Bug Bytes #99 – Bypassing bots and WAFs, JQ in Burp & Smarter JSON fuzzing and subdomain takeovers

BY ANNA HAMMOND · DECEMBER 2, 2020 · LAST UPDATED ON MARCH 6, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-99-bypassing-bots-and-wafs-jq-in-burp-smarter-json-fuzzing-and-subdomain-takeovers

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 22 to 29 of November.

Intigriti News

SEO ransomware, Vulnerability lifecycle & Stress blamed for email data breaches

Our favorite 5 hacking items

1. Conference of the week

Modern WAF Bypass Scripting Techniques for Autonomous Attacks

This is a talk for developers but hackers looking to bypass bot detection (for bruteforce, Web scraping, etc) will also probably find it insightful. @J0hnnyXm4s goes over several techniques used by WAFs to detect bots and how they can easily be bypassed.

2. Writeups of the week

Don't Fear The Bark, Ts_rewrite To Dodge The Mark
CRLF injection & SSRF in git:// protocal lead to arbitrary code execution (GitLab)

The first writeup is about some obscure PostgreSQL features that helped bypass a WAF (probably BIGIP F5) and fully exploit a SQL injection. It could be of great help if you're facing similar technologies.

The second writeup is a clever CRLF injection and SSRF in GitLab. They allow for abusing a Redis server and getting RCE.

3. Videos of the week

Finding DOMXSS with DevTools | Untrusted Types Chrome Extension
Subdomain Takeovers, beyond the basics for Pentesters and Bug Bounty Hunters

Remember @filedescriptor's Untrusted Types, the Chrome extension for logging DOM sinks? He just released a short demonstration to show how he uses it to detect DOM XSS.

The second video is gold if you're interested in subdomain takeovers. It is a type of vulnerability that is getting more and more difficult to find in bug bounties because of the competition and automation some use. So, @codingo_'s tricks are eye-opening.

4. Tools of the week

jdam
Burp JQ
Burp to Slack

These are three very practical tools for Web application security testing.

Jdam is a Go tool for JSON fuzzing. Contrary to most existing fuzzing tools, it keeps the JSON valid when replacing values with payloads for fuzzing.

Burp JQ is a Burp extension that adds a "JQ" tab to the HTTP message viewer. It allows you to apply JS queries to JSON content directly from Burp.

Burp to Slack is a Burp extension for sending notifications to Slack or a custom server based on responses matching a pre-defined condition. It is helpful when you want to be immediatly notified of a certain condition (e.g. a string found in a response in Intruder/Repeater/Proxy/Scanner) without keeping an eye on Burp.

5. Tutorial of the week

randomua – Inject random user-agent in pentest CLI tools

Randomua is a Ruby tool that generates random User-Agent strings of different types (desktop browser, mobile, email client, cloud platform...). It is not new but can help bypass WAFs. This tutorial shows how to use it in combination with other CLI tools like ffuf, sqlmap, testssl, nikto, etc.

Other amazing things we stumbled upon this week

Videos

- We Hacked Apple and Made $500,000 in Bounties
- 5 Common Critical/p1 Bugs To Look Out For!

- Server-Side Template Injections Explained
- Bounty Thursdays – Wordlists for content discovery and API bugs!
- Attacking Web applications & Linux Security
- Faster Bounty Rewards With 5 Easy Tips
- HackerOne & The Paranoids Present: #h12010 Qualifier Wrap up & Community Day
- StreamTitle Ep.2: a chat on CSP (feat. Michele Spagnuolo)
- Kali on Windows WSL for Pentester & Bug Bounty Hunter | Local Recon | Hacking Machine | No VPS / VM

Podcasts

- Cicada – Ongoing WordPress Attack, RCS Gets End-to-End Encryption
- Darknet Diaries: EP 79: DARK BASIN
- Absolute AppSec Ep. #116 – Lewis Ardern & Pwnfunction
- The Many Hats Club Ep. 77, Breaking and Entering...your network (with TinkerSec)
- New Magecart Attacks, GoDaddy DNS Attacks, & Ryan Corey – SWN #85

Webinars & Webcasts

- Continuously Hack Yourself because WAF security is not enough
- Cloud Complexities: Navigating the Headwinds

Conferences

- HITB+CyberWeek Virtual 2020 Red Team Village Talks – Day 1, Day 2 & Schedule
- GreHack 2020

Slides & Workshop material

- HITB+CyberWeek (Main Track)

Tutorials

Medium to advanced

- Socket Programming & the Bizarre TCP/IP Port 0 Saga
- Potatoes – Windows Privilege Escalation
- OffSecOps Basic Setup

- Tracking Windows Updates with Git and CI

Beginners corner

- Common Federated Identity Protocols: OpenID Connect vs OAuth vs SAML 2
- How to Execute an XML External Entity Injection (XXE)
- Testing for Directory or Path Traversal Vulnerabilities
- Dark Web Searching
- Azure Security Basics: Log Analytics, Security Center, and Sentinel #BlueTeam
- Just another SNMP article — The Hacker's Way!

Writeups

Challenge writeups

- flAWS training complementary solution
- OSINT: When Was This Photo Taken?

Pentest writeups

- Don't Fear The Bark, Ts_rewrite To Dodge The Mark
- DirectAccess and Kerberos Resource-based Constrained Delegation
- Hindering Threat Hunting, a tale of evasion in a restricted environment

Responsible(ish) disclosure writeups

- CVE-2020-28360: npm private-ip SSRF Bypass (IP Phone Home) #Web
- Detailing Saltstack Salt Command Injection Vulnerabilities #Web #CodeReview
- Securing the fight against COVID-19 through open source
- Cross-site Scripting via WHOIS and DNS Records #Web
- Drupal Core: Behind the Vulnerability #Web
- Multiple Vulnerabilities Discovered in Aviatrix #Web #RCE
- SD-PWN Part 4 — VMware VeloCloud — The Last Takeover #Web
- Vulnerabilities in Checkpoint ICA Management Tool #Web
- Discovering, exploiting and shutting down a dangerous Windows print spooler vulnerability #Windows #LPE

Bug bounty writeups

- Issue 2098: Facebook Messenger for Android: SdpUpdate message can cause audio call to connect before callee has answered the call (Facebook, $60,000)
- Subdomain Takeover in Azure: making a PoC
- Chaining Multiple Requests to Achieve Rate Limiting Vulnerabilities
- Arbitrary File Write On Client By ADB Pull (Google)
- XSS on Issue reference numbers (GitLab, $1,500)
- Host `docker` binary overwrite from Kata VM ($20,000)
- Server-Side Request Forgery using Javascript allows to exfill data from Google Metadata (Snapchat, $4,000)
- CRLF injection & SSRF in git:// protocal lead to arbitrary code execution (GitLab)
- Remote code execution on Basecamp.com (Basecamp, $5,000)

See more writeups on The list of bug bounty writeups.

Tools

- byp4xx.sh: Simple bash script to bypass "403 Forbidden" messages with well-known methods discussed in #bugbountytips
- RESTler, REST API Fuzz Testing (RAFT) & Intro: Find security and reliability bugs through automated fuzzing
- IntRudeX & Intro: Burp extension that provides an interface to generate Intruder payload positions based on results from a regex
- S3 Objects Check: Whitebox evaluation of effective S3 object permissions, to identify publicly accessible files
- JARM & Intro: Easily Identify Malicious Servers on the Internet with JARM
- jarm-go: A Go implementation of JARM
- stats.rb & Intro: Metasploit plugin to displaying stats about the current workspace such as most popular ports, total hosts/services, etc
- ADLab & Intro: Active Directory Lab Setup Tool
- Cottontail: Capture all RabbitMQ messages being sent through a broker
- NetworkSniffer: Log iOS network traffic without a proxy

Misc. pentest & bug bounty resources

- The Pwnie Awards 2020 nominations
- Wordlist of open redirect parameters from all disclosed @Hacker0x01 reports
- GitHub Dorks List v2

- Security Creators
- AzureHound Cypher Cheatsheet

Challenges

- @brutelogic XSS challenges (KNOXSS Coverage list)
- Allsafe: Intentionally vulnerable Android application
- Code Security Advent Calendar 2020

Articles

- Don't Put It on the Internet: Tesla Backup Gateway Edition
- Backdooring User Data
- Dumping Memory with AV – Avast Home Security
- 0day in Windows 7 and Server 2008 R2 Gets a Micropatch (TL;DR)

Bug bounty & Pentest news

- US Government Mandates Vulnerability Disclosure For IoT
- 2020 OSCP Contest
- KringleCon 3
- Sploitus exploit search engine comes under DMCA fire, search engine page removal
- SecureAuth Innovation Labs – New Impacket Release Available Today!
- Professional / Community 2020.11.2 & Burp Suite Enterprise Edition: six months of new features

Non technical

- How to Think for Yourself
- New features aren't Solved Problems
- Hacker Spotlight: Interview With Bagipro
- My Bug Bounty Journey & Ranking 1st in U.S. DoD & Achieving top 100 hackers in 1 year

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 11/22/2020 to 11/29/2020.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com