Bug Bytes #9 – Hacking Web Sockets, $10k Facebook Bug by @vulnano & Automated Bug Hunting

BY INTIGRITI · MARCH 12, 2019 · LAST UPDATED ON MARCH 6, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bugbytes-9-hacking-web-sockets-10k-facebook-bug-by-vulnano-automated-bug-hunting

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 1 to 8 of March.

Our favorite 5 hacking items

1. Tool of the week

> "Rescope & Introduction"

Wow, I love this tool! Have you've ever experienced the discomfort of adding several targets one by one or playing with regexes to configure your Burp scope? If yes, worry no more!
It is now possible to copy a bug bounty program's scope from their page, paste it to a .txt file, and convert it to Burp scope using one command.
Rescope takes as input a file containing your target domains, subdomains, IPs, wildcard subdomains, etc. And outputs a JSON file that you can import in Burp to *automagically* configure your scope. In one shot, and no regex required.
Here's an example input file:
Scope:
Critical admin.example.com/login.aspx
Critical https://example.com/upload:8080
Critical *.dev.example.com and *.prod.example.com
High 192.168.0.1-2 (internal testing)

Out of Scope:
!EXCLUDE
bgp.example.com:179
*.vendor.example.com
192.168.10.9
It can contain any text and descriptions. The tool extract targets wherever they are. The only thing to remember is to put **!EXCLUDE** before to list your exclusions, because by default all targets found are considered included.

2. Writeup of the week

> "Facebook Messenger server random memory exposure through corrupted GIF image ($10,000)"

This is one weird bug in Facebook Messenger for Android: @vulnano uploaded a corrupted GIF file with missing content body. The image displayed back contained data from previously used memory buffers. It

was leaking data from memory! He noticed it because the image display had white noise, while it was supposed to be blank.
Also, when the images were uploaded with Facebook Messenger for Android, nothing happened. The weird images were only visible from the Facebook Web app.
Another takeaway is to not rely on tools without understanding what they do and how to do the same job yourself. @vulnano first generated corrupted images with Gifoeb, but they caused the app to crash. So he studied the GIF image format and generated his own images.

3. Tutorial of the week

> "Hacking Web Sockets: All Web Pentest Tools Welcomed"

Web sockets testing is an area where dynamic testing tools are lacking. This tutorial introduces a great way to fill this gap.
It shows you how to use existing tools like SQLmap, Burp Pro active scanner or Commix to pentest Web sockets. This is done through a Web socket harness: a python script which acts like a proxy between the Web socket and the tool you want to run against it. It gets HTTP traffic from the tool, transforms it into Web socket traffic and sends it to the socket. Then does the opposite with the Web socket's response.
This opens a whole new world for fuzzing and automated testing of Web sockets!

4. Non technical item of the week

> "How to write a report"

This is a great article on writing good quality bug bounty reports. Whether you have experience in bug reporting or not, I highly recommend going through the article and thinking of what could be improved in your reports.
It could help you gain more reputation points and avoid being asked for more details because the explanations weren't detailed or clear enough.
On this same topic, also check out the bug bounty writeups below. Some of them (especially those by Jobert Abma) are good examples of really well written reports.

5. Slides/Workshop material of the week

> "Using Docker with Kubernetes for automating Application Security and OSINT workflows
> Automating Application Security Bug Hunting: Improving coverage with better automation"

Lately, I've been thinking about automation a lot. Using custom scripts to automate your recon is one thing, but automation Bounty Machine style is at a whole other level. It involves tools like Kubernetes, Docker, Argo and Golang (for speed).
That's why I'm so excited about studying these two new resources:
The workshop material explains how to set up Docker with Kubernetes for automated testing. It includes source code and documentation in the form of a Gitbook.
And the slides introduce the framework Intrigue-core which has an interesting Web UI and API.

Other amazing things we stumbled upon this week

Videos

- PHP: escapeshellcmd vs escapeshellarg

- 10 Minute Tip: Safely Using Google's Cached Content
- RSA Conference 2019: IoT is Next Big Target of Man-in-The-Middle Attacks
- PowerShell Basics for Security Professionals
- Tech Academy – Security Vulnerability Basics: Videos created by @TomNomNom. "The idea behind these videos is that they can be linked to if a vulnerability is reported to team that doesn't know what the vulnerability is or why it's important to fix it"

Podcasts

- Security Now 704 – Careers in Bug Hunting
- Absolute AppSec Ep. #49 – Subdomain Takeovers, DNS SSRF, Top 10 web hacking techniques of 2019 / video version
- Darknet Diaries Ep 33: RockYou
- The secure developer Ep. #18, Collaborative Security with HackerOne's Marten Mickos
- Sophos podcast Ep. 022 – Plaintext passwords, cryptocoin criminality and the Momo monstrosity
- Risky Business #533 — Ghidra release, NSA discontinues metadata program and more

Conference slides

- BSides San Francisco
- HTTP Security Headers: A technology history through scar tissue
- Abusing WCF Endpoints for RCE and Privilege Escalation
- Hacking with a Heads Up display
- Red V Blue Workshop
- Security Learns to Sprint: DevSecOps

Tutorials

Medium to advanced

- Recovering SQLCipher encrypted data with Frida
- Repacking iOS applications: A quick and easy guide for binary patching and repacking iOS apps during security audits
- A Practical Guide to Smart Contract Security Tools. Part 3: Mythril
- The worst of both worlds: Combining NTLM Relaying and Kerberos delegation
- Persistent Code Execution via XScreenSaver
- Get-AzurePasswords: Exporting Azure RunAs Certificates for Persistence

- MS Excel Weaponization Techniques
- Day 64: NMAP 2 ROOT FTW (with and without interactive mode)
- Day 67: Tar Cron 2 Root — Abusing Wildcards for Tar Argument Injection in root cronjob (Nix)
- Windows Persistence with PowerShell Empire
- Hiding IP During Pentest using PowerShell Empire (http_hop)

Beginners corner

- Penetration Testing Active Directory, Part I & Reddit discussion
- Email Spoofing for Beginners
- Exploring Google Hacking Techniques
- Network Basics for Hackers: Server Message Block (SMB) and Samba
- Wardriving with Kismet, GPS and Google Earth.
- Day 65: Change Linux Root Password with Shadow File Permission Issues
- Day 66: More Shenanigans with /etc/shadow — abusing find SETUID.
- Metasploit Basics, Part 16: Metasploit SCADA Hacking
- How to Use Burp Suite for Mobile App Testing (Additional information: Installing certificates requires a root device since Android Nougat)

Writeups

Challenge writeups

- From 4 sources to 3 sinks in DOM XSS – DomGoat level 1-10 (all levels) writeup
- Playing with CloudGoat part 5: hacking AWS with Pacu
- Insomni'Hack Teaser 2019 – exploit-space
- [BSidesSF CTF 2019] – Mobile Track

Pentest writeups

- Tomcat exploit variant : host-manager

Responsible disclosure writeups

- Hacking ski helmet audio
- Owning the Smart Home with Logitech Harmony Hub
- PHP Variable Inception
- Don't worry about being locked with Loccess

- Gone in six seconds? Exploiting car alarms: Researchers could remotely track, hijack & take control of vehicles with the alarms installed

Bug bounty writeups

- Improper access control on Gitlab ($11,000)
- Information disclosure on Shopify ($1,000)
- Information disclosure on GitLab ($300)
- SSRF on Vimeo ($5,000)
- XSS in ProtonMail for iOS ($1,000)
- Misconfigured Github wiki ($500)
- Cross-Site Frame Leakage (CSFL) on Facebook
- Authorization flaw on private program

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- WebTech & Introduction: Identify technologies used on websites
- Check.subs.sh: @Blurbdust's script for enumerating subdomains & checking them for subdomain takeover
- Data-Over-DNS & Introduction: Tool for tunnelling data over DNS as part of a blind XSS attack
- Burp-javascript-security-extension & Introduction: A Burp Suite extension for finding malicious JavaScript. It performs checks for cross-domain scripting against the DOM, subresource integrity checks, and evaluates JavaScript resources against threat intelligence data
- SPAudit & Introduction: Chrome extension for scanning SPAs (Single Page Applications)

More tools, if you have time

- GitHub Wiki Auditor: Python script to check GitHub accounts for world-editable wiki pages
- Domainker: BugBounty helper tool, includes plugins to automate testing for CRLF, check if target is hosted on Amazon, and get host CNAME and response codes
- G-suite-check: Checks if the domains MX records point at G-suite
- Shr3dKit](https://github.com/shr3ddersec/Shr3dKit): Red Team Tool Kit
- Decker: Declarative penetration testing orchestration framework & Reddit discussion
- Sheepl: Creating realistic user behaviour for supporting tradecraft development within lab environments (useful for creating red team/blue team AD network environments)
- ShellCheck](https://github.com/koalaman/shellcheck): A static analysis tool for shell scripts

- Subzy](https://github.com/LukaSikic/subzy): Subdomain takeover tool which works based on matching response fingerprings from can-i-take-over-xyz
- Subtake: Automatic finder for subdomains vulnerable to takeover. Written in Go, based on @haccer's subjack
- Legion: Open source, easy-to-use, super-extensible and semi-automated network penetration testing tool that aids in discovery, reconnaissance and exploitation of information systems
- CVE-2005-1794-check.py: Easy way to test for RDP hard coded RSA key MiTM vulnerability, without actually performing the MiTM

Misc. pentest & bug bounty resources

- Mobisec & Slides: All the slides (~800!) of @reyammer's Mobile Security class
- Courses & Introduction: A list of YouTube videos from many different creators and put it in a loosely structured order to cover the basics of pentesting
- APIsecurity.io Issue 21: Amazon Ring Doorbell camera hacked, open APIs coming to healthcare
- OSINT Guide
- Awesome Hacking Resources
- Day 63: Top 10 Essential NMAP Scripts for Web App Hacking
- OWASP ASVS 4.0
- File transfer skills in the red team post penetration test
- Privilege Escalation Reference
- Day 68: Crack File, Key and Keychain Passwords with John

Articles

- SVG XLink SSRF fingerprinting libraries version
- Chaining CSRF with Stored XSS to exfiltrate data
- How Google Can Help You to Steal Somebodies Personal Data
- What Impact Does the Autocomplete Feature Have on Web Security?
- Serverless vs Cloud vs On-prem
- Great Scott! Timing Attack Demo for the Everyday Webdev & demo
- Top 5 Ways The Red Team breached and assessed the Physical Environment
- Cyber tactics
- MachineAccountQuota is USEFUL Sometimes: Exploiting One of Active Directory's Oddest Settings

News

Bug bounty news

- Hackprenticeship Alpha: Apply before 03-15 at 20:00 EST to become @daeken's bug bounty apprentice

Reports

- Hacked Website Trend Report – 2018
- Mobile Security Index 2019 by Verizon
- The 2019 Hacker Report: Celebrating The World's Largest Community of Hackers
- ReDoS vulnerabilities in npm spikes by 143% and XSS continues to grow

Breaches & Vulnerabilities

- YouTube content creators are facing denial-of-service attacks of a different variety
- Comcast security nightmare: default '0000' PIN on everybody's account
- Google reveals BuggyCow macOS security flaw
- Buffer overflow flaw in British Airways in-flight entertainment systems will affect other airlines, but why try it in the air?
- That marketing email database that exposed 809 million contact records? Maybe make that two-BILLION-plus
- Serious Chrome zero-day – Google says update "right this minute"
- Google Photos disables sharing on Android TV
- Docker API vulnerability allows hackers to mine Monero
- Saudi mobile app Dalil exposes data of over five million users
- Hundreds of millions of Chinese chat logs leak online: "Several local governments have asked web cafés to install monitoring software on their computers"
- Supply Chain – The Major Target of Cyberespionage Groups: Citrix data breach. 6 terabytes of sensitive data stolen by Iranian group Iridium, using 2FA bypass techniques & password-spraying

Other news

- W3C and FIDO Alliance Finalize Web Standard for Secure, Passwordless Logins
- The Prototype iPhones That Hackers Use to Research Apple's Most Sensitive Code
- Unclosable browser popup! 13-year-old charged for sharing code
- Android Security Monthly Recap #2
- Facebook criticised for misuse of phone numbers provided for security

- NSA unleashes Ghidra malware analysis tool: NSA open sourced its Reverse Engineering tool Ghidra + Tutorial & Comparison with IDA Pro

Non technical

- A Beginners guide to Pen Test Reporting
- HackInterview with Tanya- Because I'm a woman, I've been asked many silly questions in interviews.
- Hacking the Imposter Syndrome
- The Only Thing You Cant Fix Is Killing Yourself

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 03/01/2019 to 03/08/2019.

Curated by Pentester Land & Sponsored by Intigriti