Bug Bytes #166 – Double-edged SSRF, ToolTime & Fun hackers stories

BY ANNA HAMMOND · APRIL 6, 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 March 28 to April 4.

Our favorite 5 hacking items

1. Writeup of the week

Exploiting a double-edged SSRF for server and client-side impact

This is the story of an SSRF that @Yassineaboukir discovered on a private bug bounty program.
It is a beautiful example of mixing several techniques to maximize the impact of a bug, for example GitHub recon to find internal subdomains, exploiting the SSRF to enumerate internal subdomains, exploiting the same bug both server-side (as internal SSRF) and client-side (as information disclosure via CSRF)...

2. Tweets of the week

@hacker_'s SSRF story, Bug hunters' "Oh Sh*t" moments & Ironic vulnerabilities
Fun hacker stories by @infosec_au & @Jhaddix

If you love fun hacker stories, make sure to follow @hacker_. He's been very active on Twitter, sharing cool stories and mini-writeups, and inspiring other hackers to do the same, for our delight.

3. Video of the week

ToolTime – FeroxBuster (Content Discovery)

@Jhaddix is another hacker to follow if you are into Web hacking. He's been very sharing a lot of tips on Twitter lately, co-hosts Bounty Thursdays Live, and started this new show, ToolTime, where he reviews hacking tools.

4. Tool of the week

TruffleHog v3 & Critical Bounties via Leaked API Keys (FT TruffleHug)

@trufflesec released TruffleHog V3 which is way faster that the previous versions, detects 639 key types, automatically validates all secrets it supports with dynamic checks, and supports not only Git but also S3 buckets, STDin, file systems and more.

5. Conference of the week

Insomni'hack 2022

Recording from Insomni'hack 2022 are out, and they include many great talks on offensive security. The ones I'm prioritizing watching are @scannell_simon's "A Common Bypass Pattern To Exploit Modern Web Apps", @abhaybhargav's "Hook, Line And Sinker: Pillaging API Webhooks", @sachinnthakuri and @1lastBr3ath's "Exploiting WebKit To Break Authentication And Authorization" and @swapgs's "Two Bugs To Rule Them All: Taking Over The PHP Supply Chain".

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Q: HOW do you get started in bug bounty?? How do you build your automation?!
- Critical Bounties via Leaked API Keys (FT TruffleHug)
- Hacking PayPal and TikTok (legally) // Featuring Ben Sadeghipour Nahamsec
- CODE INJECTION via a VULNERABLE TEMPLATE ENGINE!
- Bug Bounty Live Recon – Linked / JS Discovery!
- 100 hours of bug bounty – I made twice more than as a pentester – Bounty vlog #2

Podcasts

- Darknet Diaries Ep 114: HD

Webinars

- Finding bugs with Nuclei with PinkDraconian (Robbe Van Roey)
- A Look Into zseano's Thoughts When Testing a Target – OWASP Nagpur
- Hacking MOBILE APPS: iOS & Android w/ 7aSecurity

Conferences

- PancakesCon 2022

Tutorials

- Remote Code Execution vs. Remote Command Execution vs. Code Injection vs. Command Injection vs. RCE
- Discovering Vulnerabilities in WordPress Plugins at Scale
- Exploiting DOM Based XSS via Misconfigured postMessage() Function
- Unsafe content loading [Electron JS]
- Grabbing and cracking macOS hashes

Writeups

Challenge writeups

- Ambassador World Cup 2022 CTF
- UHC – Altered
- Forward Shell Development – Inception [HackTheBox] & Blog post
- HackTheBox – Shibboleth & Linux Shared Object Files

Pentest writeups

- My Pentest Log -12- (Out-Of-Band Sql Injection in MySQL)
- XSS — WAF Bypass

Responsible(ish) disclosure writeups

- elFinder: The Story Of A Repwning
- Insecure cipher used in forum software #Crypto
- PHP Supply Chain Attack on PEAR #Web #Crypto
- Pwning 3CX Phone Management Backends from the Internet
- ABC-Code Execution for Veeam #Windows #LPE

Spring4Shell corner

- reznok/Spring4Shell-POC
- Hunt4Spring & @RedHuntLabs's analysis
- spring-tools & @JFrogSecurity's analysis
- Free TryHackMe room

Bug bounty writeups

- NoSQL Injection in Plain Sight
- Critical SSRF on Evernote (Evernote, $5,000)
- Unauthenticated Remote Code Execution in Cisco Nexus Dashboard Fabric Controller (formerly DCNM) (Cisco)
- Pwning Microsoft Azure Defender for IoT | Multiple Flaws Allow Remote Code Execution for All (Microsoft)
- Pwn2Own Austin 2021 : Defeating The Netgear R6700V3 (Netgear)
- Pwning a Cisco RV340 with a 4 bug chain exploit (Cisco)

See more writeups on The list of bug bounty writeups.

Tools

- Dome: Subdomain enumeration tool in Python
- Difftastic: An experimental diff tool that compares files based on their syntax
- Docker-OSX: Run macOS VM in a Docker! Run near native OSX-KVM in Docker
- s3sec: Check AWS S3 instances for read/write/delete access
- Scanmycode (Community Edition): Code scanning/SAST/Static Analysis/Linting using many tools/scanners with one report

Tips & Tweets

- @Th3G3nt3lman on valid credentials exposed on GitHub
- @mcipekci's SQL injections found by manually engaging targets
- SOAP vs REST vs GraphQL vs RPC
- How to change fonts in Burp
- Infosec career advice

Misc. pentest & bug bounty resources

- BUG BOUNTY RECON DATASET
- Security List
- A curated list of various bug bounty tools
- Security related PDFs by IGNITE

- RTCSec Newsletter – OpenSSL DoS and DTLS, SIMBoxes, SIP-TLS and lots of advisories

Articles

- Burp Suite Certified Practitioner Exam – Review
- IIS – SOAP: How to run shellcode from a webshell with a .soap extension
- Firefox and Chromium
- Remotely Dumping Chrome Cookies...Revisited & Dump-Chrome-Cookies
- This busy-loop is not a security issue & My first fuzzy finding: Busyloop in curl

Bug bounty & Pentest news

- Bug bounty
  - Critical GitLab vulnerability lets attackers take over accounts
  - Microsoft: Introducing the Applications and On-Premises Servers Bug Bounty Program
- Cybersecurity
  - VMware Horizon platform pummeled by Log4j-fueled attacks
  - Sitel on Okta breach: "spreadsheet" did not contain passwords
  - Lapsus$ and SolarWinds hackers both use the same old trick to bypass MFA
- Upcoming events
  - @NahamSec is resuming Live Recon, with @Jhaddix and @stokfredrik as cohosts (April 10)
  - ComfyCon AU 2022 & Schedule (April 9 & 10)
- Tool updates
  - Uncover v0.0.4
  - AuRA (Auth. Request Analyser) v1.1
  - Sharpener v1.3

Non technical

- Two Years of Bug Bounty Hunting
- My First Year As a Pentester
- Bug Hunting Tips
- Creating a Home Office

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com