Bug Bytes #208 – Burp gets an update, Sharefile gets a CVE and JavaScript files get analysed

BY TRAVISINTIGRITI · JULY 19, 2023 · LAST UPDATED ON MARCH 6, 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 July 10th – July 16th

CLICK HERE TO SUBSCRIBE

Intigriti News

- We've seen how to exploit the jwk and jku parameters already. Today, let's take a look at the kid header!
- Top 4 SQL Injection Cheat-Sheets
- July Challenge ends Tuesday 25th July!
- What's your most commonly found vulnerability type?

From my notebook

1. Improve your API Security Testing with Burp BCheck Scripts
2. Introducing jswzl: In-depth JavaScript analysis for web security testers
3. Exploiting XSS in hidden inputs and meta tags
4. Using MiTMProxy as a scriptable pre-proxy for BurpSuite
5. Encrypted Doesn't Mean Authenticated: ShareFile RCE (CVE-2023-24489)

- Dark Web Dumpster Diving (Hunting Infostealer Malware)

- Lessons Learned From HackerOne's Live Hacking Event (h1-4420)!
- Do You NEED a College Degree to work in Cybersecurity?
- Steganography for Audio: How to Hide Files in Music || Mr Robot
- Portswigger Web Academy – Information Disclosure – Lab Walkthroughs
- Dependency Confusion with AWS CodeArtifact
- Learning sqlmap Pentesting Tool with World of Haiku
- New: HackTheBox Guided Mode!
- YouTubers Being Paid to Spread Malware?
- Portswigger Web Academy – DOM XSS – Lab Walkthroughs
- Should you strive to become self-employed? (shorts)
- Quick ways to send traffic to your proxy to help troubleshoot (shorts)
- What information can be leaked in JS files? (shorts)
- Poppin' Shells | Cyber Fireside Chat with IppSec
- This top bug bounty hunter only works with a single monitor (shorts)
- HackTheBox – Socket
- Solving a REAL investigation using OSINT
- Learning Bug Bounty with Disclosed Reports and Blogs! Where to go!
- 1M Bug Bounty From Saving $100M at risk in KyberSwap Elastic

- HTB BizCTF 2023
  - HTB BizCTF2023 – Looking at Forensics Challenges from BizCTF 2022
  - HTB BizCTF 2023 – Hacking Blue: Blue Teaming & Hacking Workshop
  - HTB BizCTF 2023 – Let's Get Cloud: Cloud Hacking Workshop
  - HTB BizCTF 2023 – Finding Logic Bugs in Your Code
- NahamCon 2023

    - #NahamCon2023: The Power of Shodan: Leveraging Shodan
    - #NahamCon2023: How to Properly Own API's for Your First Valid Submission
- BSides Leeds 2023
    - Uncommon And Advanced Techniques For Account Takeover Attacks by Ayoub Safa
    - JSluice: There's Gold In Them Thar Files by Tomnomnom
    - Red Team Keynote by Holly-Grace Williams
    - Red Red Whine by Dan Cannon
    - Evasion On Aisle Five: From Bacon To Beacon by Brad Storan
    - Social Engineering The Kill Chain by Tom Harrison
    - Whose Input Is It Anyways? by Rael Sasiak-Rushby
    - Fantastic Cloud Security Mistakes by Sarah Young
    - Hackanory: The Power Of Stories by Janette Bonar Law
    - Five Days, One Red Team, A Beach Like No Other: The Bank Job by Alex Martin
    - Being Right Is Just The Beginning (A Talk Very Much Not About Politics) by Leigh Hal
    - The NSM Ouroboros: Embracing The Endless Cycle Of Network Security
- SleuthCon
    - SLEUTHCON 2023 – Certified Bad: One malware, Two years of Certificates.
    - SLEUTHCON 2023 – Mapping the Ransomware Payment Ecosystem
    - SLEUTHCON 2023 – Look at this Graph: Prioritizing Initial Access Threats
    - SLEUTHCON 2023 – Exploring Initial Access Methods
    - SLEUTHCON 2023 – Leakonomics: The Supply and Demand of Hacked Data
    - SLEUTHCON 2023 – My 0ktapus Teacher: New Actors, New Problems
    - SLEUTHCON 2023 – Unmasking Venom Spider: The Hunt for the Golden Chickens
    - SLEUTHCON 2023 – Hunting Prolific Access Broker PROPHET SPIDER

- How I Rob Banks: A Journey into the World of Ethical Hacking with Freakyclown
- Episode 27: Top 7 Esoteric Web Vulnerabilities
- AAAAAAAAAAAAAA! You Overflowed My Integer! with George Hughey and Rohit Mothe

- SN 930: Rowhammer Indelible Fingerprinting – MOVEit SQLi flaw, China's OpenKylin v1, Firefox 115, Syncthing
- NO. 389 — The Creativity Friction Coefficient, Lockbit v TSMC, and Detecting Smart Errors
- EP129 How CISO Cloud Dreams and Realities Collide

- Beginner
  - Bypassing File Upload Mechanism with Upload_Bypass
  - Bypassing Door Passwords
  - All about CVE-2023–24488(R-XSS)
  - 10 ways to exploit JSON Web Token (JWT):
  - Deobfuscation for Beginners
  - Mastering Password Reset Functionality: Unveiling Bugs and Security Risks
  - OWASP API Top 10—API Security
  - Insecure Direct Object References (IDOR) Vulnerability
  - What is BOLA – Broken Object Level Authorization
- Intermediate
  - Synced Out: Exploring Client Side Desyncs and Server Side Desync Attacks
  - Game Hacking 101: Unleashing the Power of Memory Manipulation
  - Exploiting Time-Based SQL Injections: Data Exfiltration
  - Exploiting Incorrectly Configured Load Balancer with XSS to Steal Cookies
  - The Hidden Risks of Package Management Systems: Shedding Light on the Dependency Confusion
- Advanced
  - Efficient API Endpoint Organization with Burp Collector
  - Methodology and Mindset for Passing the OSCP
  - Smart Contract Vulnerabilities Audit Checklist 2023
  - Enhancing Malware Detection: Endpoint Detection and Response Solutions with Elastic SIEM

- Security Research
  - Encrypted Doesn't Mean Authenticated: ShareFile RCE (CVE-2023-24489)
  - MOVEit Hacks: Stories and lessons learned
  - How FBI hackers or Forensics Team identify fake Images
  - Beyond the Marketing: Assessing Anti-Bot Platforms through a Hacker's Lens
  - The Measure and Resilience of Weaponized Exploit Methods for Linux
  - Security Advisory: SonicWall Vulnerabilities
  - Unveiling the Secrets: LSASS Memory Dump Parsing
  - Uncovering weaknesses in Apple macOS and VMWare vCenter: 12 vulnerabilities in RPC implementation
  - Demo: Brute-forcing a macOS user's real name from a browser using mDNS
  - r-tec Blog | Resource Based Constrained Delegation
  - CVE-2023-36884 MS Office Zero-Day Vulnerability Exploited For Espionage – Detection and Mitigation – FourCore
  - Bee-yond Capacity: Unauthenticated RCE in Extreme Networks/Aerohive Wireless APs – CVE-2023-35803
  - Delegate call bug in ink! | CoinFabrik Blog
  - Shielder – AWS CodeBuild + S3 == Privilege Escalation
  - Critical Foswiki Vulnerablities: A Logic Error Turned Remote Code Execution | usd HeroLab
- Bugs
  - Unveiling Access Control Flaws: How a Viewer Became an Editor
  - Unexpected Zero in MySQL Injection
  - How I Found a Bug under 3 mins , that could risk the reputation of an entire organisation !
  - How I hacked CTX and PHPass Modules
  - How I got Two RCE at EPAM-Bounty Program
  - What is Force sending ether in smart contracts security?!
  - Bug Bounty Hunter—When CORS is not Configured Correctly / JSONP Attack
  - Reverse shell to your Amazon AWS EC2 instance as 'root' or 'Administrator' by injecting user-data

    - Account takeover through Response Manipulation
    - Let’s Go For Whole Company
    - Unveiling Vulnerabilities: How I Earned My First Bounty
    - Exploits Data Breach in (VoIP)Voice Over IP Systems
    - XSS in Host Header
    - Real Site that have IDOR Vulnerability with Referer Header
    - RCE(Remote Code Execution) on https://www.idfcbank.com
    - Critical Code dump from exposed .git folder
    - Decoding Puzzled XSS: Unveiling the Hidden Vulnerability
- CTF challenges
    - Solving Kioptrix Level 1 Capture the Flag (CTF)
    - HTB: Socket
    - Flagging Flaws: Micro-CMS v1
    - TryHackMe – Snapped Phish-ing Line
    - Hack-The-Box SAU [easy

- Introducing OSINT Template Engine: An open source OSINT Tool.
- Sysreptor – Fully Customisable, Offensive Security Reporting Tool Designed For Pentesters, Red Teamers And Other Security-Related People Alike
- ZeusCloud – Open Source Cloud Security
- Mantra – A Tool Used To Hunt Down API Key Leaks In JS Files And Pages
- ZephrFish/PotFileUtils
- FourCoreLabs/LolDriverScan
- IAMActionHunter: Query AWS IAM permission policies with ease
- CSTC, Modular HTTP Manipulator
- GitHub – ldpreload/BlackLotus: BlackLotus UEFI Windows Bootkit
- Bringing Monsoon to the Next Level

- CeWL – Custom Word List Generator.
- detectify-cves – Find CVEs that don't have a Detectify modules.
- SSRFPwned – Checks for SSRF using custom payloads after fetching URLs from sources & applying complex patterns.

- Synack Red Team Tip: Analytics On Aged Targets
- add for your wordlist
- List the associated CIDR ranges of a domain that are owned by the same organisation with haktrails associatedips!
- You can do so much with the Burp Piper extension: Why not send a JS file straight to the new JSluice tool using Piper extension and a small bit of bash script?...
- POST HTTP request possible with any non-existent path after "/console/" (e.g., /console/any/non-existent/path/xyz.html)
- In Safari, "new URL('javascript://test.com/%0aalert(1)').hostname" will be "test[.]com" (no [] obvi). This can be used to bypass hostname checks and execute valid JS.
- Are you a web tester who specializes in blind or out-of-band vulns?