Blog

⌂ > 2020 > April > 21 > Uncategorised > Bug Bytes #67 – Hacking Containers, Auth0 Bypass & @Hussein98d’s Methodologies

Bug Bytes #67 – Hacking Containers, Auth0 Bypass & @Hussein98d’s Methodologies

intigriti - 21st April 2020 - bugbytes / Uncategorised

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.

Click here to subscribe

This issue covers the week from 10 to 17 of April.

Intigriti news

- Monster Worldwide has launched their vulnerability disclosure program

Our favorite 5 hacking items

1. Resource of the week

> Attacking and Auditing Docker Containers and Kubernetes Clusters

After last week's training on AWS and Azure, @appseccouk is now generously open sourcing another complete training course. This one is about hacking Docker containers and Kubernetes clusters. It includes documentation, Docker Lab virtual machines and an intentionally vulnerable Kubernetes cluster (Google Cloud).

2. Writeup of the week

> JSON Web Token Validation Bypass in Auth0 Authentication API

This is a nice writeup on bypassing JWT validation. The app checks that the algorithm is not `none`, but relies on a blacklist. Using `alg: nonE` bypasses the case-sensitive filter, and allows for forging JWT tokens for any user. @zantedotnz also shares the tool he used and links to resources on JWT hacking.

3. Videos of the week

> – @hussein98d Talks About Bug Bounties, Recon Methodology, and Shows Some of the Tools He Uses!
>
> – Attacking Secondary Contexts in Web Applications – Sam Curry
>
> – Code that gets you pwn(s|'d) – Louis & Slides
>
> – Using Interlace for organising tests, and multithreading over targets – @codingo

These are the videos/talks I plan on watching in priority this week. Why? Because I want to learn about @hussein98d's recon process and bug hunting methodology, @snyff discussing less obvious vulnerabilities, how @codingo_ uses Interlace, and @samwcyo's attacks on secondary contexts.

4. Non technical item of the week

> How to Remember Everything : Using Roam for Bug Bounty Notes

Choosing a note-taking app is such a never-ending rabbit hole! 🤦‍♀️

After settling on Joplin, then discovering Notion's great UI and features, I'm now tempted to check out Roam. @bonjarber does a great job of explaining why Roam's graph-based approach solves problems all apps based on a "hierarchical tree" have (including Notion).

5. Tutorials of the week

> – The Wondeful World of OAuth: Bug Bounty Edition
>
> – The 5 Most Common GraphQL Security Vulnerabilities & vulnerable-graphql-api
>
> – Bypassing modern XSS mitigations with code-reuse attacks

Depending on the bug classes you are focusing on, these tutorials might come in very handy. The OAuth one will give you ideas for new attacks to test for. The GraphQL article will give you an idea of common GraphQL bugs, and it is accompanied with an intentionally vulnerable API playground. The last tutorial is an excellent introduction to code-reuse attacks, and how to leverage them to bypass the latest XS mitigations like CSP, WAFs and HTML sanitizers.

Other amazing things we stumbled upon this week

Videos

- Bounty Thursdays – H1 paid $2.4m to hackers in ONE week , VirSecCon aftermath & Burp Bounty update
- Bug Bounty tips demonstrated #1
- Bug bounty's 101: What you need to know before hacking (on Intigriti) & Picking a platform
- h1-213 Recap: Lights, camera, hacking!
- Q&A Mental Health during COVID19
- OSINT 10 Minute Tips: Reverse Image Searching #1, Snapchat #1 & Data Scraping and Visualizing using Instant Data Scraper, ViewDNS.info, and Maltego
- Webinar 1 Security AMA With Jayson Street (Who's Your Hacker Con)
- Build, Attack, Defend, Fix – Paving the way to DA – EP2
- CyberSecLabs – "Secret" Walkthrough

Podcasts

- Bug bounties and burnout: Learn how to preserve your mental health
- ic0de – Enumeration Talk With Abartan Dhakal
- Darknet Diaries EP 63: w0rmer
- The Many Hats Club Ep. 53, Fun society (with fs0c131y)
- Security Now 762 – Virus Contact Tracking
- To Hunt or Not To Hunt; This is Never a !=? – Tyler Robinson – PSW #646
- Application Security Weekly #103 – Zooming Alex Stamos & Building Security TestOps
- Security Weekly News #25 – Zombieware, 5G Conspiracies, & C-Suite Targets
- Paul's Security Weekly #646 – Zoom, Kubernetes, and Hacking
- Risky Business #579 — Apple and Google go all in on contact tracing
- Layer 8 Podcast – Episode 21: Adam Compton – The Ladder and the Big Gulp
- cp<radio> – Eye on the Nile

Webinars & Webcasts

- Cybersecurity for Remote Workers: 3 Unexpected Ways Hackers Hit Households
- Dirk-jan streaming ROADtools – Azure AD exploration & ROADtools
- How to Build a Home Lab (1-Hour)
- SANS webcasts:
    - DNS is Changing. So What?
    - SANS CyberCast – SANS@Mic – Successful Infosec Consulting, Getting Clients Deep Dive
    - Consulting on The Side: Top Ten Questions Answered!
    - Purple Team Tactics: A Technical Look at Windows 10 Exploit Mitigations

Conferences

- Kernelcon 2020
- ComfyCon AU

- OffensiveCon20

Tutorials

Medium to advanced

- Google Oauth2 API Explained
- Ngrok for Local Infrastructure
- Generating SSH Config Files with Ansible
- Red Team Tactics: Utilizing Syscalls in C# – Writing The Code

Beginners corner

- Server-Side Template Injection (SSTI) in ASP.NET Razor-in-ASP.NET-Razor
- Quick Burp tip: Using Burp without changing your OS proxy settings
- Attacking applications with Base64
- Hacking The Web With Unicode
- HTTP Request Smuggling in Plain English.
- Home Network Design – Part 2
- LinkedIn OSINT Techniques (II) & LinkedIn OSINT Attack Surface
- Ultimate Guide: PostgreSQL Pentesting

Writeups

Challenge writeups

- Solution to @PwnFunction's XSS challenge – Ded
- RCE can lead to privilege escalation

Pentest writeups

- Broken Authentication in Mobile Application

Responsible(ish) disclosure writeups

- How We Hacked an Android Game And Ranked First globally #Android
- SMB access smuggling via FILE URL on Windows #Windows
- TikTok Vulnerability Enables Hackers to Show Users Fake Videos #Web
- Issue 2021: git: Newline injection in credential helper protocol #Web
- Advanced Javascript injections : Amazon XSS to full account takeover #Web
- DLL hijacking vulnerabilities in Nirsoft tools #Windows
- CVE-2019-1381 and CVE-2020-0859 – How Misleading Documentation Led to a Broken Patch for a Windows Arbitrary File Disclosure Vulnerability #Windows
- What’s a 10? Pwning vCenter with #Ldap

Bug bounty writeups

- Tricky Oracle SQL Injection Situation
- Business Logic Errors – A New Look
- Netflix Party— XSS Vulnerabilities (Netflix)
- [Writeup][Bug Bounty][Instagram] Instagram Still Send New DMs and Video Calls to Device After Logout [ID][EN] (Facebook, $750)
- $55,000 Facebook token leak vs Funny Airline token leak. (50,000 miles)
- Denial of service to WP-JSON API by cache poisoning the CORS allow origin header (Automattic, $550)
- Code injection in macOS Desktop Client (Nextcloud, $250)

See more writeups on The list of bug bounty writeups.

Tools

If you don’t have time

- ffufplus & Introduction: ffuf on Steroids
- SQLTruncScanner: Burp Suite extension for identifying possible SQL Truncation vulnerabilities & SQL truncation lab
- qsinject (Query String Inject): A tool that allows you to quickly substitute query string values with regex matches, one-at-a-time
- burp-exporter: A Burp Suite extension to copy a request to the clipboard as multiple programming languages functions
- ParamSpider: Mining parameters from dark corners of Web Archives

More tools, if you have time

- Default HTTP Login Hunter & Introduction: Login hunter of default credentials for administrative web interfaces leveraging NNdefaccts dataset
- haktldextract: Extract domains/subdomains from URLs en masse
- wpvulns.com: All WordPress version vulnerabilities for free without any limitations
- ExGen: A simple python script to create exploit templates for XSSI, JSONP Hijacking, Clickjacking and CORS vulnerabilities
- FinDOM-XSS: DOM XSS scanner in Bash
- MagicRecon: Bash wrapper around many recon tools
- QuickSQL: A simple MSSQL query tool that allows you to connect to MSSQL databases and does not require administrative level rights to use
- Lollipopz: Data exfiltration utility for testing detection capabilities
- Pet: Simple command-line snippet manager, written in Go
- SweetPotato & Introduction: Local Service to SYSTEM privilege escalation from Windows 7 to Windows 10 / Server 2019
- PowerSharpPack: Many offensive C# binaries now usable from within powershell
- pwndrop & Pwndrop – Self-hosting Your Red Team Payloads: Self-deployable file hosting service for red teamers, allowing to easily upload and share payloads over HTTP and WebDAV

Misc. pentest & bug bounty resources

- Web App Pentest mindmap
- Bug bounty cheatsheet
- AWS Cloud Penetration Testing Test Cases

- SMB Enumeration checklist

Challenges

- Vulnerable REGEX
- COBOL CTF

Articles

- Exploiting POST-based XSSI
- XSS fun with animated SVG
- The Path for Testing Path Traversal Vulnerabilities with Python
- JSP ContextPath Link Manipulation – XSS
- Prepare to Write A Scanner Plugin Before Your Next Platform Test!
- Cloud WAF Comparison, Part 2
- Targeting a macOS Application? Update Your Path Traversal Lists
- New Stealth Magecart Attack Bypasses Payment Services Using Iframes
- Windows Server 2008R2-2019 NetMan DLL Hijacking

News

Bug bounty & Pentest news

- The scraping API has been discontinued due to active abuse by third parties for commercial purposes…
- Rapid7 launches AttackerKB, a service for crowdsourcing vulnerability assessments
- jQuery 3.5.0 Released! but they are evaluating options and developing a model for independent security researchers
- New service vulnerable to subdomain takeover
- Brida 0.4 is out!
- wordlists.clipboard feature added to Turbo Intruder

- New topic & labs on Web Security Academy: SSTI
- Survey to help a PhD student create a hacking board game, with a chance to win an £50 Amazon voucher!
- Participate in independent survey to understand bug hunters motivations and challenges
- Facebook is launching Payout Collaboration with HackerOne
- Ethereum 2.0 bug bounty program gathers pace ahead of major blockchain platform update

Reports

- How much is the phish? Underground market of phishing kits is booming — Group-IB
- [SURVEY] 79% of Americans Share Passwords, But Only 13% Are Worried About Identity Theft

Vulnerabilities

- Microsoft April 2020 Patch Tuesday fixes 3 zero-days, 15 critical flaws
- Kernel vulnerabilities in Android devices using Qualcomm chips explored
- Academics steal data from air-gapped systems using PC fan vibrations
- Consumer reviewer Which? finds CAN bus ports on Ford and VW, starts yelling ‘Security! We have a problem…’
- Git security: Newline injection bug tricked version control system into leaking usernames and password
- That critical VMware vuln allowed anyone on your network to create new admin users, no creds needed
- TikTok users beware: Hackers could swap your videos with their own
- Coronavirus: Cisco wanted to delay patch for critical flaw in phone used by doctors

Breaches & Attacks

- Wappalyzer discloses security breach after hacker starts emailing users
- SentinelOne researcher trolled in new MBRLocker ransomware campaign
- Clipboard hijacking malware found in 725 Ruby libraries
- GitHub users targetted by Sawfish phishing campaign
- San Francisco Airport data breach: Double website hack may have lifted users’ Windows login credentials

- ICEBUCKET group mimicked smart TVs to steal ad money
- Hackers Update Age-Old Excel 4.0 Macro Attack
- 49 malicious Chrome extensions caught pickpocketing crypto wallets
- Magecart gang bypasses iframe protection on hosted payment site
- Linksys forces password reset for Smart Wi-Fi accounts after router DNS hack pointed users at COVID-19 malware

Coronavirus

- Exclusive: Meet the cybersecurity volunteers helping to protect the healthcare industry during the coronavirus outbreak
- Microsoft opens AccountGuard to healthcare providers on the COVID-19 front lines
- So how do the coronavirus smartphone tracking apps actually work and should you download one to help?
- Coronavirus contact tracing apps are worse than useless – Schneier
- Be honest: what did you do to cause the pandemic?
- No one’s getting new emoji in 2021 because of the pandemic
- COVID Will Accelerate Trends That Were Already Coming
- Don’t compromise your security during the COVID-19 crisis
- Coronavirus scams: This is how much people have lost to online fraudsters so far

Zoom

- Hackers Are Selling a Critical Zoom Zero-Day Exploit for $500,000
- Dark web: Cybercriminals sell over 500,000 Zoom accounts
- Thread on Zoom security by Mudge
- Zooom’s 90-Day Security Plan Progress Report: April 15
- Everything is Insecure: What Matters is What You’re Getting vs. Giving Up

Other news

- US offers $5 million reward for information on North Korean hackers

- Security lapse exposed Clearview AI source code
- GitHub is now free for teams
- New tool detects AWS intrusions where hackers abuse self-replicating tokens
- Windows Defender crashes: Microsoft fixes bug causing full scans to fail

Non technical

- Meet the team: Tom Hudson – Collaboration is the way forward
- @dawgyg's Basic Bug Bounty FAQ
- Q&A: Jack Cable Advocates for Security Education for All
- Interview: Metasploit founder HD Moore on bug bounties, computer security laws, and coronavirus· ·
- BeginnersQuest(part-1)-What to do after recon?
- Reaching Out to Fellow Beginners in Bug Bounty Hunting
- How to land an OSINT job
- What is a Security Operations Center (SOC)?

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 04/10/2020 to 04/17/2020.

*Curated by **Pentester Land** & Sponsored by **Intigriti***

Share this:

Twitter Facebook LinkedIn Reddit Telegram WhatsApp Email

Like this:

Loading...

YOU MIGHT ALSO LIKE

Bug Bytes #32 – XSS in Google.org, Burp Teams & Paged out!

20th August 2019

Bug Bytes #17 – 5 Important Bug Bounty Tips by @stokfredrik & @jhaddix, @securinti Is Just Reading The Docs & the Intigriti XSS Challenge Write-ups

7th May 2019

Bug Bytes #35 – DerbyCon Roundup, From Zero To Admin & Same-Origin Summarised

10th September 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