Blog

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

intigriti - 14th 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.

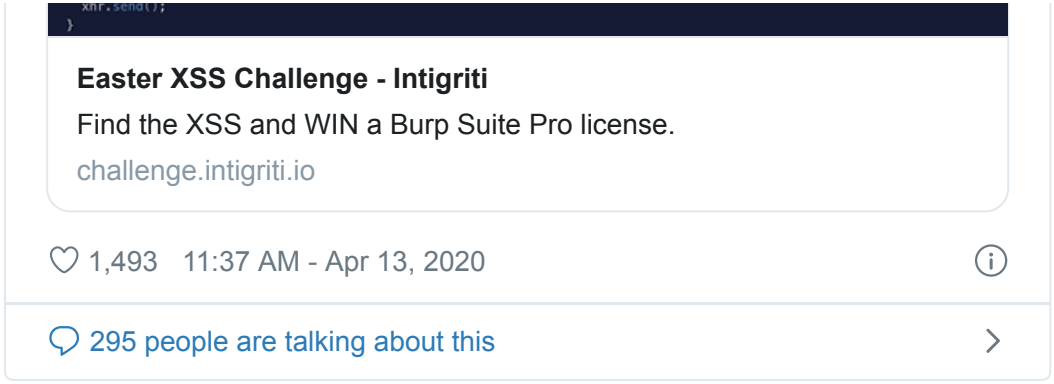
This issue covers the week from 03 to 10 of April.

Intigriti news

We launched another XSS challenge! Check it out and win a Burp Suite Pro license:

INTIGRITI
@intigriti

CHALLENGE: Find the XSS in our #EasterChallenge and WIN a @Burp_Suite Pro License! We'll tweet a tip for every 100 likes! ❤️
👇#HackWithIntigritichallenge.intigriti.io



Our favorite 5 hacking items

1. Article of the week

> Same Same But Different: Discovering SQL Injections Incrementally with Isomorphic SQL Statements

This is an excellent article on detecting SQL injections in a way that triggers less WAFs, and is more efficient than blindly firing random payloads.

The idea is to submit payloads that would have the same value if not properly sanitized (e.g. ?ID=1 and ?ID=2-1). If the output is the same, especially in multiple occurrences on the app, it indicates potential SQL injections. What can be automated is not the final payload, but testing for interesting behavior that calls for more manual tests.

This is not a new technique. @spaceraccoonsec shows examples of tools and research based on the same idea. But maybe this is the new way to test for injections in hardened targets.

2. Writeups of the week

> How we abused Slack's TURN servers to gain access to internal services ($3,500)
>
> Exploiting xdLocalStorage (localStorage and postMessage)

The first writeup is about a bug similar to SSRF but not limited to HTTP-based protocols. Slack's VoIP uses the TURN protocol (never heard of it before!). It could be abused to relay TCP and UDP traffic to the TURN server itself, and to internal addresses on Slack's AWS infrastructure.

The tool used as PoC was not shared, but this writeup has the merit of shining a light on an uncommon protocol (at least in bug bounty).

The second writeup is about a known unfixed vulnerability in the xdLocalStorage library. It is a nice read if you want to learn about localStorage, postMessage, how they work and how to abuse them to exploit common vulnerabilities.

3. Challenge of the week

> Breaking and Pwning Apps and Servers on AWS and Azure

@appseccouk open sourced their 3-day hands on training on hacking apps and servers on AWS and Azure. It is free, includes lessons for different topics, labs, and detailed documentation. A great opportunity to dive into cloud security!

4. Tutorial of the week

> Bypassing Xamarin Certificate Pinning on Android & Xamarin Certificate Pinning Bypass

The author faced a Xamarin Android app that performed certificate pinning in managed .NET code. It was resistant to all certificate pinning bypass techniques he tried. So, he created a basic Xamarin app for testing, and was able to obtain a custom Frida script that bypasses certificate pinning.

If you like a challenge, install the app without reading the tutorial and try to do the same!

5. Conference of the week

> VirSecCon2020: Hosted by NahamSec & TheCyberMentor w/ Talks on Bug Bounty, Mobile, Web, Recon &more!

Here is VirSecCon in a nutshell: 2 hackers came up with the idea to raise funds for @LLSusa and make the best of coronavirus lockdown, 11 hackers gave awesome talks on a variety of topics around Web/Mobile/IoT hacking, 1 CTF, and 14 sponsors among which 5 bug bounty platforms.

Like @Th3G3nt3lman says: 'dropping knowledge with support of all "BB platforms" for a noble cause is just WOW .. no competition shit no marketing only for the community.'

Initiatives like this are why I fell in love with this community!

Other amazing things we stumbled upon this week

Videos

- H12004 Virtual Live Hacking Event
  - Day 1: Virtual Live Hacking Event Kick-off
  - Day 2: Hacker Couch with @STÖK, @Hacker_, @BugBountyHQ, Ramsexy, @LukeTucker
  - Day 3: How To Get Started in InfoSec Panel with TheCyberMentor, zseano, STOK, Tomnomnom and jhaddix!
  - Day 4: VirSecCon (See Conf of the week⬆️)

    - Recon Sunday x Day 5: Top h1-702 Paid Hackers Dawgyg, Mayo, and cdl
    - Live Recon x Day 6: HackerOne Community Team
    - Day 7: How to Become a HackerOne Millionaire or MVH with @Inhibitor181, @Dawgyg, @0xacb, & @0xteknogeek
    - Day 8: Closing Ceremonies
- Finding Your First Bug: Impact and Report Writing
- Let's Nmap
- Google Dorks and DoD
- Complete tmux Tutorial
- The BEST Resource for your IT Career
- How to transition a suddenly remote company, lead teams, and change mindsets when working from home
- Learn Stuff with Yekki – Episode 2 – Using Responder (and not being a cardshark) & Article
- Penetration Testing Version 1

Podcasts

- Security Now 761 – Zoom Go Boom
- Risky Business #578 — ASD launches offensive campaign against criminals
- Here is what to expect from bug bounty hunting
- Zooming, Zoomie, & Zoomfest Zoo – SWN #23
- Zoom Flaws, 'Zombie' win32k Bug, & Inputscope – ASW #102
- Grace Hopper, COBOL, & AI Toilets – Wrap Up – SWN #24

Webinars & Webcasts

- SpecterOps's Webinar Week:
    - Hunting from home
    - Everything You Always Wanted to Know about BloodHound* (*But Were Afraid to Ask)
    - Kerberoasting Revisited

    - Capability Abstraction: Dumping LSASS
    - Remote Project Management & Reporting
- DC44141 – April 2020; Red Team & Blue Team / So, you want to learn red teaming?
- InfosecGirls Virtual meet with Jessica and Pragya:
- Cyber Security Career Chat with Noureen
- Introduction to Sandbox Evasion and AMSI Bypasses – Jake Krasnov, Anthony Rose, Vincent Rose
- SANS webcasts:
    - SANS CyberCast SANS@MIC – Pen Testing ICS and Other Highly Restricted Environments
    - SANS CyberCast SANS@MIC – Domain Password Auditing with the Cloud

Conferences

- What's New With OAuth and OIDC?
- OWASP NL Livestream: SKF News by Riccardo Ten Cate
- Ekoparty – Informal chat with Agarri_FR (the rest of the conference is in Spanish)

Slides & Workshop material

- DOM XSS

Tutorials

Medium to advanced

- SQL Rollback Hack
- Python Jailbreak Mastery
- Attack Graphs – How to create and present them
- Wanted: Process Command Lines
- Blue Team vs Red Team: how to run your encrypted ELF binary in memory and go undetected

- Build, Attack, Defend, Fix – Paving the way to DA – Part 1/5
- Another method of bypassing ETW and Process Injection via ETW registration entries

Beginners corner

- GraphQL — Common vulnerabilities & how to exploit them
- How to import external spidering output to Burpsuite or ZAP
- Doing Recon on a Large Scope
- Lambda, Metasploit, and Shells
- Cloud pentesting in Azure: one access key to rule them all
- Back Me Up — Hacking Android apps without root & Android-backup-app
- Customizing Kali Linux
- Introduction to Active Directory exploitation.
- Production-Ready GoPhish with NGINX, MySQL, and Docker
- Windows authentication attacks – part 1
- Attack Chain Series: Remote Access Service Compromise Part 1 — RDS
- Backdoors & Breaches: Logon Scripts

Writeups

Challenge writeups

- JWT Challenge 1 walkthrough

Pentest writeups

- Journey of a security bug — From a naive-looking PDF Download to SSRF via HTML Injection in AWS & Finding SSRF via HTML Injection inside a PDF file on AWS EC2
- Hacking the Oce Colorwave printer: when a quick security assessment determines the success of a Red Team exercise.

Responsible(ish) disclosure writeups

- Another SSRF, Another RCE – The Microstrategy case
- Several Critical Vulnerabilities on most HP machines running Windows
- OhMyZsh dotenv Remote Code Execution RCE
- CleanMyMac X 4.4.0 – LPE #PrivilegeEscalation #MacOSX
- CVE-2020-11107 #PrivilegeEscalation #Windows
- Authenticode verification vulnerability pattern #Crypto #CodeReview #C#
- Getting root on a Zyxel VMG8825-T50 router #Router #Web #PrivilegeEscalation
- GHSL-2020-011: Remote Code Execution – JavaEL Injection (low privileged accounts) in Nexus Repository Manager #RCE #CodeReview #Java
- Duo Finds SAML Vulnerabilities Affecting Multiple Implementations #Web

Bug bounty writeups

- HTML-injection in PDF-export leads to LFI (Visma, $500)
- Code injection in macOS Desktop Client (Nextcloud, $250)
- CSRF on connecting Paypal as Payment Provider (Shopify, $500)
- Unrestricted CV File Upload
- Executing scripts in Safari Reader Mode to CSP Bypass (Apple)
- Listing all registered email addresses on Google's Crisis Map thanks to IDOR and incremental IDs
- Plan Change Logic in Google Fiber (Webpass) (Google)
- How a Simple CSRF Attack Turned into a P1 Level Bug
- $3K Bounty For Elastic-Search Takeover ($3,000)
- The story of a fuzzing integration reward (Google, $10,000)

See more writeups on The list of bug bounty writeups.

Tools

If you don’t have time

- Nuclei: A fast tool for configurable targeted scanning based on templates offering massive extensibility and ease of use
- Dnsprobe: A tool built on top of retryabledns that allows you to perform multiple dns queries of your choice with a list of user supplied resolvers.
- Commit Stream: OSINT tool for finding Github repositories by extracting commit logs in real time from the Github event API
- fzf & Introduction & Demo: A command-line fuzzy finder

More tools, if you have time

- Nessus Professional Database Export & Introduction: Python tool for exporting Nessus Results into a Database
- grep.app: Regex search across a half million git repos
- Firefox Security Toolkit: A tool that transforms Firefox browsers into a penetration testing suite
- gaussrf: Fetch known URLs from AlienVault’s Open Threat Exchange, the Wayback Machine, and Common Crawl and Filter Urls With OpenRedirection or SSRF Parameters
- Vuln Cost: Open source security scanner for VS Code
- Automation Through Azure DevOps with Bob
- Firebase-Extractor: A tool written in python for scraping firebase data
- FridaAndroidTracer & A self basic audit for Android applications: Android application tracer powered by Frida
- Parallel Enumerator: Parallelized enumeration tool for red team engagements and bug bounty programs
- Print-My-Shell: Python script wrote to automate the process of generating various reverse shells
- Vuln Cost: security scanner for VS Code
- HikPwn: A simple scanner for Hikvision devices with basic vulnerability scanning capabilities written in Python 3.8
- Fudge: Hiding implants in HTML files for phishing engagements
- DroneSploit: Drone pentesting framework console
- SharpFinder: Searches for files matching specific criteria on readable shares within the domain
- Ghost In The Logs: Evade sysmon and windows event logging

Misc. pentest & bug bounty resources

- Building Secure and Reliable Systems
- Methods to Bypass Rate Limit
- API writeups
- Infosec Communities You Should Join
- CodeQL.nvim: Plugin for writing CodeQL queries from vim
- @thecybermentor's Mindmap & Hacking resources
- Bug bounty resources & advices
- Cyber Security Books and Resources | Community Project
- Capsulecorp Pentest: Vagrant VirtualBox environment for conducting an internal network penetration test
- Introducing Slingshot C2 Matrix Edition
- Learn Ruby on Rails

Challenges

- @SecurityMB's XSS challenge
- New Intigriti XSS challenge: Winner gets a Burp Suite Pro License!
- The GitLab 2020 CTF to be run at home

Articles

- Docker Registries and their secrets
- Attack matrix for Kubernetes
- Identifying Cobalt Strike team servers in the wild by using ZoomEye(Part 2)
- Phishing for SYSTEM on Microsoft Exchange (CVE-2020-0688)
- Breaking LastPass: Instant Unlock of the Password Vault
- With IoT, Common Devices Pose New Threats

News

Bug bounty & Pentest news

- Free training and free exam vouchers for the Azure AZ-900 fundamentals certification
- SAVE THE DATE!!! #LevelUp0x06 Date Announced
- Brussels Airlines leverages the power of Bug Bounty through intigriti platform to discover critical vulnerability not detected by pentests.: Great analogy on the difference between pentest & bug bounty!
- New Hacker Following feature on Hackerone, Monthly payouts & Hack for Good: Easily Donate Bounties to WHO's COVID-19 Response Fund
- Pluralsight free for April
- Free online conferences calendar
- Virtual cybersecurity conferences: An expanding list

Reports

- SilverTerrier: 2019 Nigerian Business Email Compromise Update
- Microsoft: No surge in malicious attacks, only more COVID-19 lures

Vulnerabilities

- PowerPoint 'Weakness' Opens Door to Malicious Mouse-Over Attack
- Google removes Android VPN with 'critical vulnerability' from Play Store
- Micronaut CRLF injection bug opened the door to server-side request forgery
- Serious Exchange Flaw Still Plagues 350K Servers
- Can fingerprint authentication on smartphones be fooled with 3D printing? Researchers find out
- Open TURN proxy granted unauthorized access to Slack's infrastructure

Breaches & Attacks

- Thousands of Android apps contain undocumented backdoors, study finds
- Dark_Nexus Botnet Compromises Thousands of ASUS, D-Link Routers
- These hackers have been quietly targeting Linux servers for years
- Unique P2P Architecture Gives DDG Botnet 'Unstoppable' Status
- Discord Turned Into an Account Stealer by Updated Malware
- Self-Propagating Malware Targets Thousands of Docker Ports Per Day
- DarkHotel hackers use VPN zero-day to breach Chinese government agencies
- This is why the vicious xHelper malware resists factory wipes and reboots
- Fleeceware apps discovered on the iOS App Store
- WooCommerce Falls to Fresh Card-Skimmer Malware
- Kaspersky uncovers a creative water hole attack discovered in the wild

Malicious apps/sites

Other news

- As if the world couldn't get any weirder, this AI toilet scans your anus to identify you
- Firefox now tells Mozilla what your default browser is every day
- Porting the Bug Bounty Concept to Threat Hunting
- Microsoft buys corp.com to prevent Windows account hijacking
- Linux Foundation backs security-oriented seL4 microkernel operating system
- Google backs Apple's SMS OTP standard proposal
- The Sandboxie Windows sandbox isolation tool is now open-source!
- Roaring trade in zero-days means more vulns are falling into the hands of state spies, warn security researchers
- Visa urges merchants to migrate e-commerce sites to Magento 2.x
- Chrome 81 Released With 32 Security Fixes and Web NFC API
- Cloudflare dumps reCAPTCHA as Google intends to charge for its use

Coronavirus

- COVID-19 Response: New Jersey Urgently Needs COBOL Programmers (Yes, You Read That Correctly) & Where to learn COBOL for free
- Apple and Google are building a coronavirus tracking system into iOS and Android
- ActLocal – Great initiative by @prashles!
- Iran, Colombia, and Italy Put Citizens at Risk with COVID-19 Government Mobile Apps
- UK government slams 'crackpot' 5G-coronavirus theories following mast arson attacks
- Hackers struggle morally and economically over Coronavirus

Zoom

- Zoom Security: Here's What Zoom Is Doing To Make Its Service Safer
- Zoom Fiesta
- Coronavirus home work: Zoom sued over security lapses as stock slides

Non technical

- Learn bypasses, not payloads
- Be careful what you OSINT with
- How to keep hackers motivated in bug bounty
- Bug Bounty 5 years in
- Full-time bug hunting: Pros and cons of an emerging career
- Bug Bounty Q&A #1: What is ethical hacking and bug bounty?
- The Cloud is Beige – The demise of black box testing
- The Five Levels of Remote Work — and why you're probably at Level 2
- To err is human

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 04/03/2020 to 04/10/2020.

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

YOU MIGHT ALSO LIKE

Bug Bytes #9 – Hacking Web Sockets, $10k Facebook Bug by @vulnano & Automated Bug Hunting

12th March 2019

Bug Bytes #57 – Th3G3nt3lman's Secret Recon Methods, Checkmarx VS API's & Vulns in React Native Apps

11th February 2020

Bug Bytes #61 – Facebook Account Takeover, @thedawgyg's Darknet Diaries and Bug Bounty Millionaire @inhibitor181

10th March 2020

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