Blog

⌂ > 2020 > April > 7 > Uncategorised > Bug Bytes #65 – Hacking webcams, internal servicedesks & parsers

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

intigriti - 7th 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 27 of March to 03 of April.

Our favorite 5 hacking items

1. Slides of the week

> Attacking Secondary Contexts in Web Applications

@samwcyo's Kernelcon talk explores attacking various secondary contexts (APIs, reverse proxies, middleware) in Web applications. He shows how to detect application routing (in black box), and examples of vulnerabilities that can result from interactions between different servers.

This is excellent research and an interesting area to explore further. The talk video is not available yet, but will be released soon hopefully.

Also good to know, you can reproduce the last trick (Authy 2FA bypass) in @PentesterLab's "Idor to Shell".

2. Writeups of the week

> iPhone Camera Hack ($75,000)
>
> –Hundreds of internal servicedesks exposed due to COVID-19 (>$10,000)

> How to hack a company by circumventing its WAF through the abuse of a different security appliance and win bug bounties

It was impossible to feature only one writeups as these 3 are all awesome! The iPhone Camera Hack is a deep dive into several bugs found in Safari. They allowed Ryan Pickren to gain zero-click unauthorized camera access on iOS and macOS, and earned him an impressive $75,000 bounty.

The second article sums up @securinti's findings after scanning 10.000 popular domain names for misconfigured Atlassian instances. He noticed a 12% increase of exposed instances since last summer, maybe because of remote work due to COVID-19.

The third writeup reads like an investigation. @redtimmysec identified middleware in use (a WAF and a Bluecoat proxy), and was able to bypass the WAF to exfiltrate sensitive data with SSRF. This is an excellent example of a "secondary contexts" bug.

3. Article of the week

> How to exploit parser differentials

Gitlab's transparency is amazing. This is a writeup for a file upload vulnerability found internally. It illustrates the concept of parser differentials which is similar to @samwcyo's "secondary contexts" attacks, but applied to file uploads.

This is a unique opportunity to learn about a critical bug with details, from the company itself, about the source code and how file uploads are handled.

4. Video of the week

> @Codingo_ Talks About Pentesting, Escalating Bugs, OSCP, Working at Bugcrowd, Burp Suite and More!

The interview with @codingo_ is A-M-A-Z-I-N-G! He shares so many ideas and good insights. For instance his philosophy around XSS proofs of concept got him a much bigger bounty for a duplicate XSS than its first reporter! He has a unique background, and a strong opinion on which programming languages to learn.

Also a big shout-out to @NahamSec for being a great interviewer and asking all the questions I had in mind.

5. Tool of the week

> Crithit

Crithit allows you to do directory and file brute forcing at large scale. It takes each entry from a wordlist and tests it against all targets before moving on to the next entry.

If this reminds you of something, it is probably of Inception which is similar. The difference is that Inception takes a configuration file with specific endpoints to test for as input (e.g. .env, .git, etc), while Crithit can be used with any wordlist. So, Crithit is more practical when you want to test bigger or existing wordlists. It also support filtering outputs using HTTP response codes and signatures to look for in responses.

Other amazing things we stumbled upon this week

Videos

- Note-Taking for Bug Bounty Hunters – How I Use Notion and How You Can Too, TL;DR version & Reply if you want to share your notes/organisational system
- HackerOne #h1-2004 Community Day: Intro to Web Hacking – OWASP Juice Shop
- Ron Chan's Secret to Finding Critical Security Issues on GitLab
- How to access protected intents via exported Android activity embedded intent
- Bounty Thursdays – April 2nd – zlz delivers magic, Crithit, Joberts Vulncode & ctfchallenges!
- BugBountyToolkit – Running Multiple Sessions With Tmux
- Hack the Box: How does linux work?
- Build, Attack, Defend, Fix – Paving the way to DA – EP1
- Working From Home // How to Stay Motivated, Focused, and Productive

Podcasts

- Paul's Security Weekly #645 – Security News – To Zoom or Not to Zoom
- Security Now 760 – Folding Proteins
- Darknet Diaries EP 62: Cam
- A Chat with Jonathan Cran About Intrigue and Security in the COVID-19 Pandemic
- Risky Business #577 — Stir crazy lockdown edition
- Feature Podcast: Voting in 2020 will likely be by mail
- Securiosity: How has COVID-19 changed the cybersecurity community?
- Security Weekly News #22 – DEER.IO, Maze Ransomware, & Unacast – Wrap Up

Webinars & Webcasts

- The subtle art of secure code review – Gowthami
- Webcast: Pandemic Paradigm Shift: Remote Working is the New Normal
- Real-Time OSINT: Investigating Events as They Happen | SANS OSINT Summit 2020
- Virtual Barcelona Security Community Meetup – WoSEC + CyberBCN

- Adversary emulation using CALDERA – Building custom abilities – Part #2

Conferences

- Python for AWS – Boto3 by Sanjeev Jaiswal and MITRE ATT&CK Framework by Arpan Raval & Github repo
- PancakesCon Track ONE & Schedule

Tutorials

Medium to advanced

- Quick wins with Adobe Experience Manager
- Tricks for Weaponizing XSS
- Kubernetes Security – A Useful Bash One-Liner
- Data exfiltration over DNS with Remote Code Execution
- How To Bypass CSP By Hiding JavaScript In A PNG Image
- They told me I could be anything, so I became a Kubernetes node – Using K3s for command and control on compromised Linux hosts
- How to exploit Liferay CVE-2020-7961 : quick journey to PoC
- NTLM Relay
- Mark-of-the-Web from a red team’s perspective
- Kerberos Tickets on Linux Red Teams

Beginners corner

- XML External Entity (XXE) Attacks and How to Avoid Them
- OWASP Amass: A Solid Information Gathering Tool
- DoS – Mr. Pixel Flood
- Chrome Extension Analysis
- LinkedIn OSINT Techniques: Part I

- Facebook Tips
- Lab Building Guide: Virtual Active Directory
- Credential Dumping: Wireless
- Command & Control: PoshC2

Writeups

Challenge writeups

- Yogosha Hackitivist Challenge 2019
- OSINT? More like OhSINT!
- Me and the Bois
- myClock XSS Challenge Solution Write-Up

Pentest writeups

- Combining Request Smuggling and CBC Byte-flipping to stored-XSS
- Chaining multiple techniques and tools for domain takeover using RBCD
- Understanding DTLS Usage in VoIP Communications

Responsible(ish) disclosure writeups

- [DrayTek] – Unauthenticated RCE in Draytek Vigor 2960, 3900 and 300B (CVE-2020-8515) & PoC #Web #RCE
- Exploring the minimist prototype pollution security vulnerability #Web
- CVE-2020-10560 – OSSN Arbitrary File Read #Web #Crypto
- CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers (‘HTTP Request Header Injection’) #Web #CodeReview
- Pentesting Zen Load Balancer #Web
- Imperva WAF Bypass #Web
- [BugWithoutBounty] Missing Authentication in TheCoffeeHouse Api #Mobile #API

- CVE-2020-8816 – Pi-hole Remote Code Execution #RCE

Bug bounty writeups

- Attacking HelpDesks Part 1: RCE Chain on DeskPro, with Bitdefender as a Case Study (Bitdefender, $5,000)
- Limited freemarker ssti to arbitrary liql query and manage lithium cms
- Touch ID Authentication Bypass on Evernote and Dropbox IOS Apps
- Email Confirmation Bypass in myshop.myshopify.com that Leads to Full Privilege Escalation to Any Shop Owner by Taking Advantage of the Shopify SSO (Shopify, $15,000)
- [Part II] Email Confirmation Bypass in myshop.myshopify.com that Leads to Full Privilege Escalation (Shopify, $15,000)
- Able to Takeover Merchants Accounts Even They Have Already Setup SSO, After Bypassing the Email Confirmation (Shopify, $7,500)
- Periscope iOS app CSRF in follow action due to deeplink (Twitter, $2,940)
- Relative Path Vulnerability Results in Arbitrary Command Execution/Privilege Escalation (Slack, $750)
- H1514 CSRF in Domain transfer allows adding your domain to other user's account (Shopify, $500)
- An attacker can buy marketplace articles for lower prices as it allows for negative quantity values leading to business loss (SEMrush, $2,111)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- JSScanner & Introduction: Automated scanning of JS Files for Endpoints and Secrets
- Runtime Mobile Security: A powerful web interface that helps you to manipulate Android Java Classes and Methods at Runtime

More tools, if you have time

- dupknock: Python tool to help you knockout duplicate entries from multiple files and generate the final output
- Subgen: A Go utility to concatenate wordlists to a domain name – to pipe into your favourite resolver!

- Snaffler: A tool for pentesters to help find delicious candy
- EyeWitness for Windows & Introduction: A .Net implementation of EyeWitness
- padding-oracle-attacker: CLI tool and library to execute padding oracle attacks easily, with support for concurrent network requests and an elegant UI
- linkedin-profile-scraper & Introduction: Python script for Scalable LinkedIn Username Hunting
- CVE-2020-0796 Local Privilege Escalation POC: PoC to exploit SMBGhost (CVE-2020-0796) for Local Privilege Escalation
- LockLess: C# tool that allows for the enumeration of open file handles and the copying of locked files
- payload.edn: POST-exploitation persistence using Leiningen profiles.clj (Clojure's dependency management tool)
- gTunnel: A robust tunelling solution written in Golang
- McAfee Config Decryptor

Misc. pentest & bug bounty resources

- Bug bounties. Five Weeks To Your First Bug
- Adding Undo/Redo functionality to Java Swing/Burp Extension
- Jar Files: Modification Cheat Sheet
- Android application testing (BOUNTY HUNTING)
- Awesome Risk Quantification
- C2Hack: Tips and tricks for pentesters
- mimikatz Is My New EICAR
- Rainbow Crackalack Project Releases NTLM 9-Character Rainbow Tables!

Challenges

- GraphQLab by @digininja
- @_zulln's XSS challenge
- Slayer Labs: Free for the next few weeks

Articles

- Android Webview Exploited
- You need multiple SAML IDP signing keys
- Impact of DNS over HTTPS (DoH) on DNS Rebinding Attacks
- Machine learning – Predict vulnerabilities by examining the words in a URL
- Quick exploration of the use of .chm and .hta files in APT phishing campaigns
- Taking Back What Is Already Yours: Router Wars Episode I , Episode II & Episode III

News

Bug bounty & Pentest news

- It's Time for OAuth 2.1
- ATT&CK with Sub-Techniques — What You Need to Know
- Shopify's March Bug Bounty Program stats
- Hackerone's March Bug Bounty Program stats
- Intigriti Bug Bounty Q&A #1: Isn't bug bounty only for large companies with large budgets?
- HackerOne cuts ties with mobile voting firm Voatz after it clashed with researchers
- Hackerone dark mode is now available
- Bugcrowd's Waitlisted Programs: Applying to Private Programs
- /r/netsec's Q2 2020 Information Security Hiring Thread

Reports

- Crave the Data: Statistics from 1,300 Phishing Campaigns
- Trends in Internet Exposure (by Shodan)
- Security software discovery tops latest Mitre ATT&CK threat list

Vulnerabilities

- Twitter Data Cache on Mozilla Firefox
- Pi-hole ad-blocking technology hack exposed
- Microsoft is working on mitigating an entire Windows bug class
- Remote working security: Thousands of misconfigured Atlassian instances ripe for unauthorized access
- Safari vulnerabilities created means for attackers to covertly access iPhone cameras
- Critical WordPress Plugin Bug Lets Hackers Turn Users Into Admins
- XSS vulnerability found in Mozilla's XSS-prevention library
- Patch now! Critical flaw found in OpenWrt router software

Zoom

- Dispelling Zoom Bugbears: What You Need to Know About the Latest Zoom Vulnerabilities
- Zoom simplifies privacy policy in a bid to head off security concerns
- Zoom security: Devs announce feature freeze and enhanced bug bounty program & TL;DR
- Zoom isn't Malware.
- Hackers Take Advantage of Zoom's Popularity to Push Malware
- DOJ Says Zoom-Bombing is Illegal, Could Lead to Jail Time

Breaches & Attacks

- Top Email Protections Fail in Latest COVID-19 Phishing Campaign
- Office 365 Phishing Uses CSS Tricks to Bypass Email Gateways
- Marriott Hotels hacked AGAIN: Two compromised employee logins abused to siphon off 5.2m guests' personal info
- A crypto-mining botnet has been hijacking MSSQL servers for almost two years
- Firefox gets fixes for two zero-days exploited in the wild
- Microsoft: Emotet Took Down a Network by Overheating All Computers

- Data on almost every citizen of Georgia posted on hacker forum
- Revealed: Saudis suspected of phone spying campaign in US
- A hacker has wiped, defaced more than 15,000 Elasticsearch servers
- Critical flaws in DrayTek Vigor routers patched following attacks
- Hacker hijacks YouTube accounts to broadcast Bill Gates-themed crypto Ponzi scam

Malicious apps/sites

Other news

- Houseparty app offers $1m reward to unmask entity behind hacking smear campaign
- NSO Group: Facebook tried to license our spyware to snoop on its own addicts – the same spyware it's suing us over
- The 31 Cyber Security Influencers you NEED to be following in 2020

Coronavirus

- Covid19 Tracker Apps compiled by @fs0c131y
- COVID-19 forces browser makers to continue supporting TLS 1.0
- Chinese COVID-19 disinformation campaigns commenced as early as January: Stanford
- Microsoft works with healthcare organizations to protect from popular ransomware during COVID-19 crisis: Here's what to do
- Researchers propose method to track coronavirus through smartphones while protecting privacy
- Hackers target World Health Organization in attempt to steal passwords

Non technical

- Top 12 tips every pentester should know
- Bug Bounty Hunting Tips #5 — Aim to Become World-Class in Your Niche
- How to approach a target|bug bounty tips
- Worth a read if you're ever considering reaching out to someone about mentoring

- Support Staff: Why You Should Rock The Boat
- Hacking styles: technology mastery + “evil” creativity + focussed effort = maximum result
- Training Yourself to be an Analytical Thinker
- Where does one find old web security research papers
- Working from Home? Wi-Fi Security and Tips and Tricks

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 03/27/2020 to 04/03/2020.

*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 #11 – Insecure Deeplinks, new XS-techniques and @int0x33 ‘s 365DaysOfPWN

26th March 2019

Bug Bytes #21 – Automation of the Recon Process by @armaancrockroax, Stored XSS via MIME sniffing & Building Virtual Machine Labs

4th June 2019

Bug Bytes #26 – File upload to SQLi, Google’s CTF & Data Breach 101

9th 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