Bug Bytes #68 – Memory leaks in webapps, @samwcyo's Rocket League chain & JavaScript for Hackers

BY INTIGRITI · APRIL 28, 2020 · LAST UPDATED ON JULY 17, 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 10 to 17 of April.

Intigriti news

Another public bug bounty program launched on Intigriti. Pays bounties up to €10.000! Check it out here: https://go.intigriti.com/napoleongames

Our favorite 5 hacking items

1. Paper of the week

"Uninitialized Memory Disclosures in Web Applications"

This is an excellent paper on memory disclosure vulnerabilities in Web apps. The author focuses on bugs caused by image parsing errors, such as ImageTragick, but shows how to extrapolate the attacks to libraries other than ImageMagick.

If you want to take a deep dive into this kind of bugs, this is a great opportunity. A lot of resources are provided from tools for automated detection, to a test environment, writeups, and external links on memory leaks.

2. Writeup of the week

> "Abusing HTTP Path Normalization and Cache Poisoning to steal Rocket League accounts"

What a great read! @samwcyo chained HTTP cache poisoning with an open redirect that leaks the victim's OAuth token. He explains each bug separately, how to combine them for maximum impact, what he tried that didn't work, and also how he approaches hacking video games as a Web app tester without mastering reverse engineering.

3. Videos of the week

> "– Hacker101 – JavaScript for Hackers (Created by @STÖK)
>
> – Creating Wordlists for Pentesting & Bug Bounty Hunting Using Seclists, Bigquery, and More!
>
> – @Ngalongc Talks About Hacking Uber, Airbnb and Shopify, SAML/OAuth Vulnerabilities, Recon, and More!"

If you're short on time, these 3 videos are what you need to check out from this whole newsletter. @tomnomnom shows how to analyze JavaScript and find bugs in the DOM using Chrome dev tools. @NahamSec shares how to create custom wordlists, and how to know which one you need to use. And @Ngalongc talks about his bug hunting journey, how he went from working in another industry with no security or developer background, to being a bug bounty millionaire, the type of bugs he focuses on, his recon process, etc.

4. Tutorial & tool of the week

> "– Subdomain Enumeration: Filter Wildcard Domains
>
> – gwdomains"

Detecting and filtering out wildcard subdomains is important during subdomain enumeration, to avoid wasting time on subdomains that don't exist. @0xpatrik published a cool post on exactly that.

Gwdomains automates this process. But I'm not sure how it works exactly. It would be interesting to figure it out by reading the source code, and to compare it with @0xpatrik's detection heuristic and all the cases he mentioned.

5. Resource of the week

> "Public Release of HTML5 attack and Defence course"

This is a nice introductory course on HTML5 attacks. It's a bit outdated but still a good resource to discover HTML5 technologies (CORS, DOM, Local Storage, Webworkers, Websockets, Iframe sandboxing...) and some of their common security issues.

Other amazing things we stumbled upon this week

Videos

- UMBC Cyberdawgs CTF: The Hacker One

- Bug Bounty Reports Explained
- Reported to Resolved: Bug Bounty Program Manager
- Bypassing Login forms with BurpSuite – Pentesting
- Get Certified! All You Need to Know to Rock GIAC Exams
- Learn Stuff with Yekki – Episode 3 – Creating bespoke wordlists and cracking a hash!

Podcasts

- A Day in the Life of an Ethical Hacker Podcast Series: Interview with Özgür Alp, Synack Red Team Member
- Security Now 763 – The COVID Effect
- Risky Business #580 — Czech spear phishing spurs fightin' words from Pompeo
- Layer 8 Podcast – Episode 22: Derrick Levasseur – Going to College...for the Bust
- CoalCast #14 – CovidCast w/ Marc Rogers
- Security Weekly News #27 – Starbleed, Hacking Dropbox, & FPGA Chip Flaws & – #28 – 0 Day Extravaganza, Zoom Can't Win, & Starbleed – Wrap Up
- Naked Security – S2 Ep36: Rogue Chrome extensions, Signal fears and Darth Vader – Naked Security podcast
- Cyber Security Sauna 038| Mikko Hypponen on Zoom, COVID-19 Threats, and Working During a Pandemic

Webinars & Webcasts

- Fantastic Vulnerabilities and Where to Find Them – The AppSec Edition
- Hacking Jenkins
- SANS @MIC Talk – Secure Video Conferencing – What to Train Your Workforce On

Conferences

- Disobey 2020
- TheManyHatsClub Isolation Con – Red Team Track!, Purple Track, Blue Team/App Sec Track & Schedule

Slides & Workshop material

- GitHub Security Virtual Meetup

Tutorials

Medium to advanced

- Azure AD introduction for red teamers
- Designing The Adversary Simulation Lab
- Attacking smart cards in active directory
- Exploiting VLAN Double Tagging
- Microsoft ATA Evasion (Over PTH, Golden Ticket)
- Kerberos Delegation

Beginners corner

- The Zaheck of Android Deep Links!
- Oauth and Security
- iOS Application Security — Static Analysis
- Everything You Need to Know About IDOR (Insecure Direct Object References)
- Open Redirects – Everything That You Should Know
- Content-Security-Policy (CSP) Bypass Techniques
- A guide to searching LinkedIn by email address
- Smart Meters – Assessing Hub Risk

Writeups

Challenge writeups

- Intigriti Easter XSS Challenge winner & solutions
- VirSecCon 2020 CTF – Web Challenges

Pentest writeups

- How to hack a company by circumventing its WAF for fun and profit – part 2
- NotSoSmartConfig: broadcasting WiFi credentials Over-The-Air & NotSoSmartConfig

Responsible(ish) disclosure writeups

- Multiple Vulnerabilities in IBM Data Risk Manager #Web
- Strike Three :: Symlinking Your Way to Unauthenticated Access Against Cisco UCS Director #RCE

- SSD Advisory – Cisco AnyConnect Privilege Elevation through Path Traversal #Web
- How I was able to steal millions of data and money from a Ticketing Portal. #Web
- Bestiefy — IDOR Galore #Web
- Critical CSRF to RCE bug chain in Prestashop v1.7.6.4 and below #Web
- Serious flaws found in multiple smart home hubs: Is your device among them? #IoT

Bug bounty writeups

- CORS bug on GOOGLE's 404 page REWARDED!!!
- DOM based open redirect to the leak of a JWT token
- From P5 to P2, from nothing to 1000+$
- The Secret sauce of bug bounty
- Misconfigured WordPress takeover to Remote Code Execution
- Server Side Request Forgery mitigation bypass (GitLab, $3,500)
- XXE through injection of a payload in the XMP metadata of a JPEG file (Informatica)
- An invite-only's program submission state is accessible to users no longer part of the program (Hackerone, $500)

Tools

- Proxying HTTP2 Through Burp Suite
- Docker Image Generator & Introduction: Customized docker images generation toolkit for infosec
- Burp Extension Generator: Generate Burp Suite Extension projects the easy way
- DalFox (Finder Of XSS): Parameter Analysis and XSS Scanning tool based on golang
- OpenRedireX: A python Fuzzer for OpenRedirect issues
- Pown LAU: A library and Pownjs tool for enlisting target web application URLs using several public databases (inspired by getallurls)
- 2tearsinabucket: Go script to enumerate s3 buckets for a specific target
- TitleXtractor: Go script for extracting \ tag from HTML pages
- Linkedin Scraper: A fully configurable Python tool to scrape anything within linkedin
- ReverseIP.sh: Simple bash script for Reverse IP Lookup, using whoisxmlapi.com
- Lazyhunter: A framework that provides a web UI to commonly used Bug Hunting/Pentesting tools

- Socks Over RDP & Slides: A tool that creates a virtual channel over an RDP connection and spins up a SOCKS5 proxy that is tunnelled over the remote host, just like SSH's –D switch
- eLdap & Presentation: A Python tool that helps users searching and filtering queries in Ldap environment
- PCredz & Introduction: Python script that extracts Credit card numbers, NTLM(DCE-RPC, HTTP, SQL, LDAP, etc), Kerberos (AS-REQ Pre-Auth etype 23), HTTP Basic, SNMP, POP, SMTP, FTP, IMAP, etc from a pcap file or from a live interface

Misc. pentest & bug bounty resources

- Source Code Review – ProtonMail Android App
- Harvard Univeristy's free online courses
- Billing Hack: Application that allows impersonating the Google Play Billing service. Helps bypass #Android In-app purchase when there is no server side checks
- Collection of Scripts for shodan searching stuff
- Know About 100 Best Hacking Tools
- CyberSecurityTV Youtube channel
- Nuclei templates
- How To Become A Penetration Tester

Challenges

- St4yH0me4ndH4ck CTF: April 19-29
- Space Security Challenge 2020 Hack-A-Sat: May 22-24
- PwnTillDawn: May 30
- Hack-From-Home Challenge: Ends May 11
- $10,000 NordLocker Bounty
- Game of Pwns
- New XSS challenge by @rodoassis
- Kontra OWASP Top 10

Articles

- Pillaging AWS ECS Task Definitions for Hardcoded Secrets
- The road from sandboxed SSTI to SSRF and XXE

- EyeWitness – Potential Modifications
- Abusing Firefox in Enterprise Environments
- Jamfing for Joy: Attacking macOS in Enterprise & Jamf-Attack-Toolkit
- Exploiting (Almost) Every Antivirus Software

News

Bug bounty & Pentest news

- AMA with @PyroTek3 on security & tech topics: May 1st
- EC-Council resources free during the Covid-19 pandemic
- European Cybersecurity Blogger Awards – VOTE FOR YOUR WINNERS
- Google to subsidize bug bounty hunters during pandemic
- Firefox bug bounty: Mozilla raises payouts and abandons 'first reporter wins' policy
- Report: curl's bug bounty one year in
- OWASP Web Security Testing Guide v4.1
- Bug Bounty Q&A #3: What effort does is take to set up a bug bounty program?
- Scoring $200K at the hacking event that almost didn't happen
- #ThisIsWhatHackerLooksLike
- Wanted dead or alive, a bug looking for its owner
- Pastebin hints at new research subscription model after axing scraping API

Reports

- Behind the Screen: An insight into Context's testing data
- Bad Bot Report 2020: Bad Bots Strike Back
- Following the money in a massive "sextortion" spam scheme

Vulnerabilities

- PSA: A viral text string with an Italian flag and Sindhi characters will crash your iPhone [U]
- iOS Mail bug allows remote zero-click attacks & Apple disputes recent iOS zero-day claim
- Researcher discloses four IBM zero-days after refusal to fix
- Windows 10 SMBGhost RCE exploit demoed by researchers

- Cloud security: Azure environments at risk from on-prem privilege escalation attack
- Dropwizard RCE flaw now fully patched following partial fix
- Window 10 update weakened Google Chrome's security
- Microsoft Issues Out-Of-Band Security Update For Office, Paint 3D

Breaches & Attacks

- Nintendo Confirms Breach of 160,000 Accounts
- Bot creates millions of fake eyeballs to rip off smart-TV advertisers
- DHS CISA: Companies are getting hacked even after patching Pulse Secure VPNs
- Hackers have breached 60 ad servers to load their own malicious ads
- New iOS exploit discovered being used to spy on China's Uyghur minority

Other news

- All ProtonMail apps are now open source, as Android joins the list!
- Security researcher identifies new APT group mentioned in 2017 Shadow Brokers leak
- Cynet throws down gauntlet with launch of cyber-attack incident response challenge
- NSA: Hackers exploit these vulnerabilities to deploy backdoors
- Google rolls out BeyondCorp Remote Access for browser-based apps
- Cloudflare debuts Border Gateway Protocol safety check tool

Coronavirus

- Pro-bono Pentests for COVID-19-related Apps & Software: Applications accepted until May 11
- Governments gravitate to Gapple contact tracing standard & Everything you ever wanted to know about Bluetooth contact tracing but were too scared to ask (video)
- France asks Apple to relax iPhone security for coronavirus tracking app development
- Scientists lobby government to build privacy into coronavirus contact-tracing apps
- Proposed government coronavirus tracking app falls at the first hurdle due to data breach
- Goolge's findings on COVID-19 and online security threats
- FBI says cybercrime reports quadrupled during COVID-19 pandemic
- Payment distancing: Apple and Google, we need our cashless society even more in pandemic times

- Tor Project lays off a third of staff due to coronavirus pressures

Non technical

- From Bug Bounty Hunter, to Engineer, and Beyond
- Stuck Inside? Top Books We Recommend Security Pros Read During Quarantine
- A Small Change in Life Helps to Convert Entertainment to Productive Work.
- The AWAE/OSWE Journey: A Review
- Anatomy of Automated Account Takeovers
- Things to do at home – Hacker Video Games
- Hacking 5G, Part 2 & Part 3
- How to Pick a Video Conferencing 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 04/17/2020 to 04/24/2020.

Curated by Pentester Land & Sponsored by Intigriti