Bug Bytes #41 – Reading JS, Pwning Spread Sheet Conversions & EdOverflow's CSP tool

BY INTIGRITI · OCTOBER 22, 2019 · LAST UPDATED ON JULY 30, 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 11 to 18 of October.

Our favorite 5 hacking items

1. Video of the week

> "Lets be a dork and read .js files with zseano"

JavaScript analysis is a very important step when testing the security of a website. If, like me, you never were a programmer and struggle with this, then this video is a must!
@zseano walks us through what to look for in them and how, plus an introduction to Google and Github dorks.

2. Resource of the week

> "XXE Cheat Sheet – SecurityIdiots"

This is a nice cheetsheet to help with XXE detection, exploitation and Out-Of-Band exploitation, and WAF bypass. A good reference!

3. Article of the week

> "A Tale of Exploitation in Spreadsheet File Conversions"

Do you remember this awesome video snippet with @daeken where he was clapping because obviously some kind of exploit or bug worked? It turns out that he was working on a Ghostscript payload in LibreOffice, in collaboration with @bbuerhaus, @smiegles, and @erbbysam.
It did work, and this is the writeup of the whole research that led to that bug. It touches on many topics: Ghostscript, fingerprinting LibreOffice, LFD, SSRF... This is worth reading and a great example of research in Web app security.

4. Non technical item of the week

> "A well curated 60s playlist for those slow Saturday mornings"

This is a really cool playlist. 100% Stök, only happy vibes.
I've been listening only to Deep House & Electro mixes (from Kygo, Dj Drop G...), so this is a refreshing change.

5. Tool of the week

> "CSP"

Retrieving a list of whitelisted hosts from CSP headers is not a new recon technique. But the novelty with this tool from @EdOverflow is that it automates the process.
You can get a list of hosts with a one-liner, and feed it to your other tools.

Other amazing things we stumbled upon this week

Videos

- Live Bug Bounty Recon Session and Creating a Recon Database for Yahoo W/ @Daeken
- Playing with SQLMap and Solving Hacker101's "Photo Gallery" CTF Level
- A Tale in Red Teaming – Joe
- Windows Privilege Escalation Video Series
- BUGCROWD BUGBASH SF 2019 Vlog (Hacking Atlassian)

Podcasts

- Security Now 736 – CheckM8
- Darknet Diaries Ep 49: Elliot
- Paul's Security News #623

Conferences

- SecTor 2019, especially:
  - Step by step AWS Cloud Hacking
  - The Tools of a Web App Pentester
  - Hashes, hashes everywhere, but all I see is plaintext
  - Serverless Security Top 10 Risks
  - Using Static and Runtime Analysis to Understand Third-Party Applications
  - OAuth – Everything You Wanted to Know but Not Really!
- OWASP Global AppSec Amsterdam, especially:

    - HTTP Desync Attacks: Smashing Into The Cell Next Door
    - How I Could Have Stolen Your Photos From Google
    - The Insecurity Caused By Trusting Your Client-Side Storage
    - Mobile- Or Attacker-Friendly? A Security Evaluation Of Mobile-First Websites
    - [In]secure Deserialization, And How [Not] To Do It
    - Web Apps vs Blockchain dApps (Smart Contracts): tools, vulns and standards, Slides & Smart Contract Security Verification Standard (SCSVS)
- 44con 2019, especially:
    - Owning The Cloud Through SSRF
    - The Billion Dollar IoT Attack No One Knows About
- Sniffing Routes to Pwnage: An Intro to Bloodhound & Slides

Slides only

- Prototype Pollution in Kibana
- Flash click2play in Web Browsers and other Horror Stories
- "Hands-On BloodHound" Workshop
- Bypassing Python 3.8 Audit Hooks

Tutorials

Medium to advanced

- A Thorough Introduction to PASETO
- Advisories 1-2: Azure AD and Common WS-Trust MFA Bypass explained
- Revisiting Email Spoofing
- Stupid Unix Tricks
- Share Wi-Fi Adapters Across a Network with Airserv-Ng
- SMB LFI Exploitation
- MacOS Red Teaming 210: Abusing Pkgs for Privilege Escalation
- Simple Trick For Red Teams
- Cracking Passwords with Umlauts

Beginners corner

- Taking Control of Your Passwords: How to use Github as your password manager

- Lxd Privilege Escalation
- API Hacking GraphQL
- The difference between Cross-Site and Server-Side Request Forgery

Writeups

Challenge writeups

- Orange Tsai's HITCON CTF 2019 Quals Web Challenges (source code & solutions)
- Decoding an incomplete QRCode – Intigriti Hacking Challenge at bruCON
- Writeup of a prototype manipulation challenge (like the Kibana exploit)
- XSS challenge: Theory of Browser Evolution

Pentest writeups

- Getting started with AMF Flash Application Penetration Testing !
- Pwning Cisco Devices Using Smart Install Exploitation Tool (siet.py)
- Studying "Study the Great Nation": Cure53's report on an app by the Chinese Communist Party

Responsible(ish) disclosure writeups

- Gila CMS Upload Filter Bypass and RCE #Web
- Office 365 network attacks – Gaining access to emails and files via an insecure Reply URL #Web
- Few click RCE via GitHub Desktop macOS client with Gatekeeper bypass and custom URL handlers #RCE #MacOSX
- From Stackoverflow to CVE, with some laughs along the way: Kubernetes vulnerable to "Billion Laughs" #Web #DoS

Bug bounty writeups

- Reflected XSS on Shopify ($2,000)
- SQL injection on Zoho #CodeReview
- OTP bypass on Razer ($1,000)
- 2FA bypass ($250)
- CSRF

See more writeups on The list of bug bounty writeups.

Tools

- SSRF Sheriff: A simple SSRF-testing sheriff written in Go
- The JSON Web Token Toolkit
- DOMDig: DOM XSS scanner for Single Page Applications
- Burpee: A python module that accepts an HTTP request file and returns a dictionary of headers and post data
- xmlrpc-bruteforcer: Fast XMLRPC brute forcer targeting WordPress written in Python 3. It can brute force 1000 passwords per second
- Linkedin2username: OSINT tool. Generate username lists for companies on LinkedIn
- PoshADCS: A proof of concept on attack vectors against Active Directory by abusing Active Directory Certificate Services (ADCS)
- Net-GPPPassword: .NET implementation of Get-GPPPassword. Retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences.

Misc. pentest & bug bounty resources

- New NetSec Focus channel for bug bounty
- APIsecurity.io Issue 53: Vulnerabilities in TwitterKit, JustDial, Voi e-scooters
- #CyberpunkisNow Weekly Resource List: Week 41, 2019: OSINT resources by @hackermaderas
- IoT Pentesting – Approach & Methods

Challenges

- SQL injection lab
- Type Juggling lab
- Hacking-Lab

Articles

- AngularJS CSP bypass in 56 characters
- ASP.NET Request.QueryString XSS Filter Bypass – Convert Reflected XSS to Stored XSS
- Bypassing the WebARX Web Application Firewall (WAF)
- DNS Security: Threat Modeling DNSSEC, DoT, and DoH

News

Bug bounty & Pentest news

- Firefox's New WebSocket Inspector
- Mozilla Rolls Out Code Injection Attack Protection in Firefox
- We have a small message for the hackers playing with us. (YesWeHack)
- List of All Cybersecurity Conferences to Attend in 2020
- Encouraging Native Bug Bounty Research (Facebook)
- Expanding Bug Bounty Program for Third-Party Apps (Facebook)
- HackerOne released a refresh of HackerOne user profiles

Reports

- A Look at the Pricing of Cybercrime Goods, Services
- Internet Organised Crime Threat Assessment (IOCTA) 2019

Vulnerabilities

- Linux SUDO Bug Lets You Run Commands as Root, Most Installs Unaffected
- Firefox vulnerable to trivial CSP bypass
- What was wrong with Alexa? How Amazon Echo and Kindle got KRACKed
- Google's Pixel 4 face unlock has one major privacy weakness
- Security researcher publishes proof-of-concept code for recent Android zero-day
- Samsung to patch S10 fingerprint sensor bug next week
- "Debug mode" in popular webdev tool exposes credentials for hundreds of websites, including Donald Trump's

Breaches & Attacks

- Attackers Hide Backdoors and Cryptominers in WAV Audio Files

Other news

- Germany's cyber-security agency recommends Firefox as most secure browser
- We asked a hacker to try and steal a CNN tech reporter's data. Here's what happened
- Millions of computers at risk as Windows 7 nears end of life
- 350+ hackers hunt down missing people in first such hackathon

- Planes, gates, and bags: How hackers can hijack your local airport
- Pen testers find mystery black box connected to ship's engines

Non technical

- Why Successful IoT Bug Bounties Are So Rare

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 10/11/2019 to 10/18/2019.

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.