Bug Bytes #124 – The 2021 hacker report, a port scanning Armada & SSTI to RCE in Go apps

BY ANNA HAMMOND · MAY 26, 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.

CLICK HERE TO SUBSCRIBE

This issue covers the week from May 17 to 24.

Intigriti News

The Ethical Hacker Insights Report 2021

Our favorite 5 hacking items

1. Tools of the week

Armada
IPATool

Armada is @d0nutptr's high performance TCP SYN port scanner in Rust. It doesn't do any type of scans other than TCP SYN scans (so Nmap isn't dead yet!), but does that extremely fast.
I did a mini-benchmark by scanning all TCP ports on a target just to get an idea of its performance. Masscan was fast but missed the open ports (maybe I misused it?), Nmap would've surely found them but it was so slow I stopped it, and Armada found all open ports in less than a minute. Armada's accuracy and speed make it a worthwhile tool to experiment with.

IPATool allows you to search and download iOS app packages (or IPA files) from the App Store using your Apple ID, all from the command-line. It supports 2FA and streamlines the process of fetching IPA files, making it a very useful utility for iOS app testers. Great work by @freemanrepo!

2. Writeup of the week

Finding and Exploiting Unintended Functionality in Main Web App APIs ($4,000)

This is an excellent writeup on API hacking. @bendtheory reports two vulnerabilities (IDOR and Information disclosure / Privilege escalation) found on bug bounty programs and, more importantly, the detailed methodology used to find them. It is generic enough that you can reproduce it and add to it to find similar bugs on other targets.

3. Videos of the week

SecuriTEA & Crumpets – Episode 6 – Gareth Heyes – Hackvertor
Why do Bug Bounty hunters love Obsidian?

If you're curious to know how Hackvector's own creator, @garethheyes uses it, I highly recommend the first video. In addition to the tool's basics, Gareth covers some advanced features like custom tags, tag variables, how to use Hackvector in Repeater and Intruder, how to use it for JS hacking, etc.
Make sure you're not missing out on any features of this powerful Burp extension!

The second video is about note-taking. Even if you don't want to use Obsidian, it is very informative for anyone who struggles with organizing bug bounty notes.
@InsiderPhD goes over the different types of notes you can take during bug hunting (knowledge base vs notes on targets), a methodology for note-taking, and how Obsidian has unique features that make it complementary to other tools like Notion.

4. Article of the week

Method Confusion In Go SSTIs Lead To File Read And RCE.

If you look at SSTI research and repos like PayloadsAllTheThings and HackTricks, there isn't much about SSTI in Go apps. The only resource I could find is this article about exploiting SSTI in Go to get XSS. But what if we want more than a simple PoC or XSS? What if we want RCE?

That's what this new research by @SecGus is all about. It describes how methods defined in the modules imported by an app can be called using template injection, and leading to various actions like File read or RCE.

5. Conference of the week

HTTP Request Smuggling via higher HTTP versions, Slides, Additional tip & All PHDays 10 talks

PHDays 10 videos are released, including many interesting talks for pentesters and bug hunters on topics like insecure deserialization, pentesting AI apps, pwning mobile apps and WebView security. There is only one small hiccup: talks are in Russian, dubbed in English with some slides only in Russian.
It's still worth checking out, especially @emil_lerner's presentation on new HTTP Request Smuggling research.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- No BS Guide – Advanced Burp (Free) Tricks For Bug Bounty
- Troubleshooting AFL Fuzzing Problems & Blog post
- Windows Privilege Escalation Tutorial For Beginners
- From CTFs to Real-World Exploitation & Blog posts
- TheCyberMentor Talks about Pentesting, security jobs,Certifications business, interviews& Resume

Podcasts

- DAY[0] Episode 78 – NoSQL Injection, Mobile Misconfigurations and a Wormable Windows Bug
- The Dark Escrow – Firefox Fission, Doom CAPTCHA, Conti and CNA Financial Ransomware

Webinars

- Hackin' Your Career – Top 10 Ways to Stand Out in Your Cyber Career – Russell Eubanks – 1 Hour

Conferences

- Deep dive into ART(Android Runtime) for dynamic binary analysis | SungHyoun Song | Nullcon 2021

Tutorials

Medium to advanced

- That single GraphQL issue that you keep missing
- My bounty infrastructure

- Life's a Peach (Fuzzer): How to Build and Use GitLab's Open-Source Protocol Fuzzer
- Digging into cgroups Escape
- Why DNSAdmins privilege escalation is still working ?

Beginners corner

- 5 minutes to Build a Basic Monitoring and Alerting System for New Subdomains & Video
- Web App Pentesting With Burp Suite Scan Profiles
- Hacker tools: SQLMap – Finding SQLi like a pro.
- Security headers quick reference

Writeups

Pentest writeups

- Dont just sanitize but also escape – A fable of sanitize_text_field

Responsible(ish) disclosure writeups

- NoSQL Injections in Rocket.Chat 3.12.1: How A Small Leak Grounds A Rocket #Web
- (0Day) Lepide AD Self-Service – forced browsing to RCE #LADSS #RCE
- QNAP MusicStation/MalwareRemover Pre-Auth Remote Code Execution #Web #RCE #CodeReview
- 13 Nagios Vulnerabilities, #7 will SHOCK you! #Web
- WordPress XXE Vulnerability in Media Library – CVE-2021-29447 #Web
- GHSL-2021-023: Remote code execution in squirrelly – CVE-2021-32819 #Web
- Attacking Kubernetes Clusters Through Your Network Plumbing: Part 2 #Kubernetes #BGP

Bug bounty writeups

- Finding and Exploiting Unintended Functionality in Main Web App APIs ($4,000)
- XSS via postMessage in chat.mozilla.org (Mozilla, $500)
- Oculus SSO "Account Linking" bug leads to account takeover on third party websites and inside VR Games/Apps (Facebook, $12,000)
- SSRF in PDF Renderer using SVG ($2,150)
- CVE-2020-35580
- Arbitrary file read during project import (GitLab, $16,000)
- SSRF at https://qiwi.com using "Prerender HAR Capturer" (QIWI, $1,500)

See more writeups on The list of bug bounty writeups.

Tools

- DivideAndScan: Automate port scans into 3 phases using Nmap and Masscan / RustScan / Naabu
- pyWhat: Identify anything. pyWhat easily lets you identify emails, IP addresses, and more. Feed it a .pcap file or some text and it'll tell you what it is!
- HelpColor: Agressor script that lists available Cobalt Strike beacon commands and colors them based on their type
- DNSStager & Intro: A Pythool tool to hide your payload in DNS

Misc. pentest & bug bounty resources

- Burp tips and tricks
- Bug Bounty Bootcamp (Early access, includes free chapter on Open redirects)
- Great getting started resources for new users of Burp Suite Professional
- What The F# & Intro
- SimuLand: Tool by Microsoft to help security researchers deploy lab environments that reproduce well-known techniques used in real attack scenarios
- Awesome-HTTPRequestSmuggling

Challenges

- HackMyvM
- vAPI & Walkthrough

Articles

- How to Exploit Active Directory ACL Attack Paths Through LDAP Relaying Attacks
- The Android Platform Security Model
- Introducing Firefox's new Site Isolation Security Architecture
- FragAttacks: Clarifying Some Aspects
- Extended Flow Guard Under The Microscope
- IBM Spectrum Protect: Exploiting Legacy Authentication Protocol

Bug bounty & Pentest news

- Celebrating Todayisnew With The 100k CTF, AMA, And Giveaway
- Android Security Rewards Program Rules until 6/18/21

Non technical

- Top Organizations on GitHub Vulnerable to Dependency Confusion Attacks
- The Ethical Hacker Insights Report 2021
- 'Soft skills are the most under-researched area of the bug bounty industry' – 'Reconless' YouTubers on filling a gap in infosec education
- How to Write an Effective Pentest Report: Vulnerability Reports

Community pick of the week

Excellent thinking, @CookiesHttpOnly. Very well done!

Do you also have bug bounty wins, swag and joys to share with other Bug Bytes readers? Tag us on social media, we love to hear from you!