Bug Bytes #133 – It's still DNS, A $50K stray token & Path traversal in microservices

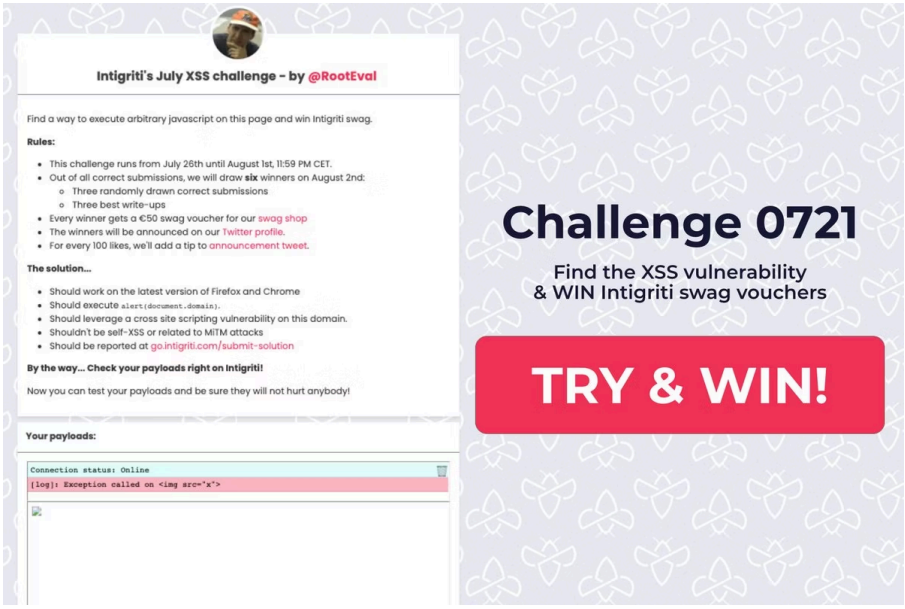
BY ANNA HAMMOND · JULY 28, 2021 · LAST UPDATED ON MARCH 6, 2025

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 July 19 to 26.

Intigriti News



Intigriti's July XSS challenge – by @RootEval

Our favorite 5 hacking items

1. Conference of the week

Traversing My Way in the Internal Network – Jasmin Landry (@JR0ch17)

What do you think when you see "?id=1337" in a HTTP request? If it is only IDOR or SQL injection, you will love this talk. @JR0ch17 demonstrates that when microservices are involved, there is much more that can be tested such as path traversal.

2. Writeups of the week

Github access token exposure (Shopify, $50,000)
Guest Blog Post – Attacking the DevTools (Microsoft, $36,000)
Pre-Auth RCE in ManageEngine OPManager
How I Found Multiple Bugs On FaceBook In 1 Month And a Part For My Methodology & Tools (Facebook)

Four beautiful findings:

- A Shopify employee's Github Access Token @auguzanellato found while reviewing a public MacOS app and the $50K bounty that ensued.
- A writeup packed with information on the attack surface of DevTools and $36K of issues @david_erceg found in Edge.
- A nice pre-auth RCE via deserialization Johannes Moritz and Robin Peraglie found in ManageEngine OPManager.
- @GodfatherOrwa's methodology for finding multiple critical bugs on Facebook in one month.

3. Article of the week

Forgot password? Taking over user accounts Kaminsky style & DNS Reset Checker

Remember 2008 when Dan Kaminsky broke DNS? Well, @sec_consult researcher Timo Longin found out that some Web apps are still vulnerable.
He tested for two DNS attacks (Kaminsky and IP fragmentation attacks) on 146 apps and was able to successfully manipulate the DNS name resolution of some of these apps. This meants that "Forgot password" features could be exploited to steal password reset URLs and take over accounts.

4. Tutorial of the week

How to achieve enterprise-grade attack-surface monitoring with open source software

In this tutorial, @hakluke shows how to make the most of the open source SpiderFoot version to monitor assets with change notifications.

One of the tools mentioned is Datasette. It's worth knowing about if you store bug bounty data using SQLite and want to turn it into a Web interface with a JSON API.
I was looking for something like this and didn't know it existed.

5. Resource of the week

blog.0xffff.info

This is a blog I've just discovered that has so much good content on Web security. Here are a few examples:

- Utilizing .htaccess for exploitation purposes & .htaccess exploitation series – Part #2
- A guide to non-conventional WAF/IDS evasion techniques

- Triggering Full Path Disclosure – the basics
- Winning the race: Signals, symlinks, and TOC/TOU
- Lame 0day #1 – MyBB hidden content bypass

Note that (for me at least) not all posts are visible when browsing the site. So, I'd recommended using an RSS reader to access all the content that is there.

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- How to bypass Jailbreak detection using Hopper Disassembler in iOS apps
- HACKING HTTP/2: h2c SMUGGLING
- Hacker Tools: JWT_Tool – The JSON Web Token Toolkit & Blog post
- S01E12: Talking Security with Hakluke — Security Shorts
- Hacker Heroes #6 – @dccybersec (Interview)
- $25,000 Stealing GitHub API token with a malicious pull request
- SecuriTEA & Crumpets – Episode 10 – Justin Collins – Brakeman
- Understanding C Pointer Magic Arithmetic

Podcasts

- SeriousSAM & PetitPotam – Kaseya Universal Decryptor, Window's Process Hacker, Chrome 92

Webinars

- No SPAN Port? No Tap? No Problem!

Conferences

- A Look Into zseano's Thoughts When Testing a Target – Sean @zseano
- BSides Vancouver 2021

Tutorials

Medium to advanced

- A Python Regular Expression Bypass Technique
- From RPC to RCE – Workstation Takeover via RBCD and MS-RPChoose-Your-Own-Adventure
- On Disk, The Devil's In The Details

Beginners corner

- Fantastic Windows Logon types and Where to Find Credentials in Them
- How To Setup MFA for Linux Login (SSH, Console, Sudo)

Writeups

Challenge writeups

- in ONE website: SSRF, 2FA bypass, Open-redirect, Security question bypass...

Pentest writeups

- Compromising a Network Using an "Info" Level Finding

Responsible(ish) disclosure writeups

- Bypassing the IPinfo API (feat. pry0cc) #Web
- PetitPotam #NTLM #AD, Microsoft's response & Different ways to leverage it:
  - Active Directory Certificate Services (ADCS – PKI) domain admin vulnerability
  - If AD CS isn't enabled
  - No auth to full domain compromise using mimikatz + kekeo + impacket
- RemotePotato0 v1.1: "Won't Fix" Windows Privilege Escalation from User to Domain Admin, updated to remove the requirement for victims to be in session 0
- Sequoia: A Local Privilege Escalation Vulnerability in Linux's Filesystem Layer (CVE-2021-33909) & Exploit #Linux #LPE
- fail2ban – Remote Code Execution
- SeriousSAM / HiveNightmare / CVE-2021-36934 #Windows #LPE
  - Microsoft SAM File Readability CVE-2021-36934: What You Need to Know
  - PoCs by @GossiTheDog & @cube0x0 & @HuskyHacksMK
  - Video demo by @thecybermentor

Bug bounty writeups

- Pre-Account Takeover by Reversing a Weak Email Verification Token Algorithm
- Pre-Auth RCE in Moodle Part I – PHP Object Injection in Shibboleth (Moodle)

- How I Bypassed a tough WAF to steal user cookies using XSS!
- Mattermost Server v5.32 > v5.36 Reflected XSS in OAuth flow (Mattermost)
- CVE-2021-22925: TELNET stack contents disclosure again (curl, $800)
- Exfiltrating a victim's exact location (to within 5m) (Bumble, $2,000)
- Fragmentation and Aggregation Flaws in Wi-Fi (The Internet, $750)

See more writeups on The list of bug bounty writeups.

Tools

- wbk: Advanced waybackurls
- hakcertstream: Basic implementation of certstream to print new subdomains and domains
- Bughound & Intro: Static code analysis tool based on Elasticsearch
- MAN-SPIDER: Spider entire networks for juicy files sitting on SMB shares. Search filenames or file content – regex supported!
- 5GC_API_parse: A BurpSuite extension to parse 5GC NF OpenAPI 3.0 files to assess 5G core networks

Tips & Tweets

- Interesting reverse proxy vulnerability
- Apache+Tomcat extension check bypass

Misc. pentest & bug bounty resources

- bughunters.google.com
- curity.io resources
- punishell/bbtips
- 0xAwali's methodology for testing "Contact – company support" features & Reconnaissance Methodology v1.0
- Free Cyber Resources
- Open Security Training 2

Challenges

- Intigriti's July XSS challenge – by @RootEval

Articles

- OpenSSH ssh-agent Shielded Private Key Extraction (x86_64 Linux)
- Every C99 / C99.php Shell Is Backdoored (A.K.A. Free Shells for Everyone!

Bug bounty & Pentest news

- Bug bounty
  - A new chapter for Google's Vulnerability Reward Program
  - Points Don't Matter; Your Skills Do
- Cybersecurity
  - Introducing the Burp Suite Certified Practitioner accreditation
  - Microsoft warns of weeks-long malspam campaign abusing HTML smuggling
  - Respect in Security: New infosec campaign aims to stamp out harassment
- Upcoming events
  - Hacker School Reboot (July 29)
  - Deep Dive On Deserialization by B1TWIS3 – Hack The Box (July 2021) (July 29)
  - Kali Linux AMA with Ben Wilson (@g0tmi1k) (July 29)
- Tool updates
  - Nuclei v2.4.1 (Added Deserialization helpers to generate payloads within templates)
  - Burp Professional / Community 2021.7.2
    - DOM Invader now allows you to customise which sources it automatically injects into
  - Tokenvator Release 3

Non technical

- A hackers perspective on bug bounty triage

Community pick of the week

Well done on the “draw our logo” competition Th4nu_0x0! Enjoy your swag

If you want some too, make sure to participate in our ongoing XSS challenge. Also tag us on social media to share your own bug hunting wins and joys, we love hearing from you!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com