Bug Bytes #105 – Playing with Spring Boot Actuators, recon API sources, JS encryption & A heaps of writeups

BY ANNA HAMMOND · JANUARY 13, 2021 · 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.

This issue covers the week from 03 to 10 of January.

Intigriti News

The cost of poor software quality, Zyxel backdoor & Yet another T-Mobile data breach

Our favorite 5 hacking items

1. Tool of the week

Microsubs

Microsubs is a new tool for interacting with recon APIs. @codingo_ presented it at BSides Brisbane. I was waiting for the talk to become public to talk about it, but it's been a month already.

It is interesting to play with Microsubs if you're interested in assets enumeration and understanding how API sources work by querying them directly. One particular use case is when different recon tools give unique results each and you want to use their sources directly instead of using all tools.

2. Writeups of the week

Exploiting Application-Level Profile Semantics (APLS)
Achieving Remote Code Execution By Exploiting Variable Check Feature
Stealing Your Private YouTube Videos, One Frame at a Time (Google, $5,000)

Create post on any Facebook page (Facebook, $30,000)
A 'Novel' Way to Bypass Executable Signature Checks with Electron

I know, FIVE writeups of the week is a lot, but they each have something different to teach.

@niemand_sec's writeup shows how to identify and exploit APLS, a data format worth learning about in case you encounter it in Web app tests.

@ShawarkOFFICIAL wrote about a remote code execution via file upload. The interesting part is that Python files uploaded are not executed directly but other endpoints process them, which lead to blind RCE (so, a sort of Out of Band unrestricted file upload).

The following two writeups by @Pouyadarabi and @xdavidhu are all about IDOR, simple bugs (doesn't mean easy to find!) with incredible impacts.

The last writeup is about exploiting Electron's update process to get local privilege escalation. This is a great piece for anyone interested in the security of Electron or desktop applications.

3. Article of the week

Remote Code Execution in Three Acts: Chaining Exposed Actuators and H2 Database Aliases in Spring Boot 2 & Sample app

This is great research on exploiting exposed Spring Boot Actuators. @spaceraccoonsec starts with exposed /actuator/env and /actuator/restart endpoints and chains them with H2 database aliases, a feature of H2 Database Engine that makes it possible to run arbitrary SQL queries. This, combined with some WAF bypass-fu results in arbitrary command injection and a very informative writeup.

If you'd like a challenge, start with the sample app and try to craft an exploit yourself before reading the article.

4. News of the week

Top 10 web hacking techniques of 2020 – nominations open

It's time to vote for your favorite Web hacking techniques of 2020! Most importantly, it is a good occasion to get acquainted with excellent research you might have missed last year.

5. Tutorial of the week

Client Side Encryption Bypass Part-1 & JavaScript Debugging Vulnerable Lab

This is the first article of a 3-parts series on breaking and bypassing JavaScript encryption when doing Web app testing. See how @sameer_bhatt does it using DevTools, practice on the provided vulnerable lab, and if you still want more there is also this related talk.

Other amazing things we stumbled upon this week

Videos

- How to Be an Ethical Hacker in 2021
- How We Hacked a TP-Link Router and Took Home $55.000 in Pwn2Own
- Exploiting PHP Type Juggling Vulnerabilities – Security Simplified
- Stealing all your cookies from your mobile Firefox browser – Bug Bounty Reports Explained
- Finding Your First Bug By U c l R a t @InsiderPhD
- What after Recon? – Manual Hunting: Escaping the Recon Trap
- How Attackers Bypass MFA (Multi-Factor Authentication) – Security Simplified
- @HackerSploit Talk About Getting Started With Ethical H@cking, CTFs,Bug Bounties & Creating Content
- How to move FAST in the Linux Terminal

Podcasts

- Security Now Out With The Old – SolarWinds Smoking Gun, Signal Influx of WhatsApp Users, Male Chastity Cage
- Risky Business #610 — Propellerheads in dark on JetBrains
- Security In Five Episode 901 – Google Titan Key Can Be Cloned, But I Wouldn't Worry About It Too Much
- Parler, Section 230, Venomous Bear, SolarWinds, UFOs, & Jason Wood – SWN #93
- FBI Warnings, SolarWinds, JetBrains, Government News, & 5G – Wrap Up – SWN #92
- Darknet Diaries Ep 82: Master of Pwn
- Malicious Life – Breaking Into Secure Buildings
- War on All Fronts: Rampant Kitten

Webinars & Webcasts

- OWASP Bangalore January 2021 Meet – OWASP Nettacker – Sam Stepanyan

Conferences

- Infosec In the City, SINCON 2020 & Abstracts

- How the Best Hackers Learn Their Craft
- A Midwinter Night's Con & Abstracts

Tutorials

Medium to advanced

- Lesser Known Techniques for Attacking AWS Environments & Some of the worst public security mistakes and delays in fixes by AWS in 2020
- Stealing your app's keychain entries from locked iPhone
- Azure AD. Attack of the Default Config #BlueTeam

Beginners corner

- A Pentester's Guide to Code Injection
- A Better Way To Use Twitter
- Understanding and Exploiting Zerologon

Writeups

Challenge writeups

- Hack The Box HTB x Uni Qualifier CTF 2020 – BoneChewerCon (Web) Write-up

Pentest writeups

- Insecure Deserialization – How To Trace Down A Gadget Chain

Responsible(ish) disclosure writeups

- Details about CVE-2020-26262, bypass of Coturn's default access control protection & TL;DR #WebRTC
- CVE-2020-35774: twitter-server XSS Vulnerability Discovered #Web
- Local Privilege Escalation 0day in PsExec Gets a Micropatch #LPE #Windows
- Getting root on a 4G LTE mobile hotspot #Reverse

Bug bounty writeups

- Create post on any Facebook page (Facebook, $30,000)
- Github Organization Takeover By Claiming Owner Invitation (Github, $5,000)
- A 'Novel' Way to Bypass Executable Signature Checks with Electron

- Unauthorized Access to OData Entities + $2K Bounty From Microsoft (Microsoft, $2,000)
- Blind XSS in Google Analytics Admin Panel — $3133.70 (Google, $3,133.70)
- Exploiting Max. Character Limitation ($500)
- Cloudflare-wide IP spoofing with Cloudflare Workers (Cloudflare)

See more writeups on The list of bug bounty writeups.

Tools

- gen.py: Open url redirect payload generator
- reconftw: Simple Bash script for full recon
- s3cario: Python3 tool for testing AWS S3 buckets (based on S3Cruze)
- takeover: A tool for testing subdomain takeover possibilities at a mass scale (similar to the discontinued SubOver)
- fcm_server_key: Python tool to extract & validate google fcm server keys from apks
- CISCO CVE-2020-3452 Scanner & Exploiter
- EarlyBird: A sensitive data detection tool (in Go) capable of scanning source code repositories for clear text password violations, PII, outdated cryptography methods, key files and more
- Pup: Go tool for parsing HTML at the command line
- Ligolo: Reverse Tunneling made easy for pentesters, by pentesters

Misc. pentest & bug bounty resources

- @harshbothra_'s Learn365 Challenge
- Comparison of subdomain enumeration tools (Aiosdns, Amass, Crtsh & Subfinder)
- Kubernetes security resources
- Find a target in a LAN via a stored XSS
- Public Bug Bounty Targets Data: 5.1M sub-domains and assets taken from @pdiscoveryio's Chaos
- OWASP Vulnerability Disclosure Cheat Sheet
- Linux Hardening Guide

Articles

- Universal Deserialisation Gadget for Ruby 2.x-3.x
- Cache Poisoning Denial-of-Service Attack Techniques

- Hacking QR code design
- An Outlook parasite for stealth persistence

Bug bounty & Pentest news

- Defense Digital Service Kicks Off Third 'hack The Army' Bug Bounty Challenge With Hackerone
- New Hacker101 resources: Report Writing, Communication Tips, and Community Guidelines
- January OWASP Diversity Scholarship Application: Deadline is January 18
- HackerConf 2021: January 20, talks in Turkish & English
- SANS Open-Source Intelligence Summit: February 11-12

Non technical

- Bug bounty isn't dying. It's the future.
- Burp Customizer! Change your burpsuite theme
- Four levels of maturity that bridge the AppSec / engineering divide
- Hacker Spotlight: Interview With Jin0ne
- Three Word Passwords
- QR codes: Best approaches to using the technology safely and securely

Tweeted this week

We created a collection of our favorite pentest & bug bounty related tweets shared this past week. You're welcome to read them directly on Twitter: Tweets from 01/01/2021 to 01/03/2021.