Bug Bytes #33 – SSRF going wild, intigriti's new challenge & JSON CSRF

BY INTIGRITI · AUGUST 27, 2019 · LAST UPDATED ON JULY 31, 2025

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 16 to 23 of August.

Intigriti news

1. WooRank premium features

Premium features are now in-scope for the Woorank project. Check out the project description for more info on how to enable them!

2. Solve the intigriti challenge & win

We announced a new XSS challenge on our Twitter profile. The challenge is simple: find a way to steal a victim's cookies and win a Burp Pro License. It's not too late to participate, as the challenge runs until Friday! Only three people have solved it so far — so your chances of getting a free Burp License are higher than usual!

We have tweeted out four tips so far:

- This is a client-side attack that works in Chrome ONLY.
- When we say "no self XSS", we do NOT say "no obscure user interaction"
- Mark my words and my URL.
- Go local.

Our favorite 5 hacking items

1. Article of the week

> "SSRF in the Wild"

This article is an analysis of publicly disclosed SSRF writeups.
@vickieli7 curated 76 unique reports, then read each one and categorized them following criteria like: vulnerable feature, presence of SSRF protection, criticality/impact, type of fix implemented...
She gives interesting statistics on each category. For example, 27 of the 76 bugs affected an image/file upload feature.
I love this idea of studying a vulnerability class by producing statistics based on specific criteria. This can

be scaled to include other bug types and more writeups.
It's also a great idea to look for bypasses each time you read a writeup. This is what allowed @vickieli7 to find one bug while learning about SSRF!

2. Writeup of the week

> "Information disclosure & SQL injection on U.S. Dept Of Defense"

The chain of bugs described in this writeup are simple but critical. File/directory bruteforce revealed a *Trace.axd* file that redirected to a login page.
Trace.axd is ASP.NET's trace feature that helps developers debug the app.
Tests credentials worked and gave @arinerron access to a lot of sensitive information through that debug page: tokens, passwords, new endpoints... One of them was vulnerable to SQL injection.
An interesting idea to keep in mind if you find a SSRF on an ASP.NET app, is to look for *Trace.axd* to escalate it.

3. Tool of the week

> "Burp Scope Monitor Extension"

This is such a useful Burp extension! It's easy to install/use, and allows you to manage a list of URLs marked as "analyzed" or "not analyzed".
You may already be using lists of endpoints during tests to keep up with large scopes, but now you can do it directly from Burp. It allows you to highlight requests, retrieve URLs from other Burp tabs, send requests you want to analyze to Burp repeater, import/export state files...
The only downside I see is that the import/export function makes my Burp freeze. I need more RAM but the other functionalities work fine.

4. Tutorial of the week

> "JSON CSRF To FormData Attack"

This tutorial explains why JSON CSRF is harder to exploit than CSRF: You can't send JSON Content-Type using an HTML form. You need AJAX which can be blocked by CORS.
So to exploit JSON CSRF, you either need to bypass CORS or one of the two techniques presented here: Change the request's Content-Type from *Content-Type: application/json* to *Content-Type: text/plain* or to *Content-Type: application/x-www-form-urlencoded*.
If one of these is accepted by the server, they allow you to exploit the CSRF by creating an HTML form, bypassing the previous limitation.

5. Non technical item of the week

> "Is It Time to Let Employees Work from Anywhere?"

I would have loved to have this study years ago when I was negotiating (rather begging for) remote work with my previous employers. Home office is one of the reasons that pushed me towards self-employment.
If you're in a similar situation, the results could help you convince management. It basically says that "If an employee has a strong track record and can do most of their work independently, research shows that

allowing them to work from anywhere would benefit both the individual and organization".
Also, the study distinguishes between Work From Anywhere (WFA, meaning geographic flexibility) and Work from Home (WFH). The first gives more flexibility and people who transitioned from WFH to WFA had their productivity increase by 4.4%!

Other amazing things we stumbled upon this week

Videos

- Hackers Couch Live @ Hackerone 702 (Night 1/3) STÖK and NAHAMSEC
- Hackers Couch Live @ Hackerone 702 (Night 2/3) : Bug hunting together ft FRANS ROSÉN & AVLIDIENBRUNN
- Live Bug Bounty Recon Session on Yahoo (Part 4 – 8/4/2019)
- Burning Out to Turning It Out: A Powerful Hacker Journey
- Web App Testing: Episode 2 – Enumeration, XSS, and UI Bypassing
- DEF CON 27: Insecurity of Things

Podcasts

- Security Now 728 – The KNOB is Broken
- Risky Business #552 — Guest host Alex Stamos on all the week's security news
- Darknet Diaries EP 45: XBox Underground (Part 1)
- HNN #230
- ASW #73 – Bugs, Breaches, and More!
- BSW #140 – Leadership Articles
- News Wrap: Linux Utility Backdoor, Steam Zero Day Disclosure Drama

Webinars & Webcasts

- Kerberos & Attacks 101 (Free registration required)

Conferences

- Chaos Communication Camp 2019, especially:
  - What you see is not what you get – when homographs attack
  - Hacking Containers and Kubernetes

Slides only

- The Cookie Monster in Your Browsers
- Hash collision exploitation (updated)

Tutorials

Medium to advanced

- Gaining persistent access to Burp Suite's Collaborator sessions – a step-by-step guide
- Automating pentests with WebDriver
- Burp Suite Pro real-life tips & tricks: Authorization testing
- The new Facebook Graph Search – part 1 & Part 2
- Getting Shell with XAMLX Files
- Obtain D.C. Hashes within Azure in 4 Easy Steps

Beginners corner

- XSS via HTTP Headers
- What Is Session Hijacking: Your Quick Guide to Session Hijacking Attacks
- Bypassing Certificate Pinning
- How Secure Are Encryption, Hashing, Encoding and Obfuscation?
- [Metasploit] Upgrading Normal Command Shell to Meterpreter Shell
- Linux For Pentester: socat Privilege Escalation

Writeups

Pentest writeups

- XSLT Injection Basics – Saxon
- Securing the Cloud: A Story of Research, Discovery, and Disclosure
- Kerberos Resource-Based Constrained Delegation: When an Image Change Leads to a Privilege Escalation

Responsible(ish) disclosure writeups

- Vulnerabilities in Ampache (<=3.9.1) #Web #CodeReview
- Breaking Into Your Company's Internal Network – SuiteCRM 7.11.4 #Web #CodeReview

- When Checking the Box Results in Two Zero Days and Root (CVE-2019-14257 and CVE-2019-14258) #Web
- The Many Possibilities of CVE-2019-8646 #iOS #Deserialization
- FusionPBX v4.4.8 authenticated Remote Code Execution (CVE-2019-15029) #RCE #CodeReview
- CVE-2019-15107: RCE in Webmin #RCE #CodeReview
- PrivEsc in Lenovo Solution Centre, 10 minutes later #PrivilegeEscalation #Windows

Bug bounty writeups

- ReDoS on GitLab ($1,000)
- Payment tampering on Zomato ($750)
- Password reset flaw ($1,000)
- Privilege escalation on ok.ru ($500)
- Cookie Based XSS to Reflected XSS
- Content leak on 1Password, Keeper & Dashlane
- 2FA bypass on Facebook ($500)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Datajack Proxy & Introduction: Proxy for intercepting TLS in Native Applications
- Exploit for CVE 2019-11510 (Pulse Secure SSL VPN Arbitrary File Disclosure), Condensed explanation of how the Pulse Secure directory traversal works, Exploitation chain & Over 14,500 Pulse Secure VPN endpoints vulnerable to CVE-2019-11510

More tools, if you have time

- AuthCov: Web app authorization coverage scanning
- B-XSSRF: Toolkit to detect and keep track on Blind XSS, XXE & SSRF
- Shadow Workers: XSS & SW exploitation framework
- ZigDiggity & Introducing ZigDiggity, a ZigBee testing framework created by Bishop Fox.
- Truegaze: Static analysis tool for Android/iOS apps focusing on security issues outside the source code

- NebulousAD & Introduction: Automated credential auditor for Active Directory. Checks AD user credentials against 2.5B unique passwords found in data breaches. Also k-anonymity is supposed to be implementeed
- Dow Jones Hammer & Documentation: A multi-account cloud security tool for AWS. It identifies misconfigurations & insecure data exposures within most popular AWS resources, across all regions & accounts
- wmiServSessEnum & Introduction: .net tool that uses WMI queries to enumerate active sessions & accounts configured to run services on remote systems
- QRGen & Introduction: Simple script for generating Malformed QRCodes
- GTFO: Search gtfobins and lolbas files from your terminal

Misc. pentest & bug bounty resources

- Paste Site Search
- PentestSec Discord channel
- Privilege Escalation Cheatsheet (Vulnhub): List of Vulnhub machines for each privilege escalation technique
- APIsecurity.io Issue 45: Hacked dating apps and smartlocks, "Egregious 11" cloud security issues
- ADSTG v2.0 – Guidance

Articles

- Ask a Pen Tester: Q&A with Rapid7 Penetration Tester Aaron Herndon
- Bug Hunting Methodology from an Average Bug Hunter
- Exploiting A/B Testing for Fun and Profit (Part 1) & Part 2
- How Secure is your Android Keystore Authentication ?
- Fingerprinting WAF Rules with Timing Based Side Channel Attacks
- Phishing with EmbeddedHTML Videos in Microsoft Word
- Attacks on Applications of K-Anonymity — For the Rest of Us

News

Bug bounty & Pentest news

- Facebook to pay researchers to hunt down Instagram apps that abuse user data
- iFrame clickjacking countermeasures appear in Chrome source code. And it only took *checks calendar* three years

- Microsoft pushes out Chromium-based Edge with new bug bounty program: Up to $30,000 for eligible vulnerabilities in Microsoft Edge based on Chromium
- The new meme for when you find an awesome bug & Long version

Vulnerabilities

- VLC Media Player Allows Desktop Takeover Via Malicious Video Files
- Moscow's blockchain voting system cracked a month before election
- American Voting Systems Were Left Online (video)
- One million Luscious porn site accounts compromised
- Lenovo High-Severity Bug Found in Pre-Installed Software
- Second Steam Zero-Day Impacts Over 96 Million Windows Users
- 'Kaspersky-in-the-Middle' bugs triaged

Breaches & Attacks

- First of its kind spyware sneaks into Google Play
- No REST for the wicked: Ruby gem hacked to siphon passwords, secrets from web devs: "Developer account cracked due to credential reuse, source tampered with and released to hundreds of programmers"
- Backdoor found in Webmin, a popular web-based utility for managing Unix servers
- Serious Security: Phishing in the cloud – the freemium way
- Hackers Want $2.5 Million Ransom for Texas Ransomware Attacks

Other news

- Alleged "snake oil" crypto company sues over boos at Black Hat [Updated]
- Humans may have been listening to you via your Xbox
- Researchers explained that carrying out attacks against the most used default Tor bridges would cost threat actors $17,000 per month.
- AWS has begun to proactively scan public-facing servers and notify customers if firewall access seem improperly permissive
- Facebook's New Privacy Tool Comes With A Crucial Caveat: "Even after you turn off the ability for Facebook to collect your data to be used for ads, the social network will carry on collecting the information"
- Get alerts about your credentials being in a data breach using Firefox Monitor (based on "Have I Been Pwned")

- Hacker Releases First Public Jailbreak for Up-to-Date iPhones in Years

Non technical

- Tribe of Hackers: Red Team Edition
- The Difference Between Red, Blue, and Purple Teams (Updated to add Yellow, Orange, & Green Teams)
- Tech Interview Handbook

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 08/16/2019 to 08/23/2019.

Curated by Pentester Land & Sponsored by Intigriti

Disclaimer:
The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com