# Bug Bytes #174 – From $0 bounties to $150k, Hacker summer school & How to hack Apache Pinot

BY ANNA HAMMOND · JUNE 15, 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 June 6 to 13.

## Intigriti news


Free webinar – The Ethical Hacker Insights Report 2022


Getting (back) together to hack!

## Our favorite 5 hacking items

### 1. Video of the week

Bug Bounty 101: #23 – From $0 to $150,000/mo – Hacking Methodology & Mindset

If you are struggling with finding your first bugs, this videos might give you new ideas to experiment with. @_zwink shares the muti-step formula he used to go from $0 bounties in his first month to $150K in less than a year and a half.

## 2. Writeups of the week

Zimbra Email – Stealing Clear-Text Credentials via Memcache injection
SynLapse – Technical Details for Critical Azure Synapse Vulnerability & TL;DR (Microsoft, $60,000)
Hacking 6.5+ million websites => CVE-2022-29455 (Elementor)

@SonarSource disclosed a cool vulnerability that allowed unauthenticated attackers to steal the login credentials of Zimbra users without interaction, using Memcache injection.

@TzahPahima shared details on a cross-tenant vulnerability in Azure Synapse that made it possible to obtain credentials of Azure Synapse customer accounts, including Microsoft's!

The third writeup demonstrates a nice strategy for bug hunters: @rotembar, @realgam3 & @naglinagli identified that their target used a specific WordPress plugin, they analyzed one of its patched vulnerabilities, found a new bug, and went over historic recon data to find other vulnerable targets.

## 3. Tutorial of the week

Not all "Internet Connections" are Equal

This is a good reminder by @Trustwave that some networking issues and configuration can interfere with your security testing and vulnerability scanning. It is good to learn about them to avoid false negatives.

## 4. Articles of the week

New technique of stealing data using CSS and Scroll-to-text Fragment feature.
Apache Pinot SQLi & RCE Cheat Sheet

@haqpl demonstrates a new CSS exfiltration technique that leverages the new Scroll-to-Text Fragment feature in Chrome. It has some limits but can be useful for leaking information on an app's users, and is worth knowing if you are interested in XSleaks attacks and CSS exfiltration.

The second article by @Doyensec provides an excellent resource on hacking Apache Pinot. It covers what Pinot is, how to set up a testing environment, how to exploit Pinot databases for SQL injection, RCE and post-exploitation.

## 5. Resources of the week

OffSec Live: PEN-200! (Starting June 22)
PNPT Live Training (Starting June 22nd at 12pm EST)

Both @offsectraining and @TCMSecurity announced that they will livestream hacking courses for free on Twitch, starting June 22.
This reminds me that @InsiderPhD also announced two upcoming free courses.
Hacker summer school will soon start, no excuses if you want to upskill!

SHARE ON TWITTER

# Other amazing things we stumbled upon this week

## Videos

- Bug Bounty 101: #21 – Hacking Pinterest for Two Weeks & Bug Bounty 101: #22 – Testing File Upload Dialogues
- 100 hours of reviewing the source code – Bounty vlog #3 – Elastic
- Learn to hack in 60 seconds?
- Performing Web Searches From Your Terminal
- How I Got Started In Cybersecurity
- Hack like Mr Robot // WiFi, Bluetooth and Scada hacking
- Deadly OSINT: The Final Hours of Pop Smoke & OSINT TikToker @georainbolt

## Podcasts & Audio

- Darknet Diaries Ep 119: Hot Wallets

## Webinars

- Making Sense of RFCs: Reading List
- Tool Talks: Debugging Ruby Exploits
- Intro to Password Guessing and Cracking (Directly from SEC560!)

## Conferences

- NDC Security 2022
- BSides Prishtina 2022

## Tutorials

### Medium to advanced

- Apache Pinot SQLi & RCE Cheat Sheet
- Using CloudTrail to Pivot to AWS Accounts
- Managed Identity Attack Paths, Part 1: Automation Accounts, Part 2: Logic Apps & Part 3: Function Apps

- WMI Providers For Script Kiddies

### Beginners corner

- Escalating privileges in Google Cloud, from app to cloud access
- How to Reverse Engineer and Patch an iOS Application for Beginners: Part I & ios-breakmedaddy
  Dockerizing A Web Testing Environment: Part 3, Part 2 & Part 1

## Writeups

### Challenge writeups

- HackTheBox – Meta
- ATM/Kiosk Hacking (Reloaded)
- CA CTF 2022: Exploiting Zip Slip and Pickle Deserialization – Acnologia Portal & Exploiting Redis
  Lua Sandbox Escape RCE with SSRF – Red Island
- Command Injection – Lab #1 OS command injection, simple case

### Pentest writeups

- Tales of sharepoint API misconfigurations
- Code review to simple RCE

### Responsible(ish) disclosure writeups

- CVE-2022-25845 – Analyzing the Fastjson "Auto Type Bypass" RCE vulnerability #Web #RCE
  #CodeReview
- Discovering a Dangerous Pattern in a Popular Python Package Manager #Python #RCE
- Technical Advisory – FUJITSU CentricStor Control Center <= V8.1 – Unauthenticated Command
  Injection #Web #CodeReview
- Exploiting Kaseya Unitrends Backup Appliance – Part 1 & Part 2 #Web #LPE #MemoryCorruption
- CVE-2022-26134: A look into bypass isSafeExpression check in Confluence Preauth RCE

### 0-day: Dogwalk

- Trustwave's high-level explanation
- Original writeup by Imre Rad in 2020
- Tweets by @j00sean (who re-discovered the vulnerability)
- Technical analysis and patches by 0patch
- PoC

### Bug bounty writeups

- Bypassing CSP with dangling iframes (Google & Mozilla)
- CVE-2022-1040 Sophos XG Firewall Authentication bypass (Sophos)
- Chaining vulnerabilities to criticality in Progress WhatsUp Gold (Progress)
- Another vision for SSRF
- SynLapse – Technical Details for Critical Azure Synapse Vulnerability & TL;DR (Microsoft, $60,000)
- Finding vulnerabilities in curl 7.83.0 without reading a single-line of C code (curl)
- How I found a Critical Bug in Instagram and Got 49500$ Bounty From Facebook (Meta / Facebook, $49,500)
- Extracting Clear-Text Credentials Directly From Chromium's Memory (Google)

See more writeups on The list of bug bounty writeups.

## Tools

- sourcegraph-scripts: Scripts for Sourcegraph search results (Useful for static analysis)
- TLS-Scanner & Features: The TLS-Scanner Module from TLS-Attacker
- HTTPLoot & Millions of Secrets Exposed via Web Application Frontend – An Internet-Wide Study: Go tool which can simultaneously crawl, fill forms, trigger error/debug pages and "loot" secrets out of the client-facing code of sites
- CRLFsuite: CRLF injection (HTTP Response Splitting) scanner in Python
- Ica2Tcp: A SOCKS proxy for Citrix

## Tips & Tweets

- @_zwink on Testing all URLs at least three times, preferably on separate days, Avoiding distractions while hacking & Things to try when testing for Broken Access Control
- When life gives you lemons
- @0xConda's tips after hitting the top 100 of all time leaderboard on Intigriti
- Bypass for Akamai WAF's XXE filters
- Are you making this mistake when you use a reflected XSS scanner?
- Code review resources & @dcuthbert's workflow
- Chain self-XSS with login CSRF to escalate it

## Misc. pentest & bug bounty resources

- JWT attacks (New Web Security Academy course & labs)
- Report templates
- Cloud Middleware Dataset & The cloud gray zone—secret agents installed by cloud service providers
- Orange Cyberdefense mindmaps
- New UUID Formats (RFC4122 update proposal)
- Security Study Plan
- brutas: Wordlists and passwords handcrafted with

## Articles

- New technique of stealing data using CSS and Scroll-to-text Fragment feature.
- Public Travis CI Logs (Still) Expose Users to Cyber Attacks
- What I learned from reading 126* Information Disclosure Writeups
- Make JDBC Attacks Brilliant Again I
- Yet another zero-day (sort of) in Windows “search URL” handling
- SeaFlower – A backdoor targeting iOS web3 wallets

## Challenges

- Can you spot the vulnerability in this code snippet?

## Bug bounty & Pentest news

- Pentest
  - New Offensive Security course (Web Attacks with Kali Linux / WEB-200) and exam (OSWA)
- Cybersecurity
  - New PACMAN hardware attack targets Macs with Apple M1 CPUs
- Upcoming events
  - Need funding for a good hacking idea? Apply to the Hacker Initiative’s 2022 Grant Cycle before June 30
- Tech
  - HTTP/3 evolves into RFC 9114 – a security advantage, but not without challenges

    - New Vytal Chrome extension hides location info that your VPN can't
    - WWDC 2022: Apple showcases next-gen security tech at annual developer event
- Tool updates
    - Exegol 4.0.0 (redesigned from scratch)
    - Burp Professional / Community 2022.5.1
    - gowitness v2.4.0 (Major release)
    - reconFTW v2.3.1
    - Project Discovery updates: httpx v1.2.2, Subfinder v2.5.2, Proxify v0.0.7, mapCIDR v1.0.0 & Cloudlist v1.0.1 (Added Hetzner Cloud provider support)

## Non technical

- Eight productivity hacks to accelerate your career
- Avoiding B.A.D. behaviour