Bug Bytes #169 – Psychic signatures, Pwning Cloudflare, Z-winK University & The Bug Hunter's Methodology for App Analysis

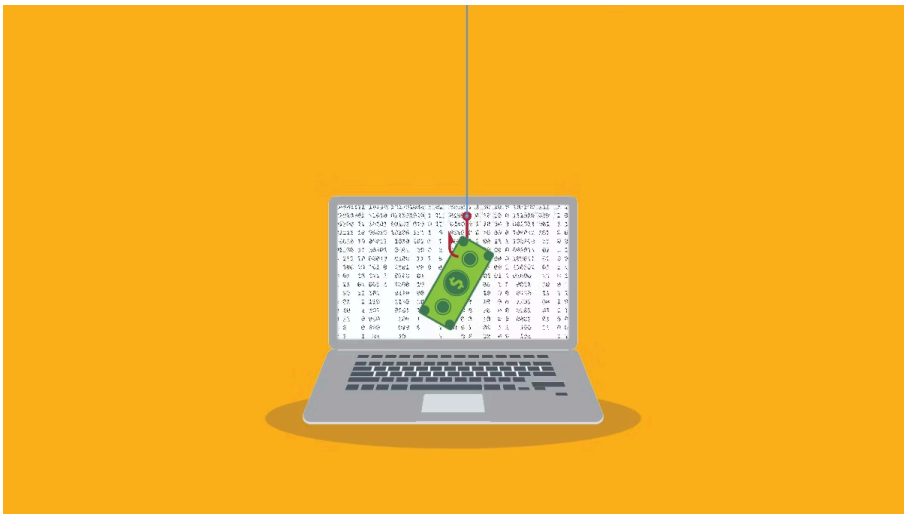
BY ANNA HAMMOND · MAY 11, 2022 · LAST UPDATED ON MARCH 6, 2025

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 April 18 to May 9.

Intigriti news



Bug bounty platform Intigriti offers new hourly payment option for vulnerability researchers

Congrats to @YnoofAssiri, @nullb0t and @0xH4rmony for reaching the top of the Intigriti Q1 2022 leaderboard!

Intigriti secures more than €21M in Series B funding

Our favorite 5 hacking items

1. Resource of the week

ThreatDEV & ThreatDEV Discord

You probably know about @hacker_'s fantastic hacker stories on Twitter, but did you know he also has a newsletter, a blog and a Discord

In the newsletter, you'll find the same kind of cool stories, tips and tricks. @Jhaddix is also contributing to it.
The blog has many older writeups, a Threads section that embeds all of @hacker_'s Twitter threads, and a roadmap if you want to Learn to Hack Web Apps.

2. Writeups of the week

Security issues with cloudflare/odoh-server-go and the ODoH RFC draft
Cloudflare Pages, part 1: The fellowship of the secret, Part 2: The two privescs, Part 3: The return of the secrets & Cloudflare advisory

@fransrosen researched ODoH (Oblivious DNS Over HTTPS) and found a lack of protections against SSRF in the ODoH RFC draft and in Cloudflare's implementation, odoh-server-go.

@seanyeoh and @devec0 also hacked Cloudflare, but focused on Cloudflare Pages's CI/CD build pipeline. They found a host of issues including command injection, container escape, Bash path injection and information disclosure.

3. Videos of the week

Z-winK University (ZU)
Diving Deeper into Subdomain Takeovers & Mitigations with Shubham Shah

@_zwink started a Youtube channel to teach how to hack and get into bug bounty, starting with the basics. The only prerequisite is to have a computer with an Internet connection.

Even if not new to hacking, I'd keep an eye on his Twitter and Youtube accounts as he shares a lot of tips and tackles more and more advanced technical topics.

Another fantastic video is a deep dive into subdomain takeover by @infosec_au. If you are interested in the topic, you might want to watch this to learn not only about different types of subdomain takeovers, but also how to mitigate them.

4. Conference of the week

NahamCon2022, Web challenges walkthrough & Slides for:
– Finding 0days in Enterprise Software
– Effectively finding vulnerabilities in web applications by debugging the source code
– The Bug Hunters Methodology Application Analysis v1

This NahamCon edition was so-o-o good! I'd recommend watching all the talks, but if you are more into black-box Web testing, start with @Jhaddix's first edition of the The Bug Hunter's Methodology: Application Analysis.

If you read all the cool writeups @assetnote have been publishing lately and wonder how they do it, start with @infosec_au's talk on finding 0days in enterprise software, or @seanyeoh and @devec0's talk on hacking CI systems.

Also, if you played the CTF, you might be interested in the video walkthrough where @gregxsunday solves all the Web challenges.

5. Vulnerabilities of the week

CVE-2022-21449: Psychic Signatures in Java, A few clarifications about CVE-2022-21449, PoC by @jfrog, Lab by @datadoghq & Lab by @SecCodeWarrior
CVE-2022-1388: F5 iControl REST Endpoint Authentication Bypass, @Horizon3Attack analysis & PoC, Rapid7 analysis, @bishopfox's BIG-IP Scanner

@neilmaddog discovered a bypass in Java's implementation of ECDSA signature validation. It made it possible to forge certificates and credentials, breaking JWTs, SAML, etc. Just like Doctor Who's "psychic paper", in the world of crypto.

The other vulnerability everyone is talking about is CVE-2022-1388. It is an authentication bypass in F5 iControl REST, that is reminiscent of the research on Abusing HTTP hop-by-hop request headers. The impact is RCE with a single unauthenticated POST request.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- ToolTime – Cloud Recon 1, SSL Certificate Parsers for Recon & FeroxBuster Content Discovery
- facts: Bug Bounty hunters has made ridiculous amounts of $$ from known DNS techniques..

- How I became a SANS Instructor & an Offensive Cyber Security Expert {RedTeamer} | Jean-Francois Maes
- XSS in 100 seconds

Podcasts & Audio

- Hacken Podcast: getting into security with @hacker_ & AMA with Ahsan Khan
- Cybersecurity Web Podcast #2 – John Hammond & #1 – Graham Helton

Webinars

- BHIS | Atomic Red Team Hands on Getting Started Guide

Conferences

- Skeleton's in the closet and other tales from beyond the grave – HYS London 2022 & Slides
- Mark Dowd- Keynote -How Do You Actually Find Bugs? (Part of OffensiveCon22)
- Ethical Hacker: Hiring & Getting Hired, Keynote, Hack @ the Harbor, Point3 Security

Tutorials

Medium to advanced

- A Guide For Advanced Message Protected API Hacking Using Hackvertor and Burp (part 2)
- How masscan works
- Bypassing OpenSSH MaxAuthTries
- Signing and Encrypting with JSON Web Tokens

Beginners corner

- ffuf it up
- Mobile MitM: Intercepting Your Android App Traffic On the Go
- The Difference Between a URL, URI, and a URN
- XSS in JSON: Old-School Attacks for Modern Applications
- Using SpiderFoot to Investigate a Public Bug Bounty Program
- Reconnaissance: Red Teamer Perspective

Writeups

Challenge writeups

- Solving all Web CTF tasks from NahamCon
- HackTheBox – Unicode & [Blog post],(https://0xdf.gitlab.io/2022/05/07/htb-unicode.html)
- 4 hackers, one XSS challenge! Solution to April '22 XSS Challenge & Blog post by the challenge's author
- HackTheBox – Search & Parsing JSON with JQ
- UHC – BackendTwo

Pentest writeups

- The Complete Compromise of a Password Manager Site
- I have 1% chance to hack this company
- Anatomy Of A Zero Day – How To Decrypt....a Robot? #CodeReview
- Reversing an Android App to Code Execution on their Server.

Responsible(ish) disclosure writeups

- CVE-2022-29464: RCE via unrestricted file upload in WSO2 products, Rapid7 analysis, Nuclei template & Metasploit module
- Microsoft finds new elevation of privilege Linux vulnerability, Nimbuspwn, Rapid7 analysis & Nimbuspwn detector by @jfrog
- CVE-2022-22954: RCE via Freemarker SSTI in VMware Workspace ONE Access and Identity Manager & Metasploit module
- Hunting bugs in Accel-PPP with CodeQL
- TLStorm 2 – NanoSSL TLS library misuse leads to vulnerabilities in common switches

Bug bounty writeups

- Exploitation of an SSRF vulnerability against EC2 IMDSv2
- Hacking a Bank by Finding a 0day in DotCMS
- Wiz Research discovers "ExtraReplica"— a cross-account database vulnerability in Azure PostgreSQL (Microsoft)
- The $16,000 Dev Mistake ($16,000)
- A Fun SSRF through a Headless Browser
- Encrypting our way to SSRF in VMWare Workspace One UEM (CVE-2021-22054) (VMware)

- Advanced sqlmap Case Study

See more writeups on The list of bug bounty writeups.

Tools

- hakoriginfinder & Intro: Tool for discovering the origin host behind a reverse proxy. Useful for bypassing WAFs and other reverse proxies
- burpsuite-project-file-parser: A Burp Suite Extension for parsing Project Files from the CLI
- np: A Go tool to parse multiple Nmap scans
- str-replace: Simple tools to handle string and generate subdomain permutations
- MITM_Intercept: A little bit less hackish way to intercept and modify non-HTTP protocols through Burp & others
- CDNStrip: Striping CDN IPs from a list of IP Addresses

Tips & Tweets

- Minimizing the bandwidth when HEAD is disabled
- Multiple WAFs bypass
- Command injection to hex-encoded DNS exfil onliner
- In Java, two entirely different URLs may be considered equal
- Bypass WAFs by finding the origin IP in email headers
- 40x bypass mini-writeup
- Don't skips hosts that redirect to Single-Sign on
- @Jhaddix on Trademark and copyright recon, Relying too much on automation, The Medical Alert Hack & The 100 Million Person Data Disclosure

See more tips on this week's Twitter collection.

Misc. pentest & bug bounty resources

- bugbounty.gg
- GraphQL Threat Matrix
- Match Replace Burp
- Resolvers (by Trickest)
- Public Hacktivity

Articles

- DNS Tools Comparison
- Technique of the week: Log Forgery
- New XSS vectors
- How much do you know about script type?
- Pixel Challenge 2022
- Authenticating with certificates when PKINIT is not supported & Bypassing LDAP Channel Binding with StartTLS

Reports

- The More You Know, The More You Know You Don't Know
- ThinkstScapes Quarterly – Q1 2022

Challenges

- Recent Threats (New TryHackMe module)
- Can you spot @honoki's interesting XSS and exploit it?

Bug bounty & Pentest news

- Bug bounty
  - Bug bounty platform Intigriti offers new hourly payment option for vulnerability researchers
- Cybersecurity
  - security.txt is officially an RFC
- Tech
  - pyscript (aka Python inside HTML) announced at PyCon US 2022 & Example of PyScript XSS vector
  - RFC 9239 updates JavaScript MIME type registrations
  - Disavowed: Chrome plans to deprecate 'document.domain' lays the groundwork for shift in browser security
  - FIDO, the New open standard for passwordless authentication is adopted by Microsoft, Google and Apple
- Upcoming events
  - Levelup0x08: Hack another day (May 21)

    - Introducing LevelUpX – Resources For The Community By The Community (Every other week, first talk on May 20)
    - Free Workshop: Hacking JavaScript Desktop apps with XSS and RCE
- Tool updates
    - SecLists 2022.2
    - reNgine v1.1
    - Osmedeus v4.1.1
    - RequestBin Next-Gen
    - Burp Professional / Community 2022.3.6
    - Project Discovery updates: Interactsh v1.0.3, Naabu v2.0.7 & Nuclei v2.6.9

Non technical

- Four Eras of JavaScript Frameworks
- What VPS to choose?
- Demystifying Security Research – Part 1