Bug Bytes #161 – Java Tomcat challenge, LFI via Markdown & Nuclei + Burp = Love

BY ANNA HAMMOND · MARCH 2, 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 February 21 to 28.

Intigriti news

1337UP LIVE

CTF SIGN UP Virtual Conference

With a little less than 10 days to go, Intigriti proudly presents the 1337UP LIVE CTF and virtual bug bounty conference!

On March 11th, we will kick off with the 24-hour long CTF with challenges from web all the way to binary exploitation. Sign up right now at ctf.intigriti.io.

On March 12th, once the CTF ends, we will directly jump into the live bug bounty conference with astonishing talks by amazing speakers. Check out the line-up over here at www.intigriti.com/1337uplive!

Win some swag!

We're inviting you to share your opinions!

As a community-driven platform, your feedback is extremely valuable to us. To get to know you better, we would like to ask you to fill out our five-minute survey. At the end of the survey, you will be able to participate in our raffle to win a **€50 Intigriti swag voucher (there are 20 available)**. Looking forward to hearing from you!

Take the survey

Our favorite 5 hacking items

1. Challenge of the week

Exploiting Java Tomcat With a Crazy JSP Web Shell – Real World CTF 2022 & Alternative writeup + Docker environment

@LiveOverflow demonstrates how his team solved Desperate Cat, a hard Java web hacking challenge from the Real World CTF.
You can run the Dockerfile locally and try to solve the challenge first, but make sure to watch the incredibly informative video walkthrough.

2. Writeups of the week

Pwning a Server using Markdown
Catching bugs in VMware: Carbon Black Cloud Workload Appliance and vRealize Operations Manager (VMware)

Next time you see markdown that references a file, in a HTTP request, remember to test for LFI. @zombie007o and @nullvoiddeath had the idea because of explicit errors saying that the file requested wasn't found, then they exploited the LFI to grab SSH keys from the server and get a shell.

The second writeup is about several bugs found by @elk0kc in a VMware product. It is interesting to see how a normalization issue caused authentication bypass, and how a `?` symbol was used to bypass an SSRF filter.

3. Tips of the week

Bypass Java URL protocol validation with "url:"
Using "procedure analyse" to increase the impact of a limited SQL injection

Two cool tricks to have in any Web app hacking arsenal: Java URL validation can be bypassed with the "url:" scheme (e.g. url://http://120.0.0.1:8080), and "procedure analyse" can be the only way to exploit a very limited MariaDB SQL injection.

4. Videos of the week

Jack Cable Talks About His Background, Bug Bounty Methodology, and Hacking the US Government
@InsecureNature Talks About Hacking, Certificate Transparency, TruffleHog, and more!

Did you miss @NahamSec's Live Recon interviews? The good news is that seven of them weren't published (after the live stream) and @NahamSec started releasing them on Youtube.
The bad news is that @NahamSec got super burnt out and sadly had to stop these streams. So, enjoy the last ones!

5. Tool of the week

nuclei-burp-plugin

This Burp extension helps generate Nuclei templates from HTTP requests/responses, with only a few clicks. Writing custom templates has never been so easy, amazing work by @forgedhallpass!

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Scanning at lightning-fast speeds! Turbo Intruder – Hacker Tools & Blog post
- Preparing for the OSCP Exam with AD
- HTB Stories #7: Meet the one behind LinPEAS – ./carlospolop & HTB Stories #6: Hacking OS 101 with Palinuro
- Ghidra – Pwn Zero To Hero 0x02
- How To Crack ZIP & RAR Files With Hashcat

Podcasts & Audio

- Bug Bounty Community Chats #3

Webinars

- Application Security How-To: Ken's Secure-Code Review of an application codebase. & Repo
- Rise of captain hindsight: Finding Log4Shell with CodeQL
- macOS Security Features Bypasses by Example | Jonathan Bar Or (JBO)

Tutorials

- The most underrated tool in bug bounty. (and the filthiest one liner possible)
- How to Create a Custom SpiderFoot Module
- Fantastic Infrastructure as Code security attacks and how to find them & Repo

- Penetrate the Protected Component in Android Part -2
- Thick Client Penetration Testing — TCP traffic interception using mitm_relay and Burp.
- Exploiting Jenkins build authorization

Writeups

Challenge writeups

- XSS for beginners – Google XSS Game Levels 1 & 2
- List Database Content For Further Exploitation!
- HackTheBox – Driver
- KeepMe Polyhx 24h CTF Writeup
- Writeups of TSJ CTF 2022 web challenges

Pentest writeups

- Give me a browser, I'll give you a Shell
- SQLi: Next Level
- Bash Tricks for Command Execution and Data Extraction over HTTP/S

Responsible(ish) disclosure writeups

- Logic Flaw Leading to RCE in Dynamicweb 9.5.0 – 9.12.7 #Web #CodeReview
- Remote Code Execution in pfSense <= 2.5.2 #Web #CodeReview
- Extensis Portfolio Vulnerability Disclosure #Web

Bug bounty writeups

- Stealing a few more GitHub Actions secrets (GitHub, $7,500)
- OAuth and PostMessage – Chaining misconfigurations for your access token.
- Write Up – Android Application Screen Lock Bypass Via ADB Brute Forcing
- Hackerone open redirect security alert bypass via view report as PDF (HackerOne, $500)
- How I bypassed PHP functions to read sensitive files on server

See more writeups on The list of bug bounty writeups.

Tools

- HTTPCustomHouse: HTTP request smuggling attack helper/CLI tools to manipulate HTTP packets

- BurpGraphQLViewer: Burp extension that provides a central location for viewing all GraphQL requests/responses
- Ostorlab & Intro: A security scanning platform that enables running complex security scanning tasks involving multiple tools in an easy, scalable and distributed way
- wpgarlic: A proof-of-concept WordPress plugin fuzzer used in this research
- FindUncommonShares: A Python equivalent of PowerView's Invoke-ShareFinder.ps1 allowing to quickly find uncommon shares in vast Windows Domains

Tips & Tweets

- One of @NahamSec's favorite and highest bounties
- Recon to SQL injection
- There has never been a better time than right now to get involved with Azure security research

Misc. pentest & bug bounty resources

- API Security Empire
- Awesome Tunneling
- Awesome Cloud Security
- GitHub Advisory Database & Intro
- GitLab community security advisory database & Intro

Articles

- How I use environment variable injection to execute arbitrary commands (in Chinese) & CentOS 7 exploit
- Automating bug bounties & HTTP Proxy
- Samesite: Hax – Exploiting CSRF With The Default Samesite Policy
- Introducing the Golden GMSA Attack
- Rogue RDP – Revisiting Initial Access Methods
- Find You: Building a stealth AirTag clone

Challenges

- Can you spot the vulnerability in this code snippet? & Solution

Bug bounty & Pentest news

- Bug bounty
  - Pre-registrations open for pathmapper (It does automated recon and test for path normalization bugs at scale)
- Upcoming events
  - Joe Grand's Open Lab: YouTube Live AMA (March 12)
  - Free webinars on Securzy (Prototype pollution on March 11, Amazon Cognito Misc-configurations on March 12, etc)
  - Web app hacking streams by @GarrGhar (Every Monday)
- Tool updates
  - Stepper v1.4.1
  - Amass v3.17.0
  - Uro 0.0.3
  - httpx v1.2.0

Non technical

- Bug Bounty: Do You Need To Be A Programmer?