Bug Bytes #206 – Citrix more like Crit-trix amiright?

BY TRAVISINTIGRITI · JULY 5, 2023 · LAST UPDATED ON APRIL 4, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The second series is curated by InsiderPhD. 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 June 26th – July 2nd.

Intigriti News

- An XSS through your User-Agent header a thread
- New Video: JWT Authentication Bypass via jwk Header Injection
- Our June Challenge is over! The explanation

From my notebook

1. Reversing Citrix Gateway for XSS and Advisory: Citrix Gateway Open Redirect and XSS (CVE-2023-24488) – You've likely already seen this as it's hit social media over the weekend but just in case you missed it!
2. Scale Your Cloud Infrastructure (Hosting CTFs) – Really interesting look to what goes into running a CTF event!
3. The Power of Bug Bounty Automation with Nenad Zaric – The founder of Trickest talks about workflows, recon and data for bug bounty hunters!
4. Episode 25: 2xMVH & Multi-million dollar hacker Inhibitor181 – There's some great strategy/how to approach a target information in this episode with Inhibitor181, definitely a must listen!
5. Testing GraphQL APIs | Web Security Academy – Portswigger add some GraphQL labs to their free Web Security Academy

- Bug Bounty Secrets

- 5 Hacking Tools I Can't Live Without
- Hacker101 CTF – Photo Gallery (Medium) – Live Walkthrough
- Road to Most Valuable Hacker and working while travelling the world
- Stealing OAuth Github Tokens with AWS CodeBuild
- Browser Exploitation Framework(BEEF)
- How Hackers Use netsh.exe For Persistence & Code Execution (Sliver C2)
- The most common vulnerabilities found in Bug Bounty! (shorts)
- MOVEit Transfer Exploitation (my API presentation recording)
- Directory Traversal attacks are scary easy
- Finding Your First API Bug (NahamCon 2023)
- HackTheBox – Pollution
- Hack The Box – Celestial (Medium) – Live Walkthrough

- 302-Self-Hosted 4: The Next Level
- Beware ChatGPT curious: Fleece-ware chabot apps.
- The Evolution of Offensive Security: Insights from Dave Mayer
- UPS smishing, ChatGPT 101, and storing secret files
- The Economics Of Cybersecurity
- Rachel Giacobozzi on the Art of Threat Intelligence Storytelling
- Hacking Past and Present: A Conversation with Moses Frost
- NO. 388 — Context Reflections, Critical Thinking, China's Decline, and NFC
- Episode 381 – WTF Reddit, APIs and risk

- Email From Bounty Program About (New Target Added) 4-5 min later => P1 for a Auth Bypass....
- I got lucky and won the first place in Meta Bug Bounty Researcher Conference
- I will be taking part in-person LHE event in Las Vegas for the first time after being unable to attend previous LHEs
- I can't believe people are calling me on Instagram at 2am because they don't like their triage decision.
- The best time to start bug bounty was 10 years ago. The second best time is now.
- I made a simple but super efficient tool to create these kinds of permutations used for fuzzing.

- Beginner
  - Bug Bounty Hunting—Let's Simulate 2FA Bypass Techniques
  - OWASP Broken Access Control
  - A User-Friendly Guide to Subdomain Enumeration for Bug Hunting
  - Discovering Company Admin Panels: Effective Methods for Bug Bounty & Ethical Hacking
  - Byte-Sized OSINT Tip: Trufflehog
  - Byte-Sized OSINT Tip: GitHub
  - Exploit WordPress with python (E-W-L-1)
- Intermediate
  - Automating recon using ChatGPT
  - Bug Bounty Hunter—Understanding SAML vulnerabilities (XSW Attacks)
  - Setup an Android Pen Testing Lab with Frida-Tools, Objection, Frida Server, and Bypass SSL Pinning
  - Mobile app security : Bugs which are actually counted
  - How improper OTP implementation could lead to Account Take Over (Part 4)
  - Unmasking Server IPs Protected by WAF: Unveiling Hidden Information with CloudBunny

- Advanced
  - What is HTTP Parameter Pollution

- Security Research
  - Huobi's Leaky Bucket Risked Massive Crypto Breach
  - Hacking Auto-GPT and escaping its docker container | Positive Security
  - Finding Gadgets for CPU Side-Channels with Static Analysis Tools
  - CVE-2023-26258 – Remote Code Execution in ArcServe UDP Backup – MDSec
  - Why ORMs and Prepared Statements Can't (Always) Win
  - Process Mockingjay: Echoing RWX In Userland To Achieve Code Execution
  - Using an Unimpressive Bug in EDK II to Do Some Fun Exploitation
  - A technical analysis of the SALTWATER backdoor used in Barracuda 0-day vulnerability (CVE-2023-2868) exploitation
  - zCamera, 100M+ installation app, from remote compromise to data leaks
- Bugs
  - A $1,000,000 bounty? The KuCoin User Information Leak
  - How i got more than 100 vulnerabilities in just one site? (zseano-challenge)
  - How did I get 200$ with WordPress vulnerability!!!
  - How i was able to get Account Takeover via Insecure Data Storage and WebView With Exported Activity
  - Inside the Invite Function: Uncovering a Potential Vulnerability of Invite User
  - My First Bug account takeover through OTP bypass
  - CSV Injection
  - How I get 1000$ bounty for Discovering Account Takeover in Android Application
  - Weakness of Integration
  - My First Valid Report and Reward in BugBounty
  - Unveiling Hidden Treasures: How I Earned my First Information Disclosure Bounty Reward
  - How I got my first bug bounty in just 5 minutes

    - How BAC(Broken Access Control) got me a Pre Account Takeover
    - DOS attack possible on Reset 2FA feature
    - [BUG BOUNTY] How I Get 2580$ USD From Blind SQL Injection [Indonesian]
    - Account Takeover: Unraveling IDOR + Stored XSS Flaws in an NFT Marketplace
    - Stored XSS via Exif Data
    - My first two valid and rewarded Web Cache Deceptions, earning $2250
- CTF challenges
    - HTB: Pollution
    - Cracking PicoCTF Challenge: GDB Baby Step 1
    - How To Crack PicoCTF ASCII FTW With Ghidra
    - ParaBank walkthrough

- GitHub – AdvDebug/NoMoreCookies: Browser Protector against various stealers, written in C# & C/C++.
- Frida 16.1.0 Released
- GitHub – mschwager/route-detect: Find authentication (authn) and authorization (authz) security bugs in web application routes.
- GitHub – Anof-cyber/ParaForge: A BurpSuite extension to create a custom word-list of endpoint and parameters for enumeration and fuzzing
- DNS Analyzer – Finding DNS vulnerabilities with Burp Suite
- Bug Bounty Hunting—Some Browser Extensions to Get Started
- Golddigger – Search Files For Gold
- Bropper – An Automatic Blind ROP Exploitation Tool
- Artemis – A Modular Web Reconnaissance Tool And Vulnerability Scanner
- ReconAIzer – A Burp Suite Extension To Add OpenAI (GPT) On Burp And Help You With Your Bug Bounty Recon To Discover Endpoints, Params, URLs, Subdomains And More!
- DCVC2 – A Golang Discord C2 Unlike Any Other

- While testing for CVE-2023-24488 I found various servers behind Akamai and since the original payload gives a Forbidden response I found this bypass
- As recon process I observed few things in dorking site:*.target.*
- I found a really interesting rXSS on a @SynackRedTeam target last night.
- Today I presented at the @SURF_NL Security and Privacy Conference how I hacked the #Zouikwatzeggen.nl app. An app that allows 15k employees to report inappropriate behaviour.
- Create an alias for pbcopy so that you can just use “c” to copy stdout
- File upload tip
- WAF Bypass tip
- MOVEIt Googledork
- Blind XSS in Contact form
- CVE-2023-24488 – Citrix Gateway XSS