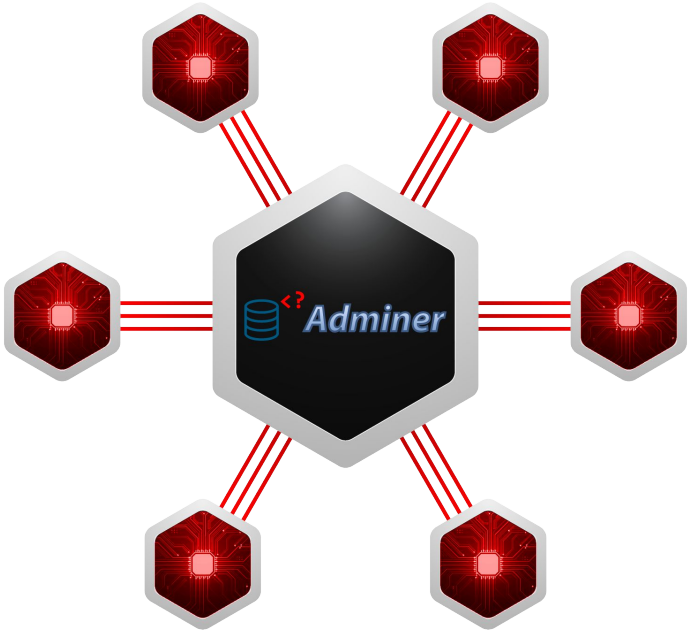
ABUSING ADMINER: How SSRF Opens the Door to Cloud Metadata



ABOUT CYBERWARFARE LABS :

CW Labs is a Global Infosec company specializing in cybersecurity practical learning situated across UK, US & India. The company has 2 primary divisions :

1. Niche Cyber Range Labs
2. Continuous Learning : Infinity Platform

ABOUT SPEAKER

SUBASHINI K B

TECHNICAL INTERN

Subashini Balaji is a Security Analyst at **CyberWarFare Labs**, specializing in **Red Teaming and APT simulations** in enterprise environments. She also writes **technical blogs and articles** focused on real-world cyber attack techniques and defenses.

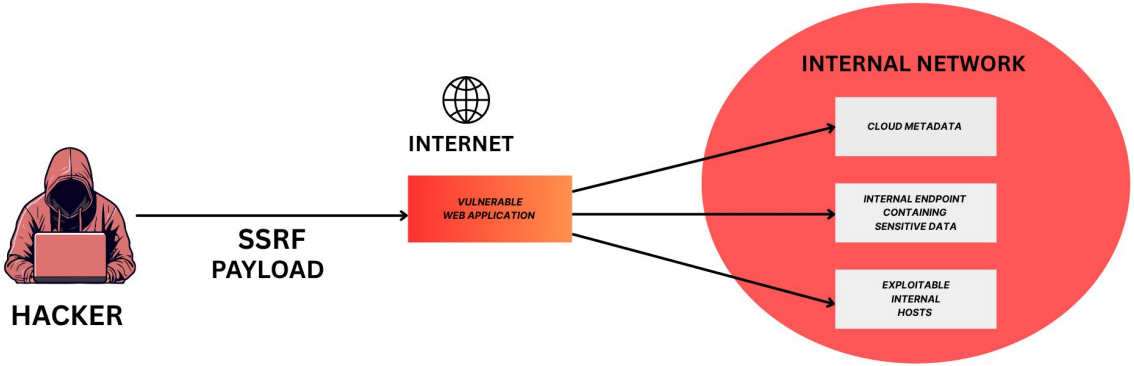
Game Plan

1. What is SSRF?
2. How it is working
3. What is metadata ?
4. What is adminer?
5. Demo

What is SSRF?

- **Server-Side Request Forgery (SSRF)** is a vulnerability where an attacker can trick a server into making unintended requests to internal or external resources.
- These requests are made from the server itself, which can have more privileges and access compared to a client-side request.
- SSRF can be exploited to gain access to **internal systems,** extract sensitive data, or conduct further attacks within the organization's network.

DIAGRAM

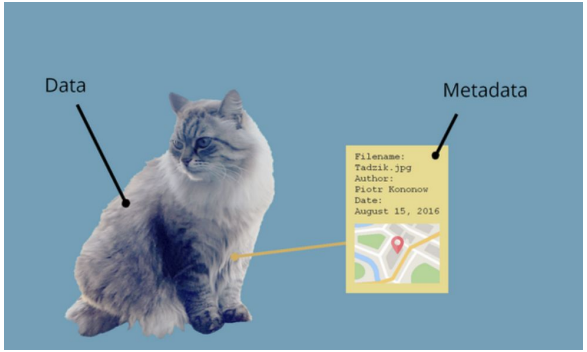


How Server-Side Request Forgery Attacks Work

1. **Identification of Vulnerability:** The attacker identifies a web application function that processes user-supplied URLs or can make HTTP requests.
2. **Crafting Malicious Request:** The attacker crafts a request that includes a URL to an internal or sensitive resource.
3. **Exploiting the Vulnerability:** The server processes the malicious request and makes the request to the specified URL.
4. **Accessing Sensitive Data:** The server's request retrieves data from internal systems, which is then sent back to the attacker, leading to data leakage or unauthorized access.

What is metadata?

- **Metadata** is information that describes other data. It's often called **data about data**
- **For example**, when you take a photo with your phone, the image itself is the data, and details like the date, time, location, and camera settings are the metadata. In documents, metadata can include the author's name, when the file was created, and when it was last edited.
- **Metadata** helps us organize, find, and understand data more easily. In cloud computing, metadata can also include important details about servers or services like IP addresses or temporary credentials(which can be sensitive if exposed).



What is adminer?

Adminer is a lightweight tool used by developers to manage databases like MySQL, PostgreSQL, and phpMyAdmin. It's a single web page of PHP file (`adminer.php`) that you can upload to your web server. When opened in a browser, it gives a simple interface to:

- Log into a database
- Run SQL queries
- View, edit, or delete data
- Manage tables and users

Why Adminer became the attacker's entry point?

1. Left exposed on the internet

- Developers often **upload Adminer temporarily** for testing and **forget to delete it**.
- This leaves it **publicly accessible**, sometimes **without proper authentication**.

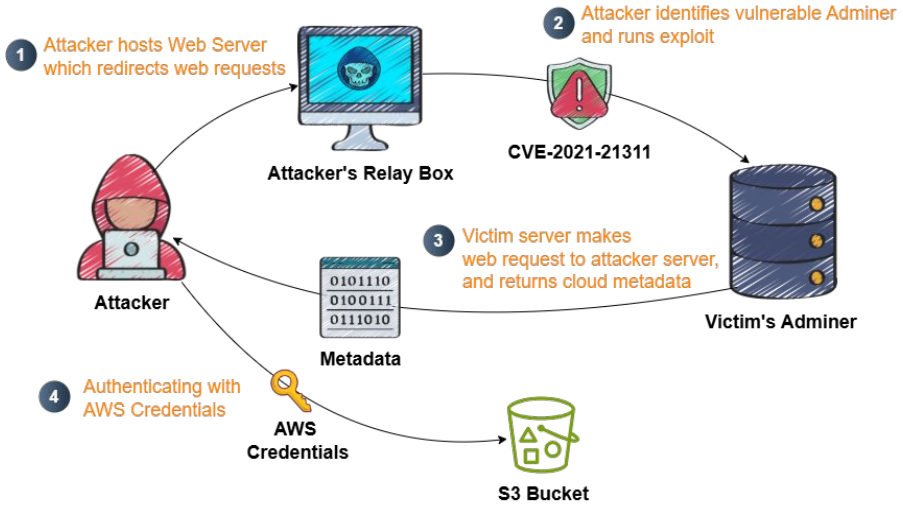
2. Allows connecting to remote systems

- Adminer can be used to **connect to any database or internal service**, not just local ones.
- Attackers abused this feature to send **SSRF (Server-Side Request Forgery)** requests.

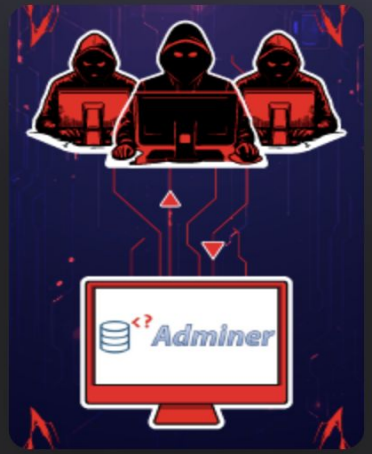
3. Enabled SSRF attacks

- By tricking Adminer into connecting to a special IP (`http://169.254.169.254`), the attackers could:
  - **Access cloud metadata**
  - **Steal temporary credentials**
  - **Take over cloud resources**

Attack Flow



Demo Challenge



UNC2903: Metadata Abuse via Adminer (SSRF Attack)

As a member of Secure-Corp's elite Red Team, your mission is to simulate a real-world cloud attack based on UNC2903's exploitation of cloud metadata service of Adminer application.

Hard | $ Free | 30 | Not Completed

CWL
CyberWarFare Labs

Certified Hybrid Multi-Cloud
Red Team Specialist

CHMRTS

AT ONLY

$99

USE CODE

99CHMRTS

29TH JUNE 2025

CWL INFINITY LEARNING PLATFORM

INFINITY PREMIUM

USE CODE

EARLY9

5TH JULY 2025

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings

Please Contact :

support@cyberwarfare.live

To know more about our offerings, please visit: **https://cyberwarfare.live**