Bug Bytes #154 – URL parsing confusion, Forging cookies for almost $100k & Exploiting impossible Pickle deserialization

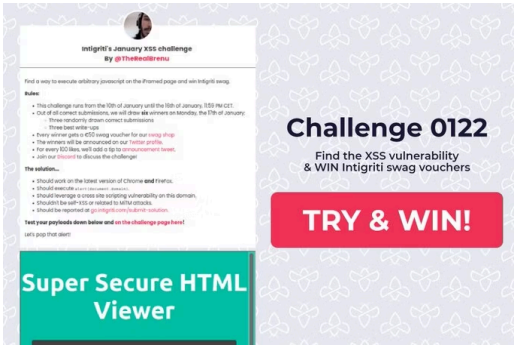
BY ANNA HAMMOND · JANUARY 12, 2022 · LAST UPDATED ON MARCH 6, 2025

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 January 03 to 10, 2022.

Intigriti news



Intigriti's January XSS challenge By @TheRealBrenu

Our favorite 5 hacking items

1. Tips of the week

HackVector custom tag to escape JSON strings
Using chrome heap snapshots to find hidden API Endpoints

@TechBrunchFR's HackVector tag is a real time saver if you often find yourself editing JSON data in Burp. It makes it easy to escape special characters especially when handling large payloads.

The second tip by @imranparray101 is intriguing. I haven't had the chance to test it but it sounds mindblowing.
The idea is to *grep* Chrome's heap snapshots for "/api" to find all endpoints mentioned in a site's JavaScript code.
The advantage over other techniques is that this finds endpoints that are never called (and so don't

appear in a Web proxy) and it is really quick, without the need to run many tools or spend time analyzing JavaScript.

2. Paper of the week

Exploiting Url Parsing Confusion

@Claroty and @snyksec collaborated on this research paper about URL parsing confusion. They analyzed 16 URL parsing libraries and found five types of URL parsing inconsistencies and eight vulnerabilities in Web apps and third-party libraries.
This is fantastic research if you are interested in vulnerabilities that result from URL validation bypass such as SSRF, Open redirect, XSS, DoS, filter bypass, and even RCE (the example given being Log4J).

3. Writeups of the week

Breaking Parser Logic: Gain Access To NGINX Plus API — Read/Write Upstreams.
Exploiting Redash instances with CVE-2021-41192 ($90,000+)

Didn't get enough of parsing inconsistencies? Then check out @z0idsec's writeup. It is full of insightful details on how to detect, exploit and increase the impact of secondary context path traversal.

The second writeup is about @iangcarroll's research on stateless authentication. It is what led him to create CookieMonster, report CVE-2021-41192 (a Redash misconfiguration issue), scan for it on bug bounty programs with the help of @haxor31337 and @naglinagli, and earn almost $100k.

4. Article of the week

Simpler unpickle payloads with the walrus operator

@ZetaTwo shares a clever trick for exploiting Pickle/Python insecure deserialization when no output is returned and outbound connections are not allowed (so no reverse shell).
By leveraging the new Python operator *walrus*, it becomes possible to get your injected commands' output.

5. Resources of the week

Security Explained
Awesome list of secrets in environment variables

One obstacle that can hinder our progress as hackers is not knowing what we do not know. Initiatives like Security Explained help with that. @harshbothra_ regularly shares notes on vulnerability types, methodologies, tools... Something new to learn (almost) everyday.

The second resource is a list of secrets (API keys, tokens, passwords, etc) that are commonly stored in environment variables. It was compiled by @pulik_io and will be useful if you find a vulnerability that allows reading environment variables (e.g. CVE-2021-44228).

SHARE ON TWITTER

Other amazing things we stumbled upon this week

Videos

- The Breach They Kept Secret
- Open-Source Intelligence (OSINT) in 5 Hours – Full Course – Learn OSINT!
- Introduction to GraphQL | GraphQL Exploitation – Part – 1 | DVGA
- #MentorshipMondays
- Hacking through screenshots! EyeWitness- Hacker Tools & Blog post
- Learning about nss (Linux Name Service Switch) During Sudo Exploitation & Creating The First Sudoedit Exploit

Webinars

- HTTP Smuggling from inception to nowadays by Milan Charniak

Slides & Workshop material

- @six2dez1's "Gotta Catch'em all" and "Subdominions" slides

Tutorials

- So You Want to Use the AWS Free Tier
- Ngrok for Penetration Tester's
- Domain Domination With Windows Shortcuts
- PWN methodology — LINUX & PWN Tips && Tricks
- Domain Persistence – AdminSDHolder & Domain Escalation – sAMAccountName Spoofing

Writeups

Challenge writeups

- HackTheBox – Previse
- UHC – NodeBlog
- SANS Christmas Challenge 2021
- DC 2 Walkthrough with S1REN
- LFI to RCE? – Archangel by @Try Hack Me

Pentest writeups

- From .git directory to AWS EC2 network takeover
- ADCS: Playing with ESC4 & modifyCertTemplate
- Intruding 5G SA core networks from outside and inside](https://penthertz.com/blog/Intruding-5G-core-networks-from-outside-and_inside.html)

Responsible(ish) disclosure writeups

- PHP 7.3-8.1 disable_functions bypass [concat_function] #Web #MemoryCorruption
- The JNDI Strikes Back – Unauthenticated RCE in H2 Database Console #Web
- The Story of How I Hacked my ISP's Cheapo Standard Issue Router #Router #Network
- How I Reverse-Engineered one of the biggest GSM Operator's application. #iOS
- Unpacking CVE-2021-40444: A Deep Technical Analysis of an Office RCE Exploit #Windows #Malware
- CVE-2021-38000: Chrome Intents Logic Flaw #Android

Bug bounty writeups

- Facebook android webview vulnerability : Execute arbitrary javascript (xss) and load arbitrary website (Facebook, $1,075)
- Remote Code Execution in Google Cloud Dataflow (Google, $3,333.70)
- Story of YouTube's Unfixable Ads Bypass (Google)
- Accessing GoDaddy internal instance through an email logic bug. (GoDaddy)
- A phishing document signed by Microsoft – part 2 (Microsoft)

See more writeups on The list of bug bounty writeups.

Tools

- PMHunter & Intro: A Python tool to automate searching in postman for public data
- Modified Nuclei Templates Version to FUZZ Host Header & Nuclei Templates to reproduce Cracking the lens's Research
- mikedesu/amass-setup: @therealdarkmage's Amass setup
- objectify-s3: A tool that recursively checks AWS S3 buckets and objects for misconfigured permissions
- ZKar: A Java serialization protocol analysis tool implement in Go

- shuji

Tips & Tweets

- HackVector custom tag to escape JSON strings
- Using chrome heap snapshots to find hidden API Endpoints
- @jstnkndy: If you're auditing Java or .NET apps, you should really try out Burp Infiltrator
- 8 different techniques to Bypass Rate Limits in Web Applications and API's
- Negative Searching added to https://ippsec.rocks
- Enumerate & validate o365 emails using ffuf
- Chrome blocks JavaScript URLs in data attributes for object tags but Firefox doesn't
- Encoded backslash to bypass domain validation filters & Why it's a good idea to use MySQL's group_concat() to exploit SQL injection

Misc. pentest & bug bounty resources

- Book – Bug Bounty Write Ups Collection – Omar Espino ($2.99)
- mess with dns
- Free Digital Forensics Classroom

Articles

- Implementing Django-rest API Throttling and Unauthenticated bypass & IP spoofing bug leaves Django REST applications open to DDoS, password-cracking attacks
- Metasploit 2021 Annual Wrap-Up
- Persistence without "Persistence": Meet The Ultimate Persistence Bug – "NoReboot"
- Finding Prototype Pollution gadgets with CodeQL

2021 retrospectives

- A Years Worth of Active Directory Privilege Escalation
- The Mac Malware of 2021 – a comprehensive analysis of the year's new malware!
- Thread on macOS vulnerability research / exploit development published in 2021
- ZDI: The Top 5 Bugs Submitted In 2021

Challenges

- Intigriti's January XSS challenge By @TheRealBrenu
- tcc-ctf source code & Solutions
- APISandbox

Bug bounty & Pentest news

- Bug bounty
  - Top 10 web hacking techniques of 2021 – nominations open
- Tool updates
  - BBRF v1.3.0 (added `where` statements & `remove` command)

Non technical

- Interview with IppSec of YouTube and HackTheBox
- Expert Advice You Don't Want To Miss
- Looking at the Portswigger Burp Suite Certification
- Review: Burp Suite Certified Practitioner (Part 3 Final)