Bug Bytes #21 – Automation of the recon process by @armaancrockroax, stored XSS via MIME sniffing & building virtual machine labs

BY INTIGRITI · JUNE 4, 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/bug-bytes-21-automation-of-the-recon-process-by-armaancrockroax-stored-xss-via-mime-sniffing-building-virtual-machine-labs

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.

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 31 of May to 07 of June.

Our favorite 5 hacking items

1. Tool of the week

Keye

Keye is a really useful recon tool. It's the first one I've come across that allows hackers to easily monitor changes in URLs.
It's written in Python with SQLite3 integrated. You give it a list of urls, and run it periodically (using Cron for example). It then requests the urls and detects changes based on the responses' Content-Length. You can also receive Slack notifications when changes are detected.

2. Writeup of the week

Stored XSS via MIME sniffing

This is a great writeup on file upload vulnerabities. The author breaks down how he found a stored XSS through file upload.
I love the way he explains what he did step by step, from detecting which extensions are allowed and which filters are in place, to bypassing them and executing an XSS. A worthy read!

3. Slides of the week

Building Virtual Machine Labs

This is an excellent resource if you want to build a pentest lab.
It's 453 slides detailing everything: which OS/VMs you need to install (including Kali, Metasploitable 2, Firewall with pfSense, SIEM with Splunk...), how to do it, how to automate OS updates, intro to

virtualization, which software you need on each OS (Linux, OS X & Windows) and much more.
I wish I had this when I had just started out. Such a time saver!

4. Conference of the week

> Automating the Recon Process by armaan pathan null Ahmedabad Meet 26 May 2019 Monthly Meet & Slides

Armaan (@armaancrockroax) got [$21,000] (https://twitter.com/armaancrockroax/status/1134664934518808576) from bug bounty last month. So when he talks about automation, I'm all ears!
In this talk, he shows how he:

- combines multiple tools to enumerate subdomains
- resolves and sorts subdomains
- finds Jenkins with Shodan
- gets Slack notifications for all scans
- found a Jenkins RCE in Verizon using this same testing methodology

This is a short, sweet and very practical talk. Code snippets are also provided (check out the slides).

5. Video of the week

> Writing a Pentest Report & Sample report

This is an awesome resource for junior penetration testers (and students who want to become professional pentesters). It provides a pentest report template and goes through each page and detail to explain the reasoning behind it.
Of course, this is not meant to be copied and used as as... Every company uses custom report templates for a reason: they tend to elvolve mission after mission, following client feedback and any new ideas that you have.
But this template is an excellent basis. It contains all the important sections and information you want to convey to clients.

6. Intigriti News

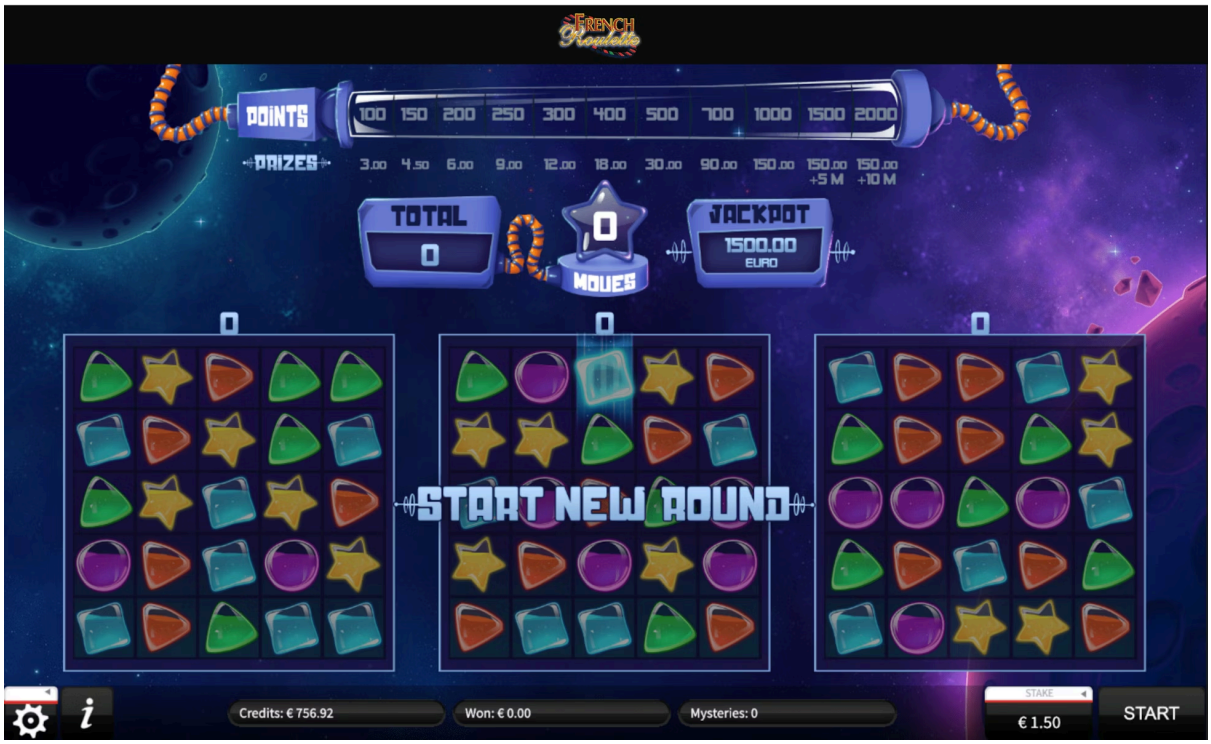
6.1 El Punto Group – a New Responsible Disclosure by Kinepolis

Kinepolis recently acquired the Spanish cinema group "El Punt" with the "Full" cinema complex in Barcelona and "El Punt Ribera" in Valencia. Their websites are often the first point of contact with their costumers. The customers can fetch an overview of currently playing movies and buy their movie tickets. El Punto Group's ticket sales rely heavily on Kinepolis's online platform which is why they allow you to research these website and to report any vulnerabilities you may have found.

Start hunting here!

6.2 Napoleon Games is challenging you!

Napoleon Games is the Belgian leading gambling website where you can play several types of games: casino games, live casino games, sports betting etc. Their biggest concerns are leaks or in game manipulations! That's why they need you! Can you increase your chances of winning?



French Roulette is one of the many games you can try to manipulate. REMEMBER STAY ETHICAL: First register yourself as an intigriti researcher, become vetted and request your test account before you try to hack the game!

Start hunting here!

Disclaimer: Stay ethical! Before you start hacking, register yourself to the platform, become vetted and request your Napoleon Games test account.

Other amazing things we stumbled upon this week

Videos

- HackerOne Hacker Interviews: Cecillia (@p0rkbun)
- HackerOne Hacker Interviews: André (@0xacb)
- My Entrepreneurial Journey – Episode 1: Quitting My 6 Figure Cybersecurity Job to Start a Business
- Short explanation of Tabnabbing
- Zero to Hero: Week 11 – File Transfers, Pivoting, and Reporting Writing

Podcasts

- Getting into Infosec: Hossam Mohamed – Young Hacker to "Not A Security Researcher"
- 7MS #365: Interview with Ryan Manship and Dave Dobrotka – Part 3
- Darknet Diaries Ep 39: 3 Alarm Lamp Scooter
- Security Now 716 – RDP – Really Do Patch
- Risky Business #543 — NYTimes blames NSA for Baltimore hacks, Assange faces espionage charges
- Security In Five Episode 503 – GitHub Releases Several Security Tools To Help Developers
- Security In Five Episode 501 – IoT Strikes Again – 90% Of IoT Devices Are Unencrypted
- Paul's Security Weekly #606 – BlueKeep Vulnerability, Robert Graham
- Secure Digital Life #112 – Game Consoles
- Hack Naked News #220 – Joomla, BlueKeep, & Chinese OS

Webinars & Webcasts

- Webcast: Attack Tactics 6! Return of the Blue Team

Conferences

- CrikeyCon 6 (2019), especially:
  - Imposter Syndrome & InfoSec
  - Breaking in with DNS rebinding
  - Stealing Chrome cookies without a password
- DIY Pen-Testing for Your Kubernetes Cluster – Liz Rice, Aqua Security

Slides only

- How does or affect our S€curity? A bughunter and offensive perspective on
- Security for Modern Webapps: New Web Platform Security Features to Protect your application
- OWASP Top 10
- Bad USB Attacks & Notes

Tutorials

Medium to advanced

- Advance SQL-Injection bypass WAF
- Exploiting Common Serverless Security Flaws in AWS
- Hacking AWS
- Frame Injection Attacks
- myBB – Add Administrator via XSS
- Stealing Certificates with Apostille
- Dynamic Reverse Tunnels in SSH
- Securing your red team kit with Uncomplicated Firewall
- Data Exfiltration using PowerShell Empire

Beginners corner

- DevTools – My Favorite Tips and Tricks
- Fix Burp Suite SSL "Secure Connection Failed"
- Ethical Hacking 101: Information Gathering
- Enumerating a digital footprint & fransRecon: Script to automate (sub)domain enumeration. Uses horizontal enumeration (WHOIS & reverse WHOIS lookups), then vertical enumeration (Sublist3r) of each domain found
- Intro to SSRF
- My first attempt at XSS

Writeups

Challenge writeups

- How our community hacked our own XSS challenge

Pentest writeups

- SSRF Vulnerability due to Sentry misconfiguration
- Exploiting UN-attended Web Servers To Get Domain Admin – Red Teaming
- When all else fails – find a 0-day

Responsible disclosure writeups

- How I hacked into a college's website again!
- Information disclosure in T-Mobile allowed anyone to obtain a customers name and account number
- Vulnerable deserialization in dnSpy and Resource.NET
- 1-click RCE with Skype Web Plugin and Qt apps
- OS Command Injection Vulnerability Patched In WP Database Backup Plugin

Bug bounty writeups

- Information disclosure on Tron Foundation ($1,000)
- Weak encryption on Automattic ($250)
- Logic flaw on HackerOne ($500)
- RCE on Nextcloud
- Information disclosure on Automattic ($100)
- IDOR on Microsoft ($500)
- Authentication bypass on Avira
- Weak encryption on Facebook ($12,500)
- CSRF / Account takeover ($750)
- Parameter pollution
- Lack of authentication
- Source code disclosure
- Authorization flaw
- CORS misconfiguration
- Bruteforce / Authentication flaw

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- YesWeBurp: Burp extension to access all the programs details from YesWeHack directly inside of Burp Suite
- ImmuniWeb's free website and GDPR compliance test
- Build Scour: Python tool which scours popular CI tools build logs
- CILeek: Find token leaks in Travis-CI logs
- Metabigor: Command line Search Engines without any API key
- Privatecollaborator: A script for installing private Burp Collaborator with free Let's Encrypt SSL-certificate

More tools, if you have time

- ASNLookup Web Application: Web version of ASNLookup
- Brutality: A fuzzer for any GET entries
- Boxer: A fast directory bruteforce tool written in Python with concurrency
- Dexcalibur: Dynamic binary instrumentation tool designed for Android application and powered by Frida. It desassemble dex, analyze, can generate hook, stored intercepted data automatically and do new things from it..
- Pga4decrypt: A tool for recovering server credentials from a pgadmin4 database
- Kubolt: Utility for scanning public kubernetes clusters
- WaybackSqliScanner & Introduction
- Iptablescript.sh: Bash script to quickly edit iptables. Useful for King of the Hill style CTFs
- Rdpscan: Rdpscan for CVE-2019-0708 bluekeep vuln & Almost One Million Vulnerable to BlueKeep Vuln (CVE-2019-0708)
- Tickey: Tool to extract Kerberos tickets from Linux kernel keys
- Gt-generator: Use BloodHound data to generate golden ticket commands without having to do all of those SID lookups!

Misc. pentest & bug bounty resources

- Nearly-9000-XSS-Payloads.txt & How-to
- XSS Fuzzing
- Keywords.txt: Keywords to search for in Git repos or info disclosures
- EdOverflow's newsletter – Wordlists
- [tl;dr sec] Research from Portswigger, fuzzing papers, and CORS tricks
- awesome-security-hardening

- Command Injection Bypass Cheatsheet
- F5 BIG-IP Security Cheatsheet & Load Balancer with RCE, Hacking F5 – SecurityFest 2019
- Useful OSCP Notes & Commands
- Email Permutator
- Endoflife.date
- Grumpy Hackers

Challenges

- WASM Challenge & Coding a WebAssembly CTF Challenge
- VulnCases: Vulnerable C/C++ code snippets for exploit dev
- SQLi challenge source code and solution

Articles

- Exploring An Application's Past & Future
- Provoking browser quirks with behavioural fuzzing
- SameSite Cookies by Default in Chrome 76 and Above
- I can see your local web servers
- When Moving To the Cloud, Don't Leave Basic Security Behind
- Disclosing TOR users' real IP address through 301 HTTP Redirect Cache Poisoning
- My HackTheBox CTF Methodology – From fresh box to root!
- How WhatsApp was Hacked by Exploiting a Buffer Overflow Security Flaw
- CVE-2019-0708: A Comprehensive Analysis of a Remote Desktop Services Vulnerability
- Avoiding the DoS: How BlueKeep Scanners Work

News

Bug bounty / Pentest news

- New BlackArch Linux ISOs and OVA (2019.06.01) released with 2200 tools included!
- New on Web Security Academy: XXE & 9 labs
- New BlackArch Linux ISOs and OVA (2019.06.01) released with 2200 tools included!

Reports

- Rapid7 Quarterly Threat Report: 2019 Q1

Vulnerabilities

- Close to a million Windows PCs at risk from BlueKeep vulnerability
- Unpatched Docker bug allows read-write access to host OS
- OnePlus 7 Pro Fingerprint Reader Hacked In Matter Of Minutes
- Zero-day in EA's Origin exposes gamers to yet more RCE pwnage
- DuckDuckGo Android Browser Vulnerable to URL Spoofing Attacks

Breaches & Attacks

- First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records
- A wave of malware add-ons hit the Mozilla Firefox Extensions Store
- In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc
- Hackers actively exploit WordPress plugin flaw to send visitors to bad sites
- Snapchat Employees Abused Data Access to Spy on Users

Other news

- APIsecurity.io Issue 33: First American leaks 885 million mortgage records
- Under-the-hood changes to Chrome will break ad blockers – unless you're a paying customer
- Windows 10 to warn about insecure WiFi networks using WEP or TKIP – Support for WEP and TKIP to be removed in future Windows 10 releases.
- Second Apple 'hacky hack hack' teen avoids jail
- Google study shows even basic authentication is pretty good at thwarting commonplace hijacking attacks
- Data leaks getting worse despite GDPR, study indicates
- 5G IoT: Literally a Matter of Life or Death
- Foreign spies may be hiding in your VPN, warns DHS
- Germany mulls giving end-to-end chat app encryption das boot: Law requiring decrypted plain-text is in the works

Non technical

- Cloud security, open S3 buckets and where do we stand now: Interview with Vincent Yiu
- Interview with Sahil Ahamad – Application Security Researcher
- What a US presidential candidate can teach us about hackers

- A lesson in journalism vs. cybersecurity
- InfoSec Fundamentals
- 10 Ground Rules for Red Teams

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 05/17/2019 to 05/24/2019.

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