Bug Bytes #156 – Python NaN Injection, Null-byte based file inclusion & $100K for hacking the Apple webcam

BY ANNA HAMMOND · JANUARY 26, 2022 · LAST UPDATED ON MARCH 6, 2025

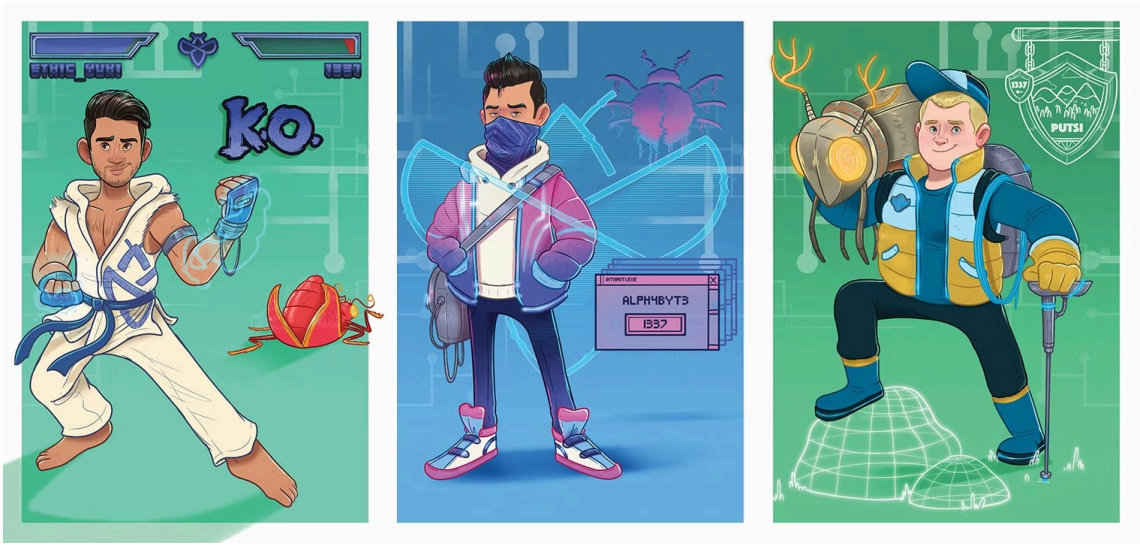
Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series is curated by Mariem, better known as **PentesterLand.** Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

CLICK HERE TO SUBSCRIBE

This issue covers the week from January 17 to 24, 2022.

Intigriti news

New responsible disclosure program



Congratulations @3th1c_yuk1, @alph4byt3 and @putsi for being Top 3 in the Intigriti Q1 2021 leaderboard!

NEWS | 19 January 2022 | Brussels | Informatics

European Commission's Open Source Programme Office starts bug bounties

Awards of up to EUR 5000 are available for finding security vulnerabilities in LibreOffice, LEOS, Mastodon, Odoo and CryptPad, open source solutions used by public services across the European Union. There is a 20% bonus for providing a code fix for the bugs they discover.

European Commission's Open Source Programme Office starts bug bounties

Our favorite 5 hacking items

1. Vulnerability of the week

Python NaN Injection, Repo & Decipher Podcast: Robert Hansen Returns

It's strange that this new Python vulnerability class went unnoticed. It may be complex and difficult to identify but it is also novel and an interesting area to explore.
For the anecdote, Robert Hansen / @RSnake is one of the first hackers I followed when I started in 2012. Among other things, he created the old ha.ckers.org XSS Cheat Sheet on which the OWASP XSS Filter Evasion Cheat Sheet was based.

2. Writeups of the week

Hacking the Apple Webcam (again) (Apple, $100,500)
CVE-2021-45467: CWP CentOS Web Panel – preauth RCE
The Tale of a Click leading to RCE

Ryan Pickren discovered a UXSS and other issues on Safari that could give an attacker access to victims' camera and any website they visited, bypassing Gatekeeper.

@0xLupin's writeup is an amazing red teaming story that demonstrates how SSRF can be upgraded to RCE in a real-world (but CTF-like) scenario.

The third writeup is about a curious RCE via local file write on CentOS Web Panel.
In @PaulosYibelo's words, `.%00./` is the new `..;/`.

3. Tutorials of the week

Creating easy proof-of-concept scripts with Python and Curl.
Debugging a Java application with decompiled source code

The first tutorial shows how to use curl.se/h2c/ and curl.trillworks.com to easily convert HTTP requests (e.g. copied from Burp) to curl commands, and curl commands to Python or other languages (PHP,

JavaScript, Go, Rust, JSON and many others).
It can be handy if you are short on time or struggle with creating custom scripts/curl commands.

The second tutorial is about dynamic analysis of Java apps using IntelliJ IDEA. If you perform static analysis of Java apps and find it difficult to trace sinks and sources, this debugging method by @dozernz can make the process much easier.

4. Resource of the week

Free SQL injection section of Bug Bounty – An Advanced Guide to Finding Good Bugs

@HusseiN98D gave an advanced bug bounty workshop at THREAT CON and published the recording on Udemy.
It is not free ($49.99 until the end of the week, then $139.99) but the SQL injection section is. It is more than one hour on SQL injection with a couple of advanced bug bounty use cases that may teach you some useful tricks.

Note that it is extremely rare for me to feature paid content in this newsletter. The only reason I am making this exception is its quality and the juicy hour long free video it includes.

5. Tip of the week

A tip for exploiting tricky blind SQL injections

If you find a blind SQL injection and have a hard time exfiltrating data, try @mcipekci's technique (adapted to your context of course) to force the app to return an error.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Finding security vulnerabilities with GitHub's new code search
- RACE CONDITION BUGS explained with test cases
- Bug Bounty Recap January 13-19
- Easy IDOR hunting with Autorize? (GIVEAWAY)
- Web App Penetration Testing – Course Introduction & Introduction To HTTP
- DEP Bypass using ROP Chains & Blog post
- Injecting code into any Homebrew Cask by attacking GitHub Actions script

Podcasts

- Find Some Way to Like Reporting with BB King
- Pentesters' Perspective: Log4Shell

Tutorials

- Demystifying JA3: One Handshake at a Time & Other ways a site can block Burp traffic
- An attempt to understand container runtime
- Art of Creating Machines
- Vulnerable AWS Lambda function – Initial access in cloud attacks
- A Beginner's guide into Router Hacking and Firmware Emulation
- WMI for Script Kiddies

Writeups

Challenge writeups

- XXE to SSH access?! – Mustacchio by @Try Hack Me
- HackTheBox – Forge
- Web Shell via Polyglot File Upload!
- Tiki Walkthrough with S1REN
- Some SANS Holiday Hack 2021 Solutions

Pentest writeups

- Log4j RCE When Remote Class File Won't Load (Newer Java Versions)

Responsible(ish) disclosure writeups

- Solarwinds Web Help Desk: When the Helpdesk is too Helpful #Web #CodeReview
- Blind Server-Side Request Forgery & Unsafe Object Deserialization in Html2Pdf <= 5.2.3 #Web #CodeReview
- Cisco Prime 3.9.1 – RCE #Web #SNMP
- Paranoids' Vulnerability Research: PrinterLogic Issues Security Alert #Printer

Known vulnerabilities

- ZohOwned :: A Critical Authentication Bypass on Zoho ManageEngine Desktop Central (Zoho)

- The Cat Escaped from the Chrome Sandbox #Browser #MemoryCorruption

Bug bounty writeups

- HOW I hacked thousand of subdomains
- Finding vulnerabilities in Swiss Post's future e-voting system – Part 1 (Swiss Post)
- CVE-2022-21661: Exposing Database Info Via WordPress SQL Injection (WordPress)
- Zooming in on Zero-click Exploits (Zoom)

See more writeups on The list of bug bounty writeups.

Tools

- ripgen: Rust-based high performance domain permutation generator
- ShadowClone: Allows you to distribute your long running tasks dynamically across thousands of serverless functions
- jo: JSON output from a shell
- Chrome Bandit: Programmatically extract saved passwords from Google Chrome
- TREVORproxy, TREVORspray 2.0 & Intro: Increasing the speed and effectiveness of password sprays

Tips & Tweets

- Search for credentials in the public Postman API network
- Gnarly pentest stories
- java.net.URL DNS leak
- Log4j / log4shell explained for the rest of us

Misc. pentest & bug bounty resources

- New InternetDB API by Shodan that lets you do fast IP lookups for free without an API key
- horrifying-pdf-experiments
- PinataHub & Intro
- HOUDINI: Hundreds of Offensive and Useful Docker Images for Network Intrusion
- OWASP Mobile Security Testing Guide v1.4.0

Articles

- Customising Blacklist3r for OWIN OAuth Access Tokens

- Captain Hook – How (Not) To Look For Vulnerabilities In Java Applications
- The best free, open-source supply-chain security tool? The lockfile
- Adding DCSync Permissions from Linux
- Capturing RDP NetNTLMv2 Hashes (even if NLA is enforced)
- SeeYouCM-Thief: Exploiting Common Misconfigurations In Cisco Phone Systems & SeeYouCM Thief

Challenges

- Apache APISIX challenge from Real World CTF
- VulnLab
- Hacktoria: Monthly story-based OSINT CTF

Bug bounty & Pentest news

- Bug bounty
  - European Commission launches new open source software bug bounty program
  - Looking Back At The Zero Day Initiative In 2021
- Cybersecurity
  - The first Dan Kaminsky Fellowship awarded to @jlleitschuh
- Jobs
  - Assetnote are looking for a full time security researcher
- Upcoming events
  - IWCon 2022 (February 26-27)
  - Bounty Hunters Hackathon (Deadline is February 20)
  - HTB giveaway (January 24 to February 4)
- Tool updates
  - A modern, elastic design for Burp Collaborator server
  - Amass v3.16.0
  - Interactsh v1.0.0
  - Major release for CrackMapExec (v5.2.2)

Non technical

- Build a stronger cybersecurity team through diversity and training
- What's In A Social Engineering Toolkit?

- Hacker Education Trends

REQUEST A DEMO	VISIT THE WEBSITE	GET IN TOUCH
intigriti.com/demo	intigriti.com	hello@intigriti.com