugbountywriteup/piercing-the-veil-server-side-request-forgery-to-niprnet-access-c358fd5e249a
5. https://medium.com/@th3g3nt3l/how-i-found-an-ssrf-in-yahoo-guesthouse-recon-wins-8722672e41d4
6. https://medium.com/@neerajedwards/reading-internal-files-using-ssrf-vulnerability-703c5706eefb
7. https://medium.com/@Skylinearafat/how-outdated-jira-instances-suffers-from-multiple-security-vulnerabilities-6a88c45e9ec6
8. https://medium.com/@androgaming1912/gain-adfly-smtp-access-with-ssrf-via-gopher-protocol-26a26d0ec2cb

Logical

1. https://medium.com/bugbountywriteup/bugbounty-how-i-could-book-cab-using-your-wallet-money-in-indias-largest-auto-transportation-e0c4252ca1a3
2. https://hackernoon.com/how-i-bypassed-state-bank-of-india-otp-f145469a9f1d
3. https://medium.com/@khaled.hassan/hacking-thousands-of-companies-through-their-helpdesk-8f180a8595ef
4. https://medium.com/@khaled.hassan/are-you-sure-this-is-a-trusted-email-291121028320
5. https://medium.com/@ciph3r7r0ll/breaking-the-logic-denying-account-login-forever-2a3e7669e8a8

6. https://medium.com/@robertchrk/bypassing-aviras-password-protection-727577f4ca76
7. https://medium.com/@neerajedwards/how-i-hacked-all-the-redact-agents-accounts-ec165b7c514a
8. https://medium.com/bugbountywriteup/how-i-was-able-to-remove-your-instagram-phone-number-d346515e79c3
9.

SQL Injection

1. https://medium.com/@mahitman1/hacking-a-crypto-debit-card-service-730f287aaee7
2. https://medium.com/@valeriyshevchenko/burpsuit-sqlmap-one-love-64451eb7b1e8
3. https://medium.com/@injector.pca_87232/sql-injection-c87a390afdd3
4.

XSS

1. https://medium.com/@jonathanbouman/persistent-xss-at-ah-nl-198fe7b4c781
2. https://medium.com/@jonathanbouman/reflected-client-xss-amazon-com-7b0d3cec787
3. https://medium.com/@jonathanbouman/reflected-xss-at-philips-com-e48bf8f9cd3c
4. https://blog.securityevaluators.com/vulnerabilities-found-in-popular-ticketing-system-dd273bda229c
5. https://medium.com/@Skylinearafat/the-story-behined-the-namecheap-xss-filter-bypass-be79624fd0c3
6. https://medium.com/@fbotes2/quick-stored-xss-on-infrastructure-giant-679a6e375089
7. https://medium.com/@momenbasel/from-parameter-pollution-to-xss-d095e13be060
8. https://gauravnarwani.com/xssed-my-way-to-1000/
9. https://medium.com/@sajeeb.l/weaponising-staged-cross-site-scripting-xss-payloads-7b917f605800
10. https://medium.com/redteam/weaponising-angularjs-bypasses-4e59790a730a
11. https://medium.com/@hninja049/stored-xss-in-https-www-bitcoinget-com-30f43202f017
12. https://medium.com/@fbotes2/quick-stored-xss-on-infrastructure-giant-679a6e375089
13. https://medium.com/@injector.pca_87232/journey-to-the-xss-bed46a39c9ee
14. https://medium.com/a-bugz-life/from-reflected-xss-to-account-takeover-showing-xss-impact-9bc6dd35d4e6
15. https://medium.com/@hakluke/upgrade-xss-from-medium-to-critical-cb96597b6cc4
16. https://medium.com/@chawdamrunal/xss-cheat-sheet-e8b8261963c9
17. https://digi.ninja/blog/jsurixss.php

Parameter Pollution

1. https://smaranchand.com.np/2019/06/parameter-pollution-issue-in-api-resulting-xxx/

Behavior & Scopes

1. https://medium.com/bugbountywriteup/how-i-was-able-to-generate-access-tokens-for-any-facebook-user-6b84392d0342
2. https://medium.com/@samm0uda/a-misconfiguration-in-techprep-fb-com-rest-api-allowed-me-to-modify-any-user-profile-9dd0ff99d757
3. https://developers.500px.com/app-crash-on-long-passwords-or-yet-another-uikit-bug-6f4fdc8314a6
4. https://medium.com/@jonathanbouman/stored-xss-unvalidated-embed-at-medium-com-528b0d6d4982
5. https://medium.com/@jonathanbouman/reflected-xss-at-philips-com-e48bf8f9cd3c

OTHER

1. https://medium.com/@fbotes2/governit-754becf85cbc

Burpsuite Related

1. https://www.jonbottarini.com/2019/06/17/using-burp-suite-match-and-replace-settings-to-escalate-your-user-privileges-and-find-hidden-features/

Usefull Tools