BugBytes #25 – To scan or not to scan, GOTCHA and live mentoring by @zseano

BY INTIGRITI · JULY 2, 2019 · LAST UPDATED ON JULY 17, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bugbytes-25-to-scan-or-not-to-scan-gotcha-and-live-mentoring-by-zseano

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series are curated by Mariem, better known as PentesterLand. Every week, she keeps us updated with a comprehensive list of all write-ups, tools, tutorials and resources we should not have missed.

This issue covers the week from 21 to 28 of June.

Our favorite 5 hacking items

1. Discussion of the week

> "Do you use vulnerability scanner on bug bounty program? How is the result?"

This is an interesting discussion for beginner bug hunters on why you shouldn't use scanners in bug bounty.
Vulnerability scanners are of low added value because many other people (including internal pentesters) have probably already run them. So it's improbable that they'll allow you to find anything new of real value. This, combined with the risk of causing Denial of Service if many bug hunters use scanners on the same target, is why scanners are generally not allowed.
The following reasons apply to pentesting too: the risk of causing an email flood to a client email address (happened to me once!), and the risk of deleting resources by using spidering on authenticated pages. These risks are good to know whether you're a bug hunter or pentester. It helps decide which tools to run or not and avoid causing service disruptions.
Also, I find *cym13*'s stance on Burp interesting. There really is no 'one size fits all'!

2. Writeup of the week

> "GOTCHA: Taking phishing to a whole new level **($100 + $1000 bonus for creativity)**"

This is a writeup of a Clickjacking attack found during a live hacking event.
What tipped off @securinti was a button that triggered an AJAX request to display the user's password. The requests didn't use X-FRAME-OPTIONS headers so he was able to display the user's password within an iframe. Classic clickjacking, but the problem is that he couldn't read the password because of CORS. His genious idea to bypass CORS and get the user's password was to create an iframe that looked like a captcha form. He also scrambled the password's letters to make it look like a captcha (so the user wouldn't recognize that it was their own password). When they would enter the captcha, he would get it, re-order the letter and get their password.
If you want to know more about this kind of attacks, I recommend the paper Tell Me About Yourself: The Malicious CAPTCHA Attack.

3. Tutorial of the week

> "Burp Suite tutorial: IDOR vulnerability automation using Autorize and AutoRepeater (bug bounty)"

This video tutorial is a must if you're serious about Web app security and don't already use Autorize and Autorepeater. These are two Burp Suite extensions that can, among other things, be used to automatically detect IDOR.
This kind of advanced Burp usage can seem overwhelming or confusing if you're starting out. So it's nice to be walked through the whole process. Thank you @Regala_ and @stokfredrik!

4. Video of the week

> "Hands on Hacking with zseano & Bugbountynotes session carrying on"

I lo-o-ove this live mentoring concept by @zseano. It is a great opportunity to spend a few hours hacking on a fake website created for the occasion, while being live with an online mentor, and also practice writing bug bounty reports. It's fun whether you're a beginner or a seasoned bug hunter.
I had network connection issues right when the live started. That was so annoying! But the next session is on July 21st.

5. Tool of the week

> "Taborator"

Taborator is a Burp extension that shows the Collaborator client in a tab (instead of a new Burp window by default).
So it's more practical if you play with Collaborator often. It's worthing checking out and is easy to install (via the BApp Store) and use.

Other amazing things we stumbled upon this week

Videos

- How to quit vim ..fast
- Haxcellent – Breaking out of Security
- Don't Fall For Manipulated Google Search Results
- Bugcrowd Researcher Eric AKA Todayisnew
- HackerOne Hacker Interviews: Cosmin (@inhibitor181)
- The Complete Linux for Ethical Hackers Course for 2019
- Teaching My Wife to Hack...Maybe
- My Entrepreneurial Journey – Episode 3: My First Sales Meeting
- Paste-Tastic! – Post Google CTF 2019 Stream
- Penetration Testing Tools – How I use Nmap – OSCP Prep

- Penetration Testing Tools – How I use Nikto for Vulnerability Scanning – OSCP Prep
- Penetration Testing – How I use Gobuster for Web Discovery – OSCP Prep

Podcasts

- SwigCast, Episode 2: ENCRYPTION
- Security Now 720 – Bug Bounty Business
- Darknet diaries Ep 41: Just Visiting
- 7MS #368: Tales of Pentest Fail
- 7MS #369: Cracking Hashes with NPK
- The Nullcon podcast Episode 6: Joe Grand – Prototype This!, L0pht, Hardware Hacking, #BadgeLife & DEFCON 27 Badge
- Smashing security 134: Sextortion, silicone face masks, and a DDoS doofus
- Paul's Security Weekly #610 – Security News
- Application Security Weekly #66 – Don't Ignore APIs
- Hack Naked News #224 – LokiBot, Anonymous, & Oracle
- Business Security Weekly #133 – Leadership Articles

Webinars & Webcasts

- Webcast: How to attack when LLMNR, mDNS, and WPAD attacks fail – eavesarp (Tool Overview)

Conferences

- Securing your mobile app with the OWASP Mobile Security Testing Guide
- BSides Cleveland 2019 Videos, especially:
  - Hack for Show, Report for Dough
  - Eval Villain: Simplifying DOM XSS and JS Reversing
- OSINT for Proactive Defense
- Layer 8 Conference 2019, especially:
  - Tinker Secor – Transitive Trust: Pivoting and Escalating Privileges in a Social Engineering Scenario

Slides only

- How to Frustrate a Penetration Tester
- Bluetooth – It's all pairing things of devices

Tutorials

Medium to advanced

- Better API Penetration Testing with Postman – Part 4
- Exploiting PHP Phar Deserialization Vulnerabilities – Part 2
- The Problem of String Concatenation and Format String Vulnerabilities
- Linux for Pentester: Taskset Privilege Escalation
- Old-school (rev|bind)-shellz with gawk
- Capturing NTLMv2 hashes by crafting a Microsoft Access database
- MacShell

Beginners corner

- Dial cURL for Content
- Finding and Testing MisConfigured S3 Buckets.
- Art of Unrestricted File Upload Exploitation
- Mounting VHD files in Kali Linux through remote share(smb).

Writeups

Responsible disclosure writeups

- dotCMS 5.1.5: Exploiting H2 SQL injection to RCE
- EA Games Vulnerability
- Outlook for Android XSS
- The not so ultra lock
- F5 Networks Endpoint Inspector – Browser-to-RCE?

Bug bounty writeups

- RCE on SEMrush ($10,000)
- Privilege escalation on HackerOne ($2,500)
- SSRF on Omise ($700)
- Improper Access Control on Twitter & PoC ($560)
- DOM XSS on Upserve ($2,500)
- Authorization flaw on Google

- Password reset flaw ($1,200)
- Account takeover via open redirect
- CORS misconfiguration & CSRF

Tools

If you don't have time

- Vim-airline: Plugin to customize Vim like @tomnomnom & @stokfredrik
- Jenkins-Pillage & Introduction: A tool for automatically gathering sensitive information from exposed Jenkins servers
- ASN Lookup API
- GraphQLmap: A scripting engine to interact with a graphql endpoint for pentesting purposes
- EsPReSSO (Extension for Processing and Recognition of Single Sign-On Protocols): An extension for BurpSuite that highlights SSO messages in Burp's proxy window & Probing for XML Encryption Weaknesses in SAML with EsPReSSO
- SpiderFoot HX: New OSINT online tool, not to confuse with the open source Spiderfoot version

More tools, if you have time

- Minesweeper: A Burpsuite plugin (BApp) to aid in the detection of scripts being loaded from over 23000 malicious cryptocurrency mining domains (cryptojacking)
- Boo-Gen!: A Python script that takes a saved HTTP request from a file and then uses that to generate an HTTP Boofuzz script. It has been updated to handle POST requests & fuzz the post data
- See-SURF: Python based scanner to find potential SSRF parameters
- BaseCrack: Decoder Tool For Base Encoding Schemes (Base16, Base32, Base36...)
- Shania: Scan secrets from Continuous Integration Build Logs (CI / Circle CI / Gitlab CI)
- Linux-smart-enumeration: Linux enumeration tool for pentesting and CTFs with verbosity levels
- Enumerate IAM permissions: Enumerate the permissions associated with AWS credential set
- Distill.io: Browser extension that allows you to monitor website changes
- Not Your Average Web Crawler: Execute your exploit against every request in scope
- Bashter: Web Crawler, Scanner, and Analyzer Framework (Shell-Script based)
- Cazador_unr: Simple Hacking tools for windows
- ADRecon: A tool which gathers information about the Active Directory and generates a report which can provide a holistic picture of the current state of the target AD environment

Misc. pentest & bug bounty resources

- Pwnlists: Custom more realistic wordlists with variety of use cases
- XSS Payload without Anything
- Ten Useful Burp Suite Pro Extensions for Web Application Testing
- APIsecurity.io Issue 37: Vulnerabilities with WebLogic and OnePlus, the Black Hat API workshop, and OAuth in action
- New OWASP cheatsheet about SSRF prevention
- Hashes.org – Leaks (919): 919 publicly leaked databases
- Kurukshetra: A framework for teaching secure coding by means of interactive problem solving
- Security Crawl Maze: A comprehensive testbed for web security crawlers. It contains pages representing many ways in which one can link resources from a valid HTML document
- VulnerableContainers.org: Scans the 1000 most popular containers in @Docker hub for open CVEs using trivy & scores their risk using @KennaSecurity
- Red Team & Physical Entry Gear
- Toggle proxies in macOS Terminal

Challenges

- CloudGoat 2.0 & CloudGoat 2: The New & Improved "Vulnerable by Design" AWS Deployment Tool
- YesWeHack ticket challenge: Challenge over but the server will keep running for a bit
- XSS challenge by @RakeshMane10
- @glennzw's old school @sensepost inspired CTF

Articles

- What I have learn in my first month of Hacking and Bug Bounty?
- Why is Your Website a Target? The SEO Value of a Website
- One-Two Punch: Using AppSec to Up Your Pentests and Phishing Gigs
- On Stranger Tides: API and Container Security Part I & Part 2
- Getting 2FA Right in 2019
- With Multi-Factored Authentication, Does Login Sequence Matter?
- You (probably) don't need ReCAPTCHA
- Attacking RSA keys
- Using Whitelisting to Remediate an RCE Vulnerability (CVE-2019-2729) in Oracle WebLogic

- OSCP Blog: Second Week Thoughts (06/26/2019)
- MFSocket: A Chinese surveillance tool
- The Lock Picking Hobbyist

News

Bug bounty news

- Burp Suite Pro/Community 2.1 STABLE released. We are now officially out of beta! & Why you should upgrade
- Burp Suite Community Edition users can now enjoy the new dark theme.
- You can now compare two snapshots on the Wayback Machine (beta) and see changes. The feature is called "Changes"
- Ask @tomnomnom a question
- Call For Papers for @Hacker0x01's Security@ event in San Francisco (October 15)
- New on Web Security Academy: CSRF course & labs

Reports

- 'Velocity does not have to come at the cost of security'
- Hack and slash: Cloud-based video games model opens up fresh security risks

Vulnerabilities

- Security firms demonstrate subdomain hijack exploit vs. EA/Origin
- New Microsoft Excel Attack Vector Surfaces
- Most UAE enterprises are vulnerable to cyber-attacks
- SEMrush Plugs Remote Code Execution Bug in Its SaaS Platform

Breaches & Attacks

- State-sponsored hacking campaign targets global telcos
- Google said a supply chain attack by one of its vendors resulted in malware being pre-installed on many budget Android devices, but it didn't name the vendor
- Social Engineering Forum Hacked, Data Shared on Leak Sites
- Your server remote login isn't root:password, right? Cool. You can keep your data. Oh sh... your IoT gear, though?
- How Two Firefox Zero Days Led to Two macOS Backdoors
- Firefox zero-day was used in attack against Coinbase employees, not its users

- Data Warehouse: How a Vendor for Half the Fortune 100 Exposed a Terabyte of Backups

Other news

- Virustotal becomes part of Google Cloud
- Government agencies still send sensitive files via hackable .zips
- Raspberry PI 4 Released – Complete specs and pricing

Non technical

- How to Write a Better Vulnerability Report

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 06/21/2019 to 06/28/2019.

Subscribe to the newsletter here!

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