Blog

Bug Bytes #64 – Hacking Captcha's, Unix-Style Testing & New Public Bounty

intigriti - 31st 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.

Click here to subscribe

This issue covers the week from 20 to 27 of March.

Intigriti news

A new public bug bounty program has been launched for Deriv.com. Check it out here: https://go.intigriti.com/deriv

Our favorite 5 hacking items

1. Article of the week

> *Solving CAPTCHA using Burp suite proxy and mitmproxy*

The first article shows a solution for testing Web apps that have a short session timeout and log you out everytime you trigger an exception, and that also require solving a captcha to log in. The captcha makes it complicated to use Burp macros, the traditional way of handling sessions.

@dinosn's method is to chain Burp with mitmproxy, another proxy that detects logouts and calls a custom script to run tesseract OCR and solve captchas.

2. Tool of the week

> *Piper & Unix-style approach to web application testing*

I haven't had the time to properly test this tool, but judging from its documentation, it offers very interesting functionality. It is a Burp extension that allows you to easily use external tools that were not designed for Burp. You can pipe requests and/or responses with Linux tools like diff, head, cut, grep...

This can be used to show each response's hash as a comment, which helps detect different responses that have the same length but a different hash. You can also apply a regex to requests and responses and add a comment if a pattern was detected. Many other uses cases are explained in the documentation that I invite you to check out.

3. Conference of the week

> *2019-12-11-Jan Masarik – Automating bug bounty + Opening ceremony, Slides, Master's thesis & Bugshop*

This is awesome work on bug bounty automation. @s14ve did a Master's thesis on this topic and presents everything he came up with: Common bugs, existing tools for automation, and his own solution. This is in the form of a conference talk, slides, the thesis report, and the tool's source code.

I've been intrigued by some of the paid/closed source tools he mentions, especially Bounty Machine. So, it is amazing to be able to play with this this free, open source, well documented alternative.

4. Tutorial of the week

> *Frida scripting guide for Java*

This is a crash course on Java for the purpose of writing Frida scripts. If you've tried using existing scripts and wondered how to modify them for you own needs, this will help you quickly understand the syntax and most of what you need to know.

5. Resources of the week

> – *Stanford CS 253 Web Security*
>
> – *Learn X in Y minutes*

The fist resource is a neat Web security course taught last quarter at Standford. It is comprehensive and up-to-date. In addition to videos, slides and external links, you'll also find asssignements and an exam!

The second resource is a cool cheatsheet/memo for most programming languages. It is helpful whether you are working with JavaScript, Bash, Python, Go, Rust or Ruby…

Other amazing things we stumbled upon this week

Videos

- @Smsecurity Talks About Oscp, Deserialization Bugs, Shodan Tips and What It Takes to Become an MVH
- Finding Your Next Bug: Blind Cross Site Scripting (XSS) & XSS Hunter
- Cross-Site Scripting (XSS) Explained
- Bounty Thursdays – VirSecCon, H1-2004, VDP Finder, Bug Bytes, Bugcrowd Community.
- Meterpreter Injection in Linux
- Hack The Planet – scshell
- How to phish for passwords and bypass 2FA

Podcasts

- Security Now 759 – TRRespass
- Risky Business #576 — Are cloud computing resources the new toilet paper?
- Hacked Off 054. Lockdown Part 1
- Cyber Security Sauna 036| From Stuxnet to WannaCry to Coinhive, The Past Decade Was All Over The Place
- Paul's Security Weekly #644 – Drobo Exploit, Docker Escape, SMBv3.11
- Paul's Security Weekly #644 – Work From Home Securely – Peter Smith, Edgewise
- Security Weekly News #21 – Zoombombing, Zero Days, & Signal Sciences
- Working from Home Pt.1: Pimp Myself, Pt.2: Pimp My Office & Pt.3 – Pimp My A/V

Webinars & Webcasts

- Matthias Wilson-OSINT around the world – researching people and companies worldwide
- SANS CyberCast – SANS@Mic -Attacking Serverless Servers: Reverse Engineering the AWS, Azure, and GCP Function Runtimes & Puma Security Serverless Prey
- Hack the Planet – Building a Home Lab
- Hacker Rights – Chloé Messdaghi

Conferences

- Black Hat Europe 2019
- NULLCON Goa 2020
- BSides SLC 2020
- BSides Doha 2020

Slides & Workshop material

- Effective Webinars: Presentation Skills for a Virtual Audience

Tutorials

Medium to advanced

- Infrastructure as Code: Setting up a web application penetration testing laboratory
- Prevent DOM-based cross-site scripting vulnerabilities with Trusted Types
- A deep dive into disable_functions bypasses and PHP exploitation
- Using the OneDrive Listener in Empire 3.1.3
- Backdooring WordPress with Phpsploit
- How Offensive Actors Use AppleScript For Attacking macOS
- Kerberoasting: AES Encryption, Protected User Group and Group MSA

Beginners corner

- Firebird Database Exploitation
- Corporate Reconnaissance
- Kerberoasting & AS_REP Roasting
- Will you stop fearing “Vim” or Not?
- Web Traffic Analysis with Wireshark

Writeups

Challenge writeups

- @insertScript’s XSS challenge & Solution
- Pentesting: Local file inclusion to remote code execution on Hackazon

Pentest writeups

- Once upon a time there was a WebSocket
- Bookstack CVE-2020–5256: RCE Through File Upload
- Pentesting a banking FTP service

Responsible(ish) disclosure writeups

- Liferay Portal JSON Web Service RCE Vulnerabilities
- Richsploit: One tool to exploit all versions of RichFaces ever released
- Imperva WAF Bypass
- Pentesting Cisco SD-WAN Part 1: Attacking vManage
- All-in-One WP Migration <=7.14 Arbitrary Backup Download
- Exploiting SSRF in RethinkDB

- Vulnerability In WPvivid Backup Plugin Can Lead To Database Leak

Bug bounty writeups

- Profile-picture name parameter with large value lead to DoS for other users and programs on the platform (HackerOne, $2,500)
- User input validation can lead to DOS (Twitter, $560)
- Getting lucky in bug bounty — shamelessly profiting off of other's work ($3,200)
- I Want that Cookie !!!
- XSS WAF & Character limitation bypass like a boss
- Self XSS to Account Takeover
- Facebook CSRF bug which lead to Instagram Partial account takeover. (Facebook, 12,500)
- Remote Image Upload Leads to RCE (Inject Malicious Code to PHP-GD Image)
- Exploiting magic links, critical bugs are one line away (Razer)
- $3,500 Bounty for SSRF (video) (Slack, $3,500)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- s3reverse: Go script that converts a list of S3 buckets addresses into the same format (that serve as input for other tools)
- InQL Scanner: Tool for speeding-up GraphQL security testing, can be used as a stand-alone script, or as a Burp Suite extension
- qsfuzz (Query String Fuzz): Go tool that allows you to build your own rules to fuzz query strings and easily identify vulnerabilities
- Zile: Extract API keys from file or url using by magic of python and regex

More tools, if you have time

- Unicollider: A fun retro lookup tool to generate Unicode collisions based on the "Hacking Github with Unicode's Dotless i" article

- Webpack Exploder: Client-side Webpack unpacking tool
- FProbe: Take a list of domains/subdomains and probe for working http/https server
- XXExploiter: Tool to help exploit XXE vulnerabilities
- AdvancedKeyHacks: API Key/Token Exploitation Made easy.
- Subra: A Web-UI for subdomain enumeration (subfinder)
- LeakLooker GUI & Introduction: Discover, browse and monitor database/source code leaks, using Binary Edge
- nullscan & Demo: A modular framework designed to chain and automate security tests
- Fuze: The easiest way to decrypt iOS applications
- CrackerJack: A Web GUI for Hashcat developed in Python that can be used for simple on-demand password cracking
- Envizon: Network visualization & vulnerability management/reporting
- yanp.sh & Introduction: Nessus CSV Parser and Extractor
- SharpML & Introduction: Password Hunting with Machine Learning in Active Directory
- IntelSpy: Perform automated network reconnaissance scans
- C2concealer & Introduction: A C2 Malleable Profile Generator for Cobalt Strike
- Ninja: Open source C2 server created for stealth red team operations
- InstaSave: Python script to download images, videos & profile pictures from Instagram

Misc. pentest & bug bounty resources

- SECrets – Offsec Pentest and Bug Bounty Notes
- Learn at home!
- WhatsMyName.app #OSINT
- Privilege Escalation on Linux Platform
- lolbas-project.github.io

Challenges

- Vulnerable code by @jobertabma

Articles

- JavaScript without parentheses using DOMMatrix
- Uncontrollable XML processing is more dangerous than you think..
- /i considered harmful
- Reverse engineering Blind's API and client side encryption
- The Resurrection of PHPUnit RCE Vulnerability
- Exploiting directory permissions on macOS

News

Bug bounty & Pentest news

- VirSecCon2020 & Discord invite : April 4
- The Many Hats Club Presents Isolation Con: April 19
- 30% off all ebooks at http://nostarch.com now through April 1st, 2020
- 2020 Pandemic SIP Hiring List
- Virtual Conference Swag
- Six years of the GitHub Security Bug Bounty program
- Bugcrowd's LevelUp 6 CFP
- Run ARM apps on the Android Emulator

Reports

- Google's Threat Analysis Group (TAG) – Identifying vulnerabilities and protecting you from phishing
- FireEye warns about the proliferation of ready-made ICS hacking tools

Vulnerabilities

- Web-based attack crashes Tesla driver interface
- Unpatched iOS Bug Blocks VPNs From Encrypting All Traffic
- Email security: Mail.ru patches critical memory disclosure flaw
- Back on the Rails: XSS flaw patched in Action View Ruby Gem
- 4G networks vulnerable to denial of service attacks, subscriber tracking
- Adobe debuts disk-cleaning tool cleverly disguised as an arbitrary file deletion bug in Creative Cloud on Windows
- Windows Defender Bug in Windows 10 Skips Files During Scans
- Microsoft Warns of Hackers Exploiting Unpatched Windows Bugs
- Kr00k exploit tool allows pen testers to probe for WiFi security vulnerability

Breaches & Attacks

- Phineas Fisher Says They Paid $10,000 Bounty to Person Who Hacked Chilean Military
- Emerging APT Mounts Mass iPhone Surveillance Campaign
- Rare BadUSB attack detected in the wild against US hospitality provider
- This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits
- TrickBot App Bypasses Non-SMS Banking 2FA
- A mysterious hacker group is eavesdropping on corporate email and FTP traffic
- Hackers Actively Exploit 0-Day in CCTV Camera Hardware
- HHS.gov Open Redirect Used by Coronavirus Phishing to Spread Malware
- Never-before-seen attackers are targeting Mideast industrial organizations

COVID-19

- How criminals profit from the COVID-19 pandemic
- Hackers Hijack Routers' DNS to Spread Malicious COVID-19 Apps
- WHO Targeted in Espionage Attempt, COVID-19 Cyberattacks Spike
- Ryuk Ransomware Keeps Targeting Hospitals During the Pandemic

Other news

- Android apps are snooping on your installed software
- Google's Chrome will give you an 'always show full URL' setting
- Mozilla Firefox Gets a HTTPS Only Mode For More Secure Browsing
- Will the coronavirus pandemic impact browser security?
- Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account
- How to prevent your Zoom meetings being Zoom-bombed (gate-crashed) by trolls

Non technical

- Threat After Death: Security Impact of EoL Devices
- Top 5 Password Managers to Keep Your Accounts Safe
- What My COVID Routine Looks Like

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 03/20/2020 to 03/27/2020.

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

YOU MIGHT ALSO LIKE

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

11th February 2020

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 #29 – Why do Penetration Testing Teams Hate You, SSL/TLS vulnerabilities & A Deep Dive into XXE Injection

30th 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