Bug Bytes #135 – Code review for bug hunters, Zoom $200K RCE & Breaking HTTP/2 and Exchange

BY ANNA HAMMOND · AUGUST 25, 2021 · LAST UPDATED ON MARCH 6, 2025

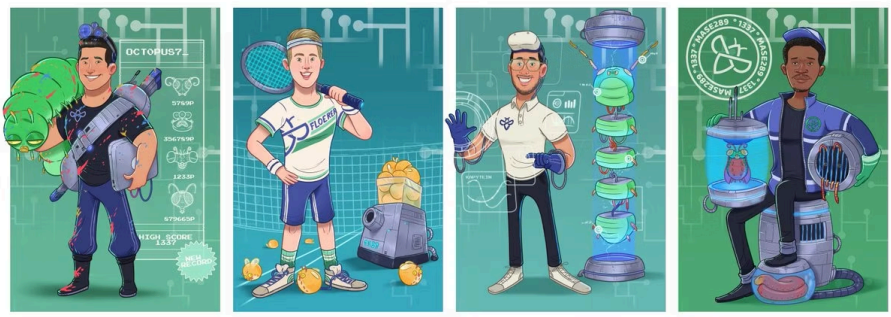
Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series is curated by Mariem, better known as **PentesterLand.** Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

CLICK HERE TO SUBSCRIBE

This issue covers the week from August 2 to 23.

Intigriti News

Intigriti launches fast lane program to incentivise cybersecurity research



© Intigriti

Welcome to the 1337-club for Q3 2021, @oct0pus7, @bug_dutch, @kapytein & @mase289!

Our favorite 5 hacking items

1. Conference of the week

DEF CON 29 Main Stage Presentations & Media Server
Recon Village, AppSec Village & Red Team Village CTF: Day 1

There are so many amazing talks and new research in this DEF CON edition! So, I'm only going to mention two of the most notable ones:

- HTTP/2: The Sequel is Always Worse by @albinowax (plus Tips on how to find a HTTP/2 playmate);
- @orange_8361's From Pwn2Own 2021: A New Attack Surface On Microsoft Exchange – Proxyshell! that earned him $200K at Pwn2Own 2021.

2. Writeups of the week

Sophos UTM Preauth RCE: A Deep Dive into CVE-2020-25223
Zoom RCE from Pwn2Own 2021 (Zoom, $200,000)

@jstnkndy came across CVE-2020-25223 in a pentest and didn't find any public exploit. So, he reverse engineered the vulnerability's patch to develop his own proof of concept. The writeup is very well written and explains the methodology in great detail.

The second writeup is about a 0-click RCE via heap buffer overflow found in Zoom. Thijs Alkemade & Daan Keuper demonstrated the bug during Pwn2Own and share details on this impressive and lucrative finding.

3. Webinar of the week

How to do Code Review – The Offensive Security Way

If you're interested in learning source code review to get a leverage as a bug hunter, this is a must-watch. @infosec_au shares insightful techniques for obtaining source code in the context of bug bounties, plus interesting bug examples and tips for both beginners and experienced code reviewers.

4. Video of the week

Working with HTTP/2 in Burp Suite & Blog post

Since @albinowax's talk on HTTP/2 desync attacks, Burp Suite was updated to enhance HTTP/2 support. This video demonstrates these new changes and how to use Burp to test for HTTP/2-exclusive vulnerabilities.

5. Tools of the week

Malicious PDF Generator
apk-recon.yaml, api-linkfinder.sh, Links & parameters wordlists extracted from the top 55 mobile

© Intigriti

apps

Malicious PDF Generator is a Python script that generates 10 different malicious PDF files and supports Burp for receiving out-of-band requests. @jonasl created it for Web app testers to automate several known attacks.

The other tools are a Nuclei template and a Bash script that @nullenc0de uses to extract parameters and links from APKs and API documentation. The regexes they use can also be tweaked if you need to dump more/different information.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Hack Chat Live at Black Hat 2021
- How to Use WPScan With ethicalhack3r
- "Game-Over For The Company" with @d0nut (Hacker Heroes #8), "I Want To Know Where The Aliens Are" with @RobinZekerNiet (Hacker Heroes #9) & "Unlimited Money To Your Account?" with @bug_dutch (Hacker Heroes #10)
- What To Do When You Have DEFCON FOMO?? :((((
- SecuriTEA & Crumpets – Episode 11 – Grant Douglas – Frida
- Interview w @SherlockSecure : Top 15 on Github \| Top 400 on BC \| Approach, Mindset & More...
- Learning to Hack in 2021: What resources should you use? & Blog post

Podcasts

- Microsoft's Reasoned Neglect – T-Mobile's Major Data Leak, Razer Mouse Hack, Overlay Networks

Webinars

- OWASP Talk – HTTP3 Security – Robin Marx
- Ethical Hacking & System Defense (Free Ethical Hacking class by @PhillipWylie)

Conferences

- Black Hat USA 2021 & Slides
- BSides Noida : Day – 1 & Day – 2
- USENIX Security '21 Technical Sessions, including:

© Intigriti

- Weaponizing Middleboxes for TCP Reflected Amplification & Video
- Can I Take Your Subdomain? Exploring Same-Site Attacks in the Modern Web
- Abusing Hidden Properties to Attack the Node.js Ecosystem
- Why TLS is better without STARTTLS: A Security Analysis of STARTTLS in the Email Context, NO STARTTLS
- Injection Attacks Reloaded: Tunnelling Malicious Payloads over DNS

Slides & Workshop material

- CyberTruckChallenge19 (Android security workshop material)

Tutorials

Medium to advanced

- Proxy managed by enterprise? No problem! Abusing PAC and the registry to get burpin'
- How does git diff –ignore-matching-lines work
- How to install Frida into an Android application
- Admin's Nightmare: Combining HiveNightmare/SeriousSAM and AD CS Attack Path's for Profit
- Knock knock, who's there? Your new DA!
- The ultimate tag team: PetitPotam and ADCS pwnage from Linux

Beginners corner

- How to Hack APIs in 2021
- Out-of-band Application Security Testing with OWASP ZAP
- Hacker Tools: Ciphey – Automatic decryption, decoding & cracking & Hacker Tools: How to set up XSSHunter
- Blast Radius: Misconfigured Kubernetes & Blast Radius: DNS Takeovers
- Common mistakes when using permissions in Android

Writeups

Challenge writeups

- DEFCON 29 Red Team Village CTF Writeup: Supply Chain Attack
- Prototype pollution in Google Analytics?! Solution to August '21 XSS Challenge & Written walkthrough by @WHOISbinit
- Intigriti's PHP challenge breakdown & Intigriti's Flask Challenge Breakdown

© Intigriti

Pentest writeups

- Microsoft 365 OAuth Device Code Flow and Phishing

Responsible(ish) disclosure writeups

- Fortinet FortiPortal Vulnerability Disclosures #Web #CodeReview
- (Authenticated) Remote Code Execution Possible in Pi-Hole Web Interface 5.5
- SSD Advisory – IP-Board Stored XSS to RCE Chain #Web
- Razer mouse + Physical access = Local admin on Windows 10 & PoC
- Don't shoot the emissary #CodeReview #Web
- elFinder – A Case Study of Web File Manager Vulnerabilities #CodeReview #Web

0-day & N-day vulnerabilities

- Sophos UTM Preauth RCE: A Deep Dive into CVE-2020-25223 #Web

Bug bounty writeups

- Zoom RCE from Pwn2Own 2021 (Zoom, $200,000)
- How to Hack Apple ID (Apple, $10,000)
- Modify in-flight data to payment provider Smart2Pay (Valve, $7,500)
- A Bug's Life: CVE-2021-21225 & Exploiting CVE-2021-21225 and disabling W^X (Google, $22,000)
- Two weeks of securing Samsung devices: Part 2 (Samsung, $18,040)
- Partial report contents leakage – via HTTP/2 concurrent stream handling (HackerOne, $2,500, related to the "Timeless timing attacks" DEF CON talk)

See more writeups on The list of bug bounty writeups.

Tools

- WARCannon: High speed/Low cost CommonCrawl RegExp in Node.js
- CAIDO: A lightweight web security auditing toolkit
- PaperChaser: A Google Drive/Docs/Sheets/Slides Enumeration Spider
- dirtywords & Intro: A targeted word list generation tool
- GoKart & Intro: A static analysis tool for securing Go code

© Intigriti

Tips & Tweets

- Using Autorepeater to automate testing for SSRF
- Outputting a specific part of a match in grep
- HTTP Parameter Pollution in PHP
- OpenID Connect / OAuth 2.0 “claims” hack

Misc. pentest & bug bounty resources

- OWASP Mobile Security Testing Guide (MSTG) v1.2
- SecurityGOAT
- Auto_Wordlists
- 31 Tips — Advanced Bug Bounty & Pentesting

Challenges

- screenshotter (web) & Video walkthrough
- Kontra AWS Top 10
- TyphoonCon CTF 2021: The impossible Chrome challenge
- SQL Injection – Challenge 1: NahamSec inspired (by BugHuntr.io)

Articles

- Find real website ip bruteforcing ipv4 ranges & real_ip_discover
- Mitigation schmitigation: Control HttpOnly cookies through XSS
- Fingerprinting Windows versions, AV, wireless cards over the network—all without authentication
- Phishing for NetNTLM Hashes
- 1Password Secret Retrieval — Methodology and Implementation & 1PasswordSuite
- Oh, Behave! Figuring Out User Behavior

Bug bounty & Pentest news

- Bug bounty
  - Intigriti launches fast lane program to incentivise cybersecurity research
  - Microsoft: Announcing the Launch of the Azure SSRF Security Research Challenge
  - Money Talks Giveaway

© Intigriti

    - Corellium Open Security Initiative
- Cybersecurity
    - Pwnie Award Winners 2021
    - Launch of the Porchetta Industries funding platform: a centralized place for organizations that rely on Infosec/Hacking tooling
- Upcoming events
    - OWASP Nagpur Meetup #12 (Virtual) featuring @codingo_ (August 28)
    - BSides Berlin 2021 (August 28)
- Tool updates
    - reNgine 1.0
    - Interactsh v0.0.4 (Added authentication for self-hosted instances)
    - Axiom controllers now support Docker
    - Turbo Intruder introduced decorators for ffuf-like response matching/filtering

Non technical

- From Chokeslams To Pwnage: Phillip Wylie Shares His Journey From Pro Wrestling To Offensive Security
- Comparison of reverse image searching in popular search engines [OSINT hints]

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com

© Intigriti