Blog

⌂ > 2020 > March > 10 > Uncategorised > Bug Bytes #61 – Facebook Account Takeover, @thedawgyg’s Darknet Diaries and Bug Bounty Millionaire @inh

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

Millionaire @inhibitor181

intigriti - 10th March 2020 - 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 28 of February to 06 of March.

Intigriti news

We stat down with hackfluencer and creator @stokfredrik and discussed his creator journey, live hacking, collaboration and his experience doing full time #bugbounty hunting. Read the full interview here:

Bug Business #2 – Hacking, traveling and vlogging with @STÖK

Our favorite 5 hacking items

1. Tools of the week

> – *FUSE* & *FUSE: Finding File Upload Bugs via Penetration Testing*
> – *Pulsar*

Pulsar is described as a Network footprint scanner platform. I didn't get to test it yet, but it looks promising. It is a wrapper around many recon tools, automates many recon features like subdomain enumeration, cloud resources discovery and basic vulnerability scanning. You can run

custom checks periodically, and results are presented in a very cool dashboard.
FUSE and its accompanying research paper are also worth checking out. It helped discover 30 file upload vulnerabilities in 23 Web apps!

2. Writeup of the week

> *Facebook OAuth Framework Vulnerability ($55,000)*

@AmolBaikar challenged himself to find a vulnerability in Facebook's "Login with Facebook" feature. And boy, did he deliver! He found a postMessage flaw that could allow anyone to steal user access tokens for vulnerable apps using Facebook's OAuth flow.
The bounty is of course impressive. But there is also the fact that this bug has been there for years (maybe up to 10!), on one of the most hardened targets.

3. Podcast of the week

> *Darknet Diaries EP 60: dawgyg*

@thedawgyg made several appearances in the media recently. But I've never heard his full story before. Who better than Darknet Diaries to recap his adventures from chat rooms, black hat days, to prison then full-time bug hunting. Brace yourself for interesting hacker tales!

4. Non technical item of the week

> *Technical Writing Courses*

Writing is a skill every one of us needs to be working on. Being able to convey ideas in a professional, concise and clear way can make all the difference in the world when you are writing blog posts or bug bounty/pentest reports. I would even argue that writing is the biggest hurdle most hackers face, especially those of us who are not native English speakers.
This course is a fantastic resource for improving technical writing skills. It is the same one Google engineers take! I am definitely going to dedicate time for this.

5. Video of the week

> *Going from a Full-Stack Developer to $1M Hacker: @inhibitor181 Talks About Recon, Hacking and More!*

Yep, another interview! This week's hacking motivation comes from @inhibitor181. @NahamSec asks him a bunch of interesting questions like how he got started, how he went from informative bugs to earning his living with full-time bug hunting, dealing with imposter syndrome, etc. Lots of fun, as always!

Other amazing things we stumbled upon this week

Videos

- OWASP insecure deserialization explained with examples
- Buying a cheap security assessment experiment ($15)
- Using components with known vulnerabilities
- OSCE – PREP and REVIEW – Offensive Security Certified EXPERT

Podcasts

- Hacking the Wi-fi of Today & Tomorrow With Mathy Vanhoef
- Layer 8 Podcast Episode 14: Dutch_OSINTGuy – Spot the Jihadi
- Security Now 756 – Kr00k
- Security Weekly News #15 – Tesla, Crypto AG, Shark Tank, COVID-19
- Application Security Weekly #98 – Ghostcat, Apache, Networks, Starliner

Webinars & Webcasts

- Mobile Application Static Analysis (Free registration required)

Conferences

- Building Secure iOS Apps (you don't have to learn it the hard way!) – iOS Conf SG 2020
- RSAC 2020 & Keynotes

Slides & Workshop material

- Entomology 101 – An introduction to studying, collecting and finding bugs…
- Offensive Python for Pentesting & Python for Pentesters Scripts
- BSidesSF 2020, especially:
  - Phishy Little Liars – Pretexts That Kill

Tutorials

Medium to advanced

- Attacking And Defending The GCPMetadata API
- EyeWitness through SOCKS proxy v4 (Cobalt Strike)
- Exploiting Hibernate Injections
- The RDP Through SSH Encyclopedia
- Computer accounts can move laterally too!
- Bypass endpoint with XLM weaponization
- 100% evasion – Write a crypter in any language to bypass AV & Xencrypt

Beginners corner

- Make Your Own Custom OSINT Bookmarklets (p2)
- Hacking the Web With Fiddler
- How to trace social media users across multiple platforms
- Intro to Macros and VBA for Script Kiddies
- Silver & Golden Tickets & Service Principal Name (SPN)

Writeups

Pentest writeups

- DNS exfiltration case study & Dora the DNS explorer

Responsible(ish) disclosure writeups

- Emoji to Zero-Day: Latin Homoglyphs in Domains and Subdomains #Web
- qdPM v9.1 Authenticated RCE Exploit #Web #FileUpload
- CVE-2020-2555: RCE Through a Deserialization Bug in Oracle's WebLogic Server #RCE #Deserialization
- Authentication bypass by supplying a regex as a session token in parse-server #Web
- Local Privilege Escalation In EA's Origin Client #Windows
- Data Tampering Issue in Spot.im Application (Write Up) #Web
- Attention to Details : Finding Hidden IDORs #Web

Bug bounty writeups

- "Bounties paid in the last 90 days" discloses the undisclosed bounty amount in program statistics (Hackerone, $500)
- Delete All Data of Any User (Nextcloud, $250)
- Got *Bounty* with Account takeover (ATO) Unicode-Case Mapping Collision !
- Account Hijack using Authorization bypass $$$$
- Arbitary File Upload too Stored XSS
- SQL Injection Via Stopping the redirection to a login page
- SOP Bypass
- SSRF on PDF generator.
- Exploiting an SSRF: Trials and Tribulations

See more writeups on The list of bug bounty writeups.

Tools

- Reports: Templating script @Rhynorater uses to generate bug bounty reports
- Cnames: Take a list of resolved subdomains and output any corresponding CNAMES en masse
- h2i: Converts a hostname (or URI) to IP address using your local resolver
- Fufluns: Easy to use APK/IPA Mobile App Inspector (experimental)
- ArchiveFuzz: Hunt down the secrets from the WebArchives for Fun and Profit
- Common Password Permutations: A script to produce a word list based on mangling a single word for password-guessing tests
- Common-substr: Go script to extract the most common substrings from an input text. Built for password cracking
- As3nt: Another Subdomain ENumeration Tool
- AutomatedHunter: Google Chrome Extension that automates testing GET parameters for LFI, RFI, SQLi and Open redirect
- PowerExfil: A collection of data exfiltration scripts for Red Team assessments
- Abaddon: Wavestone's red team operations management software

Misc. pentest & bug bounty resources

- 2019 Gravitational Security Audit Results #PentestReports
- The CORS Demos
- Web Application Hacker's Handbook Extras
- Recon Cheat Sheet
- Dorks for Google, Shodan and BinaryEdge
- Cyber Security Resources by SCSP
- Pentesting-cookbook

Articles

- RFC 8725: JSON Web Token Best Current Practices
- A Security Review of SharePoint Site Pages & TL;DR

- Serverless (in)security
- Abusing Slack for Offensive Operations
- Threat Alert: New Attack Vector Targeting Your Cloud Environment
- A Safe Excel Sheet Not So Safe

News

Bug bounty & Pentest news

- DoD VDP Annual Report 2019 (Geo-blocking used. If not accessible, use a VPN or proxy)
- Announcing PowerShell 7.0
- Dark Mode in ZAP's Weekly Release
- What's new in Burp Suite Pro/Community 2020.2
- Introducing Joinable Programs: Expanding the Pathway to Program Eligibility
- BSides Cairo: The security conference that's building information sharing from the ground up
- Support Ethical Hackers (Petition)

Reports

- DMARC email authentication: Increased adoption obscures poor enforcement problem
- Akamai 2020 State of the Internet / Security: Financial Services – Hostile Takeover Attempts
- 2020 CrowdStrike Global Threat Report
- Verizon 2020 Mobile Security Index Report

Vulnerabilities

- High severity regex bugs discovered in Parse Server
- Siri and Google Assistant hacked in new ultrasonic attack
- Android security: Google patches a dangerous flaw in these phones

- Solar panels expose home WiFi networks to password theft, remote attacks
- Zoho Fixes No-Auth RCE Zero-Day in ManageEngine Desktop Central
- Zero-Day Bug Allowed Attackers to Register Malicious Domains

Breaches & Attacks

- Next-Gen Ransomware Packs a 'Human' Punch, Microsoft Warns
- Microsoft OneNote Used To Sidestep Phishing Detection
- Hackers are actively exploiting zero-days in several WordPress plugins
- Active Scans for Apache Tomcat Ghostcat Vulnerability Detected, Patch Now

Clearview

- A not so Clearview?: Lack of authentication in API silently fixed
- @fs0c131y's analysis of the Clearview AI Android app
- Apple has blocked Clearview AI's iPhone app for violating its rules

Other news

- FuzzBench: Fuzzer Benchmarking as a Service
- Company that Apple is suing releases Android for iPhone
- Microsoft, Google Offer Free Remote Work Tools Due to Coronavirus
- Let's Encrypt scrambles to manage fallout from digital certificate system bug
- Why 'free' Wi-Fi isn't really free
- Tech support scammers hacked back by vigilante
- Have I Been S0ld? No, trusted security website HIBP off the table, will remain independent
- Chinese security firm says CIA hacked Chinese targets for the past 11 years
- Brave deemed most private browser in terms of 'phoning home'. The new Microsoft Edge and the Yandex Browser deemed the most data greedy.

Non technical

- Helpful Red Team Operation Metrics
- Meet our Security Expert: Ahmad Ashraff
- Q&A with Hacker Personality Shivam Vashisht
- A Tour Around the Bug Bounty Zoo
- How to start a personal bug bounty blog!

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 02/28/2020 to 03/06/2020.

*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 #53 – Exploiting a SSRF in WeasyPrint, The Bug That Exposed Your PayPal Password and 12 tricks for Burp Repeater

14th January 2020

Bug Bytes #60 -Bypassing AWS signing, @samwcyo’s secrets and WordPress leaks

5th March 2020

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

21st April 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