websec / **Vision-Helpdesk-Exploit** Public

Code Issues Pull requests Actions Projects Security and quality

1 Branch 0 Tags Go to file Go to file Code

websecnl Update and rename CVE-2024-XXXX.py to CVE-2024-58343.py

6037887 · 4 hours ago

CVE-2024-58343.py	Update and rename CVE-2…	4 hours ago
README.md	Update README.md	2 years ago
requirements.txt	Create requirements.txt	2 years ago

README

Serialized IDOR Exploit for Vision Helpdesk (<= v5.7.0)

Description

This repository contains a proof-of-concept (PoC) exploit for a critical **Serialized Insecure Direct Object Reference (IDOR)** vulnerability in **Vision Helpdesk** versions <= 5.7.0. This vulnerability allows unauthorized access to user profile information by manipulating serialized data within cookies, specifically targeting the `vis_client_id` parameter.

Affected Versions

- **Vision Helpdesk:** Versions <= 5.7.0

Vulnerability Reference

- **CWE-639:** Insecure Direct Object Reference (IDOR)

- **WSTG-ATHZ-04:** Testing for Insecure Direct Object References

Exploit Details

By modifying the `vis_client_id` stored in a Base64-encoded serialized cookie, an attacker can iterate through user IDs and retrieve sensitive profile information, such as email addresses, first names, and last names.

PoC Exploit

The included Python script automates the exploitation of the vulnerability:

1. Accepts the target URL and session cookie (`PHPSESSID`) as inputs.
2. Iterates over a range of possible `vis_client_id` values.
3. Extracts sensitive user data (email, first name, last name) from each profile it accesses.
4. Outputs the collected information into a text file.

Requirements

- **Python 3.x**
- **Requests** library (pip install requests)
- **BeautifulSoup** for HTML parsing (pip install beautifulsoup4)

Usage

1. Clone this repository: git clone https://github.com/websec/vision-helpdesk-idor-exploit.git cd vision-helpdesk-idor-exploit
2. Install dependencies: pip install -r requirements.txt
3. Run the script: python exploit.py
4. Provide the following inputs:
    - **URL:** The target helpdesk domain (e.g., https://helpdesk.domain.com/index.php).
    - **PHPSESSID:** The session ID of a logged-in user. (You have to login first, use your own session ID or change this code to automatically create account and obtain the session ID for you in case you want to make an improved version of this exploit)

The script will generate a Base64-encoded serialized cookie and attempt to retrieve user profile information for `vis_client_id` values starting from 1000. The output will be written to a file named `output.txt`.

Disclaimer

This code is for educational and research purposes only. Exploiting vulnerabilities without the consent of the owner of the target system is illegal and unethical. Use this responsibly.

Releases

No releases published

Packages

No packages published

Contributors 1

websecnl Joel Aviad Ossi

Languages

- **Python** 100.0%