Bug Bytes #12 – IDOR on Yahoo by @JohnH4X00R, Abusing CORS & @OWASP's talk on How to Win Big

BY INTIGRITI · APRIL 2, 2019 · LAST UPDATED ON MARCH 6, 2025

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 22 to 29 of March.

Our favorite 5 hacking items

1. Tip of the week

> "Bugbounty scope expanding"

This paste presents a set of recon steps to expand your bug bounty scope. All of them are well known and documented in most articles on recon, except one which I haven't seen anywhere before:
Once you have a first list of subdomains (using scraping or bruteforce), split them up to build a new list of subdomains to test for.
For example, let's say you first found:

- test.dev.xyz123123ccc.com
- cc.prod.xyz123123ccc.com

The new subdomains to try are:

- dev.xyz123123ccc.com
- prod.xyz123123ccc.com

It's a simple idea but might allow you to find new "hidden" subdomains. It is very similar to what Altdns does, but I'm not sure splitting up subdomains like this is included in this tool.

2. Writeup of the week

> "IDOR on Yahoo ($5,000)"

Wow, $5,000 for such a simple bug! But the difficulty was thinking about this test...
@JohnH4X00R saw a GET request to
*/ws/v3/users/**fziy4wzxr41k4qwsgumu2v2qymynzat6kclqpwmc**/items*.
The part in bold was obviously encrypted and he had the feeling that it was his username. So, get this, he replaced it with his unencrypted username (/ws/v3/users/**yahoo-username**/items) and got a successful response containing his own notes.
Then, he replayed the same request and replaced his plain username with another account's username, and also got a successful response with the other account's notes.

This is a classic IDOR, but the genius of this bug was in completely bypassing encryption by replacing the encrypted string with its plain value.

3. Tool of the week

> "CommandoVM & Introduction"

Finally a Windows-based distribution for pentesters! This is the equivalent of Kali Linux for Windows users. It includes many tools (more than 140) for all kinds of tests.
This will be handy if you prefer Windows or if, for some reason, you have to use Windows for a pentest. It happened to me on one or two missions: we had to use a Windows VPN client to remotely access the client's internal network. And I didn't have the time to install all tools and prepare a proper Windows attacking environment. This VM would have been really helpful!

4. Slides of the week

> "How to win big – Several Interesting Examples of Exploiting Financial & Gambling Apps"

I would love to see the recording of this OWASP talk! But the slides by themselves are self-explanatory and provide some ideas for testing financial apps and games.
These are examples of how to abuse an app's logic flow and play with parameters to bypass or manipulate payment, always win against a slot machine, etc.

5. Tutorial of the week

> "Abusing CORS (Improper Origin Validation)"

This is an excellent tutorial if you want to learn about exploiting CORS.
Four pratical examples are given to understand what to do when access is granted to: any domain, the subdomain, the scheme, or when the "null" origin is used.
Also included are: external references, steps for exploiting each scenario, an exploitation payload, and how to set up a MiTM environment to exploit an unvalidated origin scheme.

Other amazing things we stumbled upon this week

Videos

- How to get invited to bug bounty live hack events!
- Hacker101 – iOS Quickstart
- Excel: CSV Injection
- Zero to Hero Pentesting: Episode 2 – Python 101

Podcasts

- Security Now 707: Tesla, Pwned
- Absolute AppSec Episode #52 – Serialization Vulns, Career Growth, and Hacking your Happiness with Chris Gates / @carnal0wnage
- 7MS #354: Tales of Internal Pentest Pwnage – Part 2
- 7MS #355: Mousejacking!
- The Many Hats Club Ep. 36, Scared already? You ain't heard nothing yet (with Thugcrowd)
- The Many Hats Club Ep. 37, Snow in Summer and being a Social Engineer (with Snow)
- Building a Community of Hackers with Ted Kramer
- Ep. #18, Collaborative Security with HackerOne's Marten Mickos
- Application Security Podcast: Georgia Weidman — Mobile, IoT, and Pen Testing
- Smashing Security 121: Hijacked motel rooms, ASUS PCs, and leaky apps
- Sophos Podcast Ep. 025 – Business Email Compromise and IoT surprises
- Paul's Security Weekly #599 – OceanLotus, Russia, & Google

Webinars & Webcasts

- Intel Techniques OSINT Webinar

Conferences

- 44con 2018 new videos:
  - Automating myself out of a job: A pentesters guide to left shifting security testing
  - So You Want to Red Team?
  - For the Love of Money: Finding and exploiting vulnerabilities in mobile point of sales systems

Slides only

- Black Hat Asia 2019 presentation materials, especially:
  - Make Redirection Evil Again – URL Parser Issues in OAuth
  - Who Left Open the Cookie Jar?
  - Automated REST API Endpoint Identification for Security Testing at Scale: How Machine Learning Accelerates Security Testing
  - Preloading Insecurity In Your Electron
  - DevSecOps: What, Why and How

    - MS Office in Wonderland
    - CQTools: The New Ultimate Hacking Toolkit
- Betrayed by the Android UI
- AWS Security Assessment
- Weaponized WiFi Attack Tool & Demo
- Getting root with benign app store apps
- A Post-Exploitation_tale in real life / Fud WMI for lateral movement (PoC)
- Riding the lightning: iLO4&5 BMC security wrap-up

Tutorials

Medium to advanced

- Leveraging Exposed WADL XML in Burp Suite
- Did You Order a SQL Injection?
- Weaponising AngularJS Sandbox Bypasses
- How to audit AWS IAM and resource policies
- Running your Own Passive DNS Service
- Open WiFi Credential Harvesting – IoT Edition
- Metasploit Basics for Hackers, Part 24: The New Evasion Modules in Metasploit 5
- Playing with TLS-Attacker
- Bypassing AV (Windows Defender) ... Cat vs. Mouse
- Meterpreter Payload Delivery using DNS AXFR PoC
- MacOS Red Teaming 202: Profiles
- Setting malicious Outlook configurations through EWS & EWSToolkit

Beginners corner

- How to Find Subdomains (And Why You Should)
- The Case of the Missing API Docs
- Using Wireshark: Identifying Hosts and Users
- Cracking Microsoft Excel Documents using John The Ripper
- Understanding Android OS Architecture

- Setting up an Android Pentesting Environment
- Drozer! The Game changer tool for android pentesting
- Recon-NG How-To I, Part II & Part III
- Network Basics for Hackers: Simple Network Management Protocol (SNMP) Theory, Reconnaissance and Exploitation
- PowerShell for Pentesters, Part 5: Remoting With PowerShell

Writeups

Challenge writeups

- Automating Discovery and Exploiting DOM (Client) XSS Vulnerabilities using Sboxr — Part 1, Part 2 & Part 3
- $50 million CTF writeups
  - by @reefbr
  - by @ajxchapman & Script developed to solve it
  - by @abdilahrf
  - by Dominic
- Zixem SQLi challenges & Solutions
- Write-up: OWASP Juice Shop Challenges (v2.19.1)

Responsible disclosure writeups

- Cisco RV320 Command Injection: RCE in Cisco routers patched by blocking requests with the *curl* user-agent... because the company that disclosed it gave a PoC using curl!
- Magento 2.2.0 <= 2.3.0 Unauthenticated SQLi
- Zero-Day Stored XSS in Social Warfare
- Disclosure of Origin IP of The Exploits Trading Platform 0day.today
- Icmp-reachable
- Remote command injection through an endpoint security product
- (0-days) ENTTEC Lighting Controllers Vulnerabilities
- R7-2018-43: Username Enumeration in Okta SSO Del Auth through Response Timing

Bug bounty writeups

- DoS on Paypal ($3,200)
- DoS on Twitter ($1,120)

- Stored XSS on Dota 2 (video game client) ($750)
- Stored XSS on Google
- Link poisoning on TTS Bug Bounty ($150)
- Privacy violation on Semmle ($100)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- HTTP Request Translator: Translate curl commands or HTTP/Json requests to Python Requests code or JSON
- Find Security Bugs: The SpotBugs plugin for security audits of Java web applications and Android applications. (Also work with Groovy and Scala projects
- SSRFTest: Tool by @daeken to greatly simplify exploitation of SSRF bugs, including automatic AWS credential pulling where possible + Some open issues if you want to contribute to this open source project
- Shodan Monitor: Setup network alerts for specific networks or IPs & get a notification when something new shows up

More tools, if you have time

- Black Hat Asia 2019 – Arsenal, including:
  - Mallet: A framework for creating proxies for arbitrary protocols, along similar lines to the familiar intercepting web proxies, just more generic
  - Real time scrapper (RTS): A tool developed to scrap all pasties,github,reddit..etc in real time to identify occurrence of search terms configured & send email notifications
  - MQTT-PWN: Framework for IoT pentesting (specifically attacking/exploiting the MQTT protocol
  - Nmp-scan: An extensible, heuristic-based vulnerability scanning tool for installed npm packages (to detect malicious code
- Shodan client: Node.js/JavaScript Library for accessing the new Shodan API
- Shodmon: Monitor shodan listed servers based on the filter you provided & get email notifications when something new pops up. Useful if you want to monitor more resources than what Shodan Monitor (mentioned above) allows
- Instantbox: Get a clean, ready-to-go Linux box in seconds
- WordPress (<4.9.10, <5.0.4, <5.1.1) CSRF PoCs
- Gofuzz: Aims to reproduce wfuzz's functionality and versatility. Based on gobuster
- Linux Exploit Suggester 2: Next-Generation Linux Kernel Exploit Suggester

- Dnssecchef: A DNS/DNSSEC interception proxy for penetration testers and security researchers (based on DNSChef
- Knary: A simple HTTP(S) and DNS Canary bot with Slack/Discord/MS Teams & Pushover support
- Automated-pentest: Minimal docker container of Parrot OS for running an automated scan & pentest report
- Get-AdDecodedPassword.psm1: a basic PowerShell script for decoding common passwords stored in Active Directory properties. It's based on information found on Domain Goodness – How I Learned to LOVE AD Explorer
- BloodHound-Tools: Miscellaneous tools for BloodHound

Misc. pentest & bug bounty resources

- So You Want to Red Team?
- XXE
- Recon cheatsheet
- Bug-Hunting-Tips/Tricks
- APIsecurity.io Issue 24: Unprotected APIs in implants, storing API secrets
- Bounty Hunters Discord server by Friendly @Skeletorkeys
- Pwnd Discord server by r3dx00
- ICS and IoT Shodan Dork collection
- Vulncode-DB: A database for security vulnerabilities & corresponding source code
- OSCP Reviews Collection
- GSoC2019 Ideas: Ideas for students interested in improving open source OWASP (security-related) projects, as part of the Google Summer of Code 2019
- So you wanna be a pentester? Penetration testing resource guide

Challenges

- Mobisec challs: CTF-like challenges related to mobile security
- FliteCTF: Source code of Hacker0x01 $50M CTF
- @Blaklis_'s 1ns0mn1h4ck phuck3 and shophp challenges
- Packetwars 2019 challenges

Articles

- How Bad Can It Git? Characterizing Secret Leakage in Public GitHub Repositories
- Introducing the Metasploit Development Diaries
- Learn the flow of making tokens! #bugbounty
- Android Runtime Restrictions Bypass blog post, Report
- Paranoid Habits. Security Tips
- Finding the silver lining in getting your teeth kicked in
- How to Purge Google and Start Over – Part 1 & Part 2
- Owning the Network with BadUSB & Presentation material
- Embrace Rabbit Holes

News

Vulnerabilities

- Zero-Day TP-Link SR20 Router Vulnerability Disclosed by Google Dev: TP-Link SR20 router 0-day allows attackers to execute commands as root, no auth required
- Hundreds of millions of UC Browser users for Android are threatened: UC Browser, downloaded by over 500,000,000 Google Play users, is vulnerable to RCE via MiTM. Apps can download auxiliary software modules, bypassing Google Play servers

Breaches

- Toyota announces second security breach in the last five weeks
- A family tracking app was leaking real-time location data: This one is Family Locator, not to confuse with last week's spying app also leaking data which was Mobiispy
- Update now! WordPress hackers target Easy WP SMTP plugin
- FEMA exposes personal data of 2.3m disaster victims
- Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers: Supply-chain attack dubbed "Operation ShadowHammer". Only 600 MAC addresses were targetted. Also Check if your device was targetted

Other news

- Don't change your birth year to 2007 to Twitter or you'll be locked out
- Firefox brings Lockbox password manager to Android's autofill

- Spyware vendor defends hacking journalists, continues to embolden abusive governments
- Nmap used to discover IP camera in AirBnB rental – The Atlantic
- Preinstalled Android apps are harvesting and sharing your data
- NSA-Inspired Vulnerability Found in Huawei Laptops

Non technical

- How to prepare for a security engineer interview
- The Hunter Games
- Never Post A Picture Of Your Boarding Pass On Social Media
- Tips for a Successful Phishing Engagement
- 3 Stories Of Imposter Syndrome And How To Overcome It
- Casino Screwup Royale: A tale of “ethical hacking” gone awry
- How to fully leverage your pentest

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 03/22/2019 to 03/29/2019.

Curated by Pentester Land & Sponsored by Intigriti

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com