Bug Bytes #114 – Binary fuzzing for Web vulnerabilities, Leaky page & NahamCon2021

BY ANNA HAMMOND · MARCH 17, 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 March 8 to 15.

Intigriti News

[Channeling the Wisdom of the Crowd: Talking with Intigriti's Stijn Jans and Inti De Ceukelaire]

[Everything you need to know about the Exchange attacks frenzy, Verkada breach, F5 CVEs & Azure threat]

Our favorite 5 hacking items

1. Article of the week

Finding Issues In Regular Expression Logic Using Differential Fuzzing

I think some of the most interesting attacks and research are at the intersection of different fields of offensive security. This is a good example by @defparam. He shows how to use differential fuzzing to find logic flaws in web-related regular expressions.

2. Writeups of the week

Obtaining .NET Assemblies from Android Full AOT Compiled Applications
CVE-2020-29653: Stealing Froxlor login credentials using dangling markup
Messing with GitHub's fork collaboration for fun and profit (GitHub, $30,000)

The first writeup shows a method for extracting assemblies from Android applications compiled with AOT. It might be useful to know for a future mobile engagement.

The second writeup shows a useful technique to remember when you find a HTML injection and want to increase its impact because XSS just isn't possible.

Lastly, @not_an_aardvark found some pretty serious broken access control issues on GitHub. It's a very interesting writeup on GitHub's fork collaboration feature.

3. Vulnerability of the week

leaky.page & A Spectre proof-of-concept for a Spectre-proof web

This is worrying research on Spectre by Google's Security Team. They showed that it is a pratical attack with a Proof of Concept site that can leak information from victims' browser memory!

4. Tools of the week

Regexploit & Intro
wl

Regexploit is a Python tool that helps find regular expressions vulnerable to ReDoS. Judging from the list of vulnerabilities @doyensec discovered using it, it seems very effective and worth a try.

Wl is @s0md3v's latest tool. It's a Go utility that converts strings to different casing styles, which is so handy for credentials bruteforce and content discovery.

5. Conference of the week

Main track

- Learn To Hack, Choose A Target, ???, Get A Bounty
- Amassive Leap in Host Discovery
- Just Give me a Trial, Please
- Hacking IIS

Recon Village

- ffuf scripts and tricks
- Building Faster Than Light Reconnaissance
- Kickstart your reconnaissance with BBRF & bbrf-agents
- Introduction to Axiom – The Dynamic Infrastructure Framework for Everybody! & Slides / demo
- Introducing dooked

NahamCON 2021: Red Team Village & Slides:

- xsstools
- Learning How to Reverse Engineer an Android App
- Exploiting Layer 3 and Beyond (Lab)& VyOS 1.1.8 ISO
- Atomic Red Team: Hands-on Getting Started Guide

Wasn't NahamCon fantastic? I love a good offensive security conference! Since the main track and villages were happenning at the same time, you might've missed interesting talks. So, here's the list of all NahamCon talks and slides I found public if you want to catch up.

Other amazing things we stumbled upon this week

Videos

- [PYTHON] Differential Fuzzing to find logic bugs inside Python email validators (Atheris)
- How to Use X11 Forwarding on Windows or Linux
- You Do (Not) Understand Kerberos & Slides
- Alfred WebApp Payloads Demo (XSS & Reverse Shell Payloads!) (cool idea for MacOS users)
- SQL Injection – Lab #2 SQL injection vulnerability allowing login bypass
- Python Dependency Confusion (Demystified) & Blog post
- Browser Security – Part one : My Interview with Abdulrahman Alqabandi @qab @microsoft & Part two

Podcasts

- DAY[0] Episode 68 – Hacking Cameras, Stealing Logins, and Breaking Git
- Pentester Diaries Ep1: Understanding Business Logic
- ProxyLogon – New Chrome 0-Day, Patch Tuesday Redux, Spectre Comes to Chrome
- Darknet Diaries Ep 87: Guild of the Grumpy Old Hackers

Webinars & Webcasts

- Red Team Village – IPv6 Security Workshop

Conferences

- How Bad Can Clicking a Link Be? Getting Shells From Javascript, Offensive JS: BSidesSF2021

Tutorials

- Encoding Mutations: A Base64 Case Study
- Creating a Red & Blue Team Homelab
- How To Regex: A Practical Guide To Regular Expressions (Regex) For Hackers
- Writing Basic Offensive Tooling in Nim

Writeups

Responsible(ish) disclosure writeups

- CVE-2021-27927: CSRF to RCE Chain in Zabbix #Web
- Exploiting HTTP Request Smuggling (TE.CL)— XSS to website takeover #Web
- How we could have listened to anyone's call recordings #iOS
- CVE-2020-5377: Dell OpenManage Server Administrator File Read #Web
- SSD Advisory – GNU GRUB Command Injection #Linux #LPE
- Technical Advisory: Dell SupportAssist Local Privilege Escalation (CVE-2021-21518) #Windows #LPE

Bug bounty writeups

- Malicious repositories can execute remote code while cloning (GitHub)
- [Google VRP] How I Get Blind XSS At Google With Dork (First Bounty and HOF) (Google, $3,133.70)
- Facebook Group Members Disclosure. (Facebook, $9,000)
- Finding keys under the door (Paytm)
- Voice Confusion When Commenting On Watch Party (Facebook, $1,000)

See more writeups on The list of bug bounty writeups.

Tools

- ZAP Automation Framework: ZAP add-on that provides a framework for automation
- go-dork & Dorking on Steroids: Fast dork scanner written in Go

- jsmonitor.py: JavaScript files monitor
- SerialDetector & Intro: A proof-of-concept tool for detection and exploitation Object Injection Vulnerabilities in .NET applications
- Vajra & Intro: A highly customizable target and scope based automated web hacking framework (with GUI @ a CouchDB database)

Tips & Tweets

- Decompiling a large list of DLL files back to source code
- XSS WAF bypass by adding JS comments between a function name and its arguments
- Pentest tales by @plaverty9 and @ippsec
- PostgreSQL Injection tricks
- Burp extensions keep being disabled? Quitting Burp using +q might be the cause!

Misc. pentest & bug bounty resources

- @defparam's JSON/Structure aware fuzzer for turbo intruder & Turbo Intruder Cluster Bomb with Smart Filtering
- Bugcrowd Tip Jar
- secure-cookie.io
- Hacking the Cloud
- The Best Ethical Hacking Tools of 2021 (and their basic usage)
- Uncle Rat's ultimate bug bounty guide (50% off until March 20)

Challenges

- @theXSSrat Free labs

Articles

- API Scanning with Burp Suite
- Post-Spectre Web Development (W3C Editor's Draft)
- Github Actions and the threat of malicious pull requests
- The Battle Between White Box And Black Box Bug Hunting In Wireless Routers
- Phishing Users to Take a Test

Bug bounty & Pentest news

- ZAP Report Competition
- PancakesCon 2 (March 21)
- null Ahmedabad Meet 21 March 2021 Monthly Meet Cancel Registration (March 21)
- FuzzCon Europe (March 24)
- Bitcoin exchange Sovryn launches record $1.25m bug bounty program
- Updates on Shopify's Bug Bounty Program
- Inside the Bug Bounty Council at GitLab

Non technical

- The Penetration Testing Guide I Wish I Had
- Offensive Security Experienced Penetration Tester (OSEP) Review and Exam

Community pick of the week

Nice rig there, @plenumlab! We love it and hope it'll help you find more cool bugs.

Want to share your bug bounty wins, swag and joys with other Bug Bytes readers? Tag us on social media, we'd love to hear from you too!