Bug Bytes #102 – A $20k Outlook bug, The hacker interviewer interviewed & How to get pwned by your SIEM

BY ANNA HAMMOND · DECEMBER 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 13 to 20 of December.

Intigriti News

SolarWinds whirlwind, Malwareless ransomware & Cisco 9.9/10 bug

Our favorite 5 hacking items

1. Tips of the week

@irsdl's #XMas2020 research notes
@eur0pa_'s method for using Burp 1.7 with the latest extensions

@irsdl has been sharing awesome hacking notes and tips on topics like deserialization bugs, WAF bypass, Burp & Fiddler, SalesForce apps security & many more. Really worth checking out!

Another noteworthy tip is for people who prefer to stay on Burp 1.7. @eur0pa_ shows how to make it work with all the latest extensions.

2. Writeups of the week

Coordinated disclosure of XML round-trip vulnerabilities in Go's standard library
LogRhythm Zero Days
This is how I was able to view anyone's private email and birthday on Instagram (Facebook, $13,125)

This week's writeups are about authentication bypass in Go's XML parser, a critical chain of WebSocket-related vulnerabilities in LogRhythm (a popular SIEM solution!) and a simple but impactful information disclosure on Instagram.

3. Video of the week

STOK Interviewed Me!
I hacked Outlook and could've read all of your EMAILS!

Fans of @NahamSec's interviews with hackers will love this special edition. He is the one being interviewed and answering all the usual questions on his hacker journey, life/time balance, time management, bug bounty collaboration, etc.
The second video by @ngalongc is a cool writeup of a $20k JWT bug he found in Outlook.

4. Tutorial of the week

Subdomain Takeover: Going for High Impact

@0xpatrik noticed that subdomain takeovers are harder to find nowadays and considered less dangerous because of new mitigations by cloud providers. But they're not dead yet! If you find a subdomain takeover, make sure to increase its impact using the escalation methods he is sharing (or if you know of other ones, the **community** would love to hear them).

5. Resource of the week

OAuth 2.0 authentication vulnerabilities

PortSwigger just released this new Web Security Academy course on OAuth and OpenID Connect vulnerabilities. With their usual clear explanations and many labs, this is the perfect opportunity to practice or learn about OAuth hacking!

Other amazing things we stumbled upon this week

Videos

- Getting Organised: Finding More Time in the Day
- Hacking SSO: Authentication Bypass by Stealing OAuth Tokens
- 5 Common P2/high Severity Bugs To Look Out For!
- How to avoid duplicates in bug bounty #Shorts
- BOUNTY THURSDAYS – BURP 1.7 or 2.0 + more sweet stuff!
- Hacker Spotlight Panel EMEA
- Bug Bounty Seminar with Verizon Media's Paranoids!

- Exploits Explained: Zero Day Remote Code Execution in File Upload Feature
- Taking control over your computer with a malicious Teams message – Bug Bounty Reports Explained
- Learn to HACK (the best way) // ft. John Hammond

Podcasts

- Security Now: SolarWinds – Chrome Throttling Ads, Google Outage, 2020 Pwnie Awards, JavaScript's 25th Birthday
- A Conversation With Farah Hawa | The Uncommon Journey | Episode Seventeen | With Alyssa Miller, Chloe Messdaghi, And Phillip Wylie
- Infosec Prep Podcast 0x03 byt3bl33d3r AMA
- PyMicropsia Trojan, Alphabet Outages, SolarWinds, & Jason Wood – SWN #89
- SolarWinds Attack, AIR-FI Technique, & Zodiac Cypher Decoded – PSW #678
- SolarWinds, Gitpaste-12, G-Suite Attack, & Show Summaries – Wrap Up – SWN #90

Webinars & Webcasts

- SANS Emergency Webcast: What you need to know about the SolarWinds Supply-Chain Attack
- OWASP London Chapter Meeting Live Stream – 10-December 2020

Conferences

- SO-CON 2020 & Slides
- SECURITY@ 2020
- Serving the right recipe for API authentication
- BSides Philly 2020
- Bsides Seattle 2020

Slides & Workshop material

- Black Hat Europe 2020 slides

Tutorials

Medium to advanced

- Automating Blind Sql Injection

- Fastly and Fronting
- Dumping LAPS Passwords from Linux & LAPSDumper
- Guide to Bypassing MFA in 2020
- Salesforce Lightning – Tinting the Windows

Beginners corner

- Template Injection in Action
- Building Word-lists for Red Teamers
- Android Hooking and SSLPinning using Objection Framework
- AS_REP Roasting vs Kerberoasting
- Bug Bounty tip Automating SSRF
- Pentesting PostgreSQL With SQL Injections
- OSINT: How To Research & Investigate U.S. Phone Numbers
- Risk8s Business: Risk Analysis of Kubernetes Clusters

Writeups

Challenge writeups

- Sploosh – Web challenge – pbctf 2020

Pentest writeups

- Excel-Phish – Phish protected Excel-file passwords

Responsible(ish) disclosure writeups

- CVE-2020-25695 Privilege Escalation in Postgresql #Web
- SecureAuth uncovers SAML validation weakness in SAP HANA #Web
- Insecure by Design, Epic Games Peer-to-Peer Multiplayer Service #Web
- Serious Vulnerabilities in Dualog Connection Suite #Web #Ships
- Typo3: Leak To Remote Code Execution. #Web #CodeReview #PHP
- Attacking Unattended Installs on macOS #MacOS #LPE
- D-Link: Multiple Security Vulnerabilities Leading to RCE #Web #Routers
- CyRC analysis: Authentication bypass vulnerability in Bouncy Castle #Java #CodeReview

- Bolstering security: How I breached a WiFi Mesh access point from close proximity to uncover vulnerabilities #Wifi

Bug bounty writeups

- TikTok Careers Portal Account Takeover (TikTok, $2,373)
- My Bug Bounty Journey and My First Critical Bug — Time Based Blind SQL Injection ($3,500)
- The hacker has access to the administrative part of the management reports in publish report (HackerOne, $500)
  - https://twitter.com/jobertabma/status/1339286947429113857
- Takeover an account that doesn't have a Shopify ID and more (Shopify, $23,500)
- [3DS][SSL] Improper certificate validation allows an attacker to perform MitM attacks (Nintendo, $12,168)

See more writeups on The list of bug bounty writeups.

Tools

- WhiteChocolateMacademiaNut & Intro: Interact with Chromium-based browsers' debug port to view open tabs, installed extensions, and cookies
- Python2Intruder: Pythonize Intruder Payload
- JupyterPen: A Repository dedicated to creating modular and automated penetration testing frameworks utilizing Jupyter Notebooks
- Lazy-FuzzZ: Wrapper around ffuf
- Fast security scanners/checks: Dockerized tools for various Web security tests
- fridroid-unpacker: Defeat Java packers via Frida instrumentation
- js-x-ray: JavaScript & Node.js open-source SAST scanner. A static analyser for detecting most common malicious patterns.
- dmut: A tool to perform permutations, mutations and alteration of subdomains in golang
- Emba: Analyzer for Linux-based firmware of embedded devices
- Fortiscan: A high performance FortiGate SSL-VPN vulnerability scanning and exploitation tool.
- GRecon: Python tool that automates the process of Google Based Recon AKA Google Dorking
- deepce: Docker Enumeration, Escalation of Privileges and Container Escapes
- Go365: An Office365 User Attack Tool
- PrettyRECON & Intro: Commercial recon tool with GUI

Tools updates

- BBRF now has a Web interface (bbrf.me) for visualizing your data
- ZAP 10th Birthday Release!!!
- Param Miner has a new "Guess everything!" option
- Burp Suite Professional – evolving the future of web security testing

Misc. pentest & bug bounty resources

- OWASP TimeGap Theory Handbook, OWASP TimeGap Theory & Walkthrough video
- Bash-Oneliner
- SharpCollection: Nightly builds of common C# offensive tools, fresh from their respective master branches built and released in a CDI fashion using Azure DevOps release pipelines.
- Online Operations Security (OpSec)

Challenges

- HackerOne's 12 Days of Hacky Holidays
- Project Apollo-WAF challenge game
- GeoGuesser & GeoTips

Articles

- Cross Layer Attacks and How to Use Them (for DNS Cache Poisoning, Device Tracking and More) & TL;DR
- How we defeated libModSecurity aka ModSecurity
- Alibaba Cloud Cross Account Trust: The Confused Deputy Problem
- Domestic IoT Nightmares: Smart Doorbells
- RFID Proximity Cloning Attacks

Bug bounty & Pentest news

- Google: Announcing Bonus Rewards for V8 Exploits
- Increased bounty rewards for the GitHub Security Lab community!
- HackerOne Policies Update
- Put Another 'x' On The Calendar: Researcher Availability Now Live!

- Offensive Security Launches Bounty Program for User-Generated Machines

Non technical

- How To React To “It’s Only A Test Server” In BBP
- The “rm -rf *” Story – Insights
- Hacker Spotlight: Interview With Benteveo
- Psychology of Remote Work
- Whose Life Are You Living?
- We’re No Strangers to Bugs
- This is how XSS used to work 5000 years ago…

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 12/13/2020 to 12/20/2020.