Bug Bytes #165 – Spring4Shell, CDN WAF bypass & Practical cryptography for pentesters

BY ANNA HAMMOND · MARCH 31, 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 21 to 28.

Intigriti news

Changelog #33 – Collaboration makes you better!

Stijn Jans and Inti De Ceukelaire, Intigriti: “bad actors won’t seek your permission to hack your business”

Our favorite 5 hacking items

1. Vulnerabilities of the week

Spring4Shell & CVE-2022-22963 – Java 0-days in Spring

There is a lot of chatter about 0-days in Spring and some confusion because there isn't one but two vulnerabilities:

- Spring4Shell is a severe RCE via insecure deserialization in Spring Core. It is exploited in the wild, was leaked by a Chinese-speaking researcher, does not have a patch nor a CVE yet.
- CVE-2022-22963 is a less severe and patchable SPEL Expression Injection in Spring Cloud Function.

Some say it is the new Log4shell and others say there is no need to panic about Spring4Shell as it is only exploitable in certain configurations. Until we know more, here are some good resources to dive into both vulnerabilities:

- Spring4Shell analysis by LunaSec, Rapid7, Cyber Kendra & SANS ISC
- Non intrusive Spring4Shell PoC
- CVE-2022-22963 advisory
- CVE-2022-22963 Nuclei template

2. Writeups of the week

Ruby Deserialization – Gadget on Rails (Ruby on Rails)
PHP filter_var shenanigans

@httpvoid0x2f's latest writeup is a deep dive into insecure deserialization in Ruby/Rails. They go over the current state of ruby deserialization gadget chains, and show how they discovered a new RCE gadget for the latest version of Rails.

The second writeup is about a vulnerability in PHP that allows circumventing filter_var() in some cases. There are some limitations but it is interesting to see @pwningsystems's process for finding this, and it is a good research opportunity as @albinowax pointed out.

3. Videos of the week

HTB Stories #8: Bug Bounties 101 w/InsiderPhD
rootxharsh Talks About Recon, Finding A $50,000 Remote Command Execution in Apple, and more!

@InsiderPhD and @rootxharsh are two of my favorite hackers.
@rootxharsh is part of HTTPVoid, a crew of bug hunters who have been putting out amazing writeups lately like the Ruby Deserialization bug mentioned above.
And @InsiderPhD juggles between multiple specialties and often shares cool productivity tips in addition to technical content.

So, these interviews are a nice opportunity to get to know them more and pick up some useful insights on how they think and hack.

4. Article / Tool of the week

Bypassing CDN WAF's with Alternate Domain Routing & CDN Proxy

@Ryan_Jarv shares a really cool attack and tool for bypassing WAFs.
The tool currently supports CloudFlare and CloudFront, with two prerequisites: Knowing the server's origin IP and that the Web app is accessible from the CDN's shared IP range.
In these conditions, the "Alternate Domain Routing" attack allows you to completely bypass the CloudFlare or CloudFront WAF, access the server directly and bypass any IP restrictions or rate limiting.

5. Conference of the week

Practical Cryptography for Infosec Noobs & Slides

This is an awesome talk if you want to learn practical cryptography, beyond the easy or unrealistic challenges found in many CTFs.
@mubix demonstrates how to identify and decrypt random data in real life, for example during pentesting or bug hunting when you don't even know the type of cryptography used.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- PHP Type Juggling – Why === is Important – Sponsored Content
- # CODE INJECTION via a VULNERABLE TEMPLATE ENGINE!
- Forward Shell
- Deep dives on David Dombal's Youtube channel on Traceroute, Nmap, TCP/IP & SSL/TLS

Podcasts

- Helping Secure OSS Software – Alvaro Munoz – ASW #189

Webinars

- Bishop Fox Tool Talks: Episode 3: Nuclei Episode, Episode 2: Fuzzing & Episode 1: Eyeballer
- Tactical Burpsuite – Kevin Johnson & Nathan Sweaney

Conferences

- SchmooCon Live Streams & Agenda

Slides & Workshop material

- Understanding Windows Lateral Movements
- Insomni'Hack 2022:

- Hook, Line and Sinker – Pillaging API Webhooks
- It's Raining Shells & TL;DR
- Delegating Kerberos to bypass Kerberos delegation limitation
- Symbolic Execution Demystified

Tutorials

Medium to advanced

- Cloud-based DNS monitoring with IPinfo Enrichment & TL;DR
- Whitepaper – Double Fetch Vulnerabilities in C and C++
- What to look for when reviewing a company's infrastructure
- Supply Chain Attack as Code
- Azure Dominance Paths
- C++ Memory Corruption (std::string) – part 4

Beginners corner

- A Detailed Guide on Crunch & A Detailed Guide on httpx
- Intro to GamePwn (aka Game Hacking)

Writeups

Challenge writeups

- I've been Hacking for 10 Years! (Stripe CTF Speedrun)
- HackTheBox – Secret
- SANS Holiday Hack Challenge 2021
- Liikt1337 – Hacking the hacker – 1337UP LIVE CTF challenge writeup
- Overflows in PHP?! Solution to March '22 XSS Challenge & Winners

Pentest writeups

- Authentication bypass using root array
- Reports from the Field: Part 3
- How Clubhouse user scraping and social graphs

Responsible(ish) disclosure writeups

- ImpressCMS: from unauthenticated SQL injection to RCE #Web
- Finding bugs to trigger Unauthenticated Command Injection in a NETGEAR router (PSV-2022–0044) #Web #Router
- CVE-2022-26318 – Unauthenticated RCE in WatchGuard Firebox and XTM appliances
- CVE-2021-43008 – AdminerRead

Known vulnerabilities

- Using the Dirty Pipe Vulnerability to Break Out from Containers & PoC
- CVE-2019-0708 (BlueKeep) pre-auth RCE POC on Windows7

Bug bounty writeups

- One company: 262 bugs, 100% acceptance, 2.57 priority, millions of user details saved.
- Unauthenticated Remote Code Execution in Cisco Nexus Dashboard Fabric Controller (formerly DCNM)
- Basic recon to RCE II
- HTML parser bug triggers Chromium XSS security flaw (Google Chromium, $5,000)
- When Equal is Not, Another WebView Takeover Story
- Able to steal bearer token from deep link (Basecamp, $6,337)
- 0-day Cross Origin Request Forgery vulnerability in Grafana 8.x . (Aiven Ltd, $1,500)

See more writeups on The list of bug bounty writeups.

Tools

- Go Decrypt Jenkins: Simple tool to decrypt Jenkins encrypted strings
- IVRE
- Sourcemapper: Extract JavaScript source trees from Sourcemap files
- Spellbook: Framework for rapid development and reusable of security tools
- HTTP CL.TE & TE.CL Desync Calculator: Perform TE.CL HTTP Request Smuggling attacks by crafting HTTP Request automatically
- Right-To-Left Override POC & Initial Access – Right-To-Left Override [T1036.002]

Tips & Tweets

- Insightful tips @SecGus after triaging bugs for 5 months

- Git Temporal VSCode extension + @trick3st Inventory = asset timeline tracking
- @hacker_ on why/how “Anyone can hack”
- Using Nuclei (with default templates) is a competitive disadvantage
- @hacker_’s roadmap to develop your technical skills
- @Masonhck3571 on “Is it tool late to do bug bounty?”
- 403 bypass by appending unusual characters at the end of file names

Misc. pentest & bug bounty resources

- RegexPassive: Collection of regexp pattern for security passive scanning
- Find-gh-poc: The centerpiece of the trickest/cve project; finds CVE PoCs on Github
- Cloud Hacking Playbook ($25)
- The DOs and DON’Ts of Secure Coding
- Best platforms to learn ethical hacking!

Articles

- BreakingFormation: Technical Vulnerability Walkthrough
- LDAP relays for initial foothold in dire situations
- 2022 Threat Detection Report by Red Canary
- Analyzing the Attack Landscape: Rapid7’s 2021 Vulnerability Intelligence Report

Challenges

- New FREE TryHackMe Room: Bypassing UAC

Bug bounty & Pentest news

- Bug bounty
  - The StackHawk ZAP Fund
  - Bug Bounty Hunting Certification
- Cybersecurity
  - Urgent Update For Chrome Fixes Zero Day Under Attack (CVE-2022-1096)
  - URL rendering trick enabled WhatsApp, Signal, iMessage phishing
- Upcoming events

    - Finding bugs with Nuclei with PinkDraconian (Robbe Van Roey) (April 3)
    - APIsecure (April 6 & 7)
- Tool updates
    - ffuf v1.4.0
    - Sharpener v1.2 & Things you may not know it can do
    - Empire 4.5

Non technical

- Always Be Modeling: How to Threat Model Effectively
- Your Career in Cybersecurity
- tr33's story: from community member to HTB employee
- So You Want to be a Penetration Tester

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com