VNCERT   
Công việc của nhóm thực hành trong 06/03/2023 đến 10/3/2023

MỤC LỤC

[DANH MỤC HÌNH VẼ 2](#_Toc129382760)

[I. TÓM TẮT VIỆC ĐÃ LÀM 3](#_Toc129382761)

[1.1. Bảng Nhiệm Vụ 3](#_Toc129382762)

[1.2. Công Việc Thực Hiện Trong Tuần Tới 3](#_Toc129382763)

[II. PHISHING 4](#_Toc129382764)

[III. INSTALL JOOMLA 9](#_Toc129382765)

[3.1. Cài đặt Joomla 9](#_Toc129382766)

[3.2. Tìm kiếm lỗ hổng bằng công cụ JoomlaScan 12](#_Toc129382767)

# DANH MỤC HÌNH VẼ

[Hình 2. 1 Công cụ The Social-Engineer Toolkit 4](#_Toc129380261)

[Hình 2. 2 Option social engineering 5](#_Toc129380262)

[Hình 2. 3 Bảng danh sách của social-engineeing 5](#_Toc129380263)

[Hình 2. 4 Menu loại hình phishing 6](#_Toc129380264)

[Hình 2. 5 Menu loại web sử dụng 6](#_Toc129380265)

[Hình 2. 6 Menu danh sách các website có sẵn 6](#_Toc129380266)

[Hình 2. 7 Website đăng chờ sự kiện login của user 6](#_Toc129380267)

[Hình 2. 8 Form login của web phishing 7](#_Toc129380268)

[Hình 2. 9 Webiste chính chủ của google 7](#_Toc129380269)

[Hình 2. 10 Tài khoản được gửi về cho hacker 8](#_Toc129380270)

[Hình 3. 1 Tạo db, user cho joomla 9](#_Toc129380250)

[Hình 3. 2 Tải và giải nén joomla 9](#_Toc129380251)

[Hình 3. 3 Form nhập thông tin tạo tài khoản 10](#_Toc129380252)

[Hình 3. 4 Nhập thông tin db 10](#_Toc129380253)

[Hình 3. 5 Bước cuối trong setup dữ liệu 11](#_Toc129380254)

[Hình 3. 6 Thông báo đã cấu hình thành công 11](#_Toc129380255)

[Hình 3. 7 Trang login 12](#_Toc129380256)

[Hình 3. 8 Login thành công 12](#_Toc129380257)

[Hình 3. 9 Scan Joomla 13](#_Toc129380258)

[Hình 3. 10 Scan Joom tiếp theo 14](#_Toc129380259)

[Hình 3. 11 Lỗ hổng của joomla liên quan đến plugin 14](#_Toc129380260)

# TÓM TẮT VIỆC ĐÃ LÀM

## Bảng Nhiệm Vụ

TASK 6/3 - 9/3 (BUILD AND ATTACK VULN JOOMBLA)

|  |  |  |
| --- | --- | --- |
| LÂM ANH | DUNG | ĐỨC |
| Phising  (Sử dụng The Social-Engineer Toolkit) | Install joombla 3.7.0 in ubuntu.  Search vuln  Attack joombla (optional) | Tool scan joombla vuln  Anaylist log of tool |

## Công Việc Thực Hiện Trong Tuần Tới

TASK 10/3 - 16/3 (BUILD LAB CEH)

|  |  |  |
| --- | --- | --- |
| LÂM ANH | DUNG | ĐỨC |
| Module 9 | Module 10 | Module 13 |

# PHISHING

Công cụ ***The Social-Engineer Toolkit*** có sẵn trong kali linux

Graphical user interface, text, application

Description automatically generated

Hình 2. Công cụ The Social-Engineer Toolkit

Trong công cụ này có 6 option nhưng ta sẽ dùng option 1 là “social-engineering”

Text

Description automatically generated

Hình 2. Option social engineering

Tiếp theo chọn option 2 trong social engineering để tạo website phishing

Text

Description automatically generated

Hình 2. Bảng danh sách của social-engineeing

Trong website chúng ta chọn option 3 nhằm tạo ra một trang web giả mạo nhằm lừa đảo người dùng cung cấp thông tin đăng nhập của họ (tài khoản và mật khẩu)

Text

Description automatically generated

Hình 2. Menu loại hình phishing

Tiếp theo ta chọn option 1 là website có sẵn

Text

Description automatically generated

Hình 2. Menu loại web sử dụng

Tiếp theo ta chọn website là google để phishing.

Text

Description automatically generated

Hình 2. Menu danh sách các website có sẵn

Quá trình tạo web phishing bắt đầu

Text

Description automatically generated

Hình 2. Website đăng chờ sự kiện login của user

Khi ta truy cập website với ip của hacker sẽ hiển thị trang thông tin đăng nhập như của google, khi ta nhập tài khoản, mật khẩu vào form và tiến hành đăng nhập.

Graphical user interface, website

Description automatically generated

Hình 2. Form login của web phishing

Khi đăng nhập dù chúng ta có nhập tài khoản hay mật khẩu thành công hay thất bại thì vẫn sẽ chuyển sang trang chính thức của google khiến cho người dùng nhầm lẫn là đã đăng nhập thành công.

Graphical user interface, text, application, email, website

Description automatically generated

Hình 2. Webiste chính chủ của google

Trong khi đó tài khoản và mật khẩu được gửi về phía hacker

Text

Description automatically generated

Hình 2. Tài khoản được gửi về cho hacker

# INSTALL JOOMLA

## Cài đặt Joomla

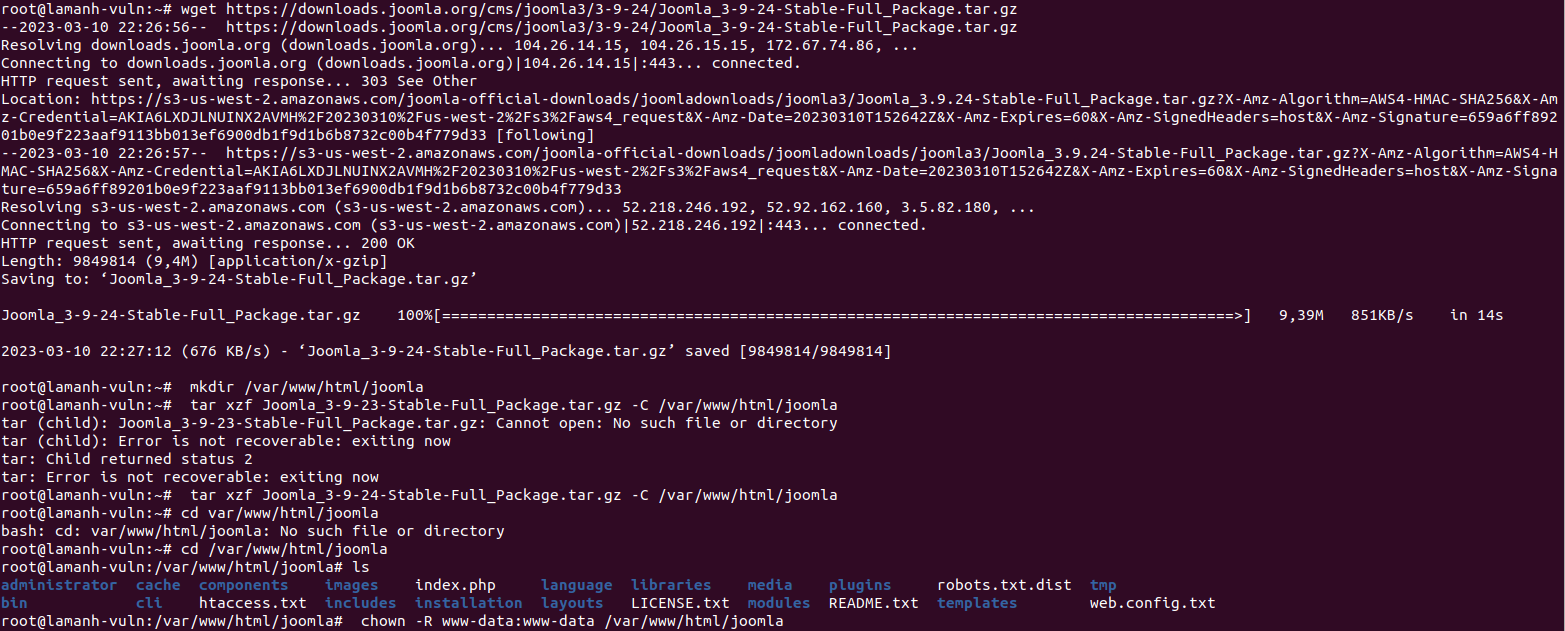
Cấu hình database cho jomlaa;

Text

Description automatically generated

Hình 3. Tạo db, user cho joomla

Tiếp theo ta tải và giải nén thư joomla như hình sau với câu lệnh tải joomla về: “wget https://downloads.joomla.org/cms/joomla3/3-9-24/Joomla\_3-9-24-Stable-Full\_Package.tar.gz”



Hình 3. Tải và giải nén joomla

Truy cập vào website thông qua http://your-ip/joomla

Graphical user interface, text, application

Description automatically generated

Hình 3. Form nhập thông tin tạo tài khoản

Nhập thông tin của cơ sở dữ liệu đã tạo tương ứng

Graphical user interface, text, application, email

Description automatically generated

Hình 3. Nhập thông tin db

Graphical user interface, text, application

Description automatically generated

Hình 3. Bước cuối trong setup dữ liệu

Graphical user interface, text, application

Description automatically generated

Hình 3. Thông báo đã cấu hình thành công

Graphical user interface

Description automatically generated

Hình 3. Trang login

Graphical user interface, text, application, email

Description automatically generated

Hình 3. Login thành công

## Tìm kiếm lỗ hổng bằng công cụ JoomlaScan

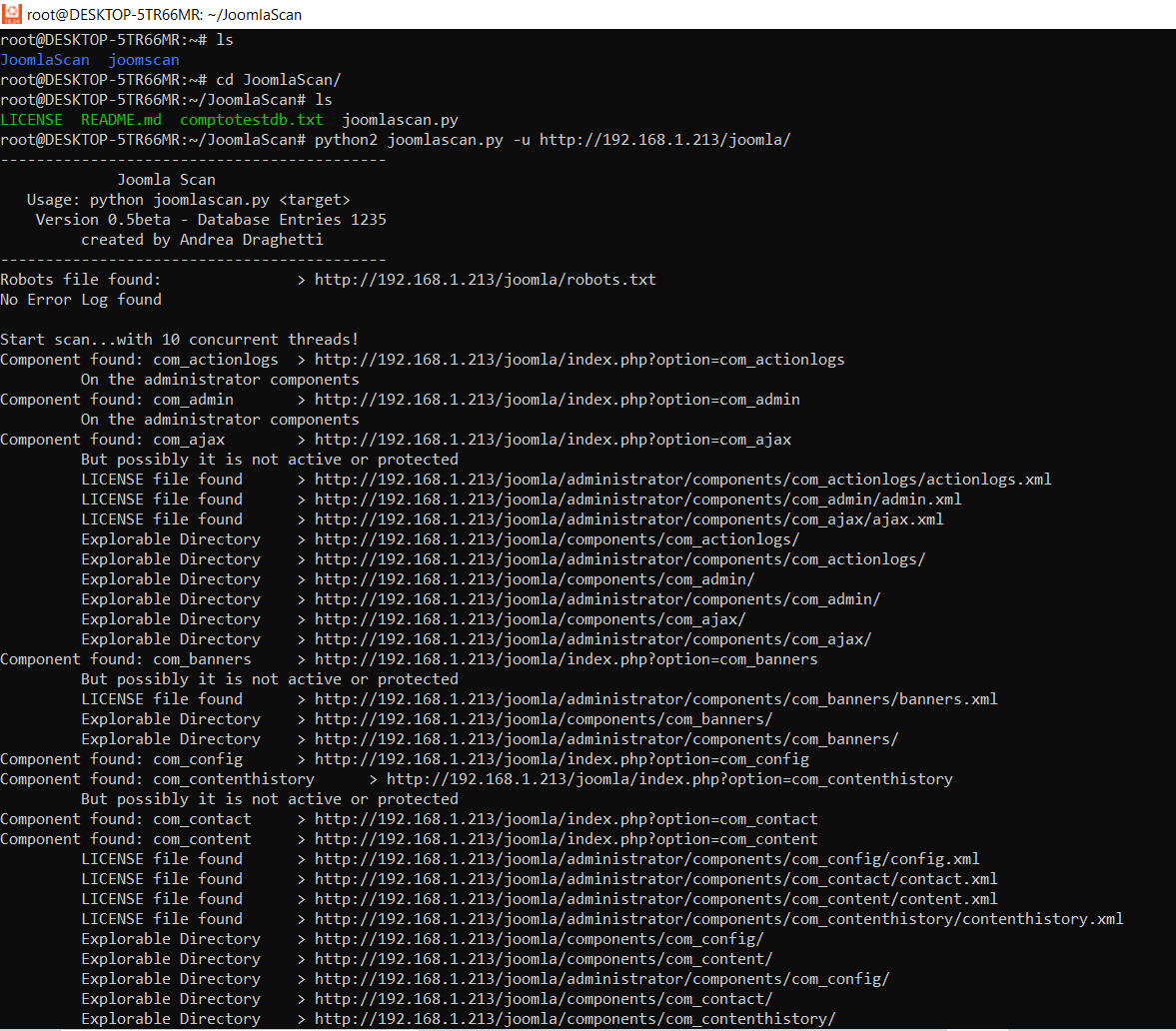
Tải công cụ JoomlaScan:

*“git clone* [*https://github.com/rezasp/joomscan.git*](https://github.com/rezasp/joomscan.git)*”*

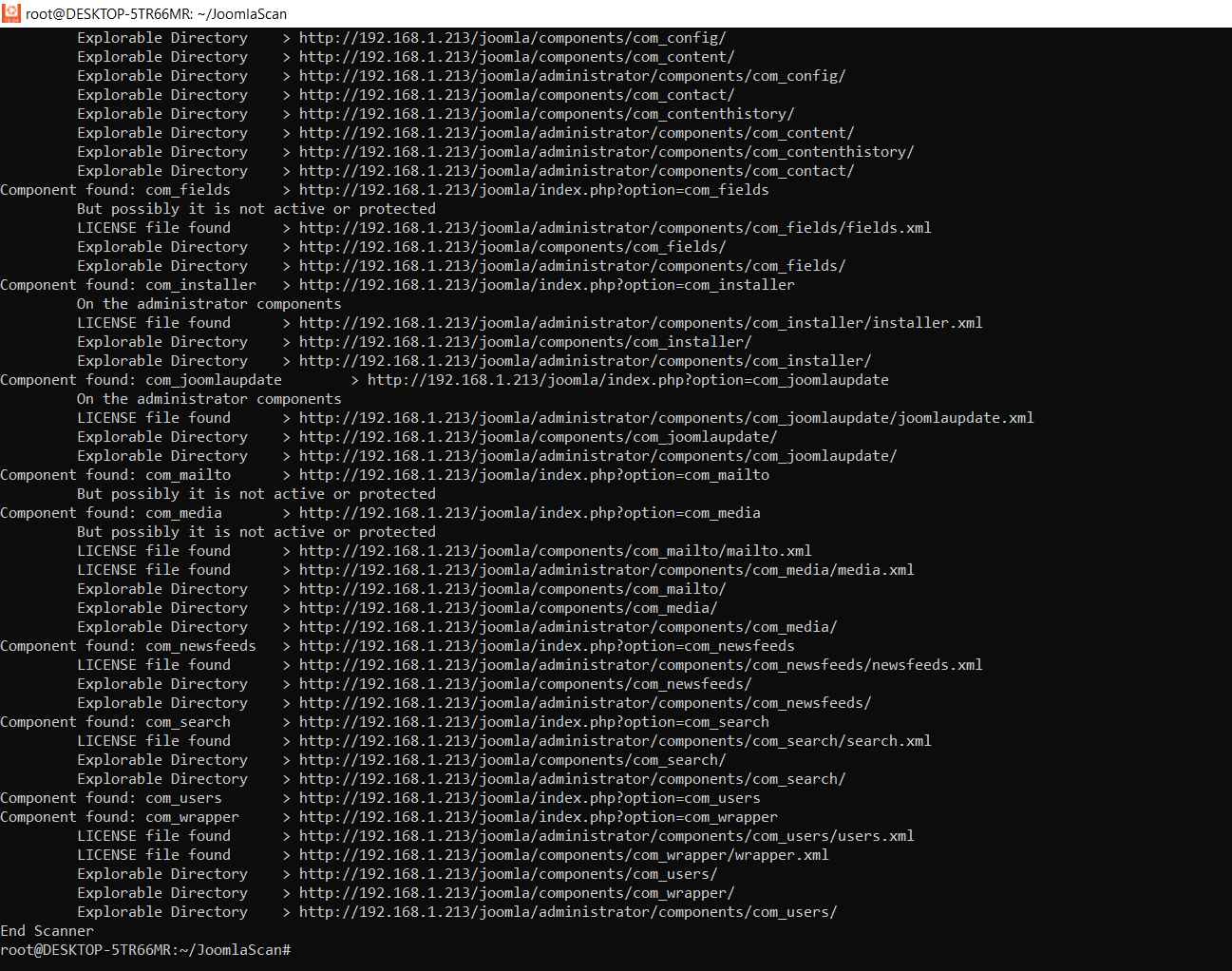
Để tìm các lỗ hổng bảo mật tiềm ẩn bằng công cụ JoomlaScan, sử dụng lệnh:

*“python2 joomlascan.py –u* [*http://192.168.1.213/joomla/*](http://192.168.1.213/joomla/)*’*

Khi chạy dòng lệnh này, Python 2 sẽ chạy file "joomlascan.py" và truyền vào giá trị URL của trang web Joomla để kiểm tra các lỗ hổng bảo mật trên trang web này. Công cụ Joomlascan sẽ kết nối đến trang web Joomla và thực hiện kiểm tra các lỗ hổng bảo mật.



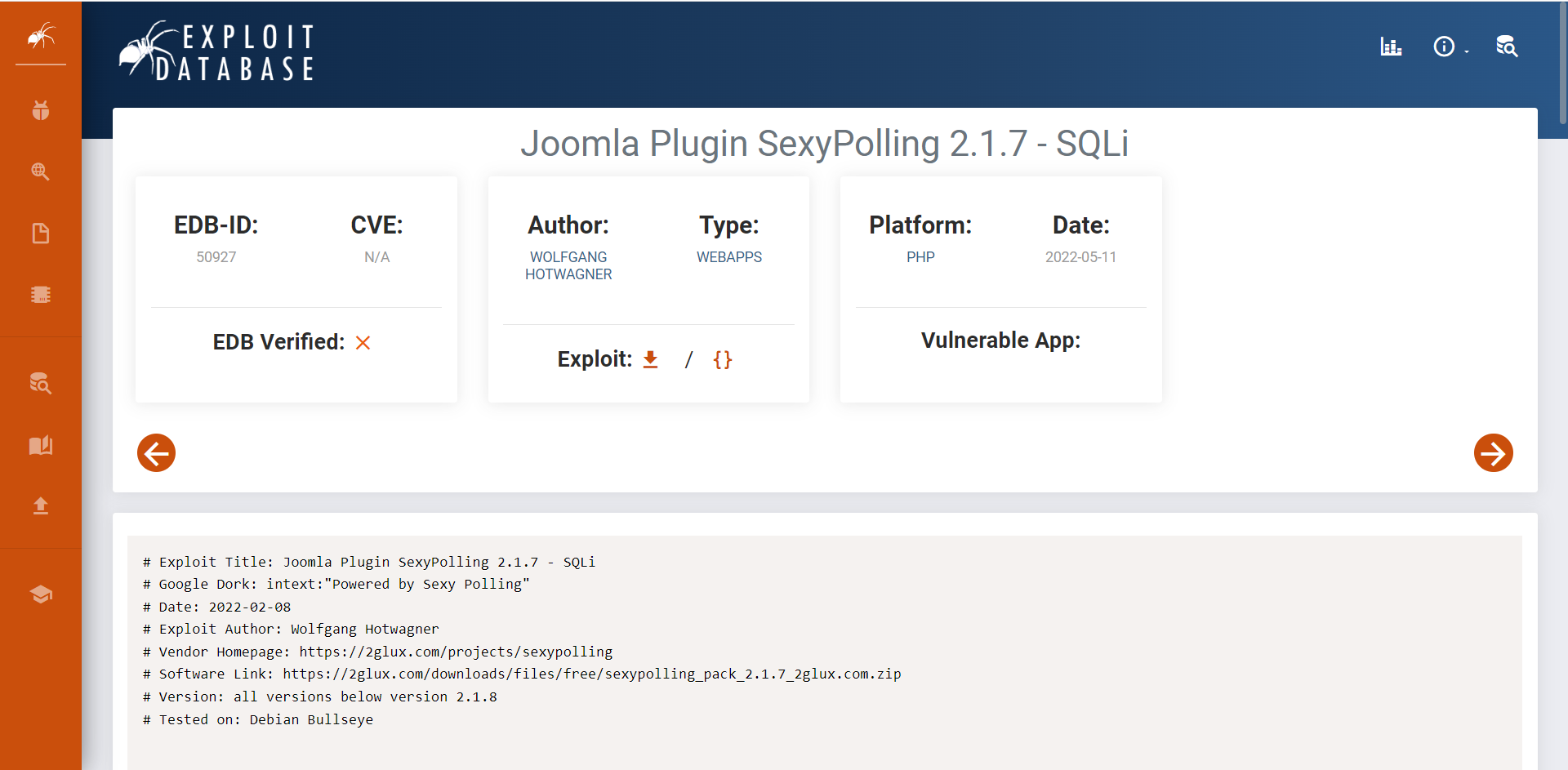
Hình 3. Scan Joomla



Hình 3. Scan Joom tiếp theo

Tiếp theo bắt đầu tìm các lỗ hổng bằng cách tìm kiếm (vd: com\_sexypolling vuln/cve). Kết quả sau khi tìm kiếm:

Dưới đây là những thông tin về lỗ hổng SexyPolling, ở dòng Software Link là một đường dẫn file zip được dùng để plugin vào Joomla và tiếp tục khai thác.



Hình 3. Lỗ hổng của joomla liên quan đến plugin