Web 200

***Lưu ý: Bắt buộc điền đầy đủ thông tin và cho file này vào cùng thư mục của mỗi challenge***

|  |  |
| --- | --- |
| **Tên** | Web 200 |
| **Tác giả** | HarDToBelieve |
| **Email** | [tuanit96@gmail.com](mailto:tuanit96@gmail.com) |
| **Phản biện** |  |
| **Lĩnh vực** | Web exploit |
| **Contest** | Grand Prix |
| **Server** | Ubuntu 16.04 |
| **Đường dẫn** | /var/www/web200 |
| **Flag** | WhiteHat{Everyone\_w4s\_Baby\_ev3n\_A\_PhD} |
| **Đánh giá mức độ** | khó |
| **Điểm** | 200 |
| **Thời điểm hoàn thành đề** | 31/10/2017 |
| **Cập nhật tài liệu lần cuối** | 24/11/2017 |

# Mô tả

Web app cho phép xem thông tin về món ăn Việt Nam ở /foods

# Phương pháp ra đề

Code php

# Hướng dẫn deploy

Thay đổi host, username, password và database trong file *setup\_exploit/setup.py* và *utils.php*

Tạo user mới ( có thư mục ở /home để đặt flag ). Config cho apache chạy trang web đề bài dưới quyền user đó ( có thể cài sudo apt-get install libapache2-mpm-itk và tham khảo file web200.conf đính kèm )

Cài đặt python sqlAlchemy ( sudo pip install sqlalchemy ). Chạy file *setup\_exploit/setup.py* để tạo bảng và đẩy dữ liệu vào db

Xoá folder *.idea* và *setup\_exploit*

# Hướng dẫn giải

* Khai thác lỗi hash extension để có thể login vào trang web với quyền premium
* Sử dụng lỗi LFI để đọc file .htaccess, từ đó phát hiện ra file proxy tên là **m21t1VxmT4feWBe8.php**
* Bypass blacklist trong file proxy bằng cách sửa lại gói tin lên server để tận dụng đc chữ GET
* —> Từ GET index.php
* ——> Thành $\_GET /\*index.php?\*/[‘c’](’s’ . ‘y’ . ’s’ . ’t’ . ‘e’ . ‘m’, ‘id’);?>
* ========> Log Injection

# Gợi ý

* Hash Extension
* Weird apache behavior