Bug Bytes #170 – Evasive vulnerabilities, Hacking Swagger UI & Reverse engineering REST APIs

BY ANNA HAMMOND · MAY 18, 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 weeks from May 9 to 16.

Intigriti news

Intigriti invites cybersecurity players to join its global Partner Program initiative

Our favorite 5 hacking items

1. Conference of the week

Keynote Day 2 | Hunting Evasive Vulnerabilities: Finding Flaws That Others Miss by James Kettle, Slides

I've been waiting for this talk recording for weeks, even more that @albinowax's previous talks. The reason is that it is not about a single vulnerability, but about broad principles and techniques that @albinowax uses to discover new attack classes and bugs that everyone else misses.
I think we all want to know how he does it, so do not miss this talk if you are interested in Web research.

2. Tool of the week

mitmproxy2swagger

mitmproxy2swagger is a very useful tool for both developers and hackers. It automatically reverse-engineers REST APIs based on traffic captured while browsing an app.
More specifically, it takes a mitmproxy capture or a HAR file (exported from browser DevTools) as input, and returns an OpenAPI 3.0 specification for the REST API.

3. Videos of the week

Bug Bounty Redacted #3: Hacking APIs & XSS, SQLi, WAF Bypass in a regional web application
Q: How to write a BUG BOUNTY report that actually gets paid?
XSSHUNTER by @IAmMandatory (Behind The Tool #2)

I know it is supposed to be just *one* "video of the week", but I want to celebrate three of my favorite shows that are true gifts for bug hunters.

In this Bug Bounty Redacted, @infosec_au covers two bug bounty findings. Although the reports are old, the tips for testing Swagger UIs and regional assets are very relevant today.

@stokfredrik's Bounty Thursday is, as usual, so enjoyable and full of insightful tips, with a focus on reporting this time.

Last but not least, Behind The Tool features @IAmMandatory. If you like XSSHunter, this is a great discussion to know more about its author and the behind the scenes of its creation.

4. Writeups of the week

Multiple bugs chained to takeover Facebook Accounts which uses Gmail. (Meta / Facebook, $44,625)
Hacking Swagger-UI – from XSS to account takeovers (Shopify, Paypal, GitLab, Atlassian, Yahoo, Microsoft, Jamf & others)

@samm0uda's fantastic writeup shows how he chained client-side vulnerabilities to take over Facebook accounts, turning an "intended-by-design XSS in a Facebook sandbox domain" into a $44+ bug bounty.

The other writeup is about a DOM XSS that @kannthu1 found in Swagger UI and reported to several bug bounty programs. This is excellent research and a good resource if you want to learn more about hacking Swagger APIs (after watching Bug Bounty Redacted #3 on the same topic).

5. Challenge / Resource of the week

Gin and Juice Shop: put your scanner to the test

"Gin and Juice Shop" is a new intentionally vulnerable web app by PortSwigger. It is intended to be used to test Burp Scanner. I think it also provides a good training ground to practice manual Web hacking after finishing the other Web Security Academy labs and courses.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Bug Bounty 101: #15 – XXE (External Entities Injection) Basics, #16 – Login Dialogue Bypass via Password Spray / Brute Force Attack & #17: Recon Sub-domains with Intruder for Auth Bypass
- How I found the $1,500 SSRF in Stripe bug bounty program
- OWASP Top 10 in 10 Min! (Kinda)
- They said this doesn't work Hacking networks with VLAN hopping and Python

Podcasts & Audio

- AMA session with Momen Eldawakhly

Webinars

- Cyber Apocalypse CTF 2022 – Intergalactic Chase: Live Hacking Workshops
- Tool Talks: ripgen
- Learning from AWS (Customer) Security Breaches with Rami McCarthy & Slides
- BHIS | How DNS can be abused for Command & Control | Troy Wojewoda

Conferences

- IWCON 2022
  - New2Cyber Summit 2022

Slides & Workshop material

- Black Hats Asia 2022, especially:
  - AutoSpear: Towards Automatically Bypassing and Inspecting Web Application Firewalls

Tutorials

Medium to advanced

- Using Stolen IAM Credentials
- Securing AWS Lambda function URLs
- 1-click RCE in Electron Applications & Electron JS
- LDAPSearch Reference

- Abusing Azure Container Registry Tasks

Beginners corner

- How To Hack Web Applications in 2022: Part 1
- The Linuxless recon for bug bounty beginners who can't code
- Hacking Electron Applications – 0x101 & Content Security Policy for Dummies
- PwnFox – An IDOR Hunter's Best Friend

Writeups

Challenge writeups

- HackTheBox – Fingerprint
- CloudGoat goes Serverless: A walkthrough of Vulnerable Lambda Functions
- PicoCTF 2022 Web, Reverse Engineering, Forensics, Cryptography & Binary Exploitation

Pentest writeups

- Diving Into Pre-created Computer Accounts
- Constrained environment breakout. .NET Assembly exfiltration via Internet Options

Responsible(ish) disclosure writeups

- Ruby on Rails – Possible XSS Vulnerability in ActionView tag helpers (CVE-2022-27777) #Web #CodeReview
- rubygems CVE-2022-29176 explained #Web #CodeReview
- CVE-2022-30525 (FIXED): Zyxel Firewall Unauthenticated Remote Command Injection & Nuclei template #Web
- Exploiting a Use-After-Free for code execution in every version of Python 3 #MemoryCorruption
- Path Traversal Vulnerabilities in Icinga Web & RainLoop Webmail – Emails at Risk due to Code Flaw #Web #CodeReview

Bug bounty writeups

- My New Discovery In Oracle E-Business Login Panel That Allowed To Access For All Employees Information's & In Some cases Passwords At More Than 1000 Companies
- The Underrated Bugs, Clickjacking, CSS Injection, Drag-Drop XSS, Cookie Bomb, Login+Logout CSRF... ($3,850)
- Can analyzing javascript files lead to remote code execution?

- Certifried: Active Directory Domain Privilege Escalation (CVE-2022–26923) (Microsoft) & Free TryHackMe room
- New Wine in Old Bottle – Microsoft Sharepoint Post-Auth Deserialization RCE (CVE-2022-29108) (Microsoft)

See more writeups on The list of bug bounty writeups.

Tools

- pipe-intercept: Intercept Windows Named Pipes communication using Burp or similar HTTP proxy tools
- badkeys: Tool and library to check cryptographic public keys for known vulnerabilities
- Skanuvaty: Dangerously fast DNS/network/port scanner
- Fastsub: A custom built DNS bruteforcer with multi-threading, and handling of bad resolvers

Tips & Tweets

- How to to export nuclei findings as markdown-styled reports
- Forcing nmap to run a script (despite no fingerprint match)
- AWS story of a special security issue
- "Not so private" private Discord servers
- A simple XXE in ArcGIS
- A Practice Target SUPER Thread
- Brief explanation of @hakluke's "useful little hacking tools"

Misc. pentest & bug bounty resources

- Awesome RCE techniques
- AD-Pentesting-Notes
- Container Training & Repo
- @cyb_detective's OSINT repos:
  - code-understanding-tools
  - Awesome Grep
  - APIs for OSINT
  - GREP FOR OSINT
  - Advanced-search-operators-list

Articles

- A Tale Of A Trailing Dot
- The art of vulnerability chaining (PyScript)
- Office365 User Enumeration & o365fedenum
- A new secret stash for “fileless” malware & Why the newly discovered Microsoft Windows ‘fileless’ log exploit is a marvel of stealth

Challenges

- Can you spot the vulnerability?

Bug bounty & Pentest news

- Pentest
  - How a pentester’s attempt to be ‘as realistic as possible’ alarmed cybersecurity firms
  - NIST revamps aging enterprise patch management guidance & NIST refreshes software supply chain risk management guidance
- Cybersecurity
  - Researcher stops REvil ransomware in its tracks with DLL-hijacking exploit
  - Some top 100,000 websites collect everything you type—before you hit submit
- Upcoming events
  - LevelUpX – Salesforce Object Recon by @B3nac (May 20 at 4 PM UTC)
- Tool updates
  - reconFTW v2.3
  - unfurl v0.4.0 (New JSON output option)
  - x8 v3.3.0
  - Burp Sharpener now supports colorization without any additional addon

Non technical

- Guide to the 2022 OSCP Exam on M1 (with Active Directory)