Bug Bytes #215 – Hackers in Lisbon, AI bug bounty and is this the end?

BY TRAVISINTIGRITI · OCTOBER 25, 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 October 15th to October 22nd

Intigriti News

- Attention Belgium! Join us at our Open Port event on 2nd November!
- Another code review challenge!
- This is how 100 elite hackers look like after smashing @IntelSecurity's live hacking event with @intigriti. Who would love to attend our next LHE?
- My friend just finished his first year in CS and made his very first calculator in PHP!
- Lots of happy faces at @IntelSecurity's #KnightsOfElektron live hacking event
- Here are 3 ways to find hidden parameters on your bug bounty target

From my notebook

1. IS THIS THE END? – STÖK says good bye to bug bounty content creation and I'm sure you'll all join us in wishing him well
2. Why Governments Love to Buy the Bugs in Your Favorite Apps Darknet Diaries Ep. 98: Zero Day Brokers – The dark side of bug bounty hunting?
3. The Circle of Unfixable Security Issues – Why don't we fix everything?
4. $0 $1,000/Month With Bug Bounties – If NahamSec talks about his approach to bug hunting
5. Microsoft's AI Bug Bounty Program: A Step Forward in AI Security – Microsoft starts a new AI bug bounty program

- I Started A Home Lab! (Automation Update)
- Two casinos hacked, one paid the ransom, one didn't. Who was right?!
- HackTheBox – Jupiter
- Signal Did NOT Get Hacked
- Learn Python in Under 30 Minutes
- AI and hacking – opportunities and threats – Joseph "rez0" Thacker
- They Made QR Codes LONGER?!?
- Cloud pentesting lab and walkthrough | cloudfoxable
- AWS Certifications for Cloud Security Engineers
- Hacktivism Erupts in Response to Israel-Hamas Conflict & more

- InfoSec Pat discusses Content Creation and Cybersecurity Careers
- From NSA to CISO: A Conversation with Ira Winkler
- Scoring cybersecurity in the NFL.
- BlueHat Oct 23 Day 1 Keynote: John Lambert
- SN 944: Abusing HTTP/2 Rapid Reset – Passkeys, ValiDrive follow-up, 2FA apps, pre-release Spinrite
- Should You Pay Ransomware Attackers? A Game Theory Approach
- 91: The Barcode with Paul V. McEnroe
- UL NO. 403: Signal Investigates Rumored Zero-Day Bug, AI Predicts New COVID-19 Strains, Dwindling US-China Scientific Collaboration
- EP143 Cloud Security Remediation: The Biggest Headache?
- Educating the Next Cybersecurity Generation with Tib3rius
- Episode 397 – The curl and glibc vulnerabilities
- Mini Masterclass: Attack Vector Ideation (Ep. 41)

- Beginner
  - How I Ethically Hacked a WordPress Site in 10 Minutes Using WPScan
  - Mastering WordPress Penetration Testing: A Step-by-Step Guide
  - Stored XSS – Simple Download Monitor 3.9.19 (WordPress Plugin)
  - File Shared < 1.6.48 (WordPress Plugin) — Sensitive Data Exposure Mysql version, enviroment, ++;
  - Broken Object Level Authorization Vs. Broken Functionality Level Authorization | API Hacking
- Intermediate
  - Automating Bug Bounty Recon: Creating the Flask API
  - Hidden Treasures: Unveiling the 403 Bypass Bug Bounty Adventure

- Security Research
  - Confluence CVE-2023–22515
  - The Anti-Recon Recon Club (using ReconFTW)
  - A $1,000,000 bounty? The KuCoin User Information Leak
  - Java Deserialization Vulnerability Still Alive
  - Abusing gdb Features for Data Ingress & Egress
  - [Crypto] SSL/TLS, part 2: Toy TLS 1.2 client with TLS_DHE_RSA ciphersuites support.
  - Microsoft Account's OAuth tokens leaking via open redirect in Harvest App"
  - Exploiting Zenbleed from Chrome
  - Multiple North Korean threat actors exploiting the TeamCity CVE-2023-42793 vulnerability
  - Persistent cross-site scripting vulnerabilities in Liferay Portal
  - The single-packet attack: making remote race-conditions 'local'
  - Getting RCE in Chrome with incomplete object initialization in the Maglev compiler

    - Synology NAS DSM Account Takeover: When Random is not Secure
    - Finding a POP chain on a common Symfony bundle : part 2
    - Data Exposure and ServiceNow: The Elephant in the ITSM Room
    - Hiding Web2 Malicious Code in Web3 Smart Contracts
    - curl – SOCKS5 heap buffer overflow – CVE-2023-38545
- Bugs
    - Bypassing 2FA for Password Reset : By Request Manipulation 500$ Bug
    - Full account takeover—Bug bounty
    - Html Injection & xss in support chat
    - The Hidden Weakness Of Improper Access Control
    - How My Report Secured A Spot?: My United Nations Hall of Fame Journey.
    - How I saved 2.8 Million PII of Indian citizens from hackers.
    - Account Takeover via Business Logic
    - From User to Admin: Gaining Admin Panel Access
    - IDOR leads to Account Takeover with JWT Week Screet
    - Bypassing AWS WAF—A story of Stored XSS (P2)
    - Bonus—My $3000 request smuggling report
    - Android Game Hacking
    - I hacked the Dutch Government and all I got was....
    - How I Discovered an Exposed API Access Token in a JavaScript File
    - Interesting email HTML injection | Easiest $$$ bounty
    - PhantomJs Exploitation – Pdf Export
    - Apache HTTP Server /server-status information disclosure
    - How I earned $9000 with Privilege
- CTF challenges
    - HTB: Jupiter
    - Shop smart, Shop S-S-T-I Mart! Halloween CTF.
    - NahamCon CTF23
    - Building Micro-CGC Events – Art of The Flag

- Kanha v0.1.1 has been released
- Gcp_Scanner – A Comprehensive Scanner For Google Cloud
- JSpector – A Simple Burp Suite Extension To Crawl JavaScript (JS) Files In Passive Mode And Display The Results Directly On The Issues
- HBSQLI – Automated Tool For Testing Header Based Blind SQL Injection
- GitHub – n0mi1k/subby: An uber fast and simple subdomain enumeration tool using DNS and web requests with support for detecting wildcard DNS records.
- lutzenfried/Delegate: Tool to perform GCP Domain Wide Delegation abuse and access Gmail and Drive data
- sterrasec/dummy: Generator of static files for testing file upload. It can generate the png file of any number of bytes!
- ServiceNow Widget-Simple-List Misconfiguration Scanner
- So you think you know web app hacking? Challenge yourself with 55 (and counting) questions that go beyond the basics

- Bypass Reflect XSS working on ASPNET Generic Microsoft WAF (detected by AFW00F)
- New update: Output of Cookie and X-User-Token
- cloudflare-origin-ip by @gwendallecoguic Via comparing HTTP responses and CloudFlair by @christophetd Uses Internet-wide scan data from @censysio
- Authentication Bypass
- wp-config.php -> 403 forbidden
- /docker-compose.yml

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com