Bug Bytes #46 – Steal customer data via CORS Misconfiguration, Dnsexpire.py and #BadBugBountyPickupLines

BY INTIGRITI · NOVEMBER 28, 2019 · LAST UPDATED ON MARCH 6, 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.

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.

This issue covers the week from 15 to 22 of November.

Our favorite 5 hacking items

1. Tip of the week

> "Rewarded with $xxxx for an issue which could have allowed me an access to stag & prod server. Sub-domain scan -> dir fuzz -> found a publicly exposed git -> extracted all committers email -> found one email in pw dump -> used it to log into git instance -> got creds for servers"

I've never thought of this, but it is a great idea for exploiting exposed .git folders: In addition to extracting source code, you can also extract committer emails and search for them on password dumps. I'd also search for them on Google, Github, etc. Good idea for recon/OSINT!

2. Writeup of the week

> "CORS misconfiguration allows to steal customer data (on LocalTapiola) **($2,100)**"

The most interesting part of this writeup is the Proof of Concept. It shows how to exploit a CORS misconfiguration to exfiltrate user data. The code can help if you're working on a CORS PoC and want to show real impact.

3. Tool of the week

> "Dnsexpire.py"

This is yet another awesome script by @gwendallecoguic. It returns expiration date of hosts, which is useful for detecting subdomain takeovers.

A good idea would be to run with a cron job and add Slack/email alerts to get notified as soon as a domain expires.

4. Non technical item of the week

> "#BadBugBountyPickupLines"

If you like bug bounty and jokes, this Twitter hashtag is a treat. Some are so bad, they're good...

- I don't care if you aren't clear verified but you get a private invite to my heart
- Are you a kudos only program? Because I feel like I'm not getting much out of this
- Are you a crit? Because I'm gonna brag about you on Twitter
- Call me vulnerable because you make my Heartbleed

5. Tutorial of the week

> "Analyzing DNS TXT Records to Fingerprint Online Service Providers"

This tutorial shows how to automatically analyze and extract information from DNS TXT records used to verify domain ownership.

Tokens used within DNS TXT records allow for fingerprinting the service provider associated with the domain (e.g. Microsoft, Google, Citrix, Atlassian...). This is useful for pentesters as it is a different way for identifying technologies used.

Other amazing things we stumbled upon this week

Videos

- I Wrote crtndstry (A Tool For Finding Root Subdomains) Live and Explained My Thought Process & crtndstry
- Live Recon Stream #2
- Ethical Hacking Job Interview
- Bug Bounty Tips: Horizontal Domain Enumeration Recon
- Bug Bounty Push Notifications – Simple Bash/Python Script
- The Bug Hunting Methodology – A Ready to Use Formula
- Open Source Intelligence OSINT on Domains [1]
- Detect Malicious domains or IPs with OSINT [2]
- Common Linux Privilege Escalation: Writable Root PATH

Podcasts

- Security Now 741 – TPM-FAIL
- Risky Business #563 — Phineas Phisher returns
- Hackable? 35 – Porch Piracy
- List of Careers in Cyber Security | DailyCyber 203

- Hack Naked News #242 – Effective Phishing Campaigns
- Paul's Security Weekly #627 – Humans vs. Machines

Webinars & Webcasts

- 1 Phish, 2 Phish , Red Phish, Blue Phish
- Cloud Security with Shira Shamban
- Building Secure React Applications

Conferences

- The world of Site Isolation and compromised renderer & Slides
- A comparative analysis of Open Source Web Application vulnerability scanners (Rana Khalil)
- Real life hacks for Windows and Office... and how to stop them (Microsoft Ignite)
- Louisville Infosec 2019 Videos
- x33fcon Europe 2019
- Defcon 27 Villages videos: Recon, Wireless & Packet Hacking

Slides only

- Offensive Ansible for Red teams & Git repo
- GraphQL Applications Security Testing Automatization
- POC2019, especially:
  - Whole New Perspective In SSRF: Make it great againd and ignore most of SSRF defense solutions that we know
  - Bug Hunting in Synology NAS
- Automated Social Engineering for the Antisocial Engineer

Tutorials

Medium to advanced

- Kubernetes Pentest Methodology Part 3
- How to create polyglot HTML/JS/WebAssembly module
- Modern Wireless Tradecraft Pt IV
- Practical Guide to Passing Kerberos Tickets From Linux
- Jupyter Notebooks for BloodHound Analytics and Alternative Visualizations !

- ATT&CK T1501: Understanding systemd service persistence

Beginners corner

- Using Bulk Extractor for Quick OSINT Wins
- Privilege escalation attacks, their impact on enterprises and mitigation
- Security Risks of CORS
- Hacking SAML
- Hacking the Same-Origin Policy
- Nmap Scripts (NSE): The Key To Enhance Your Network Scans
- Docker Privilege Escalation
- Multi Ways to Crack Windows 10 Password
- How to Dump NTLM Hashes & Crack Windows Passwords

Writeups

Challenge writeups

- ASIS CTF — ShareL Walkthrough #Mobile

Pentest writeups

- Prince of the Honeycomb

Responsible(ish) disclosure writeups

- Uncommon SQL Database Alert – Informix SQL Injection #Web
- Arbitrary Command execution in Privacy Disclaimer page of a very popular organization #Web
- Getting Malicious Office Documents to Fire with Protected View Enabled #Windows
- Linksys velop vulneraibility series #Router #Web
- Thanksgiving Treat: Easy-as-Pie Windows 7 Secure Desktop Escalation of Privilege #PrivilegeEscalation #Windows
- Technical Advisory: Multiple Vulnerabilities in Alcatel Flip 2 #Mobile

Bug bounty writeups

- Logic flaw on Starbucks
- DoS on GitLab ($1,000)
- XSS via DOM Clobbering in Google

- Cracking reCAPTCHA, Turbo Intruder style
- Logic/authorization flaw on Facebook (Instagram)
- Authentication bypass via LDAP injection
- XSS + 20 chars blind XSS payloads ($1,054)
- IDORs & bypass ($3,650)
- Authentication bypass on Facebook

See more writeups on The list of bug bounty writeups.

Tools

- memento.py: Find endpoints in archived versions of robots.txt
- Cloud-cidr: Get AWS,Azure,Google Cloud IP CIDRs
- CORS Scanner
- Subdomain_recon.py & Introduction: A subdomain reconnaissance scanner
- Bug Menace: This project contains the packer build (targeting AWS) for a Bug Bounty enumeration and attack server. It's basically just ubuntu + some osint tools
- Boucan: Dashboard/API + DNS/HTTP Servers to identify Out of Band Resolution in Payloads
- Lazyrecon_docker: Containerized version of my fork of Nahamsec's Lazyrecon
- Javafuzz: Coverage guided fuzz testing for java
- Pax: CLI tool for PKCS7 padding oracle attacks
- Flan Scan & Introduction: Cloudflare's Lightweight Network Vulnerability Scanner. Wrapper around Nmap and vulners
- Spraykatz: A tool able to retrieve credentials on Windows machines and large Active Directory environments
- nullinux: Internal penetration testing tool for Linux that can be used to enumerate OS information, domain information, shares, directories, and users through SMB
- Jackdaw: Collects all information in your domain, stores it in an SQL database & shows you nice graphs on how your domain objects interact with each-other an how a potential attacker may exploit these interactions #ActiveDirectory

Misc. pentest & bug bounty resources

- Vulnsearch
- Security Guide
- Legal Documentation for Physical Security Testing

- Predator: A prototype web application designed to demonstrate anti-crawling, anti-automation & bot detection techniques. It can be used a honeypot, anti-crawling system or a false positive test bed for vulnerability scanners.
- 1_Resources for conferences: Resources for starting a conference
- C2 Matrix & Introduction: Find out which C2 fits your what-the-newly-released-checkra1n-jailbreak-means-for-for-idevice-security
- Essential PowerShell Resources
- Good Practices for Security of IoT – Secure Software Development Lifecycle & ENISA good practices for security of Smart Cars
- Free Remote Internship Certification Programme Empowering Women in Cyber Security

Challenges

- Insecure Deserialization, PDF and lab

Articles

- [DNS Takeover] Potentially Takeover for all SubDomains That uses Campaign Monitor Newsletters Services
- Abusing Web Filters Misconfiguration for Reconnaissance
- Privacy and OSINT lessons from the IronMarch Leak
- Introducing security.plist: “tl;dr It’s like security.txt but for iOS applications.”
- Cracking passwords to prevent credential stuffing
- Reasonably Secure Electron
- Jumping the Rabbit Hole – Walking Around Web App Obfuscation with Request Interception
- Playing With Old Hacks
- Docker Patched the Most Severe Copy Vulnerability to Date With CVE-2019-14271
- Local Security Authority – Keeping Secrets Safe
- Building up a basic Physical Red Team toolkit and skillset.

News

Bug bounty & Pentest news

- My most reported issue of 2019 is SSRF by far and has made me over $500,000 USD
- AWS bolsters security to defend against SSRF attacks
- Hacker 5-O

- The vuln industry just got another player: the media
- Updates to the Mozilla Web Security Bounty Program
- @NahamSec AMA
- Intigriti challenge & Winner
- Huawei's bug bounty payment table
- Google will now pay up to $1.5 million for very specific Android exploits

Reports

- Privacy and Security Issues Found in Popular Shopping Apps
- 5G creates 'SIM-jacking on steroids' threat
- Quarterly Threat Report: Q3 2019
- SophosLabs Threat Report: A look at developments in cybersecurity for 2020

Vulnerabilities

- Update WhatsApp now: MP4 video bug exposes your messages
- Security Vulnerabilities in Android Firmware
- CVE-2019-12409: Default Configuration in Apache Solr Could Lead to Remote Code Execution
- Google reCAPTCHA outfoxed by Turbo Intruder
- Google fixes XSS bug in Gmail's dynamic email feature
- How Attackers Could Hijack Your Android Camera to Spy on You
- Critical Flaws in VNC Threaten Industrial Environments
- Popular apps on Google Play linked to old remote code execution bugs

Breaches & Attacks

- Phineas Fisher Offers $100,000 Bounty to Hack Banks and Oil Companies & HackBack – A DIY Guide
- DePriMon downloader uses novel ways to infect your PC with ColoredLambert malware
- 'More than a keylogger' – Phoenix wows small-time cybercrooks and raises security concerns
- Card Skimmer Group Replaces Checkout Page to Steal Payment Info
- New Banking Trojan Infects Victims via McDonald's Malvertising
- Baffled by bogus charges on your Amazon account? It may be the work of a crook's phantom gadget
- Thousands of hacked Disney+ accounts are already for sale on hacking forums

- A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems
- Official Monero website is hacked to deliver currency-stealing malware

Other news

- Google plans to take Android back to 'mainline' Linux kernel
- Adobe announces end of support for Acrobat, Reader 2015
- Antivirus vendors and non-profits join to form 'Coalition Against Stalkerware'
- BitCracker: Password-cracking software designed to break Windows' BitLocker
- Police confiscate surveillance van loaded with hacking tools
- Internet world despairs as non-profit .org sold for $$$$ to private equity firm, price caps axed
- What the newly released Checkra1n jailbreak means for iDevice security
- Officials warn about the dangers of using public USB charging stations

Non technical

- Team Pentesting – The Unspoken Reality of Career Ethical Hacking
- Bug bounty management, a great example: Zomato
- Top 10 Cybersecurity Trends to Look Out For in 2020

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 11/15/2019 to 11/22/2019.

Disclaimer:The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.Curated by Pentester Land & Sponsored by Intigriti