Awesome Bugbounty Writeups

Contents

- Android Pentesting
- Contributing
- Maintainers

Cross Site Scripting (XSS)

- From P5 to P2 to 100 BXSS
- Google Acquisition XSS (Apigee)
- XSS on Microsoft.com via Angular Js template injection
- Researching Polymorphic Images for XSS on Google Scholar
- Netflix Party Simple XSS
- Stored XSS in google nest
- Self XSS to persistent XSS on login portal
- Universal XSS affecting Firefox
- XSS WAF Character limitation bypass like a boss
- Self XSS to Account Takeover
- Reflected XSS on Microsoft subdomains
- The tricky XSS
- Reflected XSS in AT&T
- XSS on Google using Acunetix
- Exploiting websocket application wide XSS
- Reflected XSS with HTTP Smuggling
- XSS on Facebook instagram CDN server bypassing signature protection
- XSS on Facebook's Acquisition Oculus
- XSS on sony Subdomain
- Exploiting Self XSS
- Effortlessly Finding Cross Site Scripting inclusion XSSI
- Bugbounty a DOM XSS
- Blind XSS : a mind Game
- FireFox IOS QR code reader XSS(CVE-2019-17003)
- HTML injection to XSS
- CVE-2020-13487 | Authenticated Stored Cross-site Scripting in bbPress
- XSS at error page of repository code
- XSS like a Pro
- How I turned self XSS to stored XSS via CSRF

- XSS Stored on Outlook web
- XSS Bug 20 Chars Blind XSS Payload
- XSS in AMP4EMAIL(DOM clobbering)
- DOM Based XSS bug bounty writeup
- XSS will never die
- 5000 USD XSS issue at avast desktop antivirus
- XSS to account takeover
- How Paypal helped me to generate XSS
- Bypass Uppercase filters like a PRO(XSS advanced methods)
- Stealing login credentials with reflected XSS
- bughunting xss on cookie popup warning
- XSS is love
- Oneplus XSS vulnerability in customer support portal
- Exploiting cookie based XSS by finding RCE
- Stored XSS on zendesk via macros
- XSS in ZOHO main
- DOM based XSS in private program
- Bugbounty writeup : Take Attention and get stored XSSS
- How I xssed admin account
- Clickjacking XSS on google
- Stored XSS on laporbugid
- Leveraging angularjs based XSS to privilege escalation
- How I found XSS by searching in shodan
- Chaining caache poisining to stored XSS
- XSS to RCE
- XSS on twitter worth 1120
- Reflected XSS in ebay.com
- Cookie based XSS exolpoitation 2300 bug bounty
- What do netcat -SMTP-self XSS have in common
- XSS on google custom search engine
- Story of a Full Account Takeover vulnerability N/A to Accepted
- Yeah I got p2 in 1 minute stored XSS via markdown editor
- Stored XSS on indeed
- Self XSS to evil XSS
- How a classical XSS can lead to persistent ATO vulnerability

- Reflected XSS in tokopedia train ticket
- Bypassing XSS filter and stealing user credit card data
- Googleplex.com blind XSS
- Reflected XSS on error page
- How I was able to get private ticket response panel and fortigate web panel via blind XSS
- Unicode vs WAF
- Story of URI based XSS with some simple google dorking
- Stored XSS on edmodo
- XSSed my way to 1000
- Try harder for XSS
- From parameter pollution to XSS
- MIME sniffing XSS
- Stored XSS on techprofile Microsoft
- Tale of a wormable Twitter XSS
- XSS attacks google bot index manipulation
- From Reflected XSS to Account takeover
- Stealing local storage data through XSS
- CSRF attack can lead to stored XSS
- XSS Reflected (filter bypass)
- XSS protection bypass on hackerone private program
- Just 5 minutes to get my 2nd Stored XSS on edmodo.com
- Multiple XSS in skype.com
- Obtaining XSS using moodle featured and minor bugs
- XSS on 403 forbidden bypass akamai WAF
- How I was turn self XSS into reflected XSS
- A Tale of 3 XSS
- Stored XSS on Google.com
- Stored XSS in the Guides gameplaersion (www.dota2.com)
- Admin google.com reflected XSS
- Paypal Stored security bypass
- Paypal DOM XSS main domain
- Bugbounty : The 5k$ Google XSS
- Facebook stored XSS
- Ebay mobile reflected XSS
- Magix bugbounty XSS writeup

- Abusing CORS for an XSS on flickr
- XSS on google groups
- Oracle XSS
- Content types and XSS Facebook Studio
- Admob Creative image XSS
- Amazon Packaging feedback XSS
- PaypalTech XSS
- Persistent XSS on my world
- Google VRP XSS in device management
- Google VRP XSS
- Google VRP Blind XSS
- WAZE XSS
- Referer Based XSS
- How we invented the Tesla DOM XSS
- Stored XSS on rockstar game
- How I was able to bypass strong XSS protection in well known website imgur.com
- Self XSS to Good XSS
- That escalated quickly : from partial CSRF to reflected XSS to complete CSRF to Stored XSS
- XSS using dynamically generated js file
- Bypassing XSS filtering at anchor Tags
- XSS by tossing cookies
- Coinbase angularjs dom XSS via kiteworks
- Medium Content spoofing and XSS
- Managed Apps and music a tale of two XSSes in Google play
- Making an XSS triggered by CSP bypass on twitter
- Escalating XSS in phantomjs image rendering to SSRF
- Reflected XSS in Simplerisk
- Stored XSS in the heart of the russian email provider
- How I built an XSS worm on atmail
- XSS on bugcrowd and so many other websites main domain
- Godaddy XSS affects parked domains redirector Processor
- Stored XSS in Google image search
- A pair of plotly bugs stored XSS abd AWS metadata
- Near universal XSS in mcafee web gateway
- Penetrating Pornhub XSS vulns

- How I found a 5000 Google maps XSS by fiddling with protobuf
- Airbnb when bypassing json encoding XSS filter WAF CSP and auditior turns into eight vulnerabilities
- Lightwight markup a trio of persistent XSS in gitlab
- XSS ONE BAY
- SVG XSS in unifi
- Stored XSS in unifi V4.8.12 controller
- Turning self XSS into good XSS v2
- SWF XSS DOM Based XSS
- XSS filter bypass in Yahoo Dev flurry
- XSS on Flickr
- Two vulnerabilities makes an exploit XSS and csrf in bing
- Runkeeper stored XSS
- Google sleeping XSS awakens 5k bounty
- Poisoning the well compromising godaddy customer support with blind XSS
- UBER turning self XSS to good XSS
- XSS on facebook via png content types
- Cloudflare XSS
- How I found XSS Vulnerability in Google
- XSS to RCE
- One payload to XSS them all
- Self XSS on komunitas
- Reclected XSS on alibabacloud
- Self XSS on komunitas bukalapak
- A real XSS in OLX
- Self XSS using IE adobes
- Stealing local storage through XSS
- 1000 USD in 5mins Stored XSS in Outlook
- OLX reflected XSS
- My first stored XSS on edmodo.com
- Hack your form new vector for BXSS
- How I found Blind XSS vulnerability in redacted.com
- 3 XSS in protonmail for iOS
- XSS in edmodo wihinin 5 mins
- Stil work redirect Yahoo subdomain XSS

- XSS in azure devOps
- Shopify reflected XSS
- Muliple Stored XSS on tokopedia
- Stored XSS on edmodo
- A unique XSS scenario 1000 Bounty
- Protonmail XSS Stored
- Chaining tricky ouath exploitation to stored XSS
- Antihack XSS to php uplaod
- Reflected XSS in zomato
- XSS through SWF file
- Hackyourform BXSS
- Reflected XSS on ASUS
- Stored XSS via Alternate text at zendesk support
- How I stumbled upon a stored XSS : my first bug bounty story
- Cookie based Self XSS to Good XSS
- Reflected XSS on amazon
- XSS worm : a creative use of web application vulnerability
- Google code in XSS
- Self XSS on indeed.com
- How I accidentally found XSS in Protonmail for iOS app
- XML XSS in yandex.ru by accident
- Critical Stored XSS vulnerability
- XSS bypass using META tag in realestate.postnl.nl
- Edmodo XSS bug
- XSS in hiden input fields
- How I discovered XSS that affected over 20 uber subdomains
- DOM based XSS or why you should not rely on cloudflare too much
- XSS in dynamics 365
- XSS deface with html and how to convert the html into charcode
- Cookie based injection XSS making explitable with exploiting other vulns
- XSS with put in ghost blog
- XSS using a Bug in safari and why blacklists are stupid
- Magic XSS with two parameters
- DOM XSS bug affecting tinder shopify Yelp
- Persistent XSS unvalidated open graph embed at linkedin.com

- My first 0day exploit CSP Bypass Reflected XSS
- Google Stored XSS in payments
- XSS on dropbox
- Weaponizing XSS attacking internal domains
- How I XSSed UBER and bypassed CSP
- RXSS and CSRF bypass to Account takeover
- Another XSS in google collaboratory
- How I bypassed AKAMAI waf in overstock.com
- Reflected XSS at philips.com
- XSS vulnerabilities in multiple iframe busters affecting top tier sites
- Reflected DOM XSS and clickjacking silvergoldbull
- Stored XSS vulnerability in h1 private
- Authbypass SQLi and XSS
- Stored XSS vulnerability in tumblr
- XSS in google code jam
- Mapbox XSS
- My first valid XSS
- Stored XSS in webcomponents.org
- 3 minutes XSS
- icloud.com DOM based XSS
- XSS at hubspot and in email areas
- Self XSS leads to blind XSS and Reflected XSS
- Refltected XSS primagames.com
- Stored XSS in gameskinny
- Blind XSS in Chrome experments Google
- Yahoo two XSSI vulnerabilities chained to steal user information (750$)
- How I found XSS on amazon
- A blind XSS in messengers twins
- XSS in microsoft Subdomain
- Persistent XSS at ah.nl
- The 12000 intersection betwenn clickjaking , XSS and DOS
- XSS in google collaboratory CSP bypass
- How I found blind XSS in apple
- Reflected XSS on amazon.com
- How I found XSS in 360totalsecurity

- The 2.5 BTC Stored XSS
- XSS Vulnerability in Netflix
- A story of a UXSS via DOM XSS clickjacking in steam inventory helper
- How I found XSS via SSRF vulnerability
- Searching for XSS found ldap injection
- how I converted SSRF to XSS in a SSRF vulnerable JIRA
- Reflected XSS in Yahoo subdomain
- Account takeover and blind XSS
- How I found 5 stored XSS on a private program
- Persistent XSS to steal passwords(Paypal)
- Self XSS + CSRF to stored XSS
- Stored XSS in yahoo and subdomains
- XSS in microsoft
- Blind XSS at customer support panel
- Reflected XSS on stackoverflow
- Stored XSS in Yahoo
- XSS 403 forbidden Bypass
- Turning self XSS into non self XSS via authorization issue at paypal
- A story of stored XSS bypass
- Mangobaaz hacked XSS to credentials
- How I got stored XSS using file upload
- Bypassing CSP to abusing XSS filter in edge
- XSS to session Hijacking
- Reflected XSS on www.zomato.com
- XSS in subdomain of yahoo
- XSS in yahoo.net subdomain
- Reflected XSS moongaloop swf version 62x
- Google adwords 3133.7 Stored XSS
- How I found a surprising XSS vulnerability on oracle netsuite
- Stored XSS on snapchat
- How I was able to bypass XSS protection on h1 private program
- Reflected XSS possible
- XSS via angularjs template injection hostinger
- Microsoft follow feature XSS (CVE-2017-8514)
- XSS protection bypass made my quickest bounty ever

- Taking note XSS to RCE in the simplenote electron client
- VMWARE official vcdx reflected XSS
- How I pwned a company using IDOR and Blind XSS
- From Recon to DOM based XSS
- Local file read via XSS
- Non persistent XSS at microsoft
- A Stored XSS in google (double kill)
- Filter bypass to Reflected XSS on finance.yahoo.com (mobile version)
- 900$ XSS in yahoo : recon wins
- How I bypassed practos firewall and triggered an XSS vulnerability
- Stored XSS to full information disclosure
- Story of parameter specific XSS
- Chaining self XSS with UI redressing leading to session hijacking
- Stored XSS with arbitrary cookie installation
- Reflective XSS and Open redirect on indeed.com subdomain
- How I found reflected XSS on Yahoo subdomain
- Dont just alert(1) because XSS is more fun
- UBER XSS by helpe of KNOXSS
- Reflected XSS in Yahoo
- Reflected XSS on ww.yahoo.com
- XSS because of wrong content type header

Cross Site Request Forgery (CSRF)

- How a simple CSRF attack turned into a P1
- How I exploited the json csrf with method override technique
- How I found CSRF(my first bounty)
- Exploiting websocket application wide XSS and CSRF
- Site wide CSRF on popular program
- Using CSRF I got weird account takeover
- CSRF CSRF CSRF
- Google Bugbounty CSRF in learndigital.withgoogle.com
- CSRF token bypass [a tale of 2k bug]
- 2FA bypass via CSRF attack
- Stored iframe injection CSRF account takeover

- Instagram delete media CSRF
- An inconsistent CSRF
- Bypass CSRF with clickjacking worth 1250
- Sitewide CSRF graphql
- Account takeover using CSRF json based
- CORS to CSRF attack
- My first CSRF to account takeover
- 4x chained CSRFs chained for account takeover
- CSRF can lead to stored XSS
- Yet other examples of abusing CSRF in logout
- Wordpress CSRF to RCE
- Bruteforce user IDs via CSRF to delete all the users with CSRF attack
- CSRF Bypass using cross frame scripting
- Account takeover via CSRF
- A very useful technique to bypass the CSRF protection
- CSRF account takeover exlpained automated manual bugbounty
- CSRF to account takeover
- How I got 500USD from microsoft for CSRF vulnerability
- Critical Bypass CSRF protection
- RXSS CSRF bypass to full account takeover
- Youtube CSRF
- Self XSS + CSRF = Stored XSS
- Ribose IDOR with simple CSRF bypass unrestrcited changes and deletion to other photo profile
- JSON CSRF attack on a social networking site
- Hacking facebook oculus integration CSRF
- Amazon leaking CSRF token using service worker
- Facebook graphql CSRF
- Chain the vulnerabilities and take your report impact on the moon csrf to html injection
- Partial CSRF to Full CSRF
- Stealing access token of one drive integration by chain csrf vulnerability
- Metasploit web project kill all running taks CSRF CVE-2017-5244
- Messenger site wide CSRF
- Hacking Facebook CSRF device login flow
- Two vulnerabilities makes an exploit XSS and CSRF in bing

- How I bypassed Facebook in 2016
- Ubiquiti bugbounty unifi generic CSRF protection Bypass
- Bypass Facebook CSRF
- Facebook CSRF full account takeover

Clickjacking (UI redressing attack)

- Google Bug bounty Clickjacking on Google payment
- Google APIs Clickjacking worth 1337$
- Clickjacking + XSS on Google org
- Bypass CSRF with clickjacking on Google org
- 1800 worth Clickjacking
- Account takeover with clickjacking
- Clickjacking on google CSE
- How I accidentally found clickjacking in Facebook
- Clickjacking on google myaccount worth 7500
- Clickjacking in google docs and void typing feature
- Reflected DOM XSS and Clickjacking
- binary.com clickjacking vulnerability exploiting HTML5 security features
- 12000 intersection betwen clickjacking XSS and denial of service
- Steam fire and paste : a story of uxss via DOM XSS and Clickjacking in steam inventory helper
- Yet another Google Clickjacking
- Redressing instagram leaking application tokens via instagram clickjacking vulnerability
- Self XSS to Good XSS and Clickjacking
- Microsoft Yammer clickjacking exploiting HTML5 security features
- Firefox find my device clickjacking
- Whatsapp Clickjacking vulnerability
- Telegram WEB client clickjacking vulnerability
- Facebook Clickjacking : how we put a new dress on facebook UI

Local File Inclusion (LFI)

- RFI LFI Writeup
- My first LFI

- Bug bounty LFI at Google.com
- Google LFI on production servers in redacted.google.com
- LFI to 10 server pwn
- LFI in apigee portals
- Chain the bugs to pwn an organisation LFI unrestricted file upload to RCE
- How we got LFI in apache drill recom like a boss
- Bugbounty journey from LFI to RCE
- LFI to RCE on deutche telekom bugbounty
- From LFI to RCE via PHP sessions
- magix bugbounty magix.com XSS RCE SQLI and LFI
- LFI in nokia maps

Subdomain Takeover

- How I bought my way to subdomain takeover on tokopedia
- Subdomain Takeover via pantheon
- Subdomain takeover : a unique way
- Escalating subdomain takeover to steal sensitive stuff
- Subdomain takeover awarded 200
- Subdomain takeover via wufoo service
- Subdomain takeover via Hubspot
- Souq.com subdomain takeover
- Subdomain takeover : new level
- Subdomain takeover due to misconfigured project settings for custom domain
- Subdomain takeover via shopify vendor
- Subdomain takeover via unsecured s3 bucket
- Subdomain takeover worth 200
- Subdomain takeover via campaignmonitor
- How to do 55000 subdomain takeover in a blink of an eye
- Subdomain takeover Starbucks (Part 2)
- Subdomain takeover Starbucks
- Uber wildcard subdomain takeover
- Bugcrowd domain subdomain takeover vulnerability
- Subdomain takeover vulnerability (Lamborghini Hacked)
- Authentication bypass on uber's SSO via subdomain takeover

- Authentication bypass on SSO ubnt.com via Subdomain takeover of ping.ubnt.com

Denial of Service (DOS)

- Long String DOS
- AIRDOS
- Denial of Service DOS vulnerability in script loader (CVE-2018-6389)
- Github actions DOS
- Application level denial of service
- Banner grabbing to DOS and memory corruption
- DOS across Facebook endpoints
- DOS on WAF protected sites
- DOS on Facebook android app using zero width no break characters
- Whatsapp DOS vulnerability on android and iOS
- Whatsapp DOS vulnerability in iOS android

Authentication Bypass

- Touch ID authentication Bypass on evernote and dropbox iOS apps
- Oauth authentication bypass on airbnb acquistion using wierd 1 char open redirect
- Two factor authentication bypass
- Instagram multi factor authentication bypass
- Authentication bypass in nodejs application
- Symantec authentication Bypass
- Authentication bypass in CISCO meraki
- Slack SAML authentocation bypass
- Authentication bypass on UBER's SSO
- Authentication Bypass on airbnb via oauth tokens theft
- Inspect element leads to stripe account lockout authentication Bypass
- Authentication bypass on SSO ubnt.com

SQL Injection(SQLI)

- Tricky oracle SQLI situation
- Exploiting “Google BigQuery” SQLI
- SQLI via stopping the redirection to a login page

- Finding SQLI with white box analysis a recent bug example
- Bypassing a crappy WAF to exploit a blind SQLI
- SQL Injection in private-site.com/login.php
- Exploiting tricky blind SQLI
- SQLI in forget password fucntion
- SQLI Bug Bounty
- File Upload blind SQLI
- SQL Injection
- SQLI through User Agent
- SQLI in insert update query without comma
- SQLI for 50 bounty
- Abusing MYSQL CLients
- SQLI Authentication Bypass AutoTrader Webmail
- ZOL Zimbabwe Authentication Bypass to XSS & SQLi
- SQLI bootcamp.nutanix.com
- SQLI in University of Cambridge
- Making a blind SQLI a little less Blind SQLI
- SQLI amd silly WAF
- Attacking Postgresql Database
- Bypassing Host Header to SQL injection to dumping Database — An unusual case of SQL injection
- A 5 minute SQLI
- Union based SQLI writeup
- SQLI with load file and into outfile
- SQLI is Everywhere
- SQLI in Update Query Bug
- Blind SQLI Hootsuite
- Yahoo – Root Access SQLI – tw.yahoo.com
- Step by Step Exploiting SQLI in Oculus
- Magix Bug Bounty: magix.com (RCE, SQLi) and xara.com (LFI, XSS)
- Tesla Motors blind SQLI
- SQLI in Nokia Sites

Insecure Direct Object Reference (IDOR)

- Disclose Private Dashboard Chart's name and data in Facebook Analytics
- Disclosing privately shared gaming clips of any user
- Adding anyone including non-friend and blocked people as co-host in personal event!
- Page analyst could view job application details
- Deleting Anyone's Video Poll

2FA related issues

- 2FA Bypass via logical rate limiting Bypass
- Bypass 2FA in a website
- Weird and simple 2FA bypass
- How I cracked 2FA with simple factor bruteforce
- Instagram account is reactivated without entering 2FA
- How to bypass 2FA with a HTTP header
- How I hacked 40k user accounts of microsoft using 2FA bypass outlook
- How I abused 2FA to maintain persistence after password recovery change google microsoft instragram
- Bypass hackerone 2FA
- Facebook Bug bounty : How I was able to enumerate instagram accounts who had enabled 2FA

CORS related issues

- CORS bug on google's 404 page (rewarded)
- CORS misconfiguration leading to private information disclosure
- CORS misconfiguration account takeover out of scope to grab items in scope
- Chrome CORS
- Bypassing CORS
- CORS to CSRF attack
- An unexploited CORS misconfiguration reflecting further issues
- Think outside the scope advanced cors exploitation techniques
- A simple CORS misconfiguration leaked private post of twitter facebook instagram
- Explpoiting CORS misconfiguration
- Full account takeover through CORS with connection sockets
- Exploiting insecure CORS API api.artsy.net
- Pre domain wildcard CORS exploitation

- Exploiting misconfigured CORS on popular BTC site
- Abusing CORS for an XSS on flickr

Server Side Request Forgery (SSRF)

- Exploiting an SSRF trials and tribulations
- SSRF on PDF generator
- Google VRP SSRF in Google cloud platform stackdriver
- Vimeo upload function SSRF
- SSRF via ffmeg processing
- My first SSRF using DNS rebinding
- Bugbounty simple SSRF
- SSRF reading local files from downnotifier server
- SSRF vulnerability
- Gain adfly SMTP access with SSRF via gopher protocol
- Blind SSRF in stripe.com due to senntry misconfiguration
- SSRF port issue hidden approch
- The jorney of web cache firewall bypass to SSRF to AWS credentials compromise
- SSRF to local file read and abusing aws metadata
- pdfreactor SSRF to root level local files read which lead to RCE
- SSRF trick : SSRF XSPA in micosoft's bing webwaster
- Downnotifeer SSRF
- Escalating SSRF to RCE
- Vimeo SSRF with code execution potential
- SSRF in slack
- Exploiting SSRF like a boss
- AWS takeover SSRF javascript
- Into the borg of SSRF inside google production network
- SSRF to local file disclosure
- How I found an SSRF in yahoo guesthouse (recon wins)
- Reading internal files using SSRF vulnerability
- Airbnb chaining third party open redirect into SSRF via liveperson chat

Race Condition

- Exploiting a Race condition vulnerabililty
- Race condition that could result to RCE a story with an app
- Creating thinking is our everything : Race condition and business logic
- Chaining improper authorization to Race condition to harvest credit card details
- A Race condition bug in Facebook chat groups
- Race condition bypassing team limit
- Race condition on web
- Race condition bugs on Facebook
- Hacking Banks With Race Conditions
- Race Condition Bug In Web App: A Use Case
- RACE Condition vulnerability found in bug-bounty program
- How to check Race Conditions in Web Applications

Remote Code Execution (RCE)

- Microsoft RCE bugbounty
- OTP bruteforce account takeover
- Attacking helpdesk RCE chain on deskpro with bitdefender
- Remote image upload leads to RCE inject malicious code
- Finding a p1 in one minute with shodan.io RCE
- From recon to optimizing RCE results simple story with one of the biggest ICT company
- Uploading backdoor for fun and profit RCE DB creds P1
- Responsible Disclosure breaking out of a sandboxed editor to perform RCE
- Wordpress design flaw leads to woocommerce RCE
- Path traversal while uploading results in RCE
- RCE jenkins instance
- Traversing the path to RCE
- How I chained 4 bugs features into RCE on amazon
- RCE due to showexceptions
- Yahoo luminate RCE
- Latex to RCE private bug bounty program
- How I got hall of fame in two fortune 500 companies an RCE story
- RCE by uploading a web config
- 36k Google app engine RCE
- How I found 2.9 RCE at yahoo

- Bypass firewall to get RCE
- RCE vulnerabilite in yahoo subdomain
- RCE in duolingos tinycards app from android
- Unrestricted file upload to RCE
- Getting a RCE (CTF WAY)
- RCE starwars
- How I got 5500 from yahoo for RCE
- RCE in Addthis
- Paypal RCE
- My First RCE (Stressed Employee gets me 2x bounty)
- Abusing ImageMagick to obtain RCE
- How Snapdeal Kept their Users Data at Risk!
- RCE via ImageTragick
- How I Cracked 2FA with Simple Factor Brute-force!
- Found RCE but got Duplicated
- “Recon” helped Samsung protect their production repositories of SamsungTv, eCommerce eStores
- IDOR to RCE
- RCE on AEM instance without JAVA knowledge
- RCE with Flask Jinja tempelate Injection
- Race Condition that could result to RCE
- Chaining Two 0-Days to Compromise An Uber Wordpress
- Oculus Identity Verification bypass through Brute Force
- Used RCE as Root on marathon Instance
- Two easy RCE in Atlassian Products
- RCE in Ruby using mustache templates
- About a Sucuri RCE...and How Not to Handle Bug Bounty Reports
- Source code disclosure vulnerability
- Bypassing custom Token Authentication in a Mobile App
- Facebook’s Burglary Shopping List
- From SSRF To RCE in PDFReacter
- Apache strust RCE
- Dell KACE K1000 Remote Code Execution
- Handlebars Tempelate Injection and RCE
- Leaked Salesforce API access token at IKEA.com

- Zero Day RCE on Mozilla's AWS Network
- Escalating SSRF to RCE
- Fixed : Brute-force Instagram account's passwords
- Bug Bounty 101 — Always Check The Source Code
- ASUS RCE vulnerability on rma.asus-europe.eu
- Magento – RCE & Local File Read with low privilege admin rights
- RCE in Nokia.com
- Two RCE in SharePoint
- Token Brute-Force to Account Take-over to Privilege Escalation to Organization Take-Over
- RCE in Hubspot with EL injection in HubL
- Github Desktop RCE
- eBay Source Code leak
- Facebook source code disclosure in ads API
- XS-Searching Google's bug tracker to find out vulnerable source code

Buffer Overflow Writeups

- Buffer Overflow Attack Book pdf
- Github Repository on Buffer Overflow Attack
- Stack-Based Buffer Overflow Attacks: Explained and Examples
- How Buffer Overflow Attacks Work
- Binary Exploitation: Buffer Overflows
- WHAT IS A BUFFER OVERFLOW? LEARN ABOUT BUFFER OVERRUN VULNERABILITIES, EXPLOITS & ATTACKS

Android Pentesting

- Android Pentesting Lab (Step by Step guide for beginners!)

Contributing

- Open Pull Requests
- Send me links of writeups to My Twitter : 0xAsm0d3us

Maintainers

This Repo is maintained by :

- devanshbatham
- e13v3n-0xb