Bug Bytes #103 – Cookie tossing, Recon tools benchmarks & Stealing Google docs with screenshots

BY ANNA HAMMOND · DECEMBER 30, 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 20 to 27 of December.

Intigriti News

The SolarWinds Saga continued & The evolution of cybersecurity in 2020

Our favorite 5 hacking items

1. Articles of the week

Fun with IP address parsing
Helping secure DOMPurify (part 1) & A word about DOMPurify bypasses a.k.a why DOM parsing is crazy | Sekurak.tv

@dave_universetf wrote an IPv4+6 parser from scratch which led him to discover several cursed IP address representations. This type of corner cases are interesting when looking for URL validation bypasses (e.g. for SSRF or open redirect).

The second article (and accompanying video) are excellent resources for anyone who saw the many recent DOMPurify bypasses and wondered how to find such vulnerabilities.

2. Writeups of the week

Cookie Tossing to RCE on Google Cloud JupyterLab (Google, $3133.70)
[Google VRP] Hijacking Google Docs Screenshots (Google)
Supply Chain Pollution: Hunting a 16 Million Download/Week npm Package Vulnerability for a CTF Challenge (Node.js third-party modules)

@kl_sree found a cool PostMessage misconfiguration on Google Docs that allowed him to steal the content of documents by screenshotting them.

@spaceraccoonsec shares the details of a prototype pollution he found in the "ini" NPM package. Since it is used by almost 2000 dependent packages, this bug could've been exploited for a serious supply chain attack.

@S1r1u5_ wrote about an RCE on Google. It covers the interesting topic of "Cookie tossing" that can be used to increase the impact of XSS bugs found in out of scope or sandboxed domains.

3. Videos of the week

How to duplicate less with Bug Bounties
Automate your Bug Hunting using Nuclei | Writing our own nuclei template | Be The H.A.C.R. – Ep. 18

Continuing his excellent series for bug bounty beginners, @codingo_ shares advice to help increase bug impacts and avoid duplicates.

The second video by @AseemShrey should also help with those dreaded dupes. He explains how to write your own Nuclei templates. It is a good introduction for anyone who wants to automate some bug bounty checks and customize Nuclei to differentiate yourself.

4. Resource of the week

Subdomain tools review & Recon suites review

These are two cool benchmarks for Web application testers. Six2dez1 does an awesome job of comparing subdomain enumeration tools (based on their features and results) and recon suites (based on their features and tools).

5. Tutorial of the week

Metasploit Tips and Tricks for HaXmas 2020

This one is for Metasploit power users. It has many advanced tips and tricks with a mix of old and recent features (e.g. how to debug failed HTTP modules, how to inline options when running a module, resource scripts for streamlining repetitive workflows, refining search results, etc).

Other amazing things we stumbled upon this week

Videos

- IT Security Career Advice
- optionalctf Talks about OSCP, CTF vs Bug Bounty, Disclosed Reports, Hacking Resource and more!
- Why aren't you able to do Bounties or Anything?
- 5 Useful GitHub Repositories #Shorts
- How to Prevent Open Redirects in your Applications

Podcasts

- Best of 2020 – The Year's Best Stories on Security Now
- JavaScript Enumeration for bug bounty hunters
- Ozgur Talk About Bug Bounties, Recon Workflow, How to Learn Different Topics & Life At Synack
- Darknet Diaries Ep 81: The Vendor

Webinars & Webcasts

- Deep Dive: Burp Bounty Extension
- Verifying Sketchy Windows Apps – SANS@Mic

Conferences

- null Ahmedabad Meet 27 December 2020 Monthly Meet
- Mystikcon 2020, especially:
  - Android Pentesting
  - IOS pentesting
  - Java De-serialization vulnerability analysis
  - Introduction to AWS
- CIA Conference 2020 | DAY 1 & Day 2

Slides & Workshop material

- Source Code Audit Training Archive

Tutorials

Medium to advanced

- Detection and Hunting of Golden SAML Attack
- Docker Botnets...
- Privilege Escalation In Azure AD

Beginners corner

- Advanced XXE Exploitation
- A Pentester's Guide to Server Side Template Injection (SSTI)
- Pentest – Everything SMTP
- Handling Short Expiration Time of Authorization Tokens
- OSINT Guide To Bitcoin Investigations
- OSINT: Automate Face Comparison With Python and Face++

Writeups

Challenge writeups

- BSides Ljubljana X-MAS CTF solutions
- Regular Expressions | Quiz 1 | #WinjaCTF2021

Pentest writeups

- Android Application's Client Side Encryption Bypass Leads to Account Takeover

Responsible(ish) disclosure writeups

- Security Vulnerabilities in Smallstep PKI Software #Web
- WordPress Plugin Limit Login Attempts Reloaded & CVE-2020-35590 PoC #Web
- Oh, so you have an antivirus... name every bug #AV
- Bypassing Windows Smartscreen #Windows
- CVE-2020-25860 – Significant vulnerability discovered in RAUC embedded firmware update framework #Firmware
- Multiple critical vulnerabilities in Trend Micro InterScan Web Security Virtual Appliance (IWSVA) #Web

Bug bounty writeups

- Regular expression injection, a code review low hanging fruit
- EN | Account Takeover via Web Cache Poisoning based Reflected XSS
- Hack crypto secrets from heap memory to exploit Android application
- Blind XSS on image upload (CS Money , $1,000)
- Fixing a Google Vulnerability (Google)

See more writeups on The list of bug bounty writeups.

Tools

- paramsCFinder.py: Params combination finder
- headi: Customisable and automated HTTP header injection
- Kenzer: Automated web assets enumeration & scanning
- CrowdStrike Reporting Tool for Azure (CRT) & Intro
- Sparrow.ps1: Sparrow.ps1 was created by CISA's Cloud Forensics team to help detect possible compromised accounts and applications in the Azure/m365 environment
- HTTP Request Smuggling Detection Tool & Intro
- bitlocker-spi-toolkit & Intro: Tools for decoding TPM SPI transaction and extracting the BitLocker key from them
- Censys Python Library: An easy-to-use and lightweight API wrapper for the Censys Search Engine
- APK Lab: Android Reverse Engineering WorkBench for VS Code
- httpfuzz & Intro: HTTP fuzzer in Go
- Grawler: PHP tool with a web interface that automates the task of using google dorks, scrapes the results, and stores them in a file

Misc. pentest & bug bounty resources

- How Samesite affects cookies in different attacks in modern browsers
- Pen-testing Notes Template
- Bug Bounty Tips #10
- The Top 152 Bugbounty Open Source Projects
- Web Security Academy Learning path
- @admiralgaust's OSCP Preparation notes
- ENISA Threat Landscape for 5G Networks Report

- Security Christmas

Challenges

- The CrowdStrike Intelligence Adversary Quest: OSINT CTF beginning Jan 18

Articles

- Finding Data Leaks In Online Formatters
- Unleash The Dino: Time-based Strategies To Improve Password Cracking
- State of Pentesting 2020
- A tale of .NET assemblies, cobalt strike size constraints, and reflection. & AppDomain.AssemblyResolve

Bug bounty & Pentest news

- Hacker makes $2 Million Dollars in Bug Bounty earnings
- DEF CON's first New Year's Eve Party
- OWASP 2021 Virtual AppSec Days Training Events
- Third edition of US Army bug bounty program prepared for deployment

Non technical

- Non-technical bugbounty tips
- Forbes Cybersecurity Awards 2020: Corellium, The Tiny Startup Driving Apple Crazy
- 3 Metrics That Will Indicate We're Taking Security Seriously
- Ask a Hacker: How Close is Cyberpunk 2077 to Reality?
- Dark patterns
- Censys: How a university project became a major commercial security platform

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 12/20/2020 to 12/27/2020.