Bug Bytes #4 – Misconfigured Jira's, how to SSRF & DOM XSS challenge

BY INTIGRITI · FEBRUARY 5, 2019 · LAST UPDATED ON MARCH 6, 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. You can sign up for the newsletter here.*

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 25 of January to 01 of February.

Our favorite 5 hacking items

1. Conference of the week

> "BSides Leeds 2019, especially:
> – Confessions Of A Bug Bounty Triager & Slides
> – So You Want To Be A Pentester?
> – Hacking Companies For Internet Glory While Not Dying In A Sarlacc Pit
> – A Pentester's Guide To Left Shifting Security"

These are four very interesting talks. They're respectively about:

- Questions & tips from a bug bounty triager for both bug hunters & companies/triagers;
- Advice for anyone looking for a pentester job from the CEO of a pentesting company;
- Differences between bug bounty & pentesting;
- Ideas from a pentester on how to integrate pentesting into the development process. Automating some tests helps detect vulnerabilities early in the development lifecycle.

2. Writeup of the week

> "Guest blog: Eray Mitrani – Hacking isn't an exact science"

This is a great writeup on a simple bug that affects some misconfigured Jira instances.
When a new dashboard or shared filters are being set up, they can become inadvertently accessible without authentication if permissions are set to "everyone". You can test, for instance, if the status endpoint is accessible by trying */status/*, then if it doesn't work try */status/..;/*.
What I love about this writeup is how @ErayMitrani explains two fundamentals processes for bug hunters:

- How to apply someone else's research to find new bugs on bug bounty programs even if you don't understand the bug 100%;

© Intigriti

- How organizing his bug hunting notes allows him to go back and look for new bugs in programs he tested previously.

3. Tutorial of the week

> "SSRF — Server Side Request Forgery (Types and ways to exploit it) Part-3, Part 2 & Part 1"

This is a great series of blog posts on SSRF. It's very practical and explains the types of SSRF bugs, how to exploit them, how to bypass filters, and example of vulnerable sites.
FIY, some of the vulnerable sites were found with Shodan. These bugs were probably not disclosed to the sites' owners which I think is illegal. So please do not exploit them.

4. Challenge of the week

> "DomGoat Client XSS exercises"

DOM XSS can be harder to detect and exploit than traditional XSS. This is because everything happens client-side. The payload isn't sent to the server and reflected back in the response. So the best way to detect them is reviewing code and most tools aren't that good at it (at least not as good as manual code analysis).
This challenge can help you understand sources and sinks usually involved in the exploitation of DOM XSS bugs. There are 10 exercises with the vulnerable code highlighted.

5. Non technical item of the week

> "Tips on how to live with imposter syndrome"

A lot of hackers suffer from imposter syndrome, me included. I think it's because the more we learn, the more we know we don't know. We also have to be both versatile and specialists, which is hard because infosec/hacking has so many different vast subcategories.
If you get imposter syndrome too, then I recommend this article. It offers advice and practical tips to manage it and don't let it hold you back.

Other amazing things we stumbled upon this week

Videos

- Web Security 101 – HTTP Parameter Pollution – I didn't see that coming.
- Hacker101 – Mobile Hacking Crash Course

Podcasts

- Browser Extension Security – Security Now 699
- The Many Hats Club Ep. 33, Cooperative Forest Assistance Act and beyond (with Fred Jennings)

© Intigriti

- Smashing Security 113: FaceTime, Facebook, faceplant
- Security in 5 Episode 416 – Largest Breached Data Dump Discovered, 770 Million Records, Here's What We Know
- Getting Started in Red Teaming and Offensive Security — CyberSpeak Podcast
- Sophos podcasts Ep. 017 – DNS hijacking, a weird breach and a cybersecurity confession [PODCAST]

Conferences

- Reading Other Peoples Code (NDC London 2019) & Slides

Slides only

- We take your security seriously. Or do we?
- An Attacker's View of Serverless and GraphQL Apps – Abhay Bhargav – AppSec California 2019
- From zero to app-hero

Tutorials

Medium to advanced

- [PrivExchange] From user to domain admin in less than 60sec !
- XXE that can Bypass WAF Protection
- Unauthenticated AWS Role Enumeration (IAM Revisited)
- 0x03 Learning about Universal Links and Fuzzing URL Schemes on iOS with Frida
- Exploiting Windows PC using Malicious Contact VCF file
- Exploiting Windows using Contact File HTML Injection/RCE
- Post Recon With Wmic
- Kerberos PreAuthentication and Party Tricks
- Attacking default installs of Helm on Kubernetes
- Abusing Docker API | Socket

Beginners corner

- Expanding your scope (Recon automation #2)
- Unicorn — Low Priv Shell to Meterpreter Session
- I Spy with InSpy v3.0

© Intigriti

- Vulnerability Assessment and Management with Archerysec
- 02 – From n00b to h4x0r via clickjacking (Sarcastic tone but still informative)

Writeups

Challenge writeups

- FireShell 2019 / Bad injections

Pentest & Responsible disclosure writeups

- GPS watch issues... AGAIN
- Baking Flask cookies with your secrets
- Remote Hardware Takeover via Vulnerable Admin Software
- How I exploited ACME TLS-SNI-01 issuing Let's Encrypt SSL-certs for any domain using shared hosting
- Pwn the LIFX Mini white
- Microsoft Windows ".contact" File HTML Injection Mailto: Link Remote Code Execution 0day ZDI-CAN-7591
- Pentest-Report ExpressVPN Extension by Cure53

Bug bounty writeups

- IDOR on Twitter ($7,560)
- Logic flaw on Google ($7,500)
- Authorization flaw on private program
- Token theft via open redirect on private program
- Authorization flaw & XSS on Leo Express
- Logic flaw on Hackerone ($500)
- Path traversal on Bower & Severe Security Vulnerability in Bower's Zip Archive Extraction
- Logic flaw on Shopify

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Burp Bounty profiles by @egarme and other profiles by @crowdshield & @GochaOqradze

© Intigriti

- ClassModifier: Utility to easily modify compiled Java class files with an interactive GUI (allows you to change their equivalent smali code). This can help in testing java desktop application and can change behavior of pre-compiled classes

More tools, if you have time

- Sn0int: Semi-automatic OSINT framework and package manager
- Open-source vulnerability assessment tool: The officially recommended open-source scan tool for Java applications at SAP. Analyses Java & Python apps for open-source dependencies with known vulnerabilities, using both static analysis and testing to determine code context and usage for greater accuracy
- Beemka: Basic Electron Exploitation
- Aztarna: A footprinting tool to find vulnerable robots on the Internet
- Adapt: A tool that performs automated Penetration Testing for WebApps
- Pown Recon: A powerful target reconnaissance framework powered by graph theory
- XSS Chef: A web app (inspired by CyberChef) to help people create custom XSS Payloads when on pentests, rather than having to keep referring back to old scripts from past tests
- XLESS: The Serverless Blind XSS App
- Buildscript: Wrapper around Nmap & NSE scripts
- Blackbuntu Linux: Pentest distribution based on Ubuntu

Misc. pentest & bug bounty resources

- Companies-hiring-security-remote: A list of companies that hire security people full remote
- Collection Of Bug Bounty Tip-Will Be updated daily
- Web Application Security & Bug Bounty (Methodology, Reconnaissance, Vulnerabilities, Reporting)
- Learn Android Security
- Using Firefox Add-Ons for #BugBounty
- IoT/passwords/list-2019-01-29.txt: Default credentials list for telnet/ssh IoT devices
- Learning Resources
- OSCP Methodology
- Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World (free book)
- Steganography – A list of useful tools and resources & two other stegano tools
- 2019 Cybersecurity Excellence Awards

© Intigriti

Challenges

- DomGoat Client XSS exercises
- Hacking For Kids: Project to teach kids hacking techniques to get them started early security, programming and technology in general.
- Wizard Labs: Online penetration testing lab
- Secure Coding Dojo & Attack-Grams
- NetSec Focus's list of oscp-like boxes

Articles

- How Does The SDK Version Affect The Security of Android Applications?
- Security testing advice for Automotive OEMs and Tier ones
- How my Instagram account got hacked
- Hackerone is not respecting their own policy & Hackeorne's response
- Hacking Android: Attack Surfaces
- Hacking floating hotels. Cruise ship compromise on the high seas
- OSINT and the new perimeter
- ClickJacking and JavaScript KeyLogging in Iframes
- Pushing Lft, Like a Boss, Part 5.8 Securing Your Cookies
- 5 Tips for OSCP Prep

News

Bug bounty news

- Bug Bounty Radar // Jan 2019
- Facebook Consumer Device Bounty Bonus Announcement: Hardware products added to Facebook's bug bounty program + limited-time added bonus for findings in Portal and Oculus
- Brace yourself: $50 Million in Bounties is Coming—and we are celebrating the whole way there!
- Launching the Hacker Calendar, Never Miss a Challenge Again

Breaches & Vulnerabilities

- Apple scrambles to fix FaceTime eavesdropping bug
- Hacker Selling Database of 159 Million Clients Leaked from LinkedIn Online

© Intigriti

- Credential dump contains another 2.2 billion pwned accounts
- Targeted Attacks Abusing Google Cloud Platform Open Redirection
- Dailymotion hit by credential stuffing cyber-attack
- iCloud Possibly Suffered A Privacy Breach Last Year That Apple Kept a Secret

Malicious apps/sites

- Everything you need to know about Facebook, Google's app scandal

Other

- Japanese government will try to hack its citizens' IOT devices
- Twitter scammers jump in on real-time complaints to companies: Story of a scammer scammed
- Mayhem is a machine that can automatically detect, exploit, and patch cybersecurity vulnerabilities: Automated white-hat hacking machines
- Cybersecurity Workforce Study, 2018
- Designing Security for Billions: Facebook's defense-in-depth approach to security

Non technical

- Tips on how to live with imposter syndrome
- Awesome Mental Health
- Getting started in bugbounties
- HackenProof Interview with @zseano
- Researcher Spotlight: Ambassador Tony aka Tj null
- How to protect yourself this Data Privacy Day

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 01/25/2019 to 02/01/2019.

*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

© Intigriti