Bug Bytes #89 – What $635,387.47 of bounties in 4 years looks like, A 14-year-old's impressive Instagram XSS & The ultimate ffuf guide

BY ANNA HAMMOND · SEPTEMBER 23, 2020 · LAST UPDATED ON MARCH 6, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series is curated by Mariem, better known as **PentesterLand.** Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

This issue covers the week from 11 to 18 of September.

Intigriti News

Intigriti wins 'Cybersecurity Innovator of the Year'

Inti De Ceukelaire voted "IT Person of the Year"

Our favorite 5 hacking items

1. Videos of the week

How to Master FFUF for Bug Bounties and Pen Testing & Everything you need to know about FFUF

Finding Hidden Files and Folders on IIS/.NET (Recon), Hacking IIS (APIs and using BigQuery) (Part 2) & Finding Hidden Files and Folders on IIS using BigQuery

These are two very informative videos with accompanying blog posts. Michael Skelton (@codingo_)'s guide to ffuf is so good that the tool's creator, @joohoi, is linking to it from the main ffuf repo!

Shubham Shah (@infosec_au) shares cool explanations on bruteforcing IIS hidden files and folders, and leveraging BigQuery (without ruining yourself!).

2. Writeups of the week

$25K Instagram Almost XSS Filter Link — Facebook Bug Bounty (Facebook, $25,000)

When you browse Instagram and find former Australian Prime Minister Tony Abbott's passport number

Bug bounty amounts aren't everything, but they're often an indicator of the seriousness of a vulnerability. Andres Alonso's (@al0nnso) finding is impressive considering not only the bounty but also the hardened target and his young age. He found an open redirect on Facebook that could be escalated to XSS. WAF bypass was possible by injecting code to change the page's charset and encoding the XSS payload.

The second writeup is a fun vulnerability disclosure story. @mangopdf found a former Australian Prime Minister's boarding pass on Instagram and could use it to obtain his passport and phone numbers. Followed an entertaining crusade to report this without getting arrested.

3. Tool of the week

Graphtage

Graphtage is a command line utility and library for semantically comparing and merging tree-like structures (e.g. JSON, JSON5, XML, HTML, YAML, TOML and CSV). It's a great tool for diffing files and automating recon data analysis.

4. Non technical item of the week

Hacking on Bug Bounties for Four Years

This is an illuminating read for anyone who is doing bug bounties who aspiring to. @infosec_au shares his past four years experience as a part-time bug hunter. This includes the type of bugs he reported, bounty amounts for each, total earnings, his methodology, collaboration experience... Amazing insights of a seasoned bug hunter's life!

5. Tutorial of the week

Bypassing WAF by Playing with Parameters

This is an introduction to HTTP Parameter Fragmentation, and how it can be leveraged to bypass WAFs and exploit SQL injection. A nice read to get familiar with this technique!

Other amazing things we stumbled upon this week

Videos

- JavaScript Prototype Pollution – Part 2
- $4,000 Starbucks secondary context path traversal – Hackerone
- BOUNTY THURSDAYS – Loads of new bugbounty content creators that create awesome content for you!
- Getting Started with Android App Testing with Genymotion
- Send Push Notifications For Your Recon – Pt. 1

Podcasts

- Security Now – BlindSide & BLURtooth – Chrome vs Abusive Ads, Patch Tuesday Palooza
- Risky Business #599 — You get domain admin! And YOU get domain admin!
- Darknet Diaries EP 74: MIKKO
- Is the AWS Free Tier Really Free? (AMB Extras)
- The InfoSec & OSINT Show 25 – Jeremiah Grossman and Asset Inventory
- 7MS #432: Tales of Internal Network Pentest Pwnage – Part 21

Webinars & Webcasts

- Abusing Wi-fi Beacons And Detecting & Preventing Attacks
- Gcp Lateral Movement And Privileged Escalation Spill Over And Updates From Google

Conferences

- Securi-Tay 2020, especially:
  - Saving user data one company at a time – Hacking with zseano – Sean Roesner
  - From Low to PWN: A CTF challenge in the wild – Charlie Hosier
- Bug Bounty Village @ c0c0n (Virtual Mode)
- Real World Cloud Compromise

Slides & Workshop material

- Post-Exploitation Tradecraft in an EDR World

Tutorials

Medium to advanced

- tmpmail – A temporary email right from Linux / Unix terminal
- Hijacking a Domain Controller with Netlogon RPC (aka Zerologon: CVE-2020-1472), How to exploit Zerologon (CVE-2020-1472), Thread about the impact of Zerologon & New mimikatz release with Zerologon detection
- Weaponizing Group Policy Objects Access
- Online Casino Roulette – A guideline for penetration testers and security researchers
- Custom DLL injection with Cobalt Strike's Beacon Object Files
- Run as SYSTEM using Evil-WinRM

Beginners corner

- Domains, Servers, and IPs (aka no, that's not a subdomain takeover)
- Web Application Hacking — Analyzing the Application
- 10 Password Reset Flaws
- Game Hacking Part 1 – Equipping Your Loadout & FPS Sample
- Windows 10 as a pentest OS
- Create a Fully Loaded, Free Active Directory Lab in 15 Minutes

Writeups

Challenge writeups

- coin_artist – 34700 $coin Puzzle Write-Up ($20,000)
- XSS on the Wrong Domain T_T – Tech Support (web) Google CTF 2020
- VolgaCTF 2020 Qualifier Writeup

Pentest writeups

- How I bypassed Cloudflare's SQL Injection filter
- Evil Twins, Eavesdropping, and Password Cracking: How the Office of Inspector General Successfully Attacked the U.S. Department of the Interior's Wireless Networks
- Clash of the (Spam)Titan
- Pentest-Report Ethereum Mist 11.2016 – 10.2017

Responsible(ish) disclosure writeups

- CVE-2020-16171: Exploiting Acronis Cyber Backup for Fun and Emails #Web #CodeReview
- Falco Default Rule Bypass #Kubernetes
- Aruba Clearpass RCE (CVE-2020-7115) #Web
- Firefox for Android LAN-Based Intent Triggering #Android
- Backdoors and other vulnerabilities in HiSilicon based hardware video encoders #Network
- Alfresco Reset Password Add-on – 0day Vulnerabilities #Web
- SSD Advisory – rConfig Unauthenticated RCE #Web

Bug bounty writeups

- Email Confirmation Bypass in your-store.myshopify.com which leads to privilege escalation (Shopify, $22,000)
- [authmagic-timerange-stateless-core] Improper Authentication (Node.js third-party modules) #JWT
- Change the username for any Facebook Page (Facebook, $15,000)
- Business logic vulnerabilities — Low-level logic flaw
- Account takeover by OTP bypass
- Periscope HTTP Request Smuggling Attack 2020

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- kb: A minimalist knowledge base manager
- Arsenal: Quick inventory, reminder and launcher for pentest commands
- Mapboxapiscanner: Python script to determine whether a leaked/found Mapbox API Key is vulnerable to unauthorized access by other applications or not
- query-json: Faster and simpler implementation of jq in Reason Native

More tools, if you have time

- nvd-scrapper: Pull data from the national vulnerability database and push it to a GCP bucket
- OneFuzz: A self-hosted Fuzzing-As-A-Service platform by Microsoft
- GKE Auditor: A tool by Google to detect a set of common Google Kubernetes Engine misconfigurations

- LambScan & Offensive Security Testing Using Cloud Tools: AWS Lambda-based port scanner
- wordlist_generator: Unique wordlist generator of unique wordlists
- Tafferugli: Twitter Analysis Framework #OSINT
- Darkshot: Lightshot scraper on steroids with OCR #OSINT
- mzap: Multiple target ZAP Scanning
- Bantam: A PHP backdoor management and generation tool/C2 featuring end to end encrypted payload streaming designed to bypass WAF, IDS, SIEM systems
- crlfmap: Go tool to find HTTP Splitting vulnerabilities
- MIDNIGHTTRAIN & Intro: A Covert Stage-3 Persistence Framework weaponizing UEFI variables

Misc. pentest & bug bounty resources

- @ITSecurityguard's Bug Bounty Tools mind map
- A Hacker's Guide to the Shopify GraphQL API
- Active Directory pentest mindmap
- The Hacker Recipes
- The only Penetration testing resources you need
- Trace Labs CTF – Exploring interesting URL submissions
- Windows_OneLiners
- Lateral Movement Detection GPO Settings Cheat Sheet #BlueTeam

Challenges

- CdkGoat: Vulnerable AWS CDK Infrastructure
- Cfngoat & Intro : Vulnerable Cloudformation Template
- OWASP Top 10 Lab Updated

Articles

- Oh, the Places You'll Go! Finding Our Way Back from the Web Platform's Ill-conceived Jaunts
- Advanced boolean-based SQLi filter bypass techniques
- Postgresql Code Execution: UDF Revisited
- Smart Home Devices: assets or liabilities? – Part 1: Security

- phpbash – A Terminal Emulator Web Shell
- A Technical Analysis of the 4k Facebook Scam
- ModSecurity, Regular Expressions and Disputed CVE-2020-15598
- Defeating Macro Document Static Analysis with Pictures of My Cat
- Purple Team Candidates for Modern Tech Environments
- Inside Amazon's Ring Alarm System

News

Bug bounty & Pentest news

- Amazon S3 bucket owner condition helps to validate correct bucket ownership
- User-Generated Content
- The IRS offers a $625,000 bounty to anyone who can break Monero and Lightning
- Story of a $45.000 (that should've been $350.000) on BRZX

Reports

- Secure development: 'Shift left' becomes 'shift everywhere' thanks to increased adoption of automated security tools
- COVID cybercrime: 10 disturbing statistics to keep you awake tonight
- 2020 Threat Hunting Report: Insights From The Crowdstrike Overwatch Team
- Darknet markets likely to continue despite exit scams and law enforcement takedowns

Vulnerabilities

- US 2020 Presidential apps riddled with tracking and security flaws
- Video encoders using Huawei chips have backdoors and bad bugs – and Chinese giant says it's not to blame
- Researcher kept a major Bitcoin bug secret for two years to prevent attacks
- Billions of devices vulnerable to new 'BLESA' Bluetooth security flaw
- ModSecurity maintainers contest denial-of-service vulnerability claims
- Libinjection's SQL injection defenses cracked

Breaches & Attacks

- First death reported following a ransomware attack on a German hospital

- Cardbleed: a massive Magento1 hack
- US govt: China-sponsored hackers targeting Exchange, Citrix, F5 flaws
- Android Malware Bypasses 2FA And Targets Telegram, Gmail Passwords
- Google App Engine feature abused to create unlimited phishing pages
- Maze Ransomware Adopts Ragnar Locker Virtual-Machine Approach
- Office 365 phishing runs real-time check of stolen domain logins
- US charges Iranian hackers for breaching US satellite companies... with one being a famous security researcher

Other news

- Riot Games Hires a Cheat Hunting Vigilante
- Chinese database details 2.4 million influential people, their kids, addresses, and how to press their buttons
- UPDATE – TikTok Ban: Security Experts Weigh in on the App's Risks
- Internet Society launches toolkit to safeguard open, secure 'network of networks'
- Google Chrome is making it easier to reset compromised passwords
- Three middle-aged Dutch hackers slipped into Donald Trump's Twitter account days before 2016 US election
- MITRE releases emulation plan for FIN6 hacking group, more to follow
- UK government releases toolkit to easily disclose vulnerabilities

Non technical

- Hacker Spotlight: Interview With Honoki
- Please Stop Asking For "advanced" Learning Content
- Hacking Your Pen Testing / Red Teaming Career: Part 2 & Part 1
- How to build an effective red team
- TomNomNom uses this

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 09/11/2020 to 09/18/2020.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com