Bug Bytes #117 – Writeups à gogo, Google blind SSRF challenge & InfoSec drama

BY ANNA HAMMOND · APRIL 7, 2021 · 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 March 29 to April 5.

Our favorite 5 hacking items

1. Writeups of the week

Breaking GitHub Private Pages for $35k (GitHub, $35,000)
This Man Thought Opening A TXT File Is Fine, He Thought Wrong. MacOS CVE-2019-8761 (Apple)
Facebook account takeover due to a wide platform bug in ajaxpipe responses (Facebook, $30,000)
I Built a TV That Plays All of Your Private YouTube Videos (Google, $6,000)

The first finding is a cool bug chain by @NotDeGhost that involves XSS, CRLF and Web cache poisoning on GitHub.

The second writeup will forever change what you think about TXT files being harmless. @PaulosYibelo found a way to inject HTML into TXT files that steal local MacOS passwords when opened.

The third writeup is about @Samm0uda finding yet another creative way to pwn Facebook, with an impressive account takeover.

Lastly, @xdavidhu shared an excellent writeup on a CSRF in YouTube for Android TV that made it possible to access anyone's private videos.

2. Challenges of the week

$31,000 Google Cloud blind SSRF + HANDS-ON labs
NodeJS WebSocket SQLi vulnerable WebApp

The first link is actually a video explanation of @david_nechuta's $31k blind SSRF on Google Cloud Monitoring. It also links to a lab by @gregxsunday that recreates the vulnerability. This is an excellent opportunity to not only understand but also practice exploiting a real-world blind SSRF.

The second challenge is a WebSocket Web app vulnerable to blind SQL injection. @rayhan0x01 created it to practice automating SQL injection over WebSockets, and made it public to our great delight.

3. Article of the week

Never a dill moment: Exploiting machine learning pickle files & Fickling

Machine Learning is one of those topics that seem so complex, I don't dare to try and learn how it works let alone how to exploit it. This article makes the topic approachable.

Most Machine Learning models are just Python pickle files under the hood which makes them potentially vulnerable to deserialization. The article explains all that with a bug example found in PyTorch, plus Fickling, a Python pickling decompiler and static analyzer.

4. Tools of the week

COOK
intitools

If you find yourself often tweaking wordlists to change their format, you might like COOK. It's a handy Go tool for quickly generating wordlists following "recipes".

Another cool tool is intitools. @0xJeti created it to monitor his Intigriti activity feed, which you might find useful too. Any new program updates and submission messages are detected and sent as notifications to Slack or Discord.

5. Video of the week

Security YouTuber Drama...

All drama aside, this is the most heartwarming InfoSec video I've ever seen. I'm not gonna say more in case you haven't watched it yet, except that you really need to!

Other amazing things we stumbled upon this week

Videos

- SQL Injection – Lab #5 SQL injection UNION attack, retrieving data from other tables
- Freshdesk Subdomain TKO PoC
- Introduction to Executables | Binary Exploitation 0x00 & Dangerous Functions | Binary Exploitation 0x01
- Attacking Active Directory – Kerberoasting

Podcasts

- DAY[0] Episode 71 – Speculation in Predictive Store Forwarding, Broken Fixes, and Owning Rocket.Chat
- A Spy in Our Pocket – Ubiquity Coverup, Facebook Data Dump, Malicious Call of Duty Cheats
- The InfoSec & OSINT Show 51 – Jim Manico & Developing Securely

Conferences

- Security Weekly Unlocked
- POC 2020 – CodeQL as an auditing oracle – GitHub Security Lab

Tutorials

Medium to advanced

- on ios binary protections
- Why is your Meterpreter session dying? Try these fixes..
- HowTo: intercept mutually-authenticated TLS communications of a Java thick client
- http2smugl: HTTP2 request smuggling security testing tool
- Kubernetes Namespaces Isolation – What It Is, What It Isn't, Life, Universe And Everything

Beginners corner

- Microsoft Teams Proxy DLL Hijacking(Tutorial)
- Wireshark Tutorial: Decrypting RDP Traffic

Writeups

Responsible(ish) disclosure writeups

- Bootstrap Fail – Persistent XSS via Opportunistic Domain Sniping #Web
- GHSL-2020-050: Arbitrary code execution in Pebble Templates #Web
- Click Here For Free TV! – Chaining Bugs To Takeover Wind Vision Accounts #Android
- ForeScout Secure Connector Local Privilege Escalation #LPE #Windows
- Elevate Yourself to Admin in Umbraco CMS 8.9.0 (CVE-2020-29454) #Web

Bug bounty writeups

- Facebook account takeover due to a bypass of allowed callback URLs in the OAuth flow (Facebook, $12,000)
- Zero click vulnerability in Apple's macOS Mail (Apple)
- Apple TV for Fire OS code execution
- RCE on Starbucks Singapore and more for $5600 (Singapore, $5,600)
- Who Contains the Containers? (Microsoft)
- HackerOne Jira integration plugin Leaked JWT to unauthorized jira users (HackerOne, $3,000)
- Remote code execution through unsafe unserialize in PHP
- Automate Cache Poisoning Vulnerability – Nuclei ($1,500)

See more writeups on The list of bug bounty writeups.

Tools

- wappalyzergo: A high performance go implementation of Wappalyzer Technology Detection Library
- hakcron: Easily schedule commands to run multiple times at set intervals (like a cronjob, but with one command)
- Reflection: Automated Reflected Parameter Finder & XSS/SQLi/SSRF tester
- scanlimits: Tool to examine the behaviour of setuid binaries under constrained limits
- ldsview: Offline search tool for LDAP directory dumps in LDIF format

Tips & Tweets

- Default behavior to test for in Ruby apps
- 2nd order path traversal
- Fuzz CDN servers for hidden JS files

Misc. pentest & bug bounty resources

- The OAuth 2.0 Authorization Framework: JWT Secured Authorization Request (JAR) – draft-ietf-oauth-jwsreq-32
- Free Bug Bounty Guide – Essentials (video only, slimmed down) ($0+)
- Pluralsight Skills Free April
- The External Pentest playbook ($29.99)

Challenges

- SSTIC Challenge 2021 (English)
- BSidesSF 2021 CTF repo
- @d0nutptr's AWS challenge

Articles

- Your E-Mail Validation Logic is Wrong
- A Hack to render untrusted content in an isolated process (or why sandboxed iframes with *srcdoc* are bad)
- nOtWASP bottom 10: vulnerabilities that make you cry
- Presenting the Risk: Do You Know About this AWS Authorization Misuse? & Red-Shadow
- How good is Burp's API Scanning?

Bug bounty & Pentest news

- Meetup — Div0 x AiSP MoU Signing + Software Security Knowledge Exchange on April 14 (@spaceraccoonsec will talk in depth about a one-click RCE on Facebook Gameroom)
- CyberApocalypseCTF21 (Free 5 day CTF starting April 19)
- Tool updates:
  - Burp Professional / Community 2021.4
  - Bulk-scanning support added Backslash Powered Scanner

Non technical

- Is Foundational Knowledge (Networking, Coding, Linux) Really That Important When Learning To Hack?
- Giving Back to the Community with Ben Bidmead aka pry
- Mentoring the Upcoming Generation of Bug Bounty Hunters with Hakluke
- Hacker Spotlight: Interview With Edduu

Community pick of the week

Nice ride @abison_binoy Congrats on this cool achievement!

Do you also have bug bounty wins, swag and joys to share with other Bug Bytes readers? Tag us on social media, we love to hear from you!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com