Bug Bytes #212 – XSS Payloads, IDOR prediction and Cloud Security

BY TRAVISINTIGRITI · SEPTEMBER 27, 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 September 18th to September 24th

Intigriti News

- It's CHALLENGE O'CLOCK!
- XXE! Automate or search for it manually
- Exploiting SQL Injection vulnerabilities!

From my notebook

1. Hacker Tweets Explained
2. Tokyo Hacking & Interview with 0xLupin (Ep. 37)
3. IDOR – how to predict an identifier? Bug bounty case study
4. 22.6k+ GitHub Stars Note-Taking App Hit by XSS Vulnerability
5. Build It Before Breaking It !!

- India hacks Pakistani websites post-terrorist attack
- How is cloud pentesting different to config review? (shorts)
- How to Look For Virtual Hosts // How To Bug Bounty
- Data Security RoadMap in 2023
- Application Security vs Cloud Security (shorts)

- Michael Taggart's Journey in Education and Information Security
- GCP Service Account explained! (shorts)
- Authentication Vulnerabilities – Lab #10 Offline password cracking | Short Version
- I Explored Ransomware Cybercrime on the Dark Web
- How to Stop an Army of 14 Million Zombie Computers Darknet Diaries Ep. 94: Mariposa Botnet
- Hacking a vice presidential Yahoo account (shorts)
- Which Visual Studio Code Extensions Can Be Hacked?
- Cloud Pentesting: AWS vs GCP (shorts)
- Run ANY Linux Program In Memory
- Automated Password Hacking (for the lazy hacker)
- Directory Traversal / File Read Into Zip with Python [HackTheBox Snoopy]
- HackTheBox – Snoopy
- How "Mimikatz" works (shorts)
- Tesla insiders leaked tons of data! #shorts #cybersecurity #infosec (shorts)
- UK changing laws to stop security patches to software to make spying easier! #cybersecurity #privacy(shorts)
- Start doing cloud pentesting in GCP? (shorts)
- Do not forget about this attack scenario #bugbounty #bugbountytips #bugbountyhunter (shorts)

- Sherrod DeGrippo on Why She Loves Cyber Crime
- Risky Business #722 — Microsoft embraces Zero Trust… Authentication?
- SN 940: When Hashes Collide – Secure-wipe best practices, browser identity segregation, bye bye Twitter (X)
- Episode 393 – Can you secure something you don't own?

- Beginner
  - Unmasking Directory Traversal: Navigating Vulnerabilities in Web Applications
  - Guarding the Cosmos: The Dark Secrets of Your WordPress `wp-config.php` File
  - Bruteforcing Files and Directories is Easy... Right?
  - Extracting Sensitive Data from HTML and JS Files.
  - [CORS] Easy peasy lemon squeezy
  - Race Condition Vulnerabilities: A Hands-On Primer—Part 1
- Intermediate
  - Injecting Danger: Understanding Server-Side Template Exploits
  - The Introduction to AXIOM
  - The Ultimate SQLmap Tutorial: Master SQL Injection and Vulnerability Assessment!
  - Automating Reconnaissance with Sling Shot R3con—powered by project Discovery tools
  - Mastering Reconnaissance with Project Discovery
  - Cloud Security: Protecting Your Digital Oasis in the Cloud
  - Behind the Hack: The Mechanics of SQL Injection Attacks
- Advanced
  - How a Simple Spreadsheet Can Hack Your Computer | CSV Injection
  - How to use Burp Suite Like a PRO?
  - Ethical Hacker's Passive Reconnaissance Toolkit
  - Find Bugs While Sleeping ? Get Phone Notifications When A Bug Is Found
  - Understanding CVE-2023–24329 -Python urlparse Function
  - New ways to inject system CA certificates in Android 14

- Security Research
  - Exploit Analysis: Request-Baskets v1.2.1 Server-side Request Forgery (SSRF)
  - CVE-2023–39612: CSP bypasss + XSS to achieve Admin Account Takeover + Remote Command Execution
  - Defeating Visual Studio Code embedded reverse shell
  - Critical DICOM Server Misconfigurations Lead to Exposure of 1.6M Medical Records
  - The WebP 0day
  - Multiple Memory Corruption Vulnerabilities
  - LUCR-3: Scattered Spider Getting SaaS-y in the Cloud
  - The indomitable maintainer spirit versus the indifferent cruelty of JavaScript
  - Writing API exploits using Postman Flows
  - Wind River VxWorks tarExtract directory traversal vulnerability
  - Fileless Remote Code Execution on Juniper Firewalls – Blog
  - Account Takeover in Canvas Apps served in Comet due to failure in Cross-Window-Message Origin validation
  - I hacked macOS! (CVE-2022-32947)
- Bugs
  - Reverse Search IDOR approach to Exposure of all Organizational Sensitive Information.
  - $1,250 worth of Host Header Injection
  - Csrf with content type change.
  - Discovering 7 Open Redirect Bypasses and 3 XSS Bypasses Within a Single Program
  - Cross-site Scripting (XSS) On Small Crm Portal CVE-2023–43331
  - Subdomain Takeover
  - How I Earned My Place Among Ferrari's Elite-16 in the Hall of Fame
  - Broken access control (username or email enumeration)
  - Uncovering a Critical Vulnerability in Samsung Mobile Security: A Bug Bounty Journey
  - My debut with a Critical Bug: How I found my first bug (API misconfiguration)
  - My $1000 Bounty Bug: How I Stopped Companies from Losing Money with an IDOR Flaw
  - Stored XSS in Admin Panel
  - How 2 Cute Bugs offered me a reward of 650€
  - Discovering PII with Google Dorking: My Journey of Finding Vulnerabilities in Government Website
  - Tricky 2FA Bypass Leads to 4 digit Bounty $$$$
  - Unlocking Premium CV Features: My Journey to Downloading CVs for Free
  - How I Got 4 SQLI Vulnerabilities At One Target Manually Using The Repeater Tab

    - OTP Bypass leads to Account Creation
    - Weird LFI and escalating the impact from High to Critical
    - One click Account Takeover & IDOR leaks all user information
    - API Information Disclosure Leading to Admin Account Takeover
    - OTP Bypass via Source Page Inspection
    - How i found an Stored XSS on Google Books
    - No Rate Limit for Forgot Password
    - Privilege Escalation: How I Earned $500 by Discovering the Ability to Delete Documents as a Student
    - Bypassing ML based phishing and spam detection using evasion
    - Webinar Pro or Not: The $500 Access Control Bug
    - Hacking into gRPC-Web
- CTF challenges
    - PatriotCTF 2023-My phone! (Crypto+OSINT)
    - PatriotCTF 2023-Capybara (Forensics) & what is Morse Code?
    - HTB: Snoopy
    - OnlyForYou HTB | LFR | RCE | Cypher Injection (Neo4j) graph database | pip3 download code execution

- Haylxon: Take screenshots of urls/websites from terminal new release
- Automating Reconnaissance with Sling Shot R3con—powered by project Discovery tools
- MFMokbel/Crawlector: Crawlector is a threat hunting framework designed for scanning websites for malicious objects.
- HTMLSmuggler – HTML Smuggling Generator And Obfuscator For Your Red Team Operations
- SMShell – Send Commands And Receive Responses Over SMS From Mobile Broadband Capable Computers
- Surf – Escalate Your SSRF Vulnerabilities On Modern Cloud Environments

- Mastering BTL1: Journey, Tips, and Insights for Cyber Defenders
- that was very quick and amazing LFI
- Good morning! I've been using this payload for over a year to discover XSS via open redirect
- DB credentials are stored in the file