Bug Bytes #34 – Challenge Winner, Bounty Economy and CSRF bible

BY INTIGRITI · SEPTEMBER 3, 2019 · LAST UPDATED ON JULY 31, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series are curated by Mariem, better known as **PentesterLand.** Every week, she keeps us updated with a comprehensive list of all write-ups, tools, tutorials and resources we should not have missed.

This issue covers the week from 23 to 30 of August.

Intigriti news

- BPost launched their vetted program. If you want to become vetted, follow these steps and gain access to more bug bounty programs!
- Our "Outside the Box"-XSS challenge is over! Check out the winner and the writeup by @Fady_Othman!

Our favorite 5 hacking items

1. Non technical item of the week

> "Economics of the bug bounty hunting"

This is a great read about how @dmi3sh uses specific metrics to increase his hourly rate as a full-time bug hunter.
The main takeaway for me is that he relies on a list of criteria to decide on which target, functionality and bug type it is best to focus. These are things like: Probability of finding a bug, payout, chance of being duped, of getting N/As and out of scope, chances of being paid, etc.
Using these objective elements helps make decisions about what to focus on a lot easier.

2. Tools of the week

> "LinkDumper
> Jsonp"

These are two very handy Burp extensions. I couldn't choose just one as I plan on using both!
LinkDumper extracts links and anything that could be an endpoint from responses. It decodes them, sorts them and displays the findings in a tabs next to the request's "response" tab (anywhere in Burp, like in Target, Proxy History, Repeater...).
What I like about this tool is that it also extracts anything that remotely resembles a link, even "junk". This allows for finding endpoints that could have been missed with a simple regex. I noticed that it can also return URL parameters.
Jsonp is also worth testing. It helps reveal JSONP functionality by probing each JSON endpoint passively detected. When it sees an endpoint responding with *application/json*, it replays the request by appending

parameters and/or changing the extension to *.jsonp*.
If a JSONP functionality is found, it could help you bypass CSP or find bugs like XSS and Cross-Site Script Inclusion (XSSI).

3. Article of the week

> "Analysis of Common Federated Identity Protocols: OpenID Connect vs OAuth 2.0 vs SAML 2.0"

This is an excellent introductory article for anyone who struggles with understanding the difference between SSO, OAuth 2, OpenID Connect, and SAML.
You'll find clear and concise definitions, comparison elements, common vulnerabilities, and links for further reading.

4. Slides of the week

> "Active Directory security workshop: A red and blue guide to popular AD attacks"

This is a 227 pages presentations on Active Directory security. It is full of resources, tools, attacks, techniques and how to protect against them (useful for pentest recommendations).
A great resource for AD security!

5. Tutorial of the week

> "Bypassing CSRF Protection"

What do you test for if you see CSRF protection on an app? This tutorial lists several techniques that may gives you new ideas to try.
They are not groundbreaking, but they are basics that every tester should know. The techniques are: Clickjacking, changing the request method, deleting the token parameter or send a blank token, using another session's CSRF token, session fixation, removing the referrer header, and bypassing the regex.

Other amazing things we stumbled upon this week

Videos

- Bounty Thursdays #1 – Personal Burp Suite collaborator, Pulse RCE, Government VDPs. XSS challenge
- Solving challenges from HackTheBox, Hacker101, and Bug Bounty Notes – Every Tuesday!
- 8/18/2019 – Live Bug Bounty Recon Session w/ @TheCyberMentor @zseano @StokFredrik
- How to Get Started with Car Hacking (with @_specters_)
- Web App Testing: Episode 3 – XSS, SQL Injection, and Broken Access Control
- How NOT to Approach a Cybersecurity Mentor
- Basic concurrency in Go

- How They Got Hacked Episode 24

Podcasts

- Security Now 729 – Next Gen Ad Privacy
- Risky Business #553 — Imperva's cloud WAF gets owned hard
- 7MS #379: Tales of Internal Network Pentest Pwnage – Part 7
- Hack Naked News #231
- Paul's Security Weekly #618
- ThugCrowd S2:E11 – Bug Bounty: On the Front Lines

Webinars & Webcasts

- Purple Teaming: The Pen-Test Grows Up
- Practical tips to build a successful purple team

Slides only

- Exploring flAWS in S3 & beyond
- Fuzzing Bay Area Meetup: Modern fuzzing of C/C++, Fuzzing APIs and web apps for fun and profit, Increasing Red Team Capabilities with Smart Fuzzing
- Seeing Inside The Encrypted Envelope

Tutorials

Medium to advanced

- Burp Suite Tips — Volume 1
- Using Burp's session Handling Rules to insert authorization cookies into Intruder, Repeater and even sqlmap
- Hail Frida!! The Universal SSL pinning bypass for Android applications
- Setup up your Out-of-Band DNS Server
- Vim Config Update: 2019 Edition
- Privilege Escalation: How to build RPM payloads in Kali Linux
- Common Language Runtime Hook for Persistence
- Pwning Wireless Peripherals

Beginners corner

- How to use Burp Suite with multiple profiles in Firefox
- Finding Hidden API Keys & How to use them
- Certificate Transparency
- Cracking WordPress Passwords with Hashcat
- [iOS Application Security] Jailbreak 12.4 and SSL pinning bypass | How to set up your iOS Testing Lab
- Rumble Network Discovery: A Powerful Cloud-Based Infosec Mapping Platform

Writeups

Challenge writeups

- No Fatshaming (Web Challenge WriteUp)— CodeFest'19 CTF

Pentest writeups

- Time-Based Blind SQL Injection In GraphQL
- Referer XSS with a Side of Link Injection
- How I escalated into super admin's privileges in 3 minutes.
- Kerberos Resource-Based Constrained Delegation: When an Image Change Leads to a Privilege Escalation

Responsible(ish) disclosure writeups

- Lojack'd: Pwning Smart vehicle trackers #CarHacking #Web
- (CVE-2019-TBA –> CVE-2019-TBA) Enigma NMS Multiple Vulnerabilities #Web
- CVE-2019-15092 WordPress Plugin Import Export Users = 1.3.0 – CSV Injection #Web
- Handlebars 4.1.2: Command Execution #SSTI #RCE
- [GTSA-00130] Webmin 1.920 Remote Code Execution.txt & TL;DR #Web #RCE
- Multiple critical vulnerabilities in Cisco UCS Director, Cisco Integrated Management Controller Supervisor and Cisco UCS Director Express for Big Data #RCE #Web #AuthBypass
- Script Kiddie Nightmares: Hacking Poorly Coded Botnets #CodeReview #RCE

Bug bounty writeups

- Password theft via HTTP Request Smuggling on New Relic ($3,000)

- SSRF on GitLab ($2,000)
- Open redirect on Twitter ($560)
- Authorization flaw on GitLab ($1,000)
- Information disclosure via LocalStorage on MyEtherWallet ($250)
- XSS via Kaspersky ($2,500)
- RCE via exposed Marathon UI
- SQL injection
- Account takeover via password reset flaw on Facebook ($10,000)
- Cookie Based XSS to Reflected XSS
- Information disclosure via JS files

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- DNS Validator: Maintains a list of IPv4 DNS servers by verifying them against baseline servers, and ensuring accurate responses
- Hashcatch: Capture handshakes of nearby WiFi networks automatically

More tools, if you have time

- Yar: A tool for plundering organizations, users and/or repositories from Github
- Recursebuster: Rapid content discovery tool for recursively querying webservers, handy in pentesting and web application assessments
- http-pulse_ssl_vpn.nse: Nmap NSE script to detect Pulse Secure SSL VPN file disclosure CVE-2019-11510
- Sudomy: Subdomain enumeration tool in Bash
- Kibanarec: A Tool to Extract Open Kibana Instances on Internet & Map them to their Corresponding Organizations using SSL certificates
- apk_api_key_extractor: Automatically extracts API Keys from APK files
- xss2png: PNG IDAT chunks XSS payload generator
- CCAT & Tutorial: Cloud Container Attack Tool, a tool for testing security of container environments

Misc. pentest & bug bounty resources

- RegHex: A collection of regexes for every possible use
- Automated Github Queries
- Top 7 IP Scanner Tools for Network Mapping
- APIscurity.io Issue 46: Cisco and Facebook patch APIs, Solr API parameter injection
- Windows Hacking/Red teaming resources
- Awesome Embedded and IoT Security

Challenges

- EVABS: Extremely Vulnerable Android Labs
- Intigriti's Out of the box XSS challenge

Articles

- Getting shell and data access in AWS by chaining vulnerabilities
- Phishing with SAML and SSO Providers
- China Chopper still active 9 years later
- Android Hard Coded Secrets
- Analysis of Survival Password Genetics
- Three Most Common Security Flaws (and How to Fix Them) #PhysicalSecurity

News

Bug bounty & Pentest news

- Meet Six Hackers Making Seven Figures: Congrats to @santi_lopezz99, @bugbountyhq, @fransrosen, @nnwakelam, @ngalongc & @thedawgyg!
- Follow @agarri_fr to know where he'll held his next free Burp v2 workshop
- Serving the Best with the Best: Synack Announces Productivity Assessment Program
- Expanding bug bounties on Google Play: Scope now includes all apps in Google Play with 100 million or more installs, and data abuse issues in Android apps, OAuth projects, and Chrome extensions.
- Valve says turning away researcher reporting Steam vulnerability was a mistake

Reports

- Hacker-Powered Security Report 2019
- 2019 Midyear Security Roundup Evasive Threats, Pervasive Effects
- In Plain Sight II: On the Trail of Magecart

Vulnerabilities

- Protocol used by 630,000 devices can be abused for devastating DDoS attacks
- Telegram Bug 'Exploited' By Chinese Agencies, Hong Kong Activists Claim
- AV Oracle: New hacking technique leverages antivirus to steal secrets
- Web clickjacking fraud makes a comeback thanks to JavaScript tricks
- For everyone wondering how spam events got added to your Google Calendars without having a source in your inbox...

Breaches & Attacks

- Magecart: How a single skimming case evolved into widespread credit card theft
- Avast and French police take over malware botnet and disinfect 850,000 computers
- Malicious App on Google Play Tallies 100 Million Downloads
- Hackers Tweeted Racial Slurs From Twitter CEO Jack Dorsey's Account
- Cybersecurity Firm Suffers Security Breach, Client Info Exposed
- Instagram Security Warning: Millions At Risk From 'Believable' New Phishing Attack
- Malicious websites were used to secretly hack into iPhones for years, says Google
- Sources say China used iPhone hacks to target Uyghur Muslims

Other news

- The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks
- Snake oil or genius? Crown Sterling tells its side of Black Hat controversy
- New Microsoft Edge browser fires off more than 130 requests to almost 50 endpoints on first run
- Microsoft Wants exFAT in Linux Kernel, Opens File System Specs
- Apple apologizes for humans listening to Siri clips, changes policy
- Freelance Site Fiverr Offers Illegal Private Spying Services
- Venmo's Public Transactions Policy Stirs Privacy Concerns
- Microsoft: Using multi-factor authentication blocks 99.9% of account hacks

Non technical

- Use the Source, Luke
- Out of Scope
- Every Computer Science Degree Should Require a Course in Cybersecurity
- Phishing A Never-Ending Story
- Social Engineering: What Is It? Types of Social Engineering Attacks and How to Protect Yourself from Them
- Mentoring: the biggest problem we don't know we have
- The Shy Person's Guide to Winning Friends and Influencing People

Tweeted this week

We created a collection of our favorite pentest & bug bounty related tweets shared this past week. You're welcome to read them directly on Twitter: Tweets from 08/23/2019 to 08/30/2019.

*Curated by Pentester Land & Sponsored by Intigriti*Disclaimer:
The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.