Bug Bytes #71 – 20K Facebook XSS, LevelUp 0x06 & Naffy's Notes

intigriti - 20th May 2020 - bugbytes

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 08 to 15 of May.

Our favorite 5 hacking items

1. Tool of the week

Wuzz

If you ever want to send HTTP requests for a quick test without firing up Burp/ZAP, this is the tool for you. It is an interactive CLI tool for HTTP inspection. It allows you to send HTTP requests from the terminal, while controlling everything from the headers to the request's type and data.

2. Writeup of the week

$20000 Facebook DOM XSS (Facebook, $20,000)

DOM XSS through postMessage is trendy and lucrative. @vinodsparrow found one in Facebook's login button, and shares all the details in this cool writeup. The nice thing is, he not only shares the code to exploit it, but also explains what led him to believe that there was an issue in the first place.

3. Videos of the week

- Naffy (@nnwakelam) Talks About His Hacking Approach, Recon Methodology, and How to Get Started!

- LevelUp 0x06 – Hacking The New Normal

@nnwakelam is one of the current bug hunter millionaires, and is particularly known for his recon skills. It is awesome to have this almost 2-hour interview where he chats with @nahamsec about his specialty, extending the attack surface, plus many other things like bug examples, Burp, vulnerability indicators... Also, just in case, here is his TL;DR.

LevelUp is also a rendez-vous I never miss. Topics range from automotive testing to security code review, writing résumés, choosing targets, and making better decisions as bug hunters.

4. Non technical items of the week

- Don't Force Yourself to Become a Bug Bounty Hunter
- Pushing yourself through hard hunting days: A bug hunter's perspective

These are two good pieces that point out important questions every struggling bug hunter should ask themselves. The idea is to find out what is hindering you. So, even if these exact questions don't apply to you, try to extrapolate to find your own missing pieces.

5. Tutorial of the week

How To Scan AWS's Entire IP Range to Recon SSL Certificates

This article expands on an idea mentioned in Naffy's interview, that is scanning AWS's entire IP range and identifying certificates belonging to your target. This is done by chaining existing open source tools, and could be applied to other Cloud providers like Azure.

Other amazing things we stumbled upon this week

Videos

- FUZZING FOR BEGINNERS (KUGG teaches STÖK American fuzzy lop)

- Mental Health For Hackers Among COVID-19: Introduction to CBT
- BOUNTY THURSDAYS – Bugcrowd Levelup0x06 RECAP, amass update, Intigriti May XSS challenge, Nuclei
- HackerOne Hacker Interviews: Douglas (@the_arch_angel), HackerOne Hacker Interviews: André (@0xacb), Aspen (@urazeebo) & Douglas (@the_arch_angel)
- $3,000 CodeQL query for finding LDAP Injection – Github Security Lab – Hackerone
- Beginner Web Application Hacking
- Bug Bounties 101: how much can I earn?
- Learn Stuff with Yekki – Episode 4 – SMBClient
- Bug bounty tips for broken access control on BurpSuite Part 1
- SharpHose Password Spraying and Azure App Services For Offensive Operations

Podcasts

- Security Now 766 – ThunderSpy
- Naked Security Podcast S2 Ep 39: Thunderspy, government encryption, and reply all mistakes
- Darknet Diaries EP 65: PSYOP
- Red team hacking in the age of COVID-19
- 7MS #414: Tales of Pentest Fail #4
- [CPRadio] Phishing in Canada
- Risky Business #583 — COVID-19 collection intensifies, tensions mount
- ASW #107 – Samsung RCE 0-Click, Whispers, & Compromising Pluton
- PSW #651 MITRE ATT&CK & Security Visibility: Looking Beyond Endpoint Data – Mike Nichols
- PSW #651 – Ramsay Malware, Top 10 CVE's, & Reverse RDP Attacks
- PSW #650 – Vulnerability Madness, IoT Botnets, & Breach Chaos
- SWN #33 – ThunderSpy, Hacking COVID Research, & GDPR Fines

Webinars & Webcasts

- Semgrep and the future of Static Analysis
- Securing Active Directory: Resolving Common Issues & Slides
- Introduction to OAuth 2.0 and OpenID Connect
- WAF bypass using SQL injection
- Online Training Sneak Peek: PowerShell for Offense and Defense
- Privilege Escalation in GCP – A Transitive Path
- SANS @Mic Talk – Cloud Native Payloads: A Matryoshka Doll of Exploits

Conferences

- CYBERWARCON 2019 – RedSourcing: Cyberwar On a Budget
- Android Kernel Exploitation

Tutorials

Medium to advanced

- Mix-Up, Revisited
- Finding secrets by decompiling Python bytecode in public repositories
- AWS Pass-through Proxy
- Attacking Azure Container Registries with Compromised Credentials
- Breaking Typical Windows Hardening Implementations
- Securely Deploying IPv6 in 2020 Part 1: Internet Facing Perimeter
- Decrypting ADSync passwords – my journey into DPAPI
- Reflective PE Injection in Windows 10 1909
- Roasting your way to DA – Build-Break-Defend-Fix

Beginners corner

- Android Studio Emulator (Android 9.0) with ARM Binaries
- Open Redirection Guide
- Frida Cheagynvaeltsheet and Code Snippets for Android
- The Bash Scripting Tutorial, Part 3
- A Pentester's Voyage – The First Few Hours
- Adding a Certificate to Android System Trust Store
- ngrok FTW
- Proxying Unaware Thick Clients
- Thick Client Proxying – Part 10 – The hosts File
- #CQLabs – How UAC bypass methods really work by Adrian Denkiewicz
- Exploring the Exploitation of the Java Debug Wire Protocol
- Building a FreeIPA Lab

Writeups

Challenge writeups

- Testing the testers: solving a customer's private CTF
- HTTP Request Smuggling
- Hack-From-Home Challenge Walk Through
- CloudGoat AWS Scenario Walkthrough: "EC2_SSRF"

Pentest writeups

- Microsoft Office 365 Enumeration

Responsible(ish) disclosure writeups

- Stored XSS in Paytium 3.0.13 WordPress Plugin #Web

- SSD Advisory – MyLittleAdmin PreAuth RCE #Web
- CVE-2020-11108: How I Stumbled into a Pi-hole RCE+LPE #Web #RCE
- Playing with GZIP: RCE in GLPI (CVE-2020-11060) #Web
- Grandstream PBX Hacking #PBX #Web
- Reverse RDP – The Path Not Taken #MacOS #RDP
- Another Zoho ManageEngine Story #CodeReview #Java
- Two vulnerabilities in Oracle's iPlanet Web Server (CVE-2020-9315 and CVE-2020-9314)

Bug bounty writeups

- Magic of the Back Slash ($2,100)
- $3000 Bug Bounty Award from Mozilla ($3,000)
- I Found XSS Security Flaws in Rails – Here's What Happened. (Ruby on Rails, $500)
- Customer private program can disclose email any users through invited via username (Hackerone, $7,500)
- No redirect_uri in the db for web-internal clientKey leads to one-click DoS on gitter.im (Gitlab, $1,000)
- GraphQL node interface for ActiveResource models lacks encoding for resource identifier, enabling parameter injection in Payments backend

See more writeups on The list of bug bounty writeups.

Tools

- Authentication Token Obtain and Replace (ATOR) & Introduction: Burp extension for handling complex login sequences
- rulesfinder & Rulesfinder, automatically create good password cracking rulesets: Machine-learn password mangling rules
- Stormspotter: Azure Red Team tool for graphing Azure and Azure Active Directory objects
- Cloudsplaining: An AWS IAM Security Assessment tool that identifies violations of least privilege and generates a risk-prioritized HTML report
- SSRFIRE: An automated SSRF finder. Just give the domain name and your server and chill! 😉 Also has options to find XSS and open redirects
- Wfuxx: Web based fuzzer – Wrapper around ffuf & gobuster
- ApkUrlGrep: Extract endpoints from APK files

- Open-sesame: A python tool to display random publicly disclosed Hackerone reports when bored. Automatically opens the report in browser
- Project Eagle: Yet another vulnerability scanner
- rate-limit-checker: Check whether the domain has a rate limit or not
- Ultra Recon: A tool for running recon tools with Docker
- grafana-ssrf: Authenticated SSRF in Grafana
- Words Scraper: Selenium based web scraper to generate passwords list
- Thns: Telegram HTTP notification script, created for a phishing red team operation
- Clipboardme: Grab and Inject clipboard content by opening a link
- Screenshooter: The Beacon Screenshot Savior: A C# tool to screenshot user's desktop(s) complete with multiple checks. Will work with Cobalt Strike's Execute-Assembly
- Minimalistic SMB login bruteforcer: A simple SMB login attack and password spraying tool

Misc. pentest & bug bounty resources

- Q&A session with TomNomNom
- Workshop: Finding security vulnerabilities in Java with CodeQL
- Chaos: A DNS dataset API, collected actively, meant to enhance and analyse internet wide changes
- Dorks for Intelligence X and Google
- Pentesting/Bugbounty Dockerfiles
- gwen001/sslsub.sh: Oneliner to retrieve altnames from ssl certificates

Challenges

- @gynvael's Express.js Web security challenge Level 4 & Level 5
- Pwn2Win Warmup challenge!
- OSINT Twitter Challenge
- @GouveaHeitor's XSS challenge
- xss.normguard.com

Articles

- Short beacon analysis on the NHS iOS Tracking application
- Evading Detection with Excel 4.0 Macros and the BIFF8 XLS Format & Macrome: Excel Macro Document Reader/Writer for Red Teamers & Analysts
- Preventing SQL injection: a Django author's perspective
- PHPUnit: A Security Risk?
- Spear phishing in Google Cloud
- Shell Arithmetic Expansion and Evaluation Abuse
- Faxing Your Way to SYSTEM — Part Two & faxhell ("Fax Shell"): A Bind Shell Using the Fax Service and a DLL Hijack
- Relaying NTLM authentication over RPC
- WS-Management COM: Another Approach for WinRM Lateral Movement
- Why Electron apps can't store your secrets confidentially: — inspectoption
- No more JuicyPotato? Old story, welcome RoguePotato! & RoguePotato

News

Bug bounty & Pentest news

- Kali Linux 2020.2 Release
- CISSP Qualification Given Status Equivalent to Master's Degree Level
- Breaching the Cloud Perimeter w/ Beau Bullock: 4-hour free online training course on May 28
- DEF CON 2020: 'Safe Mode' virtual event will be free to attend, organizers confirm
- Hacker Days: Kubernetes from a Attacker's Perspective: May 28

Reports

- House of cards: Majority of commercial apps contain outdated, abandoned open source components, study claims

- The State of Ransomware 2020 – Results of an independent study of 5,000 IT managers across 26 countries
- US-CERT lists the 10 most-exploited security bugs and, yeah, it's mostly Microsoft holes people forgot to patch

Vulnerabilities

- New Thunderbolt security flaws affect systems shipped before 2019
- PrintDemon vulnerability impacts all Windows versions
- 900 Million iPhones Affected By Updated Apple iOS Warning (MailDemon)
- Squid patches security flaws in HTTP digest authentication
- Obscure, decade-old vulnerability finally unearthed in GLPI asset management app
- HackerOne co-founder unearths information leakage bug in Rails package
- Researchers spot thousands of Android apps leaking user data through misconfigured Firebase databases

Breaches & Attacks

- Multi-part Android spyware lurked on Google Play Store for 4 years, posing as a bunch of legit-looking apps
- Android app promised to serve news updates, served ESET with a DDoS attack instead
- New Ramsay malware can steal sensitive documents from air-gapped networks
- Hackers target the air-gapped networks of the Taiwanese and Philippine military
- Digital Ocean says it exposed customer data after it left an internal document online
- US govt exposes new North Korean malware, phishing attacks
- New COMpfun malware variant gets commands from HTTP error codes
- Papa don't breach: Contracts, personal info on Madonna, Lady Gaga, Elton John, others swiped in celeb law firm 'hack'
- Scammers steal $10 million from Norway's state investment fund
- Cloud security: Attacking Azure AD to expose sensitive accounts and assets

Other news

- The Confessions of Marcus Hutchins, the Hacker Who Saved the Internet

- ‘iOS security is f**ked’ says exploit broker Zerodium: Prices crash for taking a bite out of Apple’s core tech
- US Computer Fraud and Abuse Act: How an upcoming Supreme Court ruling could have serious ramifications for ethical hackers
- Senator demands deep probe into spyware-for-cops after NSO Group touts hacking toolkit to American plod
- Clearview AI won’t sell vast faceprint collection to private companies
- This new cybersecurity school will teach kids to crack codes from home
- Microsoft: Here’s how we’re killing a class of memory security bugs in Windows 10
- Windows 10 gets DNS over HTTPS support, how to test
- The best way to protect the US electrical grid is with open source

Coronavirus

- Ohio Has Stopped Kicking Workers Off Unemployment After A Hacker Targeted Its Website
- US warns of Chinese hackers targeting COVID-19 research orgs
- COVID-19 blamed for 238% surge in cyberattacks against banks
- DDoS surge driven by attacks on education, government, and coronavirus information sites
- RDP attacks skyrocket amid Covid-19 lockdown

Non technical

- Bug Bounty Hunting Tips #6 — Simplify
- Are you really in the #bugbounty game?
- How Does Mind Mapping Help for Better Bug Bounty
- To Avoid Burnout, Work Less and Ignore ‘Productivity Propaganda’
- 7 Rules for Staying Productive Long-Term
- Crappy CTF Bingo
- How to Practice Safe Hex and Reduce Your Risk Online
- A 3-tiered Approach to Securing Your Home Network
- Security 101: Two Factor Authentication (2FA)

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 05/08/2020 to 05/15/2020.

Curated by Pentester Land & Sponsored by Intigriti

Bug Bytes #57 – Th3G3nt3lman's Secret Recon Methods, Checkmarx VS API's & Vulns in React Native Apps

11th February 2020

Bug Bytes #65 – Hacking webcams, internal servicedesks & parsers

7th April 2020

Bug Bytes #27 – Secretz, Privilege Escalation on New Relic & How To Keep Your Bugs Organised

15th July 2019

Search

RECENT POSTS

Bug Bytes #71 – 20K Facebook XSS, LevelUp 0x06 & Naffy's Notes

Bug Bytes #70 – Gmail XSS, Decrypting HTTPS without MiTM & Hakluke's TikTok Tips

Bug Bytes #69 – @FransRosen's postMessage tracker, the @zseano files & SSRF in e-mail addresses

What Telenet, UZ Leuven and an ethical hacker say about Intigriti's ethical hacking and bug bounty platform.

Bug Bounty Q&A #4: How does Intigriti optimize bug bounty success?

CATEGORIES

bugbountytips

bugbusiness

bugbytes

challenge

changelog

customer story

events

general

Q&A

ARCHIVES

Select Month