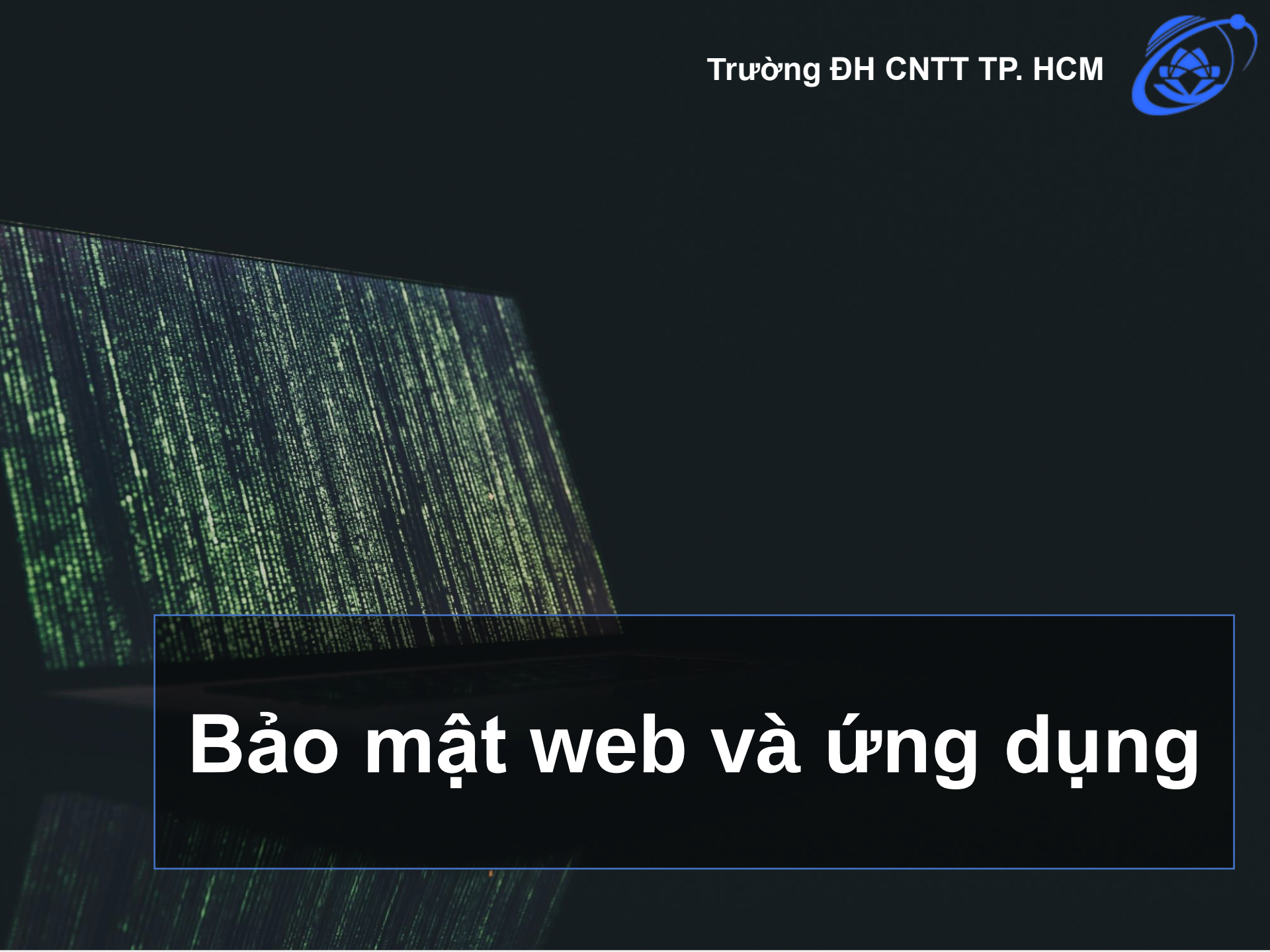
Trường ĐH CNTT TP. HCM



# Bảo mật web và ứng dụng

# Nội dung

- Hacking
- Hacker
- Hacking Phases
- Penetration Testing
- OWSAP
- CVE
- CWE
- Một số công cụ Reconnaissance

# Hacking là gì?

- Hacking refers to **exploiting system vulnerabilities and compromising security controls** to gain unauthorized or inappropriate access to the system resources

- It involves **modifying system or application features** to achieve a goal outside of the creator's original purpose

- Hacking can be used to steal, pilfer, and redistribute intellectual property leading to **business loss**

# Hacker?

**01**

Intelligent individuals with **excellent computer skills**, with the ability to create and explore into the computer's software and hardware

**02**

For some hackers, **hacking is a hobby** to see how many computers or networks they can compromise

**03**

Their intention can either be to gain knowledge or to **poke around to do illegal things**

Some do hacking with **malicious intent** behind their escapades, like stealing business data, credit card information, social security numbers, email passwords, etc.

# Hacking Phases: Reconnaissance

- Reconnaissance refers to the preparatory phase where an **attacker seeks to gather information** about a target prior to launching an attack
- Could be the future point of return, noted for ease of entry for an attack when more about the **target is known on a broad scale**
- Reconnaissance **target range** may include the target organization's clients, employees, operations, network, and systems

## Reconnaissance Types

### Passive Reconnaissance

- Passive reconnaissance involves acquiring information **without directly interacting with the target**
- For example, searching public records or news releases

### Active Reconnaissance

- Active reconnaissance involves **interacting with the target directly by any means**
- For example, telephone calls to the help desk or technical department

# Hacking Phases: Scanning

| | | |
|---|---|---|
| **Pre-Attack Phase** | Scanning refers to the pre-attack phase when the attacker **scans the network** for specific information on the basis of information gathered during reconnaissance |  |
| **Port Scanner** | Scanning can include use of dialers, **port scanners**, network mappers, ping tools, vulnerability scanners, etc. |  |
| **Extract Information** | Attackers extract information such as **live machines**, port, port status, OS details, device type, **system uptime**, etc. to launch attack |  |

# Hacking Phases: Gaining Access

1. Gaining access refers to the point where the attacker obtains access to the **operating system or applications** on the computer or network

2. The attacker can gain access at the **operating system level**, **application level**, or **network level**

3. The attacker can **escalate privileges** to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised

4. Examples include **password cracking**, buffer overflows, denial of service, **session hijacking**, etc.

# Hacking Phases: Maintaining Access

1. Maintaining access refers to the phase when the attacker tries to retain his or her **ownership of the system**
2. Attackers may prevent the system from being owned by other attackers by securing their exclusive access with **Backdoors**, **RootKits**, or **Trojans**
3. Attackers can upload, download, or **manipulate data**, applications, and configurations on the **owned system**
4. Attackers use the compromised system to **launch further attacks**

# Hacking Phases: Clearing Tracks

1

Covering tracks refers to the activities carried out by an attacker to **hide malicious acts**


2

The attacker's intentions include: **Continuing access** to the victim's system, remaining **unnoticed and uncaught**, deleting evidence that might lead to his prosecution

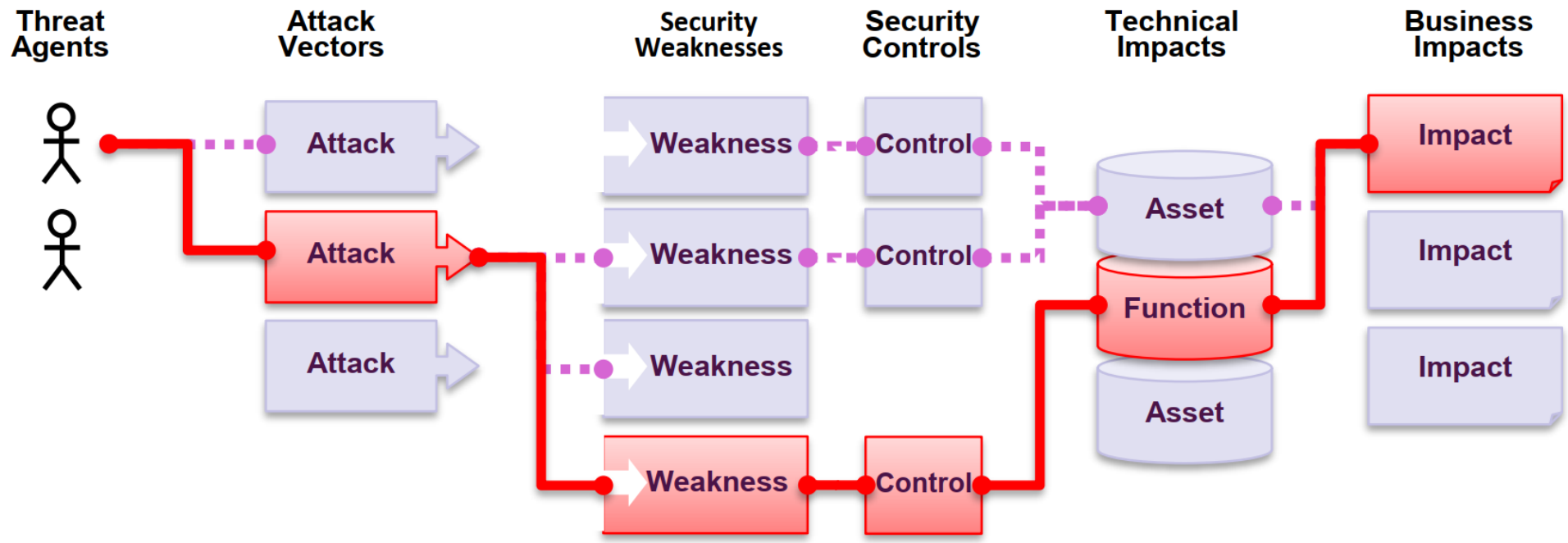
3

The attacker overwrites the server, system, and application logs to **avoid suspicion**

**Attackers always cover their tracks to hide their identity**

# Application Security Risks

- Attackers can potentially use many **different paths** through your application to **do harm** to your business or organization



# Khái niệm Penetration Testing

- Penetration testing is a method of evaluating the security of an information system or network by **simulating an attack to find out vulnerabilities** that an attacker could exploit
- **Security measures** are actively analyzed for design weaknesses, technical flaws and vulnerabilities
- A penetration test will not only point out vulnerabilities, but will also **document** how the weaknesses can be exploited
- The results are delivered comprehensively in a **report**, to executive management and technical audiences

# Tại sao phải Pentest?

Identify the threats facing an **organization's information assets**

Reduce an organization's expenditure on IT security and enhance **Return On Security Investment** (ROSI) by identifying and remediating vulnerabilities or weaknesses

Provide assurance with comprehensive **assessment of organization's security** including policy, procedure, design, and implementation

Gain and maintain certification to an **industry regulation** (BS7799, HIPAA etc.)

Adopt **best practices** in compliance to legal and industry regulations

For testing and validating the efficacy of **security protections and controls**

For changing or upgrading **existing infrastructure** of software, hardware, or network design

Focus on **high-severity vulnerabilities** and emphasize **application-level security issues** to development teams and management

Provide a comprehensive approach of **preparation steps** that can be taken to prevent upcoming exploitation

Evaluate the efficacy of **network security devices** such as firewalls, routers, and web servers

# So sánh Security Audit, Vulnerability Assessment và Pentest

## Security Audit

- A security audit just checks whether the organization is following a set of standard **security policies and procedures**

## Vulnerability Assessment

- A vulnerability assessment focuses on **discovering the vulnerabilities in the information system** but provides no indication if the vulnerabilities can be exploited or the amount of damage that may result from the successful exploitation of the vulnerability

## Penetration Testing

- Penetration testing is a methodological approach to security assessment that **encompasses the security audit** and vulnerability assessment and demonstrates if the vulnerabilities in system can be successfully exploited by attackers

# Phân loại Pentest

| | |
|---|---|
| **Black-box** | **No prior knowledge** of the infrastructure to be tested<br>• Blind Testing<br>• Double Blind Testing |
| **White-box** | **Complete knowledge** of the infrastructure that needs to be tested |
| **Grey-box** | **Limited knowledge** of the infrastructure that needs to be tested |

# Giai đoạn Pentest

### Pre-Attack Phase

- Planning and preparation
- Methodology designing
- Network information gathering

### Attack Phase

- Penetrating perimeter
- Acquiring target
- Escalating privileges
- Execution, implantation, retracting

### Post-Attack Phase

- Reporting
- Clean-up
- Artifact destruction

# Phương pháp kiểm tra bảo mật

- A security testing or pen testing methodology refers to a methodological approach to **discover and verify vulnerabilities in the security mechanisms of an information system**; thus enabling administrators to apply appropriate security controls to protect critical data and business functions

**Examples of Security Testing Methodologies**

| | |
|---|---|
| **OWASP** | The Open Web Application Security Project (OWASP) is an open-source application security project that **assist the organizations to purchase, develop and maintain software tools**, software applications, and knowledge-based documentation for Web application security |
| **OSSTMM** | Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed methodology for performing **high quality security tests** such as methodology tests: data controls, fraud and social engineering control levels, computer networks, wireless devices, mobile devices, physical security access controls and various security processes |
| **ISSAF** | Information Systems Security Assessment Framework (ISSAF) is an open source project aimed to provide a security assistance for professionals. The mission of ISSAF is to "**research**, **develop**, **publish**, and **promote** a complete and practical generally accepted information systems security assessment framework" |
| **EC-Council LPT Methodology** | LPT Methodology is a industry accepted comprehensive **information system security auditing framework** |

# ISO/IEC 27001:2013

- ISO/IEC 27001:2013 specifies the requirements for **establishing**, **implementing**, **maintaining** and continually improving an **information security management system** within the context of the organization
- It is intended to be suitable for several different types of use, including the following:

1. Use within organizations to formulate **security requirements** and **objectives**
2. Use within organizations as a way to ensure that security risks are **cost effectively managed**
3. Use within organizations to **ensure compliance with laws and regulations**
4. Definition of new **information security management processes**
5. Identification and clarification of existing **information security management processes**
6. Use by the management of organizations to determine the **status of information security management activities**
7. Implementation of **business-enabling information security**
8. Use by organizations to provide relevant information about **information security** to customers

*https://www.iso.org*

# CVE

**Common Vulnerabilities and Exposures**

✓Cung cấp thông tin về các lỗ hổng bảo mật

✓Giúp đánh giá sơ bộ công cụ bảo mật

Thống kê:

- Theo năm
- Theo loại
- Sản phẩm

…

https://www.cvedetails.com/

# Thống kê lỗ hổng JRE - Oracle

**Oracle » JRE : Vulnerability Statistics**

Vulnerabilities (**499**) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

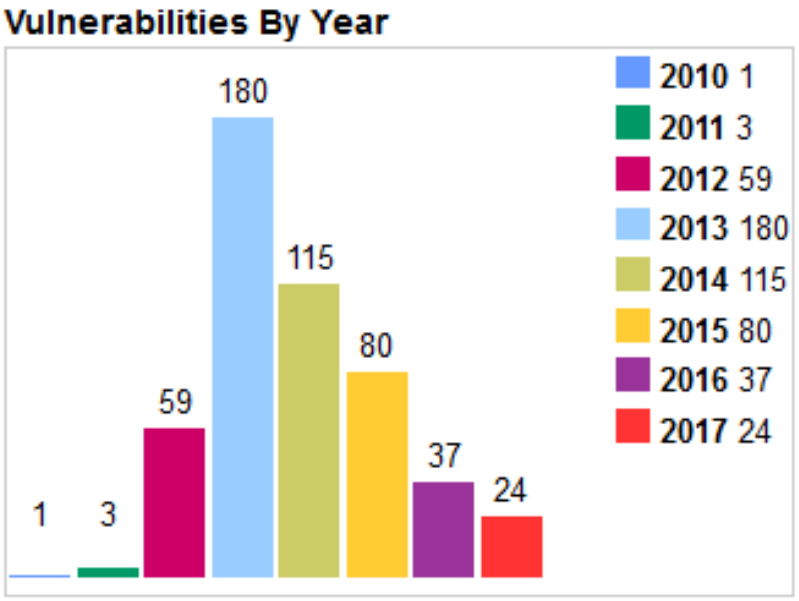
Related OVAL Definitions : Vulnerabilities (839) Patches (556) Inventory Definitions (3) Compliance Definitions (0)

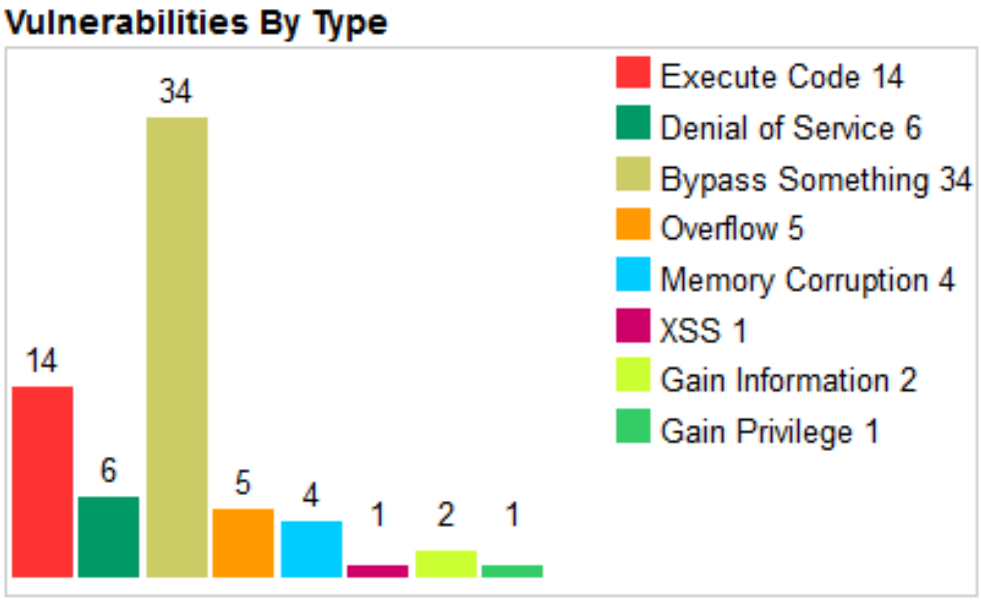
Vulnerability Feeds & Widgets

**Vulnerability Trends Over Time**

| Year | # of Vulnerabilities | DoS | Code Execution | Overflow | Memory Corruption | Sql Injection | XSS | Directory Traversal | Http Response Splitting | Bypass something | Gain Information | Gain Privileges | CSRF | File Inclusion | # of exploits |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2010 | 1 | | 1 | | | | | | | | | | | | |
| 2011 | 3 | | | | | | | | | | | | | | |
| 2012 | 59 | 3 | 1 | | | | | | | 2 | | | | | |
| 2013 | 180 | 1 | 10 | 4 | 4 | | 1 | | | 32 | | | | | 2 |
| 2014 | 115 | 1 | 1 | | | | | | | | | | | | |
| 2015 | 80 | | | | | | | | | | | | | | |
| 2016 | 37 | | 1 | 1 | | | | | | | 1 | 1 | | | |
| 2017 | 24 | 1 | | | | | | | | | 1 | | | | |
| Total | 499 | 6 | 14 | 5 | 4 | | 1 | | | 34 | 2 | 1 | | | 2 |
| % Of All | | 1.2 | 2.8 | 1.0 | 0.8 | 0.0 | 0.2 | 0.0 | 0.0 | 6.8 | 0.4 | 0.2 | 0.0 | 0.0 | |

# Thống kê lỗ hổng JRE - Oracle



# Thống kê lỗ hổng JRE - Oracle

**Oracle » JRE : Security Vulnerabilities**

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **499** Page : 1 (This Page) 2 3 4 5 6 7 8 9 10

Copy Results Download Results

| # | CVE ID | CWE ID | # of Exploits | Vulnerability Type(s) | Publish Date | Update Date | Score | Gained Access Level | Access | Complexity | Authentication | Conf. | Integ. | Avail. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | CVE-2017-3544 | 284 | | | 2017-04-24 | 2017-07-12 | 4.3 | None | Remote | Medium | Not required | None | Partial | None |

Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SMTP to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | CVE-2017-3539 | 284 | | | 2017-04-24 | 2017-07-10 | 2.1 | None | Remote | High | Single system | None | Partial | None |

Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | CVE-2017-3533 | 284 | | | 2017-04-24 | 2017-07-10 | 4.3 | None | Remote | Medium | Not required | None | Partial | None |

Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via FTP to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | CVE-2017-3526 | 284 | | | 2017-04-24 | 2017-07-10 | 7.1 | None | Remote | Medium | Not required | None | None | Complete |

Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).

# Thống kê lỗ hổng JRE - Oracle

## Vulnerability Details : CVE-2017-3526

Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).

Publish Date : 2017-04-24 Last Update Date : 2017-07-10

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

### – CVSS Scores & Vulnerability Types

| | |
|---|---|
| CVSS Score | 7.1 |
| Confidentiality Impact | None (There is no impact to the confidentiality of the system.) |
| Integrity Impact | None (There is no impact to the integrity of the system) |
| Availability Impact | Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.) |
| Access Complexity | Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | |
| CWE ID | 284 |

### + Related OVAL Definitions

### – Products Affected By CVE-2017-3526

| # | Product Type | Vendor | Product | Version | Update | Edition | Language | |
|---|---|---|---|---|---|---|---|---|
| 1 | Application | Oracle | JDK | 1.6 | Update 141 | | | Version Details Vulnerabilities |
| 2 | Application | Oracle | JDK | 1.7 | Update 131 | | | Version Details Vulnerabilities |
| 3 | Application | Oracle | JDK | 1.8 | Update 121 | | | Version Details Vulnerabilities |
| 4 | Application | Oracle | JRE | 1.6 | Update 141 | | | Version Details Vulnerabilities |
| 5 | Application | Oracle | JRE | 1.7 | Update 131 | | | Version Details Vulnerabilities |
| 6 | Application | Oracle | JRE | 1.8 | Update 121 | | | Version Details Vulnerabilities |
| 7 | Application | Oracle | Jrockit | R28.3.13 | | | | Version Details Vulnerabilities |

# Common Weakness Enumeration

*A Community-Developed List of Software Weakness Types*

- A community-developed **list of common** software security **weaknesses**.
- Serves as a **common language, a measuring stick** for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

https://cwe.mitre.org/

# Common Weakness Enumeration

*A Community-Developed List of Software Weakness Types*

## Common Weakness Enumeration

*A Community-Developed List of Software Weakness Types*




**CWE™** is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

### View the List of Weaknesses

by Research Concepts | by Development Concepts | by Architectural Concepts

### Search CWE

Easily find a specific software weakness by performing a search of the CWE List by keywords(s) or by CWE-ID Number. To search by multiple keywords, separate each by a space.

Google Custom Search

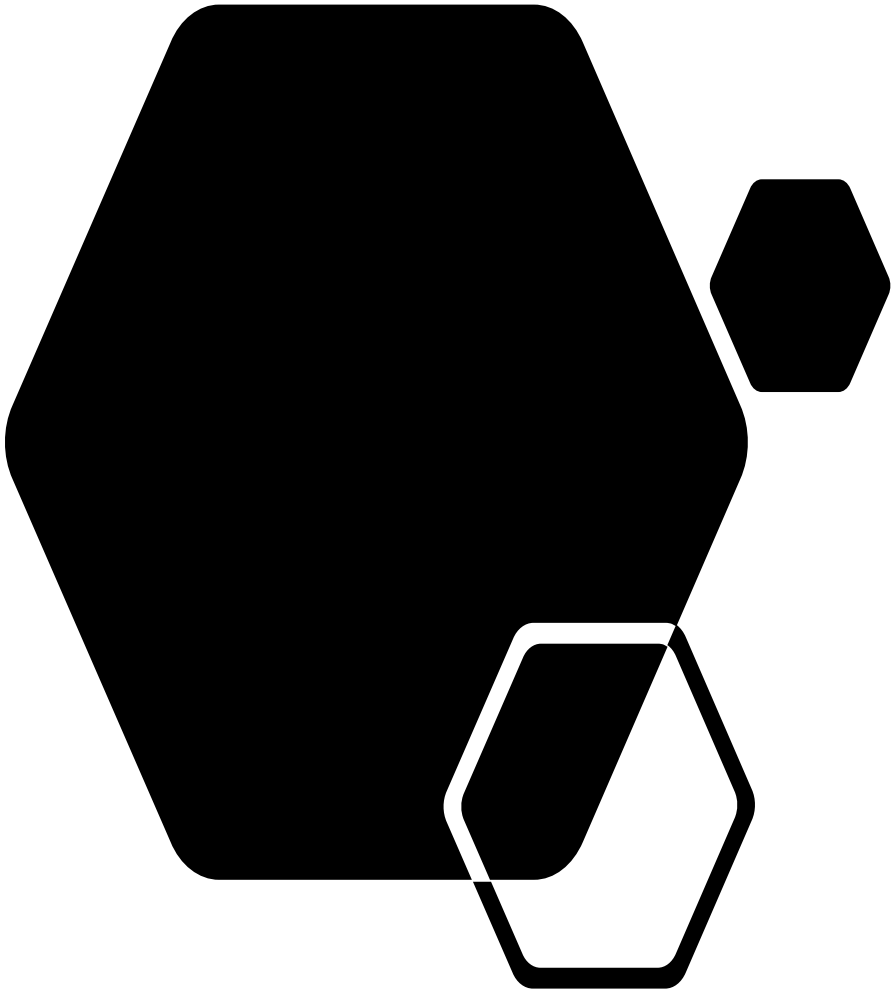
**See the full CWE List page for enhanced information, downloads, and more.**

**Total Software Weaknesses: 716**

**Page Last Updated:** April 03, 2018

# Footprinting

Giai đoạn nhận dạng tất cả tài nguyên trong network, firewall, IDS



# Footprinting

- Footprinting is the first step of any attack on information systems in which an attacker **collects information about a target network** for identifying various ways to intrude into the system

**Types of Footprinting**

| Passive Footprinting | Active Footprinting |
| --- | --- |
| Gathering information about a target **without direct interaction** | Gathering information about the target **with direct interaction** |

**Information Obtained in Footprinting**

| Organization Information | Network Information | System Information |
| --- | --- | --- |
| Employee details, telephone numbers, location, background of the organization, web technologies, etc. | Domain and sub-domains, network blocks, IP addresses of the reachable systems, Whois record, DNS, etc. | OSes and location of web servers, users and passwords, etc. |

# Mục tiêu Footprinting

| | |
|---|---|
| **Know Security Posture** | Footprinting allows attackers to know the **security posture of the target organization** |
| **Reduce Focus Area** | It **reduces the attacker's focus area** to a specific range of IP addresses, networks, domain names, remote access, etc. |
| **Identify Vulnerabilities** | It allows attacker to **identify vulnerabilities** in the target systems in order to select appropriate exploits |
| **Draw Network Map** | It allows attackers to **draw a map or outline the target organization's network infrastructure** to know about the actual environment that they are going to break |

# Nmap: Scan và nhận dạng dịch vụ

- Port scanner dùng phổ biến nhất
- Tính năng:
  - Nhận dạng host (live or die)
  - Scan port TCP, UDP đang mở
  - Phát hiện firewall
  - Lấy version của dịch vụ đang chạy trên host
  - Tìm và khai thác lỗ hổng

# Nmap: Scan và nhận dạng dịch vụ

- Kiểm tra máy đang hoạt động, gửi ICMP:
  **nmap –sn <IP>**
- Kiểm tra port đang mở:
  **nmap <IP>**
- Xem phiên bản của dịch vụ và đoán OS
  **nmap -sV –O <IP>**

```
root@kali:~# nmap -sV -O 192.168.56.102

Starting Nmap 6.47 ( http://nmap.org ) at 2015-06-09 21:43 CDT
Nmap scan report for 192.168.56.102
Host is up (0.00026s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-
1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/...)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
443/tcp  open  ssl/http    Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-
1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/...)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
5001/tcp open  ovm-manager Oracle VM Manager
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8081/tcp open  http        Jetty 6.1.25
MAC Address: 08:00:27:3F:C5:C4 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at http://
Nmap done: 1 IP address (1 host up) scanned in 14.14 seconds
```

# Nmap: Scan và nhận dạng dịch vụ

- **Tham số khác:**
  - -sT: SYN scan, chậm, bị ghi log trên server, ít bị IDS phát hiện
  - -Pn: bỏ ping test, scan tất cả mục tiêu chỉ định
  - -p N1,N2,…,Nn: scan những port chỉ định
  - --script=script_name: run script trên các port (mở) mục tiêu[1]

[1]: https://nmap.org/nsedoc/scripts/

# Scan và nhận dạng dịch vụ

**Công cụ khác có sẵn trên Kali Linux:**

- unicornscan
- hping3
- masscan
- amap
- Metasploit scanning modules

# Nhận dạng Web App Firewall

- WAF:

  Thiết bị hay phần mềm kiểm tra package gửi đến server → nhận dạng và block mã độc

- Yêu cầu: xác định và nhận dạng WAF → tránh bị chặn khi pentest

# Nhận dạng Web App Firewall

- Scan script bằng Nmap:

  **nmap -p 80,443 --script=http-waf-detect <IP/domain>**

- Script xác định chính xác hơn:

  **nmap -p 80,443 --script=http-waf-fingerprint <IP/domain>**

- Công cụ khác trong Kali:

  **wafw00f <IP/domain>**

# Xem mã nguồn

Hiểu logic của chương trình → phát hiện lỗ hổng → có thể bypass

- Thường sử dụng Javascript, third-party library hay framework để kiểm tra input

# Sử dụng Firebug

- Firebug cho phép:
  - Phân tích và chỉnh sửa trạng thái cơ bản
  - Phân tích thành phần web: css class, frame,…
  - Hiển thị Dom Object, lỗi code, request và respond giữ client-sever
- Chức năng:
  - Console: hiện lỗi, cảnh báo,…
  - HTML: hiện source và cho phép chỉnh sửa
  - CSS: hiện và chỉnh sửa css
  - Script: hiện toàn bộ code HTML, có thể đặt break point
  - DOM: hiện DOM Object
  - Net: hiển thị request và respond
  - Cookies: chứa cookie được set bởi server

# Lấy và chỉnh sửa cookie

- Cookie là mẫu thông tin được gửi từ server đến browser để lưu thông tin cục bộ:
  - color theme configuration
  - object arrangement preferences
  - previous activity
  - (more importantly) the **session identifers**
- Trên OWASP Mantra menu, chọn **Tools \ Application Auditing \ Cookies Manager +**
- Có thể edit, del, tạo mới → chèn mã độc, cướp quyền.
- Ví dụ: sửa Http Only = true;

# Lợi dụng robots.txt

- **Robots.txt:** được dùng bởi web server, báo cho search engine file, folder không được index
- **Mục tiêu:** tìm ra file, folder không được hiện thị với user bình thường

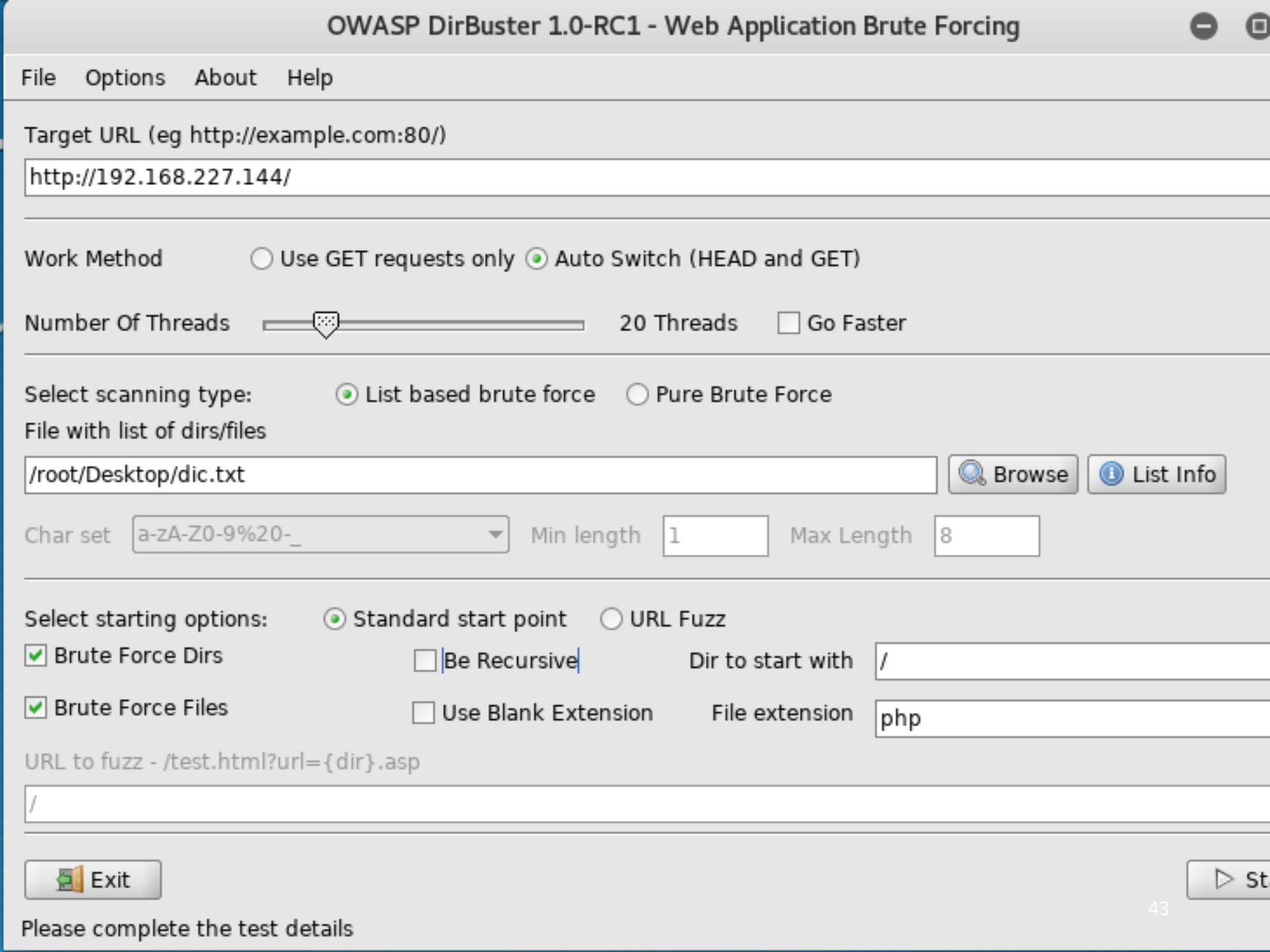
  Ví dụ: login nội bộ, admin của CMS,…
- **Cách sử dụng:**

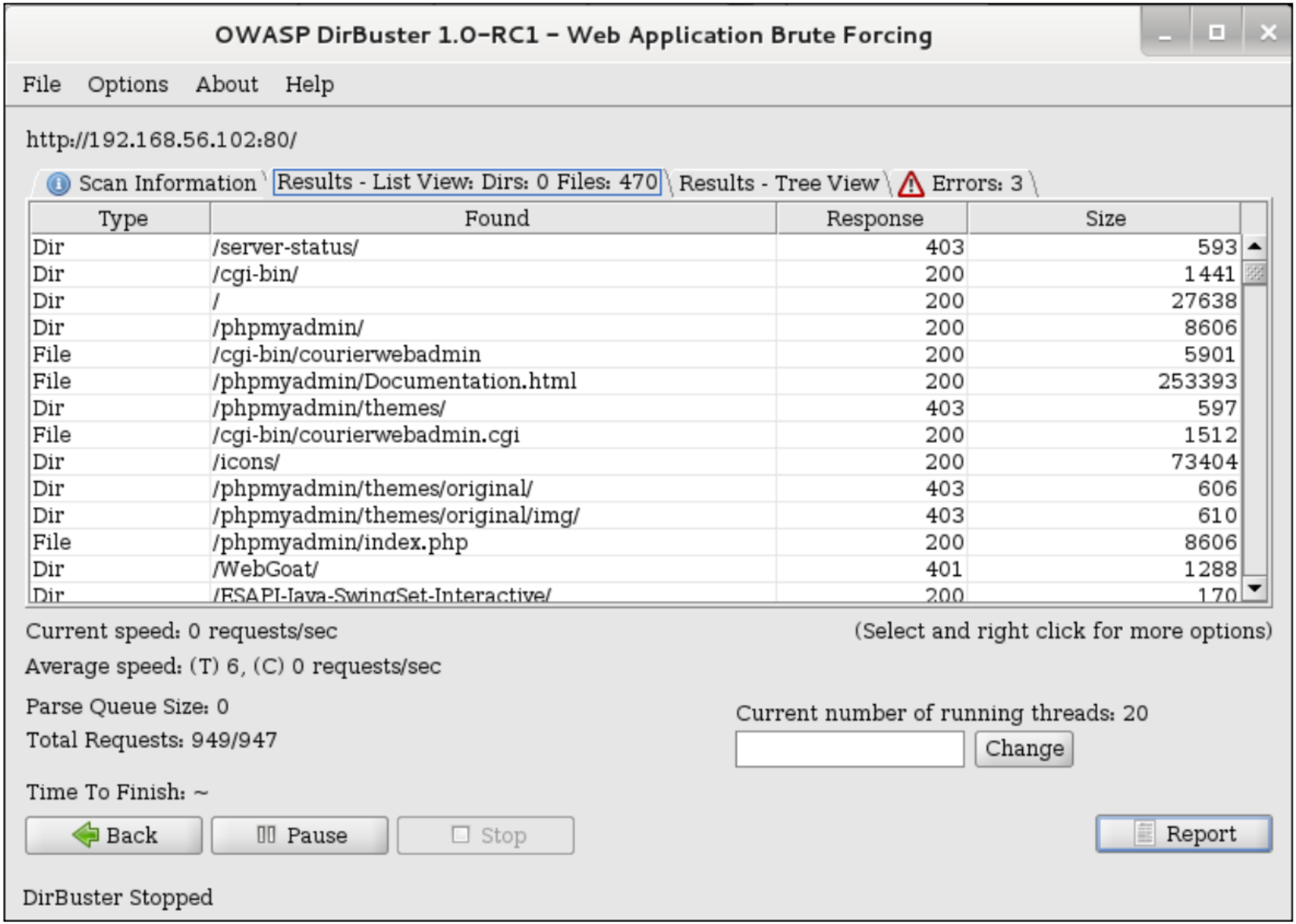
  **<IP/Domain>/robots.txt**

# Tìm file và folder với DirBuster

- Công cụ khám phá File và Folder tồn tại trên web server bằng cách brute force
- **Cách sử dụng:**
  - Bước 1: tạo file dictionary.txt chứa text muốn tìm
  - Bước 2: Mở **Applications | Kali Linux \ Web Applications \ Web Crawlers \ dirbuster** và thiết lập
  - Bước 3: qua tab Results để xem kết quả.

    Giá trị Respond code:
    - 200. OK: file, folder tồn tại và có thể read
    - 404. File not found
    - 301. Moved permanently: chuyển đến URL cho sẵn
    - 401. Unauthorizedd: yêu cầu quyền để truy cập
    - 403. Forbidden: request hợp lệ nhưng server từ chối trả lời


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Target URL (eg http://example.com:80/)
http://192.168.227.144/
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
20 Threads
Go Faster
Select scanning type:
List based brute force
Pure Brute Force
File with list of dirs/files
/root/Desktop/dic.txt
Browse
List Info
Char set
a-zA-Z0-9%20-_
Min length
1
Max Length
8
Select starting options:
Standard start point
URL Fuzz
Brute Force Dirs
Be Recursive
Dir to start with
/
Brute Force Files
Use Blank Extension
File extension
php
URL to fuzz - /test.html?url={dir}.asp
/
Exit
Please complete the test details


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
http://192.168.56.102:80/
Scan Information
Results - List View: Dirs: 0 Files: 470
Results - Tree View
Errors: 3
Type
Found
Response
Size
Dir /server-status/ 403 593
Dir /cgi-bin/ 200 1441
Dir / 200 27638
Dir /phpmyadmin/ 200 8606
File /cgi-bin/courierwebadmin 200 5901
File /phpmyadmin/Documentation.html 200 253393
Dir /phpmyadmin/themes/ 403 597
File /cgi-bin/courierwebadmin.cgi 200 1512
Dir /icons/ 200 73404
Dir /phpmyadmin/themes/original/ 403 606
Dir /phpmyadmin/themes/original/img/ 403 610
File /phpmyadmin/index.php 200 8606
Dir /WebGoat/ 401 1288
Dir /ESAPI-Java-SwingSet-Interactive/ 200 170
Current speed: 0 requests/sec
(Select and right click for more options)
Average speed: (T) 6, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 949/947
Current number of running threads: 20
Change
Time To Finish: ~
Back
Pause
Stop
Report
DirBuster Stopped

# Trích xuất danh sách từ CeWL

- Lấy danh sách từ được sử dụng bởi ứng dụng để brute force trang login
- **Câu lệnh:**
  - Help: **cewl --help**
  - Lấy danh sách từ với độ dài tối thiểu 5 và đếm số lượng: **cewl -w cewl_WackoPicko.txt -c -m 5 <URL>**
- **Công cụ khác:**
  - Crunch: có sẵn trên Kali, tạo DS dựa trên tập kí tự user cung cấp
  - Wordlist Maker (WLM): tạo DS từ tập ký tự và rút trích từ text file hoặc web
  - Common User Password Profler (CUPP): tạo DS mật khẩu cho user phổ biến

# Tạo từ điển với John the Ripper

- Công cụ crack mật khẩu được ưu thích:
  - Nhận diện hầu hết thuật toán mã hóa và hash
  - Hỗ trợ tấn công từ điển và brute force
  - Áp dụng rule để chỉnh sửa và mở rộng từ điển
- **Câu lệnh:**
  - Hiện thị những mật khẩu dùng để crack

    **john --stdout --wordlist=dictionary.txt**
  - Áp dụng luật để mở rộng từ điển (chữ Hoa thường, prefix, suffix, chuyển ký tự thành số và symbol)

    **john --stdout --wordlist=dictionary.txt --rules**
  - Lưu từ điển

    **john --stdout --wordlist= dictionary.txt --rules > Finaldict.txt**

# Tìm File và Folder với ZAP

OWASP ZAP (Zed Attack Proxy) là công cụ linh hoạt:

- proxy, passive and active vulnerability scanners, fuzzer, spider, HTTP request sender và nhiều đặc trưng khác
- Forced Browse: tính năng mới (DirBuster)

# Tìm File và Folder với ZAP

- Cần sử dụng ZAP như proxy cho trình duyệt web
- Mở ZAP: **Applications | Kali Linux \ Web Applications \ Web Application Analysis \ owasp-zap**
- Trên Mantra hay Iceweasel, chọn **Preferences \ Advanced \ Network,** trong **Connection** chọn **Settings…**
- Chọn **Manual proxy configuration**:
  - HTTP proxy: 127.0.0.1:8080
  - Check option: Use this proxy for all protocols

# Tìm File và Folder với ZAP

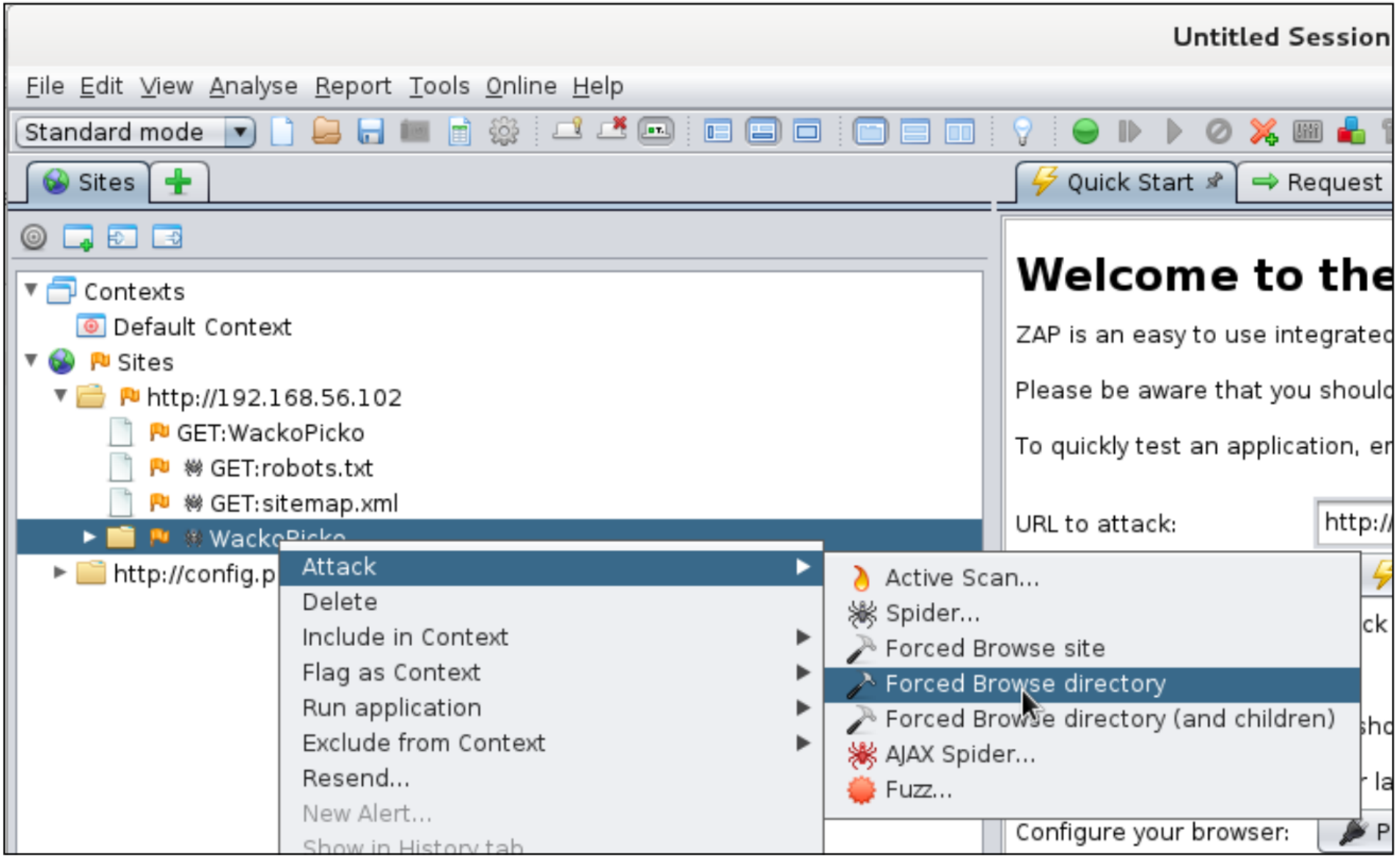
- Thiết lập file chứa tên thư mục (từ điển):

  **Menu** chọn **Tools \ Options \ Forced Browse** và chọn **Select File…**

  Trong Kali có nhiều word list tại đường dẫn:

  **/usr/share/wordlists/dirbuster/**

  Chọn directory-list-lowercase-2.3-small.txt và **Open**
- Duyệt web và xem cấu trúc cây của host vừa duyệt
- Tại **Sites Tab**, chọn folder (URL) cần tấn công, nhấp chuột **Phải** và chọn **Attack \ Forced Browse directory** và xem kết quả tại tab **Forced Browse** phía dưới


Untitled Session
File Edit View Analyse Report Tools Online Help
Standard mode
Sites
Quick Start
Request
Contexts
Default Context
Sites
http://192.168.56.102
GET:WackoPicko
GET:robots.txt
GET:sitemap.xml
http://config.p
Attack
Delete
Include in Context
Flag as Context
Run application
Exclude from Context
Resend...
New Alert...
Active Scan...
Spider...
Forced Browse site
Forced Browse directory
Forced Browse directory (and children)
AJAX Spider...
Fuzz...
Welcome to the
ZAP is an easy to use integrated
Please be aware that you should
To quickly test an application, en
URL to attack:
Configure your browser:

- Bài tập CTF làm thêm

https://overthewire.org/wargames/natas/

# Tài liệu tham khảo

- https://www.most.gov.vn/Images/editor/files/1649-CATTT-NCSC%20Tai%20lieu%20huong%20dan.PDF

# Bảo mật web và ứng dụng

Trường ĐH CNTT TP. HCM