Bug Bytes #53 – Exploiting a SSRF in WeasyPrint, The Bug That Exposed Your PayPal Password and 12 tricks for Burp Repeater

BY INTIGRITI · JANUARY 14, 2020 · LAST UPDATED ON MARCH 6, 2025

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

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.

This issue covers the week from 03 to 10 of January.

Our favorite 5 hacking items

1. Videos of the week

> "– Exploiting a Server Side Request Forgery (SSRF) in WeasyPrint for Bug Bounty & HackerOne's $50M CTF
> – [[BURP] 12 tricks for Burp Repeater]"

The first video is about an interesting SSRF that was tricky to exploit. @NahamSec explains why it is important to identify the backend, and how to do it (by requesting an image or iframe).
In this case, the backend was WeasyPrint. Since it is open source, analyzing its code helped find a tag which was not blacklisted and could be used to read internal and external resources.
The second video taught me 3 new helpful tips on Burp Repeater:

- How to save the entire history of a tab – Useful for reporting
- You can replay urls by copying them from browser into repeater – Saves times
- Repeater has an option to "URL-encode as you type" – Encodes values automatically without having to do it manually with Burp Decoder

2. Writeups of the week

> "– The Bug That Exposed Your PayPal Password ($15,300)
> – Hunting Good Bugs with only html"

The first writeup is about an impressive XSSI found on Paypal's login form. It goes beyond simple detection and proof of concept, to show how this can be exploited to take over user accounts.
This is also a good opportunity to revisit this old but excellent introduction to XSSI: Cross-Site Script Inclusion: A Fameless but Widespread Web Vulnerability Class.

The second writeup shows how multiple bugs (such as open redirest and SSRF) can be chained to significanlty increase the impact.

3. Tutorials of the week

> "– Bypass SameSite Cookies Default to Lax and get CSRF & CSRF challenge by @RenwaX23
> – Unicode Normalization Vulnerabilities & the Special K Polyglot"

SameSite cookies are not yet the end of CSRF. There is a special feature called LAX+POST which basically disables SameSite for 2 minutes. In other words, there is a window of 2 minutes where users are vulnerable to POST CSRF despite the SameSite attribute being used.
@RenwaX23 explains some ways in which this behavior can be exploited in real-life attacks. He also provides a challenge if you want to play with this.
The second tutorial is excellent if you want to start leveraging Unicode for bypassing XSS and SQL injection filters.

4. Non technical item of the week

> "The need for note making and an organized methodology in Bug Bounty Hunting"

@sharathsanketh makes the case for maintaining a written organized methodology. He gives concrete examples of taking notes on CSRF and "Forgot password" bugs.

And most importantly, he explains an essential idea for beginners: No one will give you a ready-to-use complete methodology. You have to read, do deep searches (especially on Twitter) and take notes of anything you learn so that it is not just passive reading.

Nowadays the question is not "Where will I find information?", but rather "How can I exploit iteffectively?"."

5. Tools of the week

> "– Burp Share Requests
> – ReconNess"

Burp Share Requests is a Burp Suite extension that allows you to share requests with another Burp user. Useful for collaboration or sharing information with triagers!
To use it, righ click on any request you want to share, click on "create link" and share the link generated. When the other person opens the link (with the same extension installed), it imports the request into their Burp.
ReconNess seems fantastic for bug bounty. It's an open source Web app that helps organize recon and is easily extensible. You can add targets, notes, and agents to run any commands (for assets enumeration, port scanning, directory bruteforce, etc). Using custom-built Bashs cripts achieves the same results but this GUI tool can make the process much more pleasant.

Videos

- Exploiting a Server Side Request Forgery (SSRF) in WeasyPrint for Bug Bounty & HackerOne's $50M CTF

- Finding Your First Bug: Cross Site Scripting (XSS)
- Live Recon Stream #3: Tesla
- Mark Litchfield (@BugBountyHQ) shares his experience and talks about becoming a $1M hacker
- How to setup a BIND9 DNS server for OOB Exfiltration! (step by step)
- How I Made $100,000 in a Month
- How to get Started with Bug Hunting – An Unconventional Story by Katie Paxton-Fear (@InsiderPhD)
- Getting started with TCPDump – John Strand
- Getting started with Wireshark – John Strand
- Best InfoSec Tools of 2019!
- iOS 13.3 / 13.2 / 13.0 CheckRa1n JAILBREAK How To Make CheckRa1n Bootable Drive (Ra1nUSB) On WINDOWS

Podcasts

- Security Now 748 – Our Malware Lexicon
- Darknet Diaries EP 56: Jordan
- 7MS #395: Tales of Internal Pentest Pwnage – Part 12
- Detections – Dead OST Society
- Business Security Weekly #157 – Leadership Articles
- Paul's Security Weekly #634
- Application Security Weekly #90
- Security Weekly News #1
- Risky Business #567 — ToTok, Iran and big-game ransomware galore

Conferences

- BSides Belfast 2019
- HITB+ CyberWeek Main Conf Tracks, CommSec Track & Keynotes & highlight talks, especially:
  - Practical Approaches For Testing And Breaking JWT Auth – Mazin Ahmed
  - The IPV6 Attack Must Be Understood
  - Wireless Ethical Hacking And Defenses
  - IoT Pentesting The Right Way

- Unveiling the Underground World of Anti-Cheats
- GrrCON 2019, especially;
  - Beginner's Guide to Mobile Applications Penetration Testing
  - Network exploitation of IoT ecosystems
  - Using Next Generation Fuzzing Tools: Fixing Bugs and Writing Memory Corruption Exploits & Slides
  - Understanding how public places introduce additional risks to business travelers & how the tools used by hackers continue to evolve
  - Hashes; Smothered and Scattered: Modern Password Cracking as a Methodology

Tutorials

Medium to advanced

- Using JS2PDFInjector to check risks of PDF files with embedded JavaScript & JS2PDFInjector
- Fuzzing JavaScript WebAssembly APIs using Dharma/Domato (on Chrome/V8)
- Phishing Sites with Netlify
- A tale of a lesser known NFS privesc
- Persistence – AppInit DLLs
- Persistence – Change Default File Association
- Covenant Tasks 101

Beginners corner

- Exploiting XML External Entity (XXE) Injections
- Hacking Encryption With Signing Oracles
- Ethical Hacking Lessons — Building Free Active Directory Lab in Azure
- Mass Exploitation, Hunting While Sleeping
- What is Clickjacking (UI Redressing) attack?
- Bash Shell —Other Useful commands
- OSINT — Certificate Transparency Lists
- SSH Pentesting Guide
- SSH Client Auditing & Hardening
- Windows for Pentester: BITSAdmin

- Windows 10 Hardening
- Pokémon GO OSINT Techniques: Part I

Writeups

Challenge writeups

- Reverse engineering and modifying an Android game (.apk) — CTF
- Reversing Web Assembly (WASM)
- Blind SQL Injection without an “in”
- Advent Challenge Complete Resources

Pentest writeups

- The Cypher Injection Saga & Cypher Injection Scanner
- Breaking PHP’s mt_rand() with 2 values and no bruteforce

Responsible(ish) disclosure writeups

- Tik or Tok? Is TikTok secure enough? #Web #Android
- Cable Haunt & Reddit discussion #DNSRebinding #BufferOverflow
- PandoraFMS v7.0NG authenticated Remote Code Execution (CVE-2019-20224) #CodeReview #Web
- The Curious Case of WebCrypto Diffie-Hellman on Firefox – Small Subgroups Key Recovery Attack on DH #Crypto #Web
- Postauth RCE in latest NagiosXI #Web
- Drupal 8 File Upload Vulnerability #Web

Bug bounty writeups

- Saying Goodbye to my Favorite 5 Minute P1
- Potential unprivileged Stored XSS through wp_targeted_link_rel ($650) #CodeReview
- Update: Want to take over the Java ecosystem? All you need is a MITM! ($2,300)
- How I found a Privilege Escalation Bug in a private Ecommerce?
- xmlrpc.php FILE IS enable it will used for Bruteforce attack and Denial of Service(DoS) ($200)

Tools

If you don’t have time

- Filter Options Method & Introduction
- hakrevdns: Small, fast tool for performing reverse DNS lookups en masse
- hakcheckurl: Takes a list of URLs and returns their HTTP response codes

More tools, if you have time

- Electric Scan: Electron based screenshot scanner
- XposedOrNot: A tool is to search an aggregated repository of xposed passwords comprising of ~850 million real time passwords
- Bucket Flaws (S3 Bucket Mass Scanner): A Simple Lightweight Script to Check for Common S3 Bucket Misconfigurations
- GIXY: Nginx configuration static analyzer
- DNSolver: Recon tool that parses a list of domains and returns a list of unique IP adresses
- VULNREPO & Online version: A free project designed to speed up the creation of IT Security vulnerability reports
- Frida Injector for Android: Inject frida agents on local processes through an Android app
- Npq: Install packages safely with npm or yarn by auditing them as part of your install process
- AD Fly Tool: Active directory query tool using LDAP Protocol. Helps red teamer / penetration testers to validate users credentials, retrieve information about AD users, AD groups...
- RFCpwn: An enumeration and exploitation toolkit using RFC calls to SAP
- AUTO_RECON.bat: Automated host recon, persistence and exfiltration
- SharpStat: C# utility that uses WMI to run “cmd.exe /c netstat -n”, save the output to a file, then use SMB to read and delete the file remotely
- Apache2 mod_backdoor: A backdoor module for Apache2
- Cobalt_aliases: Tired of typing execute-assembly everytime you use Cobalt Strike? Clone this

Misc. pentest & bug bounty resources

- Open Reference Architecture for Security and Privacy
- EICAR test QR
- Nmap compatible list of all vulnerable software from National Vulnerability Database
- Awesome Hacking
- Semi-automation of dorking
- STARTING OSINT RESEARCH

- OSINT Cheat-Sheet
- Introduction to Information Security
- Kali Linux – An Ethical Hacker's Cookbook, 2nd Edition ($44.99 Value) FREE for a Limited Time (Free until January 21)
- Regex cookbook — Top 10 Most wanted regex

Challenges

- Modern Windows Attacks and Defense Lab
- Can you find out how to exploit this code?
- VulnNodeApp: A vulnerable application made using node.js, express server and ejs template engine

Articles

- Deep Dive in to Citrix ADC Remote Code Execution, CVE-2019-19781
- Multiple Exploits for CVE-2019-19781 (Citrix ADC/Netscaler) released overnight – prepare for mass exploitation
- Two-factor authentication security testing and possible bypasses
- Guest blog: streaak – my recon techniques from 2019
- Down the Rabbıt Hole....
- 7 of the Most Memorable CVEs of 2019
- Tricky Phish Angles for Persistence, Not Passwords
- Building Your Own Web Application Firewall as a Service And Forgetting about False Positives
- The Anatomy of Website Malware Part 2: Credit Card Stealers
- Leveraging Disk Imaging Tools to Deliver RATs

News

Bug bounty & Pentest news

- Significant Changes to Accessing and Using GeoLite2 Databases
- Announcing the Microsoft Identity Research Project Grant (grant awards of up to $75,000 USD)
- Windows 7 support will end on January 14, 2020
- DNS information monitoring with Shodan
- Pwn2Own Returns to Vancouver for 2020

Reports

- Academic research finds five US telcos vulnerable to SIM swapping attacks
- Microsoft: RDP brute-force attacks last 2-3 days on average
- Half of the websites using WebAssembly use it for malicious purposes

Vulnerabilities

- Citrix ADC CVE-2019-19781 Exploits Released, Fix Now!
- Researchers demonstrate practical break of the SHA-1 hash function
- Web security holes left TikTok users wide open to pwnage
- Hundreds of millions of cable modems are vulnerable to new Cable Haunt vulnerability
- Google Fixes Critical Android RCE Flaw
- Browser zero day: Update your Firefox right now!
- Critical security vulnerability in PrestaShop modules

Breaches & Attacks

- IT exec sets up fake biz, uses it to bill his bosses $6m for phantom gear, gets caught by Microsoft Word metadata
- 'Maze' ransomware threatens data exposure unless $6m ransom paid
- Travelex ransomware attack: Pulse Secure VPN flaw implicated in security incident
- VPN warning: REvil ransomware targets unpatched Pulse Secure VPN servers
- Malicious photo app exploits Android kernel vulnerability
- UK man sentenced to prison for hacking and spying on victims through their webcams Or why you should use a webcam cover!
- Landry's restaurant chain disclose POS malware incident
- New Magecart skimmers practice steganography, data transfer via WebSocket
- New Iranian data wiper malware hits Bapco, Bahrain's national oil company
- Google details its three-year fight against the Bread (Joker) malware operation

Malicious apps/sites

Other news

- On the brink of cyber warfare: Attacks feared over US-Iranian escalation

- Iran courted US security expert for years, seeking industrial hacking training
- Microsoft Phishing Scam Exploits Iran Cyberattack Scare
- The Iran Cyber Warfare Threat: Everything You Need To Know
- Some coalescing thoughts on Iran's cyber capability
- Interpol hails 78% drop in cryptojacking infections across Southeast Asia
- Dixons Carphone hit with £500,000 fine after data breach affecting 14 million people
- 4 Ring Employees Fired For Spying on Customers
- Why is a 22GB database containing 56 million US folks' personal details sitting on the open internet using a Chinese IP address? Seriously, why?
- U.S. Funds Program With Free Android Phones For The Poor — But With Permanent Chinese Malware
- India's answer to GDPR: Data protection legislation set to pass this year
- The Biggest Tech Fails of 2019
- Google Ditches Patch-Time Bug Disclosure in Favor of 90-Day Policy

Non technical

- It's All Fun and Games
- Getting real
- What Happens When You Don't Sleep for a Day?
- Who do you serve? Who do you protect?

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 01/03/2020 to 01/10/2020.

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***