Bug Bytes #22 – Disabling distracting Firefox traffic from Burp, A 2019 Workflow for Subdomain Enumeration by @0xpatrik & DirectoryImporter

BY INTIGRITI · JUNE 11, 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.

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. Tip of the week

> "Foxyproxy.json for disabling distracting Firefox traffic from Burp"

If you're a regular Firefox + Burp user, you probably have noticed that Firefox generates some traffic that shows up in Burp, like requests to http://detectportal.firefox.com/ or update checks.
This JSON file is @liamosaur's Foxyproxy configuration file that allows him to disables this unwanted traffic.

2. Writeup of the week

> "Ability to reset password for account on Upserve ($3,500)"

This isn't a fully disclosed writeup, but the little information shared is mind-boggling.
Ilya/exadmin was able to steal other users' password reset link by entering an array of email addresses instead of one email address.
The request's body looked like this: *{"email_address":["admin@breadcrumb.com","attacker@evil.com"]}*.
It would be interesting to see what the backend code looks like, but even without knowing this is an interesting idea to try on other programs.

3. Article of the week

> "Subdomain Enumeration: 2019 Workflow"

@0xpatrik shares his new subdomain enumeration wokflow.
I know, there are already dozens (hundreds?) of subdomain enumeration articles out there, and @0xpatrik himself already talked about this same topic... but here he shows how he improved his methodology for more efficiency and better results. Interested yet?

4. Resource of the week

> "Guide 001 | Getting Started in Bug Bounty Hunting.."

This is a great guide for anyone interested in Web app security or bug bounty. It has 3 sections that correspond to the following learning phases:

- Basics of Networks, Programming & Automation
- Learning about Vulnerabilities, Resource for practicing, Tools...
- Selecting a target, starting tests & writing reports

Each phase is explained with the necessary resources to get you started. So if you don't know where to start, this is perfect!

5. Tool of the week

> "DirectoryImporter"

DirectoryImporter is a Java Burp Suite extension that allows you to import directory bruteforcing results into Burp.
Until now, the alternative was to proxy bruteforcing tools through burp to check the results (or do it manually).
So this can be pretty handy. For now, only Dirsearch and Gobuster are supported. But you can add any other bruteforcing tool you want by adding a parser.

Other amazing things we stumbled upon this week

Videos

- BUG BOUNTY PRO TIPS : DON'T SPRAY AND PRAY! With Nahamsec
- Hacker101 – Game Hacking Basics
- My Entrepreneurial Journey – Episode 2: Week One of Business Ownership
- Drunk Hacking My Own Website (Web App 101)
- Bug Bounty World's Pranav Hivarekar Interviews Rahul Maini – Bug Bounty Talks
- AusCERT2019 Day 1 – Heidi Winter (Intro to CTFs)

Podcasts

- Security Now 717 – The Nansh0u Campaign
- Risky Business #544 — NYTimes Baltimore report falls over

- Coalcast Episode 5 PT 1 – Marcello Salvati (Byt3bl33d3r) and Dan McInerney
- Application Security Podcast: Björn Kimminich — The new JuiceShop, GSOC, and Open Security Summit
- Smashing Security 131: Zap yourself from the net, and patch now against BlueKeep
- Hack Naked News #221 – Weather Channel, Shopify, & SAC
- Paul's Security Weekly #607 – Mental Health & Wellness

Conferences

- LevelUp 0x04 2019
- BSides Budapest
- Circle City Con 2019
- HITB 2019 Amsterdam – Ten Years In The NL Box

Slides only

- Cache Me If You Can Messing with Web Caching
- Attacking AWS: the full cyber kill chain
- Internet-Scale analysis of AWS Cognito Security
- OAuth 2.0 Security Reinforced
- API Security Project: API Security Top 10 project launched by OWASP
- Bad Meets Evil
- The Darkside of Red-Teaming? Common Traps & Pitfalls In Recent Red-Teaming

Tutorials

Medium to advanced

- WAF through the eyes of hackers
- IP Disclosure of Servers Behind WAFs Using WordPress XML-RPC
- Bloodhound walkthrough. A Tool for Many Tradecrafts
- Hacking IOS Xamarin apps with Frida
- Bypassing Root CA checks in Flutter based apps on Android
- Logging Passwords on Linux

- Syncing yourself to Global Administrator in Azure Active Directory
- Kerberos (II): How to attack Kerberos?
- How to create an EVIL LTE Twin
- Hunting COM Objects
- How to Bypass AMSI with an Unconventional Powershell Cradle
- How Red Teams Bypass AMSI and WLDP for .NET Dynamic Code

Beginners corner

- Digging into Android Applications—Part 1—Drozer + Burp
- Exploiting SSRFs
- Linkedin OSINT
- API Hacking GraphQL
- How to find an easy P2
- TLS Security 6: Examples of TLS Vulnerabilities and Attacks
- Hidden Helpers: Security-Focused HTTP Headers & Security Header Scanner
- Top GitHub Dorks and Tools Used to Scan GitHub Repositories for Sensitive Data
- Fuzzing: Common Tools and Techniques
- Everything You Need to Know About Wireshark
- Linux for Pentester: APT Privilege Escalation

Writeups

Responsible disclosure writeups

- Hacking Smart TV
- Vim/Neovim Arbitrary Code Execution via Modelines
- Microsoft Edge Extensions Host Permission Bypass (CVE-2019-0678)
- We Decide What You See: Remote Code Execution on a Major IPTV Platform
- Hack the Hackers and Track the Trackers: CVE-2017-17713 and CVE-2017-17714 – Multiple SQL Injections and XSS Vulnerabilities found in the Hackers tracking tool “Trape” from “Boxug”
- NVIDIA GeForce Experience OS Command Injection CVE-2019-5678

Pentest writeups

- Simple PathTraversal bypass

Bug bounty writeups

- Open redirect on Upserve ($1,200)
- Auhtorization flaw on Shopify ($2,000)
- Violation of Secure Design Principles on HackerOne ($500)
- Information disclosure via Debug on Grammarly ($300)
- CSP bypass on Paypal ($900)
- Missing access control on Google
- RFI & SSRF
- Funny RCE
- XSS using Unicode

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- GPOCheck: Tool for auditing GPO on Windows AD
- Seccubus: Automates vulnerability scanning with: Nessus, OpenVAS, NMap, SSLyze, Medusa, SkipFish, OWASP ZAP and SSLlabs

More tools, if you have time

- Ansible-burp_extensions: Ansible playbook to install Burp extensions
- Cloud_enum: Multi-cloud OSINT tool. Enumerate public resources in AWS, Azure, and Google Cloud
- H2buster: A threaded, recursive, web directory brute-force scanner over HTTP/2
- Venom: Auto Recon Bash Script
- Liffy: Local file inclusion exploitation tool
- Taint'em All: Taint analysis tool for PHP
- Fatt /fingerprintAllTheThings: A pyshark based script for extracting network metadata and fingerprints from pcap files and live network traffic
- Leprechaun & Tutorial: This tool is used to map out the network data flow to help penetration testers identify potentially valuable targets.

- Mirage: A powerful and modular framework dedicated to the security analysis of wireless communications
- CloudCopy: Stealing hashes from Domain Controllers in the Cloud
- Byepass: Automates a large number of password cracking tasks using optimized dictionaries and mangling rules
- Zydra: A file password recovery tool and Linux shadow file cracker. It uses the dictionary search or Brute force method for cracking passwords
- Recsech: Websites footprinting and recon tool. It collects DNS Information, subdomains, Subdomain takeovers, does Github recon, detects honeypots...
- Sshd-poison: A tool to get creds of pam based sshd authentication
- ReverseTCPShell: Reverse Encrypted (AES) Shell over TCP using PowerShell SecureString, to Bypass Detection (FW\AV\IPS\IDS). Useful for RedTeams

Misc. pentest & bug bounty resources

- Reddit /r/websecurityresearch
- Internal Network Penetration Test Playbook
- 99-XSS-Polyglots.txt
- WordLists-20111129: Lists of words based on common web directory and file names
- Mobile: Xecurity Labs mobile security & applications reports
- Kerberos Attacks cheatsheet

Challenges

- secDevLabs: Laboratory for those who are interested in learning about web security
- Simple SQL Injection Training App & Introduction
- Cryptopals crypto challenges
- CyberSecurity Ninja challenges

Articles

- The Hidden Flaws of Archives in Java
- Penetration testing & window.opener—XSS vectors part 2
- Curl, Slight of Hand, & Exploit Hysteria
- Writeup of a cybersecurity interview

- Mimikatz and Windows RDP: An Attack Case Study
- Understanding UNC paths, SMB, and WebDAV
- Eternalblue | The NSA-developed Exploit That Just Won't Die

News

Bug bounty / Pentest news

- Get "Breaking into Information Security: Learning the Ropes 101" for free until the end of the month
- Cookies with SameSite by default: ""SameSite" is a reasonably robust defense against some classes of cross-site request forgery (CSRF) attacks, but developers currently need to opt-into its protections by specifying a SameSite attribute. In other words, developers are vulnerable to CSRF attacks by default."

Reports

- Rapid7 Threat Report Meets MITRE ATT&CK: What We Saw in 2019 Q1

Vulnerabilities

- Researcher Exploits Microsoft's Notepad to 'Pop a Shell'
- Critical bug impacts more than half of all email servers
- Microsoft Windows RDP Network Level Authentication Bypass (CVE-2019-9510): What You Need to Know
- Microsoft dismisses new Windows RDP 'bug' as a feature
- Cryptocurrency startup Komodo hacks itself to protect its users' funds from hackers
- Researchers Finds Thousands of iOS Apps Ignoring Security
- 'A Windows flaw so bad, even the NSA is begging users to update'

Breaches & Attacks

- Forget BlueKeep: Beware the GoldBrute
- BlueKeep 'Mega-Worm' Looms as Fresh PoC Shows Full System Takeover: "A working exploit for the critical remote code-execution flaw shows how an unauthenticated attacker can achieve full run of a victim machine in about 22 seconds."
- Quest Diagnostics says 11.9 million patients' financial and medical information may have been exposed in data breach
- New adware "BeiTaAd" found hidden within popular applications in app store

- Plot to steal cryptocurrency foiled by the npm security team
- Google confirms that advanced backdoor came preinstalled on Android devices
- The “pizza” method – a new way for hackers to get company data

Other news

- Apple launches privacy-focused login tech to throw web trackers off users’ scent
- Apple sunsets iTunes: iTunes will be replaced with 3 standalone desktop apps called Music, Podcasts & TV
- Hollywood lie: Bank hacks take months, not seconds
- Don’t blink, but 5G is about to change a lot more than just watching movies
- This is how hackers make money from your stolen medical data

Non technical

- Presentation Tips for Technical Talks
- Information Security Mental Models
- Warren Buffett: “Really Successful People Say No To Almost Everything”
- Information security career resume tips

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 05/31/2019 to 06/07/2019.

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***