Blog

Bug Bytes #63 – Bruteforce With Selenium, XXE Through Request Smuggling & Bug Bounty Podcast

intigriti - 24th March 2020 - bugbytes

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.

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 13 to 20 of March.

Our favorite 5 hacking items

1. Tutorials of the week

– Absolute Bruteforce with Selenium– A secret note to Bug hunters about URL structure and its parsers

The first article shows how to bruteforce an OTP when your target is using Web Sockets with encryption. In this scenario, traditional bruteforce with Burp Intruder is not possible so @MilindPurswani uses Selenium instead. I don't think this is a scenario you will often encounter but if you do, this might be of great help.

The second tutorial is an introduction to URL structure. Understanding these basics helps understand how differences in URL parsers can cause serious vulnerabilities.

2. Writeup of the week

XXE-scape through the front door: circumventing the firewall with HTTP request smuggling

In this writeup, @honoki shows how he leveraged a low impact HTTP request smuggling vulnerability to bypass a firewall and fully exploit an XXE found in a file upload functionality.Each bug taken separately had limited impact: the request smuggling bug only affected port 80, so only HTTP

requests could be poisoned. The XXE could be exploited to exfiltrate data via DNS, but it was non-sensitive data. And HTTP requests were blocked by the firewall, except for a few whitelisted domains.By finding a domain that was both whitelisted and vulnerable to HTTP request smuggling, it was possible to chain the two bugs and exfiltrate sensitive data .

3. Podcast of the week

The Bug Bounty Podcast – Episode #3 ft. NahamSec

Yes, it is back! One of my favorite podcasts, with @Regala_ interviewing @NahamSec. They discuss many topics like @NahamSec's motivation for streaming, why he finds it harder to do bug bounty as someone who works for a bug bounty platform, how he makes most of his money, mass recon, doing deep work, the power of long term collaboration, etc.This episode is an excellent way to spend one hour and a half!

4. Tool of the week

Progress Tracker

Remember Scope Monitor, the Burp extension for keeping track of tested endpoints? His author, @Regala_, discontinued it and started using Progress Tracker by @dariusztytko instead.This new extension offers interesting functionality. You can capture requests, exclude specific extensions and status codes, associate each request with tags and one of 6 different statuses (Ignored, Done, In progress...), etc.

5. Video of the week

@infosec_rohk Talks About Hacking Uber, Working at Synack, and His 120 Reports in 120 Challenge

Great interview of @rohk_infosec. He talks about how he accidentally got into bug bounty, how he taught himself hacking, how he chooses which bugs to focus on, his experience from Computer Science student to bug hunter, to triager, to senior application security engineer, the top 3 things he wished he knew when he started out, and much more.

I loved hearing about the 4 months bug hunting challenge (120 bugs reported in 120 days) he did while having a full-time job, and more importantly the steps he took to deal with stress and burnout despite a crazy schedule.

Other amazing things we stumbled upon this week

Videos

- Every Type of XSS Attack, Explained
- Hacker101: Common Android Bugs Pt. 1 & Pt. 2
- How (we) Run a Virtual Conference and How You Can Too
- SANS CyberCast Gear Review
- Android Exported Activities and how to exploit them

Podcasts

- Darknet Diaries Ep 61: Samy
- The SMBGhost Fiasco – Security Now 758
- Risky Business #575 — World drowns in Coronavirus phishing lures as crisis escalates
- 7MS #405: Tales of Internal Pentest Pwnage – Part 16
- ToTok, Part 1: How to Convince Someone to Download Spyware, Part 2: The Masterminds of Mobile Malware & ToTok, Part 3: Becoming a Spyware Superpower
- Layer 8 Podcast – AMA with Snow and TinkerSec

Webinars & Webcasts

- Passwords are NOT what they are CRACKED up to be
- How to Run a Virtual Con
- 2020 SANS @MIC: “Moving Past Googling It” Companion Post

- Getting Started with Consulting: Top Ten Questions Answered!

Conferences

- #OBTS v3.0, Day 2 & Slides
- Shmoocon 2020
- CyberCiderSecCon Day 1, Day 1 part 2, Day 2 & Wrap Up

Tutorials

Medium to advanced

- Bounty Tip : How to Push Injection through JSON/XML stubs for API
- Using Content-Security-Policy with multiple policies
- How to open postman:// url or protocol in any Linux Distribution from Firefox
- Gaining AWS Console Access via API Keys
- Kubernetes Namespace Breakout using Insecure Host Path Volume — Part 1
- DNS for red team purposes
- Hiding Your .NET – ETW
- Cisco Password Cracking and Decrypting Guide

Beginners corner

- Abusing JSON Web Tokens
- What is LDAP Injection and How to Prevent It
- From Default Printer Credentials to Domain Admin
- Basic Recon Using A Domain Name
- Proxying Like a Pro
- Extracting Domain Hashes: Mimikatz

- How to listen to a VOIP-based phone?

Writeups

Challenge writeups

- Hacking Docker Remotely

Pentest writeups

- Turning Blind RCE into Good RCE via DNS Exfiltration using Collabfiltrator [Burp Plugin] & Collabfiltrator
- LDAPFragger: Command and Control over LDAP attributes & LDAPFragger

Responsible(ish) disclosure writeups

- I Know What Azure Did Last Summer #Cloud #Web
- Vesta Control Panel Second Order Remote Code Execution 0day Step-by-Step Analysis #Web #CodeReview
- Don't Clone That Repo: Visual Studio Code^2 Execution & 2nd writeup by @justinsteven #RCE #Python
- [CVE-2020-8518] Horde Groupware Webmail Edition 5.2.22 — RCE in CSV data import #RCE #PHP #CodeReview
- SimpleMachines Forums Vulnerability Report #Web
- CVE-2020-7931: SSTI exploitation in Artifactory Pro #Web
- CVE-2020-2551: Unauthenticated Remote Code Execution in IIOP protocol via Malicious JNDI Lookup #RCE #Java

Bug bounty writeups

- Race Condition leads to undeletable group member (HackerOne, $500)
- Accepting error message on twitter sends you to attacker site (Twitter, $560)
- Cache poisoning DoS to various TTS assets ($750)
- Full account takeover (Reverb.com, $800)

- Using Vulnerability Analytics Feature Like a Boss
- My Weirdest Bug Bounty — Getting PII from O365. (Microsoft, $1,000)
- EN | Administrator level Privilege Escalation story

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Dangerzone & Introduction: Take potentially dangerous PDFs, office documents, or images and convert them to a safe PDF
- Catffuf: Alias and function for ffuf to get a cooler output

More tools, if you have time

- Reckdns: Go DNS resolver
- Burp-AnonymousCloud: Burp extension that performs a passive scan to identify cloud buckets and then test them for publicly accessible vulnerabilities
- AWSGen.py: Generates permutations, alterations and mutations of AWS S3 Bucket Names
- Token Reverser: Word list generator to crack security tokens
- ProjectOpal: Stealth post-exploitation framework for WordPress
- r00kie-kr00kie & Introduction: PoC exploit for the CVE-2019-15126 kr00k vulnerability
- harbian-audit Hardening: Hardened Debian GNU/Linux distro auditing
- MSOLSpray: A password spraying tool for Microsoft Online accounts (Azure/O365)
- MSSQLi-DUET: MSSQL Injection-based Domain User Enumeration Tool
- ADE – ActiveDirectoryEnum: Enumerate AD through LDAP and a collection of helpfull imported scripts being bundled
- Ps-Tools & Red Team Tactics: Advanced process monitoring techniques in offensive operations

Misc. pentest & bug bounty resources

- Full Report on the Voatz Mobile Voting Platform & @jackhcable's worrying feedback
- Upgrade Your Workflow, Part 1: Building OSINT Checklists
- Upgrade Your Workflow, Part 2: Building Phishing Checklists
- Executing Python in MSSQL
- Notes from @NahamSec's awesome interview with @inhibitor181: Nice presentation method!
- The Ultimate PCAP
- Collection of #bugbountytips (from Twitter, Facebook,Portswigger,Medium..etc)

Challenges

- UnSAFE_Bank
- @PwnFunction's new #XSS Challenge "Me and the Bois"

Articles

- Automating Pentests for Applications with Integrity Checks using Burp Suite Custom Extension
- HTTP Desync Attacks with Python and AWS: New desync technique added to HTTP Request Smuggler
- google.news is not google.news: POC For Google Phishing with SSL
- Practical Insider Threat Penetration Testing Cases with Scapy (Shell Code and Protocol Evasion)
- Desktop.ini as a post-exploitation tool
- Red Team Use Case with Cloudflare's Argos Tunnel Service

News

Bug bounty & Pentest news

- VirSecCon2020: April 4th
- SRT Team America Invitational CTF (Spring Edition): April 3rd-10th
- Understanding SANS CyberCast – So Much More Than Live Virtual Training: First free challenges start April 2

- OSINT Missing CTF: April 6 & 7
- Changes to Facebook's Whitehat program
- Pwn2Own 2020: Live hacking contest goes virtual amid coronavirus pandemic
- Talkspace threatened to sue a security researcher over a bug report

Reports

- They Come in the Night: Ransomware Deployment Trends
- Vulnerabilities in web and app frameworks fall, but weaponization rate jumps – study
- The State of Open Source Security Vulnerabilities

Vulnerabilities

- Adobe Fixes Nine Critical Vulnerabilities in Reader, Acrobat
- Virtual machines, real problems: VMware fixes bug trio including guest-to-host hole in Workstation, Fusion
- Azure Red Flag: Microsoft Accidentally Fixes Cloud Config 'Bug'
- All the major Intel vulnerabilities

Breaches & Attacks

- Oh-so-generous ransomware crooks vow to hold back from health organisations during COVID-19 crisis
- Beware of 'ZoomBombing:' screensharing filth to video calls
- This Stalkerware Delivers Extra-Creepy Features
- The Inside Scoop on a Six-Figure Nigerian Fraud Campaign
- Security Researchers bought a German armed forces laptop for €90/$99 on eBay containing classified military data, including ways to defeat a mobile air defense system in use today
- Two Trend Micro zero-days exploited in the wild by hackers
- DDoS botnets have abused three zero-days in LILIN video recorders for months

Other news

- GitHub Mobile is officially leaving beta and entering general availability today
- Microsoft's GitHub acquires npm to help JavaScript developers
- Firefox to remove support for the FTP protocol
- WordPress to get automatic updates for plugins and themes
- Google APP users won't be allowed to install apps from outside the Play Store
- Spying concerns raised over Iran's official COVID-19 detection app & @fs0c131y's analysis

Coronavirus

- 'Dirty little secret' extortion email threatens to give your family coronavirus
- US, Israel, South Korea, and China look at intrusive surveillance solutions for tracking COVID-19
- Thousands of COVID-19 scam and malware sites are being created on a daily basis

Non technical

- Undetected podcast e.01 recap: The evolution of web security and hacking
- Attacking the Web: The Offensive Security Way
- From heroes to deviants: Discussing the cultures of hacking with Gabriella Biella Coleman

Remote work resources

- A Random List of Free Resources
- These Trainers and Studios Are Offering Free Online Workout Classes Amid the Coronavirus Pandemic
- SANS Security Awareness Work-from-Home Deployment Kit
- Remote work emergency plan: What to do (and where to start)
- Working from home: tell staff about phishing & data leakage [template e-mails included]

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 03/13/2020 to 03/20/2020.

Share this:

Twitter Facebook LinkedIn Reddit Telegram WhatsApp Email

Like this:

Loading...

YOU MIGHT ALSO LIKE

Bug Bytes #15 – New Content Discovery Wordlist, IDOR on Shopify & #askstok Bug Bounty live stream by @stokfredrik

23rd April 2019

Bug Bytes #5 -Lazy Hackers, Stök's blind XXE and Inception

12th February 2019

BugBytes #25 – To scan or not to scan, GOTCHA and live mentoring by @zseano

2nd July 2019

Search

RECENT POSTS

- Bug Bounty Q&A #3: What effort does is take to set up a bug bounty program?
- Bug Bytes #67 – Hacking Containers, Auth0 Bypass & @Hussein98d's Methodologies

Bug Bytes #66 – Abusing Slack's TURN, Breaking AWS & Azure & @spaceraccoonsec SQLi secrets

Bug Bounty Q&A #1: What is ethical hacking and bug bounty?

Bug Bytes #65 – Hacking webcams, internal servicedesks & parsers

CATEGORIES

bugbountytips

bugbusiness

bugbytes

challenge

changelog

events

general

Q&A

testimonial

Uncategorised

ARCHIVES

Select Month