Bug Bytes #168 – Behind The Tool, NotGitBleed & Custom Transport Encoding in Burp

BY ANNA HAMMOND · APRIL 20, 2022 · LAST UPDATED ON JULY 25, 2025

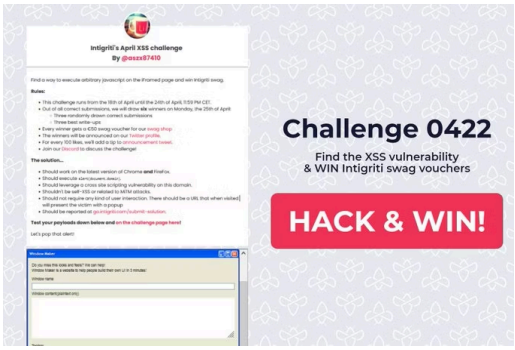
Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-168-behind-the-tool-notgitbleed-custom-transport-encoding-in-burp

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 April 11 to 18.

Intigriti news



Intigriti's April XSS challenge By @aszx87410

Our favorite 5 hacking items

1. Video of the week

Live Recon | @IppSec Talks About Hacking, His Favorite Tools, HackTheBox and More!
FFUF by @joohoi (Behind The Tool #1)

@NahamSec's Lire Recon show is baaaack! It has a new format and two new co-hosts, @Jhaddix and @stokfredrik.
This first episode is must watch if you enjoy hacking or want to hear @ippsec talk about programming, recon, CTF, etc.

Another new show is Intigriti's Behind The Tool, hosted by @hacksplained.
The first episode is so-o-o good! @joohoi shares a lot about *ffuf*, how to pronounce it, the context behind

its creation, his favorite functionalities, and more.

2. Writeup of the week

NotGitBleed (GitHub)

Just when I start thinking that it may be getting harder to find leaked secrets on GitHub... MDSec's Aaron Devaney shows that not only there are still GitHub leaks to be found, there are so many that he collected them at scale with automation.

3. Tools of the week

wister
NMAP-Formatter

Wister is a wordlist generation tool. It takes a list of words as input, and can output variants with different encodings, casings, homographs, etc.

Another handy tool is NMAP-Formatter, a Go tool that can convert NMAP's XML output to HTML, CSV, JSON and markdown.
There are many other tools to convert Nmap output, but I'm personally starting to use this one because it supports many formats including JSON, so it makes it easy to chain Nmap with jq and other recon tools.

4. Vulnerability of the week

CVE-2022-26809 MS-RPC RCE:

- Vulnerability Analysis – SANS Institute
- Akamai analysis
- SANS.edu blog post

CVE-2022-26809 is an integer overflow in MSRPC. It does not have a public exploit but is worrisome for its 9.8 CVSS score, and its wormable potential as an unauthenticated zero-click RCE.

5. Tutorial of the week

Teaching Burp a new HTTP Transport Encoding

If you encounter a HTTP client/server that use custom Transport Encoding or encryption, this tutorial could save you a lot of headache.
@pentagridsec demonstrates how to solve the problem by writing a Burp extension.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- Q: HOW do you find hidden stuff on websites? (this episode is all about CONTENT DISCOVERY!)
- How I became a leading Red Teamer {and Cyber Security Expert} | @byt3bl33d3r Marcello Salvati

- Learn with @j3ssiejjj – Automating Recon at scale using Osmedeus!! & Repo
- They just didn't check the balance before making a transfer. $3,4 mln bounty in Polygon blockchain
- Awkward VLOG at Nullcon Berlin 2022

Slides & Workshop material

- BugBounty hunting tips & tricks & Video (in Arabic)

Podcasts / Audio

- Bug Bounty Community Chats #5

Webinars

- Bishop Fox: Tool Talks: Unredacter Episode
- CVE-2022-26809 MS-RPC Vulnerability Analysis – SANS Institute

Conferences

- Exploiting esoteric android vulnerability by Sharan & Sanjay
- THCon 2022 – day 1, Day 2 & Programhttps://thcon.party/program/, especially:
  - Two bugs to rule them all: Taking over the PHP supply chain
  - Everything I wanted to know about AD LDAP
  - Credential harvesting in 2022: Making initial access through publicly exposed secrets in git repositories and docker images
- Shmoocon 2022

Tutorials

Medium to advanced

- Why using a FIDO2 security key is important
- Demystifying iOS Code Signature
- Run Shell Commands on EC2 with Send Command or Session Manager
- Breaking the Cloud via Azure AD Connect

Beginners corner

- Cypher Injection (Neo4j) Graph Databases
- Jenkins: Remote Execution Via Malicious Jobs

- Active Directory – Introduction, Offensive PowerShell, Local Privilege Escalation, Lateral Movement, Domain Persistence & Domain Privilege Escalation
- Extracting Credentials from Multifunction Devices

Writeups

Challenge writeups

- THCon 2k22 CTF – "Local Card Maker" Writeup
- Securinets CTF Quals 2022 – Infrastructure and Web writeups
- HackTheBox – Toby, Blog post & Troubleshooting Python Socket Timing
- CORS – Lab #2 CORS vulnerability with trusted null origin, Lab #3 CORS vulnerability with trusted insecure protocols & Lab #4 CORS vulnerability with internal network pivot attack

Pentest writeups

- How I chained two vulnerabilities to steal credit card details?
- Obfuscated obfuscation

Responsible(ish) disclosure writeups

- Markdown Menace: Discovering an LFI Vulnerability on a Blogging Platform
- CVE-2022-29072 – Privilege escalation and RCE in 7-Zip for Windows #Windows #LPE #MemoryCorruption
- CVE-2022-24527: Microsoft Connected Cache Local Privilege Escalation (Fixed) #Windows #LPE
- CVE-2022-25165: Privilege Escalation to SYSTEM in AWS VPN Client #Windows #LPE
- CVE-2022-28345 – Signal client for iOS version 5.33.2 and below are vulnerable to RTLO Injection URI Spoofing #iOS

Known vulnerabilities

- Diving Deeper into WatchGuard Pre-Auth RCE – CVE-2022-26318
- Proof of Concept: CVE-2022-21907 HTTP Protocol Stack Remote Code Execution Vulnerability

Bug bounty writeups

- An attacker can archive and unarchive any structured scope object on HackerOne (HackerOne, $12,500)
- CVE-2022-26133 – Bitbucket Data Center – Java Deserialization Vulnerability (Atlassian)
- Bypass Apple Corp SSO on Apple Admin Panel (Apple, $6,000)
- How we spoofed ENS domains for $15k (ENS, $15,000)

- Palisade identifies Wormable Cross-Site Scripting Vulnerability affecting Rarible's NFT Marketplace (Rarible, $5,000)
- Multiple Vulnerabilities in Cisco Expressway & STUNNER: A tool to test and exploit STUN, TURN and TURN over TCP servers

See more writeups on The list of bug bounty writeups.

Tools

- SecretScanner: Find secrets and passwords in container images and file systems
- KnockKnock: A simple reverse whois lookup tool which returns a list of domains owned by people or companies
- linWinPwn: Bash script that automates Active Directory enumeration and vulnerability checks

Tips & Tweets

- Full-Time Bug Bounty Hunting
- @Jhaddix on mistakes he made in hacking or bug bounty
- Hacker stories by @Jhaddix, @hacker_ & @ArmanSameer95
- Interesting facts about unicode support in regex
- Best search engines for Pentesters
- @nav1n0x's Nginx Merge Slashes vulnerability
- Can you figure out exactly what this one-liner is doing?

See more tips on this week's Twitter collection.

Misc. pentest & bug bounty resources

- @hacker_'s threat.dev/newsletter
- asnlookup.com & Intro: ASNLookup.com refactored and relaunched with a new API
- Burp to ZAP Feature Map
- Cloud Security Resources
- Compromising CI/CD Pipelines & Proxy server simplified (Security Zines flyers)
- A list of new(ish) command line tools

Articles

- Persisting XSS With Iframe Traps
- Coercing NTLM Authentication from SCCM & SharpSCCM

- Make phishing great again. VSTO office files are the new macro nightmare?
- Bypassing Cortex XDR

Challenges

- Intigriti's April XSS challenge By @aszx87410
- IVNA: Intentionally Vulnerable Nodejs Application & APIs

Bug bounty & Pentest news

- Cybersecurity
  - Critical Apache Struts RCE vulnerability wasn't fully fixed, patch now
  - Tarrask malware uses scheduled tasks for defense evasion (ScheduleRunner was updated to include this new technique)
  - Git security vulnerability announced
- Upcoming events
  - NahamCon 2022 (April 30 – 09:00 AM PDT) & NahamCon CTF (April 28 – 30)
  - Cyber Apocalypse CTF 2022 (May 14 – 20) & Live Hacking Workshops
- Tool updates
  - Burp Suite Extension: AWS Signer 2.0 Release
  - reFlutter update
  - feroxbuster v2.7.0