Bug Bytes #3

BY INTIGRITI · JANUARY 29, 2019 · 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-3

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series are curated by Mariem, better known as PentesterLand. Every week, she keeps us updated with a comprehensive list of all write-ups, tools, tutorials and resources we should not have missed. You can sign up for the newsletter here.

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week. This issue covers the week from 18 to 25 of January.

Our favorite 5 hacking items

1. Article of the week

> A More Advanced Recon Automation #1 (Subdomains)

If you want to automate some of your recon tasks but don't know where to start, this is an excellent beginning.
A recon workflow chart is given as an example. This is the first article of a series. It explains how to automate subdomains enumeration using a Bash script, and includes commands, tools plus tips like how to check for wildcard resolution (i.e. false positive subdomains).
Looking forward to the sequel(s)!

2. Writeup of the week

> How I abused 2FA to maintain persistence after a password change (Google, Microsoft, Instagram, Cloudflare, etc)

Logic vulnerabilities are my favorite. This one is an authentication flaw found on big sites like Google, Microsoft, Instagram, Cloudflare & many more.
Ironically, it abuses 2FA. The first thing that Luke Berner noticed is that if you request a 2FA code and change your password, the 2FA code remains valid for 20 minutes. And you can make it valid for a longer period of time by waiting indefinitely in the 2FA input page.
From there he concluded with this attack scenario:

- The attacker compromises someone's account, enables 2FA, requests a 2FA code, stays on the 2FA page, then disables 2FA
- The victim changes his/her password to get back control of the account
- The attacker is still be able to access the account using the 2FA code, even without knowing the victim's new password!

3. Tool of the week

> Turbo Intruder: **Burp extension link**
> Turbo Intruder: Embracing the billion-request attack: **Article & Video**
> Debug.py: **Example script to help debug/diagnose issues with Turbo Intruder failing to connect**

Turbo Intruder is a new Burp Suite extension for sending large numbers of HTTP requests and analyzing the results. Here are some things to know about it:

- It's open source.
- It's really incredibly fast because it's built on a custom HTTP stack.
- Despite its speed, it has a low risk of causing Denial of Service on the target server. According to @albinowax, "it's certainly possible but the low number of concurrent connections helps avoid this – it tends to just run slowly on struggling websites rather than overwhelming them.
- It doesn't need Burp Suite to run, you can launch it from the command line.
- It can be used for file/directory bruteforce, detecting race conditions or any other attacks that require more speed, duration or complexity that Burp Intruder

4. Conference of the week

> LevelUp 0x03 2019
> **Slides:**
> – Bad API, hAPI Hackers!
> – AEM hacker approaching Adobe Experience Manager webapps in bug bounty programs

Yes! It's that time of the year again. A new LevelUp conference with so many good talks on Web app security, social engineering, API, IoT and mobile security, plus some non technical talks.
A must, especially for bug hunters!

5. Tutorial of the week

> How to add a module to Metasploit from Exploit-DB

Have you ever found an Exploit-DB exploit that you wanted to test and didn't know how to do so? One very easy and quick way to use these exploits is to add them to Metasploit and use them as any other Metasploit module.
This isn't a new trick but it might be very helpful if you're starting out in penetration testing. I remember when I discover this, it was mind-boggling.

Other amazing things we stumbled upon this week

Videos

- XS-Search abusing the Chrome XSS Auditor – filemanager 35c3ctfs
- How to get started in bug bounty (9x pro tips)
- Open Redirects – What can go wrong?

Podcasts

- Darknet diaries Ep 30: Shamoon
- Security Now 698: Which Mobile VPN Client?
- ThugCrowd, Episode 43 @TinkerSec
- 7MS #346: Baby's First Red Team Engagement
- The Many Hats Club Ep. 32, She hacks purple (with Tanya Janca)
- Application Security Podcast: OWASP Glue
- Smashing Security 112: Payroll scams, gold coin heists, web giants spanked
- Ep. 016 – Email fraud, Android apps, Collection #1 and the 10 year challenge [PODCAST]

Conference slides

- Automated Security Analysis AWS Clouds
- Bug Bounties With Bash

Tutorials

Medium to advanced

- Game with content-disposition
- Reverse port forwarding SOCKS proxy via HTTP proxy (part 1)
- Obtaining a *.cloudapp.net domain in 2019
- JWT Attack Walk-Through
- Basic Electron Framework Exploitation
- Code completion for Burp Jython extensions: Develop Burp Extensions in Python with code completion
- Abusing Exchange: One API call away from Domain Admin & PrivExchange

Beginners corner

- Web Application Scanning Automation
- SSRF — Server Side Request Forgery (Types and ways to exploit it) Part-2
- Web Application finger web_app_finger_printing
- Day 22: Upload .htaccess as image to bypass filters
- Wireless Hacking, Part 10: Creating an Evil Twin Wi-Fi AP to Eavesdrop on the Target's Traffic
- Identifying and Cracking Hashes

- Configure Sqlmap for WEB-GUI in Kali Linux
- How I made a programmable hacking USB device to infiltrate PCs?

Writeups

Challenge writeups

- Playing with CloudGoat part 1: hacking AWS EC2 service for privilege escalation, Part 2, Part 3 & Part 4

Pentest & Responsible disclosure writeups

- SSRF's up! Real World Server-Side Request Forgery (SSRF)
- Why you should not have plain numbers as IDs in your database
- PHP CVE-2018-5711 – Hanging Websites by a Harmful GIF
- Intrusion Testing – From Evil Printers to Parent Domain Controllers
- Rooting Nagios Via Outdated Libraries
- Pen-test Challenge
- Remote Code Execution in apt/apt-get
- How to Hack an Expensive Camera and Not Get Killed by Your Wife
- SickSploit – Finding and exploiting open SickChill instances
- Some issues with GitHub Forks

Bug bounty writeups

- Account takeover via open redirect on Uber ($8,000)
- Information disclosure on Twitter ($2,940)
- Authentication/OAuth flaw on Uber ($7,500)
- Domain hijacking on Starbucks ($1,000)
- Blind XSS combined & Unrestricted file upload on AntiHack.me
- SSTI on ERPNext
- CSRF/Oauth flaw on private program
- IDOR/Privilege escalation on private program

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Wpeprivate-config.sh
- Objection: Runtime mobile exploration toolkit, powered by Frida

More tools, if you have time

- bXSSRequest: Literally spray blind xss payloads everywhere/. “A tool that would spray payloads at a list of urls or endpoints in request headers”
- Electronegativity: A tool to identify misconfigurations and security anti-patterns in Electron applications
- Htcap: A web application scanner able to crawl single page application (SPA) in a recursive manner by intercepting ajax calls and DOM changes
- Malice: VirusTotal Wanna Be. “A free open source version of VirusTotal that anyone can use at any scale from an independent researcher to a fortune 500 company “
- Passcreator: Create your own wordlist or passaword list
- Nmap for Go: Idiomatic nmap bindings for go developers
- SSHReverseShell: Full TTY reverse shell over SSH. “tool to automatically drop you into a full TYY shell and implemented secure file transfer over SSH”
- Tiny SHell: SSH-like backdoor with full-pty terminal
- sshtranger_things.py: SSHtranger Things Exploit POC

Misc. pentest & bug bounty resources

- Top 10 web hacking techniques of 2018: Vote before 11 February 2019
- Disclose bug-bounty-list.json & Explanation: Disclose.io project updated with a JSON file containing the details of 771 companies where security researchers can disclose security vulnerabilities (Safe harbor status included)
- 1.6 Billion Passwords in a Single List
- Webauthn.guide
- Secjuice jobs: Infosec Employment Board, 100% Free, No Advertising
- APIsecurity.io Issue 15: Fortnite hack, TLS MITM attacks, SQL injections for NoSQL
- Hak.lnk: Resources For Hackers
- Steganography – A list of useful tools and resources
- Day 26: The Complete List of Windows Post-Exploitation Commands (No Powershell)

Challenges

- WebSploit: All-in-one Kali VM including DVWA, Multidae, Hackazon, WebGoat, Juice-shop & Mutillidae 2

- SQLi Platform: Training for SQL injections

Articles

- Web Application Security & Bug Bounty (Methodology, Reconnaissance, Vulnerabilities, Reporting)
- Getting Started in Bug Bounties
- A Fresh Look On Reverse Proxy Related Attacks
- Basic Electron Framework Exploitation
- Cross Site Cookie Manipulation
- When Everyone's Dog Is Named Fluffy
- Top Findings from Red Team Engagements
- Pushing Left, Like a Boss, Part 5.7 URL Parameters
- Security bugs are fundamentally different than quality bugs
- Should I pentest my cloud infrastructure? RE: Why the heck haven't you done it yet?!
- CVSS: Characterizing and Scoring Vulnerabilities
- What the Fuzz

News

Bug bounty news

- En garde! 'Cyber-war has begun' – and France will hack first, its defence sec declares

> **At the end of February we are going to announce the first bug bounty of the MoD. Ethical hackers were recruited in the cyber operational research [department] and they're going to track down the faults of our system**

Breaches & Vulnerabilities

- South Korean Android delivery apps found to be leaking passwords and financial data
- Critical, Unpatched Cisco Flaw Leaves Small Business Networks Wide Open
- The huge 'Collection #1' data breach is only a small part of much larger hacker dataset: The "Price for access lifetime" is only $45
- Millions of bank loan and mortgage documents have leaked online
- Rogue websites can turn vulnerable browser extensions into back doors

Other

- Google Chromium changes may break ad blockers

- This is amazing and going to lead to a lawsuit
  - Google fined with €50 million ($57 million) by French regulators at CNIL for GDPR breach
  - Google launched a phishing quizz to test if you can identify phishing emails
- ThreatList: Credential-Sniffing Phishing Attacks Erupted in 2018
- DHS Issued Emergency Directive Ordering Federal Agencies To Audit DNS Activity for their Domains
- Unsupervised Learning: No. 161
- Twitter Android Glitch Exposed Private Tweets for Years

Non technical

- How to prevent burnout from taking over your life
- Tips for Creating a Strong Cybersecurity Assessment Report
- Write a Strong Executive Summary for Your Security Assessment Report
- Security Assessment Report as a Critique, Not Criticism
- Day 21: Top 10 Public Speaking Tips
- Hacker Spotlight: Nicole Anderson-Au
- My Path to Security – How Tom Wilhelm Got Into Security
- 5 Tips for an Effective AppSec Testing Strategy

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 11/18/2019 to 01/25/2019.

Curated by Pentester Land & Sponsored by Intigriti