Bug Bytes #62 – Talks worth watching in self-quarantine, $6K Google and Slack bug and bug hunting tips

BY INTIGRITI · MARCH 17, 2020 · LAST UPDATED ON MARCH 6, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-62-talks-worth-watching-in-self-quarantine-6k-google-and-slack-bug-and-bug-hunting-tips

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.

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 06 to 13 of March.

Our favorite 5 hacking items

1. Conference of the week

- BSidesSF 2020, especially:
- – Panel: Let's Get 360 w/Bug Bounty!
- – The GCP Metadata API
- – How To Write Like It's Your Job
- – The Voight-Kampff Test for Discovering Vulnerabilities
- – Panel: Mental Health for Hackers
- – Non-Political Security Learnings from the Mueller Report
- – Transform Your Presentation Skills

The range of (interesting) topics tackled in this conference is amazing. There are at least 10 talks I really need to watch. During these difficult times of Coronavirus quarantine / social distancing, this is an excellent way to pass time.

2. Writeups of the week

- – The unexpected Google wide domain check bypass (Google, $6,000)
- – Mass account takeovers using HTTP Request Smuggling on https://slackb.com/ to steal session cookies (Slack, $6,500)

These are two very impressive findings! The first one was found by analyzing a Regex found in obfuscated JavaScript code. It was used for URL validation in a Google app. @xdavidhu found a way to bypass the check. The impact was low/medium, but he later found that the vulnerable code was part of a JS library common to many Google Web apps including Gmail and Google Docs.The second vulnerability is an HTTP Request Smuggling CL.TE hijack attack found on Slack. It was possible to steal victims' session cookies by

redirecting them to an attacker-controlled Collaborator server. The writeup is pretty explanatory. And the attack could have been exploited for massive account takeovers.

3. Video of the week

> @Mrtuxracer Talks About Monitoring Endpoints, Binary Exploitation, Continuous Recon and More!

This is @NahamSec's latest interview, with @Mrtuxracer. I find it particularly interesting because of @Mrtuxracer's approach. He explains his unique recon process, talks about continuous monitoring of JavaScript files and endpoints, some of his custom tools, API hacking, etc.This is definitely worth watching if you want to learn about bug hunting methodology, differentiating yourself, or which kind of custom tools other bug hunters are using.

4. Non technical item of the week

> Bug Bounty Hunting Tips #4 — Develop a Process and Follow It

"Admittedly, it can feel great for the first hour or so but after that, you can start to become bored and frustrated if you don't find anything. And without a structured bug bounty hunting process, you probably won't find anything new."Do this ring any bell? This excellent article goes over how to create a high-level process for bug hunting. Apart from technical methodologies, some decisions can help avoid frustration. This includes choosing a bug hunting approach, deciding minimum and maximum time to spend on a target and minimum time for writing reports.

5. Article of the week

> Bug Business #2 – Hacking, traveling and vlogging with @STÖK

There are only two publications related to bug bounty that I wait for impatiently and devour as soon as they're published: EdOverflow's newsletter and this new interview series.

The first issue was with EdOverflow. The last one is an excellent read if you want to learn how Stök juggles between different projects, his filming process, how he manages full-time bug hunting without pulling all-nighters (Early birds, hello!)...

Other amazing things we stumbled upon this week

Videos

- $100k Hacking Prize – Security Bugs in Google Cloud Platform
- Reviewing the Updated PWK (OSCP) Course 2020

Podcasts

- Security Now 757 – The Fuzzy Bench
- Security Weekly News #16 – Security Weekly News Wrap Up & #17 – James Adams and the News
- Risky Business #574 — EARN IT Act targets crypto, Joshua Schulte to be retried on most serious charges

- How to become a penetration tester
- The Privacy, Security, & OSINT Show – 160-Telephone Search Offense & Defense
- SwigCast, Episode 6: EDUCATION
- The Many Hats Club Ep. 51, Honk! (With Ian Coldwater)

Webinars & Webcasts

- Vulnerability Scanner Fails: 5 Ways You Can't Fake The Human Element
- Innovative Application Security Testing Techniques for Modern Software Development

Conferences

- Argument Injection – Invited presentation for Team Bi0s
- Brooke Point High School Presentation – Tommy Devoss

Slides & Workshop material

- Modern PHP security

Tutorials

Medium to advanced

- Filter Bypass in Multi Context
- ZAP SSRF Setup
- Abusing File System functions in web applications – steal NTLMv2 hash
- Kerberosity Killed the Domain: An Offensive Kerberos Overview
- Offensive Development with GitHub Actions
- Red Team Tactics: Advanced process monitoring techniques in offensive operations
- Defeating RunAsPPL: Utilizing Vulnerable Drivers to Read Lsass with Mimikatz

Beginners corner

- Recon with waybackmachine. For BugBounty!
- Exploiting ReDoS
- Jailbreak Your iPhone Through Linux
- Internal Information Disclosure using Hidden NTLM Authentication
- Practical VoIP Penetration Testing

- Breaking Enterprise Wireless

Writeups

Challenge writeups

- Using Burp Intruder for auth bypass – CTF, root-me.org / BSCorp – Linux

Pentest writeups

- How I Hacked a Domain Controller in Azure during a Penetration Test.
- How I bypassed the OTP verification process? Part – 3

Responsible(ish) disclosure writeups

- Twisted Version 19.10.0 #Web #RequestSmuggling
- Multiple vulnerabilities found in Zyxel CNM SecuManager #Network

Bug bounty writeups

- Slack DTLS uses a private key that is in the public domain, which may lead to SRTP stream hijack (Slack, $2,000)
- Disabled account can still use GraphQL endpoint (Hackerone, $500)
- TURN server allows TCP and UDP proxying to internal network, localhost and meta-data services (Slack, $3,500)
- Lack of input validation that can lead Denial of Service (DOS) (Twitter, $560)
- Vulnerable design leads to personal data leakage- yet another case of an inter-application vulnerability...
- Generate valid signatures for files hosted in Facebook CDNs.
- Broke limited scope with a chain of bugs (tips for every rider CORS)

Tools

If you don't have time

- BGP Search: A Python wrapper for searching on https://bgp.tools (Takes organization name as input & output IP ranges)
- iprobe: Take a list of IP addresses or IP range and probe for working HTTP and HTTPS servers (similar to *httprobe* but also takes IPs and IP ranges as input)
- HTTP-FUZZER: Go fuzzer that is burp-compatible and able to fuzz some random parameters in the raw http request

More tools, if you have time

- Sub-Drill: A very (very) simple Subdomain Finder based on online certification services (threatcrowd, hackertarget, crt.sh, certspotter & findsubdomains)
- Exegol: A Kali light base with a few useful additional tools and some basic configuration
- Brownie tub: A Standalone Web Shell Client
- Mimimalistic AD Login Bruteforcer
- Starkiller & Introduction: GUI application for interfacing with Empire. It allows for multi-user support and ease of operations
- NTLM scanner: A simple python tool based on Impacket that tests servers for various known NTLM vulnerabilities
- Password Guesser: Script to generate custom password wordlist to guess weak passwords
- Sifter: OSINT, recon & vulnerability scanner in Bash for penetration testing
- Callidus & Introduction: C# tool that allows red team operators to leverage O365 services for establishing command & control communication channel

Misc. pentest & bug bounty resources

- Eventory Pentest Report by Securitum
- Crxcavator.io
- Morph.io & The Only Step-by-Step Guide You'll Need to Build a Web Scraper With Python
- Doxxing Training
- Web Security Dojo Version 3.4.1

Challenges

- Exploit-workshop: A step by step workshop to exploit various vulnerabilities in Node.js and Java applications

Articles

- Cloud WAF Comparison Using Real-World Attacks
- Throwback Threat Thursday: WordPress 4.7 WP-JSON Content Injection Vulnerability
- Paid posts or how Facebook pages are hijacked
- Busting Ghostcat: An Analysis of the Apache Tomcat Vulnerability (CVE-2020-1938 and CNVD-2020-10487)
- This PIN Can Be Easily Guessed
- Wireless Penetration Tips
- 3-D Secure SMS-OTP Phishing

News

Bug bounty & Pentest news

- Earn cash or a free month of Pentesterlab by contributing to @codingo_'s Interlace
- Google awards $100k to Dutch bug hunter for cutting-edge cloud security research
- @TheParanoids's next Live Hacking Event in Singapore is converted into a Virtual Hacking Event

Reports

- Android Users Beware: This Is Why You Should Never Rely On Google's Own Malware Protection
- 99% of compromised Microsoft enterprise accounts lack MFA
- More Than Half of IoT Devices Vulnerable to Severe Attacks
- Now Is the Time to Focus on API Security

SMBGhost

- Microsoft SMBv3.11 Vulnerability and Patch CVE-2020–0796 Explained
- I'm SMBGhost, daba dee daba da
- 48K Windows Hosts Vulnerable to SMBGhost CVE-2020-0796 RCE Attacks

Vulnerabilities

- Vulnerable TV streaming app could give attackers full control over users' devices
- Avast disables JavaScript engine in its antivirus following major bug
- Avast AntiTrack certificate bug allowed others to snoop on your online activities
- WordPress Terror: Researchers discover a massive 5,000 security flaws in buggy plugins
- Intel CPUs vulnerable to new LVI attacks
- AMD processors from 2011 to 2019 vulnerable to two new attacks
- Modern RAM used for computers, smartphones still vulnerable to Rowhammer attacks
- Jenkins security: Latest advisory highlights more than 20 vulnerable plugins

Breaches & Attacks

- Years-long campaign targets hackers through trojanized hacking tools
- This ransomware campaign has just returned with a new trick
- FYI: When Virgin Media said it leaked 'limited contact info', it meant p0rno filter requests, IP addresses, IMEIs as well as names, addresses and more
- NordVPN HTTP POST bug exposed customer information, no authentication required

- NSA Warns About Microsoft Exchange Flaw as Attacks Start
- How poor IoT security is allowing this 12-year-old malware to make a comeback

Coronavirus

- Nvidia's calling on gaming PC owners to put their systems to work fighting COVID-19
- List of Free Software and Services During Coronavirus Outbreak
- Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak
- Live Coronavirus Map Used to Spread Malware
- Two people who went to RSA security conference test positive for COVID-19

Other news

- Alleged Vault 7 leaker trial finale: Want to know the CIA's password for its top-secret hacking tools? 123ABCdef
- Trial for accused CIA leaker ends in hung jury
- New US Bill Aims to Protect Researchers who Disclose Govt Backdoors
- Microsoft shares nightmare tale: 6 sets of hackers on a customer's network
- Brave to generate random browser fingerprints to preserve user privacy
- Google engineers open-source Linux tool that prevents USB keystroke injection attacks

Non technical

- Help! I Can't Find Bugs!
- Broken Into Offensive Security
- Severities and Risks: Relations and Differences
- Lessons learned on written social engineering attacks
- The Debate Around Password Rotation Policies

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 02/06/2020 to 02/13/2020.

Curated by Pentester Land & Sponsored by Intigriti