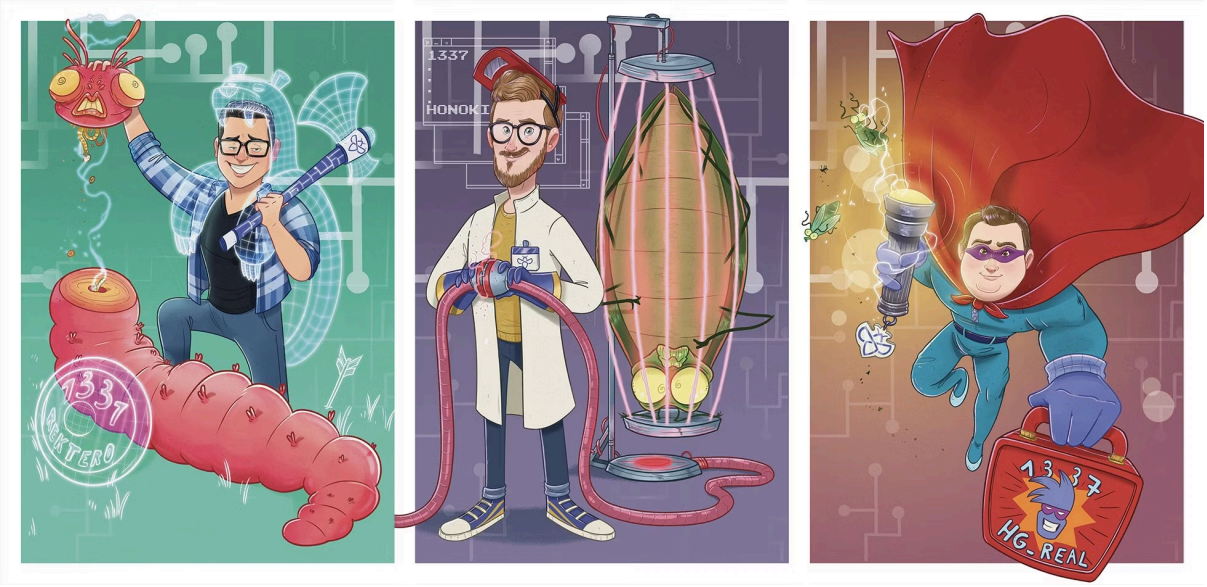
Bug Bytes #96 – AI applied to bug bounty, Burp Collaborator notifications & @zseano's BugBountyHunter

BY ANNA HAMMOND · NOVEMBER 11, 2020 · 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.

This issue covers the week from 01 to 08 of November.

Intigriti News



[Congratulations to our new Intigriti 1337 members!]

Our favorite 5 hacking items

1. Tips of the week

> “Not particularly restricted to browser based features. I've had success in custom apps from Electron to Qt based with the following:
>
> custom-app://views/layout.html
>
> to
>
> custom-app://views/../../../../secret.txt#bugbounty #bugbountytip #bugbountytips #security #infosec https://t.co/WCuti9ZXoE
>
> — Dominik Penner (@zer0pwn) November 8, 2020”

> “Great #BugBountyTip by @JR0ch17: before copy pasting blind XSS payloads, think about the context they might render in! Use blind template injection payloads to increase your chances of success! #HackWithIntigriti #BugBountyTips pic.twitter.com/AyrNYtPpII
>
> — Intigriti (@intigriti) November 3, 2020”

These are two things probably not a lot of people are testing for: Blind XSS in JavaScript payloads and using “view-source” to bypass LFI blacklists. Fantastic tips by @JR0ch17 and @HusseiN98D!

2. Writeups of the week

Facebook DOM Based XSS using postMessage (Facebook, $25,000)
Github: Widespread injection vulnerabilities in Actions (Github)

The first post by @samm0uda is about a beautiful bug chain resulting in DOM XSS on Facebook. A must read if you’re interested in XSS, postMessage vulnerabilities or participating in BountyCon.
The second bug report is the reason why GitHub has deprecated “set-env” and “add-path” commands in GitHub Actions. @_fel1x found that they made Actions vulnerable to command injection attacks.

If you just want a high-level view of these complex findings, I recommend The Daily Swig’s coverage of both the Facebook bug and the GitHub Actions bug.

3. Video of the week

Hacking with OpenAI GPT-3 | Hacking Without Humans

@ngalongc and @filedescriptor experiment with OpenAI GPT-3 and share ideas on how to leverage it for bug hunting. So, this is about using AI to write bug reports, spot false positive in tools output and even detect logic flaws. An interesting glimpse into the future of bug hunting.

4. Tool of the week

Notify

Notify is @pdiscoveryio’s latest Go tool. Its main purpose is to pull results from Burp Collaborator instances and send notifications to Slack, Discord or the CLI. It also support piping with any other tools to notify you of their output too. A pretty handy utility!

5. Resource of the week

BugBountyHunter, Intro & A look inside BugBountyHunter's member section

After @zseano brought down his excellent BugBountyNotes site, many of us were waiting for his promised new platform. Here it is finally!

BugBountyHunter.com is a Web security training site. The paid membership gives access to @zseano's hacking methodology ebook, a private vulnerable Web application and reports triage. The free area includes challenges, guides, and an intentionally vulnerable Web application that sometimes has hidden flags to get free access to the membership area.

Other amazing things we stumbled upon this week

Videos

- Web Cache Poisoning For Beginners + Giveaway(Closed)
- @ITSecurityguard Talks About Getting Into Bug Bounty, Recon, Automation, Triage, and more!
- 5 Bug Bounty Time Investments
- Zoom – turning on someone's camera using SQL injection vulnerability – Bug Bounty Reports Explained
- How Hacking Actually Looks Like – ALLES! CTF Team in Real Time
- Best Ways To Learn Linux
- Best OS For Hacking?

Podcasts

- Security Now: Google's Root Program – Google One VPN, WordPress Update Fail, Windows 7 0-Day
- The InfoSec & OSINT Show
- Billions of Bitcoins, Zoom Snooping, & Doxing Russian Bears – Wrap Up – SWN #80
- China's Top Hacking Contest, GitHub Actions, & Vulnonym – ASW #129
- Multiple iOS 0-Days, Intel Malware Defense, & Windows 0-Day Under Attack – PSW #673

Webinars & Webcasts

- Using Research To Gain Attack Intelligence
- The Act of Balancing: Burnout in Cybersecurity with Chloé Messdaghi!
- Abusing JWT (JSON Web Tokens) – Sven Morgenroth – PSW #673

Conferences

- 2020 BSides Boston
- SecTor 2020 Keynote: Paula Januszkiewicz – A Hacker's Perspective on Your Infrastructure

Tutorials

Medium to advanced

- Cheating at Online Video Games and What It Can Teach Us About AppSec (Part 1), Part 2 & Part 3
- # { Abusing pipelines to hijack production } # & Part 2
- How to fuzz MySQL looking for weird characters
- Setting up a WireGuard VPN Server Architecture for Internal Network Access
- MalDoc Fu – Some Ideas for Malicious Document Delivery
- Yantra Manav – A wormable SSH bot

Beginners corner

- Using search engines for fun and bounties
- A Guide to make your own Serverless Blind XSS and Blind OOB payload
- Constructing powerful search queries in OSINT investigations

Writeups

Challenge writeups

- Intigriti's November XSS Challenge
- Hack this repository: The EkoParty 2020 GitHub CTF challenges
- Cross-Site Scripting (XSS) All in One: Part 1 & Part 2 (videos)

Pentest writeups

- Alert Function Hijacking
- Re-discovering a JWT Authentication Bypass in ServiceStack
- AggressiveProxy — A tale of two proxies and a sad beacon & AggressiveProxy

Responsible(ish) disclosure writeups

- DISCLOSURE: Unlimited Chase Ultimate Rewards Points #Web
- Code vulnerabilities put health records at risk #Web

- CVE-2020-26886: Local Privilege Escalation using softaculous/bin/soft #LPE
- CVE-2020-16877: Exploiting Microsoft Store Games #Windows #LPE
- TP-Link Takeover with a Flash Drive #Router

Bug bounty writeups

- 1000$ for Open redirect via unknown technique [BugBounty writeup] (GitLab, $1,000)
- From a 500 error to Django admin takeover ($3,000)
- Attack of the clones: Git clients remote code execution (Github)
- SMTP interaction theft via MITM (PortSwigger Web Security, $1,000)
- GitLab-Runner on Windows `DOCKER_AUTH_CONFIG` container host Command Injection (GitLab, $6,500)
- Insufficient Type Check leading to Developer ability to delete Project, Repository, Group, ... (GitLab, $5,000)

See more writeups on The list of bug bounty writeups.

Tools

- LemonBooster-v2: Automation and monitoring tool for bug bounty
- Aura: Python source code auditing and static analysis on a large scale
- MNS (monitor-new-subdomain): Python script to monitor new subdomains
- lorsrf: Python tool that bruteforces hidden parameters to find SSRF vulnerability using GET & POST Methods
- rexsser: Burp extensions to extract keywords from response using regexes & test for reflected XSS on the target scope

Misc. pentest & bug bounty resources

- WebHackersWeapons
- Pi-PwnBox -RogueAP
- Kubernetes Security Demos
- Awesome Penetration Testing
- Infosec Bugbounty AMAs with Calum Boal, Paras Arora & Devansh

Articles

- URL Eccentricities In Java
- The Same-Origin Policy Gone Wild

- How Facebook was used as a proxy by web scraping bots
- Diving Into A Websocket Vulnerability In Apache Tomcat
- Using and detecting C2 printer pivoting

Bug bounty & Pentest news

- Upcoming Google Chrome update will eradicate reverse tabnabbing attacks
- Intigriti's November XSS Challenge winners
- Hackerone Is Excited To Launch Triage Ratings For Customers And Hackers

Non technical

- Hacker Spotlight: Interview With Putsi
- How I Manage Impostor Syndrome, Fear of Failure, and Other Common Programmer Problems
- The future of AppSec and why I joined r2c
- Demand, CyberInsurance, and Automation/AI Are the Future of InfoSec
- A Google a day: OSINT/googling game

Tweeted this week

We created a collection of our favorite pentest & bug bounty related tweets shared this past week. You're welcome to read them directly on Twitter: Tweets from 11/01/2020 to 11/08/2020.