Bug Bytes #74 – Testing for SSTI in Go, SSRF in Facebook and Kubernetes & PwnFox for a better Burp/Firefox experience

BY ANNA HAMMOND · JUNE 10, 2020 · 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 29 of May to 05 of June.

Our favorite 5 hacking items

1. Article of the week

[SSTI] Breaking Go's template engine to get XSS

This is some cool research that will come in handy if you want to test a server written in Go, especially for SSTI. Existing public payloads like `{{7*7}}` will not work. Thankfully, @0xtakemyhand dissected the documentation and came up with the right syntax and payloads for detecting and exploiting SSTI in Go.

2. Writeups of the week

How I made $31500 by submitting a bug to Facebook & Additional info on the payout (Facebook, $31,500)

When it's not only about a Kubernetes CVE... (Microsoft, +$40,000)

SSRF is all the rage. These are two detailed writeups of SSRF vulnerabilities found on Facebook and Kubernetes.

They're worth reading with attention considering the hardened targets, the impressive bounties, the quality of the writeups that include a lot of details on detection, exploitation, and increasing impact.

3. Tools of the week

PwnFox

Hardcodes

PwnFox is THE browser extension I was waiting for. It is similar to Autochrome but for Firefox. The feature I like the most is that when you use Firefox containers, PwnFox can automatically color Burp requests depending on the corresponding container. So helpful for authorization tests! Other cool features are a PostMessage logger, a checkbox to enable/disable Burp proxy, the ability to remove security headers...

Hardcodes is @s0md3v's latest tool. It extracts hardcoded strings from source code, and can handle any syntax and 20+ languages. It can be used as a library or a CLI program, and returns less noise than existing search tools (like *grep* or *strings*). So, it is useful for extracting hardcoded credentials from mobile apps, secrets and endpoints from Github code, etc.

4. Video of the week

@irsdl Talks About Value Behind Certificates, Pentesting vs Bug Bounty, Deserialization and more!

@irsdl / Soroush Dalili's blog posts are regularly listed in this newsletter. I associate his name with good research, numerous responsible disclosures, and with deserialization bugs in particular. This is an excellent interview where we can get to know the man behind the bugs, his unique journey as a hacker that started way back in 2003, his views on work-life balance, etc. I really appreciate the candor and humility with which he shares his experience and advice.

5. Tutorial of the week

Hacking a GWT application from scratch, Companion blog post & GWTab

This tutorial will be very helpful if you come across Google Web Toolkit requests. It explains what GWT is, how to analyze the requests, how to detect vulnerabilities like IDOR, with a new tool to make the process easier.

Maybe you've already seen GWT requests, they look like this: `7|0|8|http://127.0.0.1:8888/helloworld/|0AA7A0C25ADF167CC648926141094922|com.example.test.client.GreetingService|...`.

GWT is an old technology that may not be often encountered, but I think it worth knowing because it is not dead. Google released an update just a month ago and, at the time of writing this, 41,993 websites are using it.

Other amazing things we stumbled upon this week

Videos

- Burp for Beginners: Introduction to Burp
- Bounty Thursdays – CHAOS, HTTPX, XSS challenge, H1-2006 CTF, DNSCEWL, NAHAMCON and much more.
- Hacking a GWT application from scratch #bugbounty #hacking #pentest & Companion blog post
- 10 Minute Tip: Finding User Accounts Across Social Media
- CTFs are TERRIBLE! & CTFs are AWESOME!
- Bug bounty starter tips and resources

- Bug Bounty Queries: stealth scan, why reverse Whois, finding webservers and much more(+Thebinarybot)

Podcasts

- 7MS #417: Vulnerability Scanning Tips and Tricks
- Hack for Fun and Profit – Bug bounty tools for beginners: Recon and subdomain enumeration & Bug bounty tools from enumeration to reporting
- Security Now 769 – Zoom's E2EE Design
- Risky Business #586 — Google TAGs Indian mercenaries
- Naked Security podcast – S2 Ep42: Apple auth attack, Octopus Scanner, Escobar escapades
- The Many Hats Club Ep. 54, Web is all around (with Sean Wright)
- The Many Hats Club Ep. 62, From Hacker to CISO and beyond (with Mike Koss)
- SWN #39 – Anonymous Returns, Zephyr Vulns, & SpaceX Docks
- SWN #40 – Wrap Up – Anonymous Returns, Deep Fakes, & IP in IP Vulns
- PSW #654 – Root Cert Chaos, Octopus Scanner, & RobbinHood & the Merry Men

Webinars & Webcasts

- Introduction to Writing Nmap NSE Scripts
- Webinar: Seeing the Entire Software Security Picture
- A Blue Team's Perspective on Red Team Hack Tools
- Securing your code with CodeQL with Sasha Rosenbaum! – OWASP DevSlop
- DC44141 June 2020 – Ladder Logic and Social Engineering

Conferences

- OWASP Chapters All Day 2020 & Schedule
- GRIMMCon – Track 1 & Track 2

Tutorials

Medium to advanced

- How SSL Kill Switch works on iOS 12
- Bypassing Android's RootBeer Library — Part 1

- Semgrep: Stop grepping code
- Apache Tomcat RCE by deserialization (CVE-2020-9484) – write-up and exploit
- Attacking FreeIPA — Part III: Finding A Path
- Introduction to PLCs and Ladder Logic

Beginners corner

- PowerPoint — What data is beneath the surface?
- Guide to Harnessing the Power of 360 Virtual Tours for Everyday Investigations.
- Pimp my terminal
- Web Security 101: Cross-Site Scripting (XSS) Attacks
- How to exploit the PHAR Deserialization Vulnerability
- Building an Active Directory Lab
- Building an ActiveDirectory Lab with just 4GB of RAM
- Linux Privilege Escalation with LinEnum
- What Is the POODLE Attack?
- Offense and Defense – A Tale of Two Sides: (Windows) OS Credential Dumping

Writeups

Challenge writeups

- Pwn2Win 2020 Challenges, Solutions for Watchers & Scriptless
- Out-of-Band Remote Command Execution Challenge

Pentest writeups

- Accessing PowerShell in Restricted VDI Environment — VDI Pentesting
- Reflected File Download (RFD) — Windows Script Host

Responsible(ish) disclosure writeups

- Kibana Blind SSRF PoC (CVE-2019-7616) #Web
- Full infrastructure takeover of VMware Cloud Director (CVE-2020-3956) #Web
- Vulnerability Spotlight: Two vulnerabilities in Zoom could lead to code execution
- CVE-2019-16384, 85: Cyblesoft Thinfinity VirtualUI – Path Traversal, HTTP Header Injection #Web

- Web Application Firewall bypass in Bitrix CMS #Web
- Smart Phishing using Ticket Feature of a Customer Support Software #Web
- Pwn2Own or Not2Pwn, Part 2.5: A brief tale of free 0days #Windows #.NET

Bug bounty writeups

- How I made $31500 by submitting a bug to Facebook
- When it's not only about a Kubernetes CVE... (Microsoft, +$40,000)
- Another image removal vulnerability on Facebook (Facebook, $10,000)
- Hunting on ASPX Application For P1's [Unauthenticated SOAP,RCE, Info Disclosure]
- Privilege Escalation in Google Cloud Platform's OS Login (Google)
- h1{Error based XXE – bug bounty writeup}
- Weird "Subdomain Take Over" pattern of Amazon S3
- Information disclosure and reflected XSS on Tokopedia (Tokopedia)
- From CRLF to Account Takeover
- Analysis of CVE-2020-13693 (WordPress)
- Unauthorized access to metadata of undisclosed reports that were retested (HackerOne, $2,500)
- Code injection possible with malformed Nextcloud Talk chat commands (Nextcloud, $3,000)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Shodanfy.py: Get ports,vulnerabilities,informations,banners,..etc for any IP with Shodan (no apikey & no rate-limit)
- Cf-check: Check an IP is Owned by Cloudflare

More tools, if you have time

- wwwordlist: Python tool to generate a wordlist from either text or the links in HTML
- GitMonitor: A Github scanning system to look for leaked sensitive information based on rules
- ssrf-finder: Pass list of urls with FUZZ in and it will check if it has found a potential SSRF
- Jecretz: Jira Secret Hunter – Helps you find credentials and sensitive contents in Jira tickets

- Urldedupe: Pass in a list of URLs with query strings, get back a unique list of URLs and query string combinations
- AWS_Loot: Pull secrets from an AWS environment by searching for high entropy values, useful for post-exploitation
- Burp-samesite-reporter: Burp extension that passively reports various SameSite flags
- URLProbe: Urls status code & content length checker in Go
- TeaBreak & Intro: A productivity Burp extension which reminds to take break while you are at work!
- Njsscan: A SAST tool that can find insecure code patterns in node.js apps using simple pattern matcher from libsast & semgrep
- O365enum: Office 365 User Enumeration Reloaded
- Go-gtfo: GTFO, now with the speed of Golang
- Enumy: Linux post exploitation privilege escalation enumeration
- ADCollector: A lightweight tool to quickly extract valuable information from the Active Directory environment for both attacking and defending

Misc. pentest & bug bounty resources

- List of all links in Web Application Hacking Techniques since 2006
- Phonebook.cz
- Hacktory (30-day free trial) & Beginner tutorials
- HackTricks
- @madhuakula's content from 30+ conferences
- Active Directory Security Assessment Checklist by CERT-FR
- random-robbie/bruteforce-lists
- vict0ni's Bug Bounty scripts
- Osint Curious OSINT Resource List
- Linux Privilege Escalation Cheatsheet for OSCP & Windows Privilege Escalation Cheatsheet for OSCP

Articles

- Comparison of Different Android Root-Detection Bypass Tools
- Keeping a Grip on GoogleID's

- Who do you trust?
- From Azure AD to Active Directory (via Azure) – An Unanticipated Attack Path
- Quantifying the Impact of Micro-Segmentation
- Tampering with Digitally Signed VBA Projects
- Common Insecure Practices with Configuring and Extending Salesforce
- Chimichurri Reloaded – Giving a Second Life to a 10-year old Windows Vulnerability

News

Bug bounty & Pentest news

- NahamCon 2020 & CTF: June 13
- Interesting discussion on XSS PoCs
- InQL added to Burp's BApp Store
- ZAP 2.9 Highlights
- Microsoft throws weight behind machine learning hacking competition
- Intigriti quarterly top 3 get exclusive hacker portraits
- A PortSwigger impossible lab was solved by @shafigullin & @lbherrera_
- Rendering non-printing characters in the Burp Suite message editor (June 2020 feature release) (Video)

Reports

- Psychology of Passwords – The Online Behavior That's Putting You at Risk
- Cloud security: 'Suspicious superhumans' behind rise in attacks on online services
- Veracode's Open Source Security Report Finds Library-Induced Flaws in 70% of Applications
- Threat Spotlight: Form-based attacks

Vulnerabilities

- This wallpaper will crash your Android phone: don't try it.
- Haveibeenpwned.com pwned our helpdesk! GLPI 9.4.5 SQL Injection
- Web Browsers still allow drive-by-downloads in 2020
- Grafana fixes vulnerability in data visualization tool
- Windows 10 SMBGhost bug gets public proof-of-concept RCE exploit

- Severe Cisco DoS Flaw Can Cripple Nexus Switches
- VMware Cloud Director vulnerability allowed for full cloud infrastructure takeover
- Google's indexing of WhatsApp numbers raises privacy concerns
- New cold boot attack affects seven years of LG Android smartphones
- Two Critical Android Bugs Open Door to RCE
- Linus Torvalds rejects 'beyond stupid' AWS-made Linux patch for Intel CPU Snoop attack

Breaches & Attacks

- USBCulprit malware targets air-gapped systems to steal govt info
- Hacker leaks database of dark web hosting provider
- This new ransomware is targeting Windows and Linux PCs with a 'unique' attack
- REvil ransomware creates eBay-like auction site for stolen data
- Google: Chinese and Iranian hackers targeted Biden and Trump campaign staffers
- Hackers tried to steal database logins from 1.3M WordPress sites
- Cloudflare tracks massive spike in cyber-attacks as protests rage against George Floyd death

Other news

- How do tech giants know so much about you?
- Got $50k spare? Then you can crack SHA-1 – so OpenSSH is deprecating flawed hashing algo in a 'near-future release'
- Clearview AI facial recogition sued again – this time by ACLU
- FIRST updates guidelines for multi-party vulnerability disclosure
- Apple Jailbreak Zero-Day Gets a Patch
- Zoom Restricts End-to-End Encryption to Paid Users
- Analysing the (Alleged) Minneapolis Police Department "Hack"
- YouTube channel credentials in high demand on hacker forums
- Mulled Chrome API shines light on long-neglected privacy gap: Sites can snoop on your find-in-page searches
- $5bn+ sueball bounces into Google's court over claims it continues to track netizens in 'private browsing mode'

Non technical

- Top #10 Vulnerabilities: Internal Infrastructure Pentest
- Theft From Online Shopping Carts – Past and Present
- A Pentester Setup
- Hacker Spotlight: Interview with alyssa_herrera
- So you want to be a hacker?
- IT Security Certifications & Degrees: Necessary or Not?
- Extracting yourself from the quagmire of a successful Red Team.
- Wargaming GIAC Certifications

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 05/29/2020 to 06/05/2020.