

Penetration Testing

Lecture-12

Department of CSE, IUT



Contents

- Penetration Testing
- Penetration Tester
- Necessity of Penetration Testing
- Benefits and Drawbacks
- Types of Penetration Testing
- Penetration Testing Process



Penetration Testing

- Definition: The art of testing a running application to find vulnerabilities. It is also called “Ethical Hacking”. (abbreviated as ***Pen Testing*** also)
- Penetration testing assesses security by actively trying to find exploitable vulnerabilities
 - It’s a white hat activity for good purpose.



Who, and how

- Pen testers employ **ingenuity** and **automated tools**
 - To rapidly explore a system's attack surface, looking for weaknesses to exploit
- Typically carried out by **a separate group within, or outside**, an organization, **separate from developers**
 - It allows a fresh look to the system like hackers.
 - It is done by ethical hackers called red teams/tiger teams etc.
- Given varied access to system internals
 - **No access**, like outside attacker
 - **Full access**, like a knowledgeable insider



Why we need *Pen Testing*?

- A Professional's view:

70% messing with parameters

If the URL is <http://buyme.com/buy?item=1&price=10.00>

Then change it to:

- /buy?item=1&price=0.05
- /buy?item=10&price=0.05
- /buy?item=1&price=10.00<script>alert("Hello there!!");</script>
- /buy?item=1&price=0.05 ‘

Clients parameter input
(unwisely) trusted?

Susceptible to XSS?

Susceptible to
Injection?



Why we need *Pen Testing*?

10% default passwords

- Always research the default password and try it. Works way more than you'd think

10% hidden files and directories

- Look through the manuals for clues
- Directory brute forcing

10% other

- Authentication problems (bypass, replays...)
- Insecure web services
- Configuration page give away root password



Benefits

- Ensure total system's security
- Pen-testing teaches you things that security planning will not
 - What are the vulnerability scanners missing?
- Are your users and system administrators actually following their own policies?
 - host that claims one thing in security plan but it totally different in reality
- “Feel good” factor
 - Produces evidence of real vulnerabilities that would otherwise have gone unfixed
 - Thus results in a clear improvement to security



Benefits

- Raises security awareness
- Helps identify weakness that may be leveraged by insider threat or accidental exposure.
- Provides Senior Management a realistic view of their security posture
- If I can break into it, so could someone else!



Drawbacks

- Absence of penetrations is not evidence of security
 - After fixing any issues there may be others still exist.
- Changes to the system necessitate a retest
 - Security is not compositional: a change to one component may render another component insecure.
 - So must retest the entire system
 - Changes are common in software development, so frequent testing is not possible or can be expensive.
- Nevertheless, Penetration testing worth doing



Penetration Tester versus Hacker

- Pen Tester's have prior approval from Senior Management
- Hackers have prior approval from themselves.
- Pen Tester's social engineering attacks are there to raise awareness
- Hackers social engineering attacks are there to trick legitimate users give away sensitive information



Types of Penetration Testing

- **Network Penetration Testing**

Testing a network environment for potential security vulnerabilities.

- **Web Application Penetration Testing**

Web application host critical data like credit card number, username, password. It is common nowadays.

- **Mobile Application Penetration Testing**

Newest type of penetration testing, as the emerge of mobile application. It also hosts user sensitive information.

- **Social Engineering Penetration Testing**

The organization ask to attack its users. This is where you use spread phishing attacks and browser exploits to trick a user into doing things that they did not intend to do.

- **Physical Penetration Testing**

Rarely doing. Walk into the organization building physically and test physical security controls such as locks and RFID mechanisms.



Categories based on scope of Pen Testing

- **Black Box**

- which provides only basic or no information about the specified target except the company name
- No info about target OS, OS version, server info, open ports etc.
- In web application/mobile application no source code will be provided
- Works like real life hacking

- **White Box**

- All the information about the target is provided
- Info about OS, versions, server, ports, network range etc., are given.
- Source code of web application is given, so, static/dynamic analysis can be performed

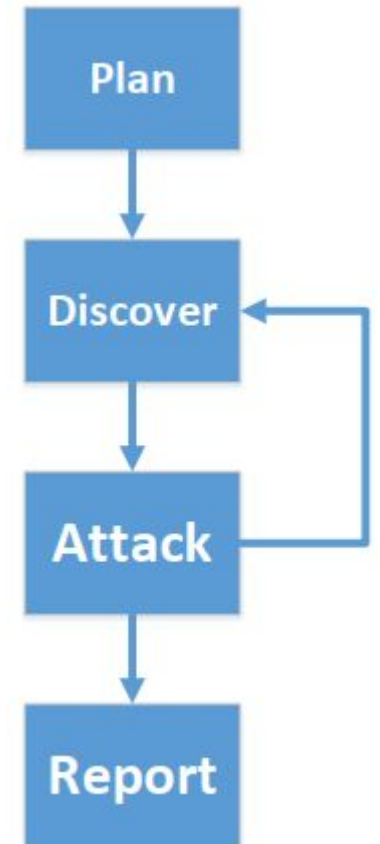
- **Gray Box**

- It is a combination of black and white box testing.
- For network pen testing, IP will be given, however, which services are running will not be disclosed
- For web app, server and database name are given without other details.



Penetration Testing: Two Primary Phases

- Information gathering
 - Understand environment and the application
 - Determine access points, inputs
- Methodically test across a variety of controls
 - Configuration and deployment management
 - Identity, authentication, authorization session management
 - Input validation
 - Error handling
 - Cryptography
 - Business logic
 - Client side evaluation



Planning

- Penetration Test may be included in a scheduled audit or independently
- May be announced or unannounced
- Define the scope and rules of engagement

Try to answer such questions:

- Who performs the Pen testing?
- What is the scope of Pen testing?



Rules of Engagement

- Every pen testing comprise of a rules of engagement, which defines
 - How a pen testing would be laid out
 - What methodology would be used
 - Start and end dates
 - The milestones
 - The goals of penetration test
 - The liabilities and responsibilities etc.,
- Ethical hackers and organization should be mutually agreed upon this.

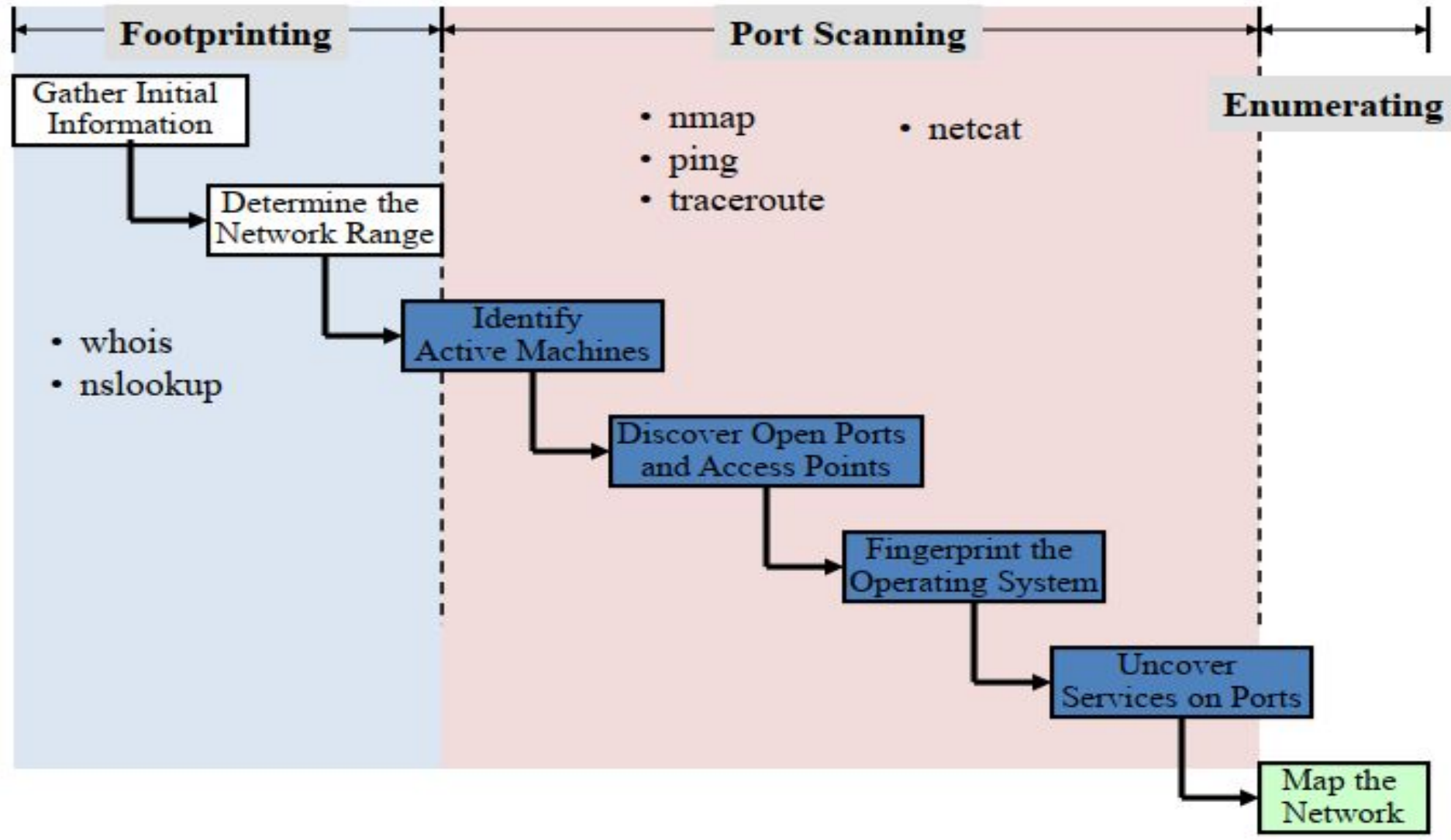


Information Gathering

- Goal: discover as much information about the system under evaluation
- Methods
 - WHOIS
 - Nmap (<https://www.holmsecurty.com/blog/what-is-nmap>)
 - Network Enumeration and Scanning
 - Google Searching and Hacking
 - Website browsing
 - Social Media



Information Gathering Discovery Phase



Nmap (whois)

[<https://nmap.online/>]



Nmap (whois)

nmap --script whois-domain.nse du.ac.bd

```
domain:      BD

organisation: Posts and Telecommunications Division
address:     Ministry of Posts, Telecommunications and Information Technology
address:     Bangladesh Secretariat
address:     Abdul Ghani Road
address:     Dhaka 1000
address:     Bangladesh

created:     1999-05-20
changed:     2017-03-03
source:      IANA

contact:     administrative
name:        Director (Telecom)
organisation: Posts and Telecommunications Division
address:     Ministry of Posts, Telecommunications and Information Technology
address:     Bangladesh Secretariat
address:     Abdul Ghani Road
address:     Dhaka 1000
address:     Bangladesh
phone:       +880 2 9574446
fax-no:      +880 2 9515599
e-mail:      dirt@ptd.gov.bd

nserver:     BD-NS.ANYCAST.PCH.NET 2001:500:14:6108:ad:0:0:1 204.61.216.108
nserver:     DNS.BD 123.49.12.112 2407:5000:88:5:0:0:0:3
nserver:     JAMUNA.BTCL.NET.BD 203.112.194.231 2407:5000:88:4:0:0:0:231
nserver:     SURMA.BTCL.NET.BD 203.112.194.232 2407:5000:88:4:0:0:0:232

contact:     technical
name:        Divisional Engineer (Administration and Coordination)
organisation: Bangladesh Telecommunications
organisation: Company Limited (BTCL)
address:     Telejogajog Bhaban, 37/E, Eskaton Garden
address:     Dhaka 1000
address:     Bangladesh
phone:       +880 2 9331798
fax-no:      +880 2 9357877
e-mail:      deanc@btcl.com.bd
```



Information Gathering: Google Searching and Hacking

- Google Advanced Operators
 - Standard part of a google query
 - Syntax (no spaces)

operator:search_term



Information Gathering (Google hacking)

Advanced Operators at a Glance

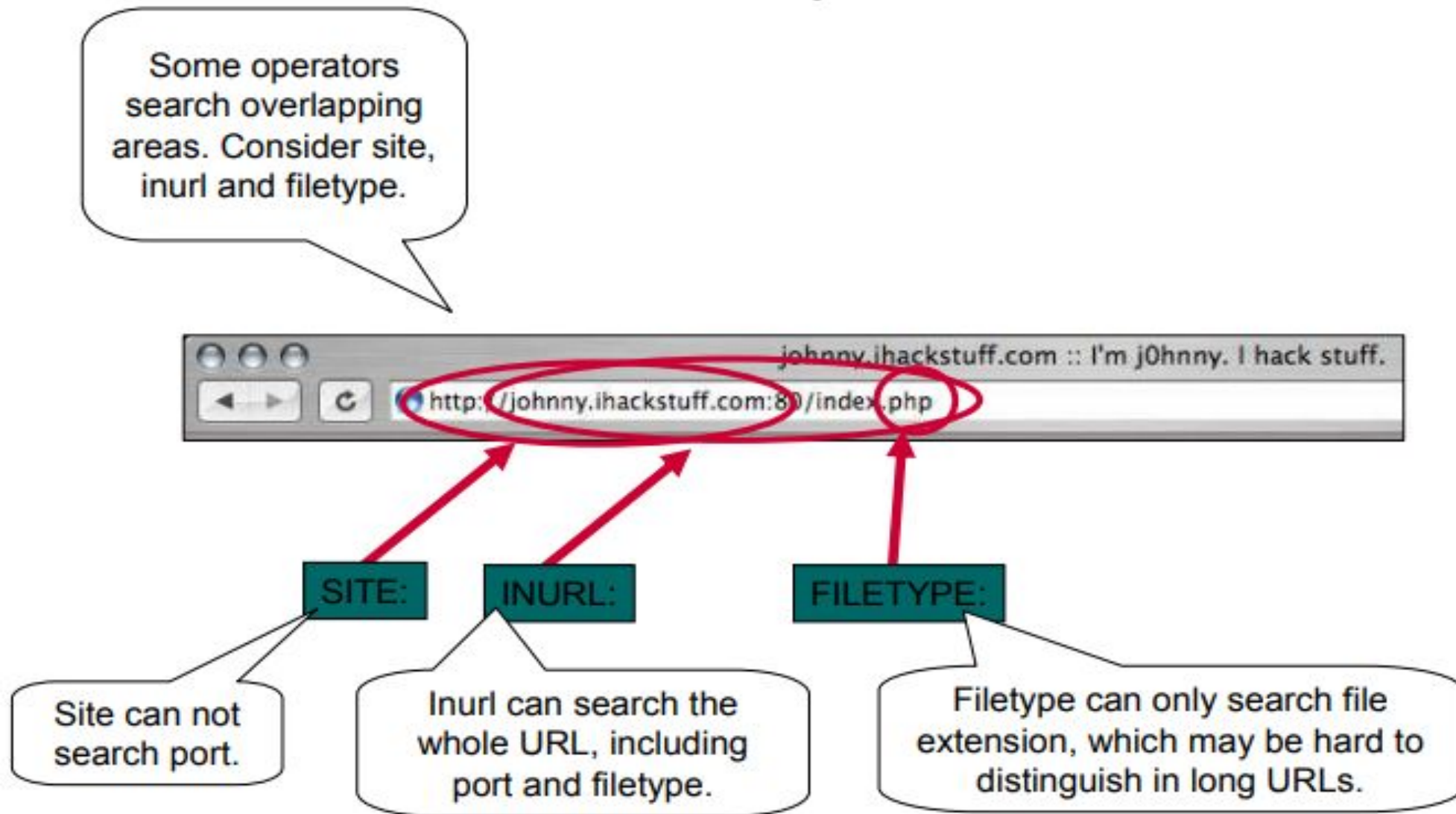
Advanced operators can be combined in some cases.

In other cases, mixing should be avoided.

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

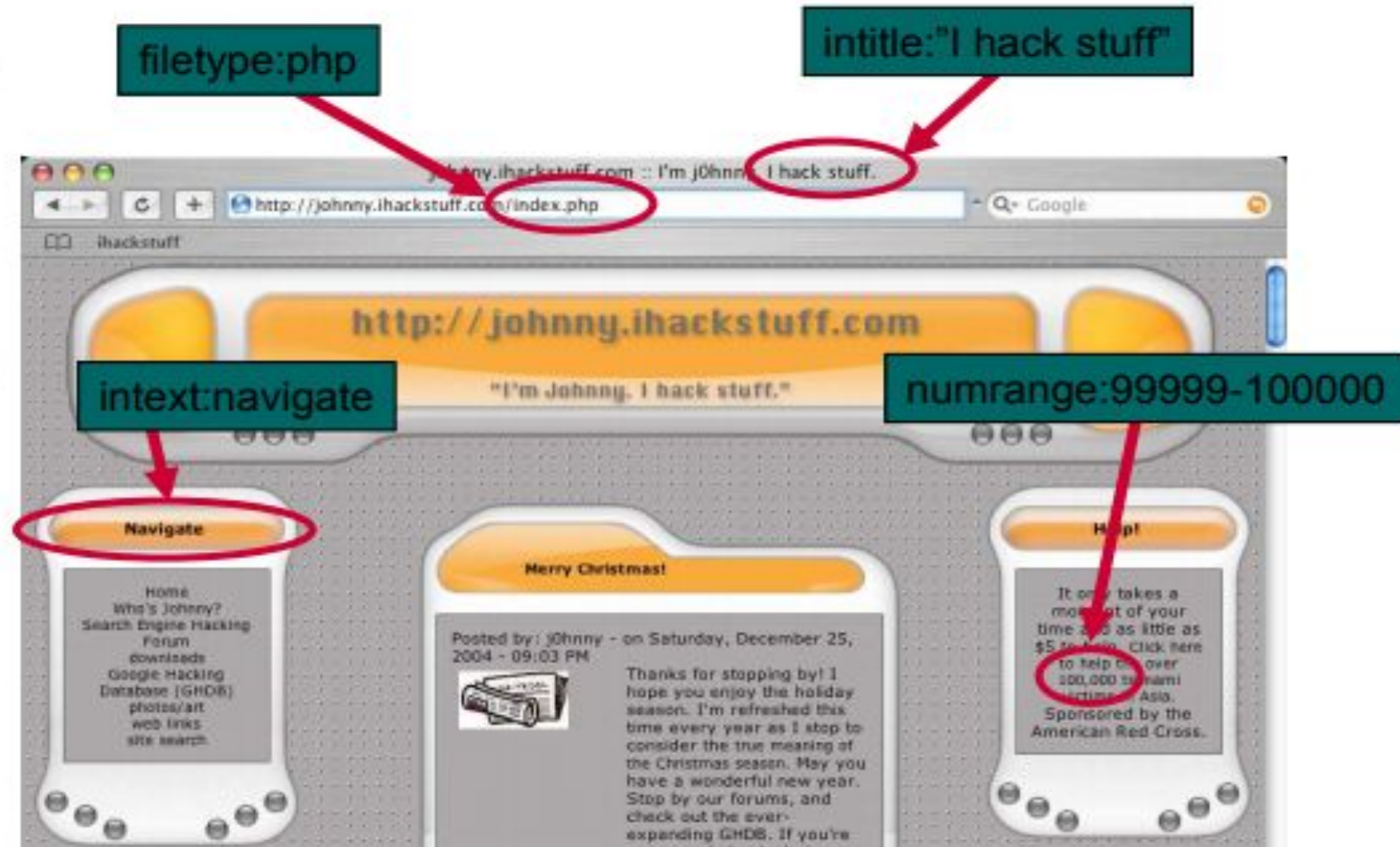
Some operators can only be used to search specific areas of Google, as these columns show.

Information Gathering (Google hacking)



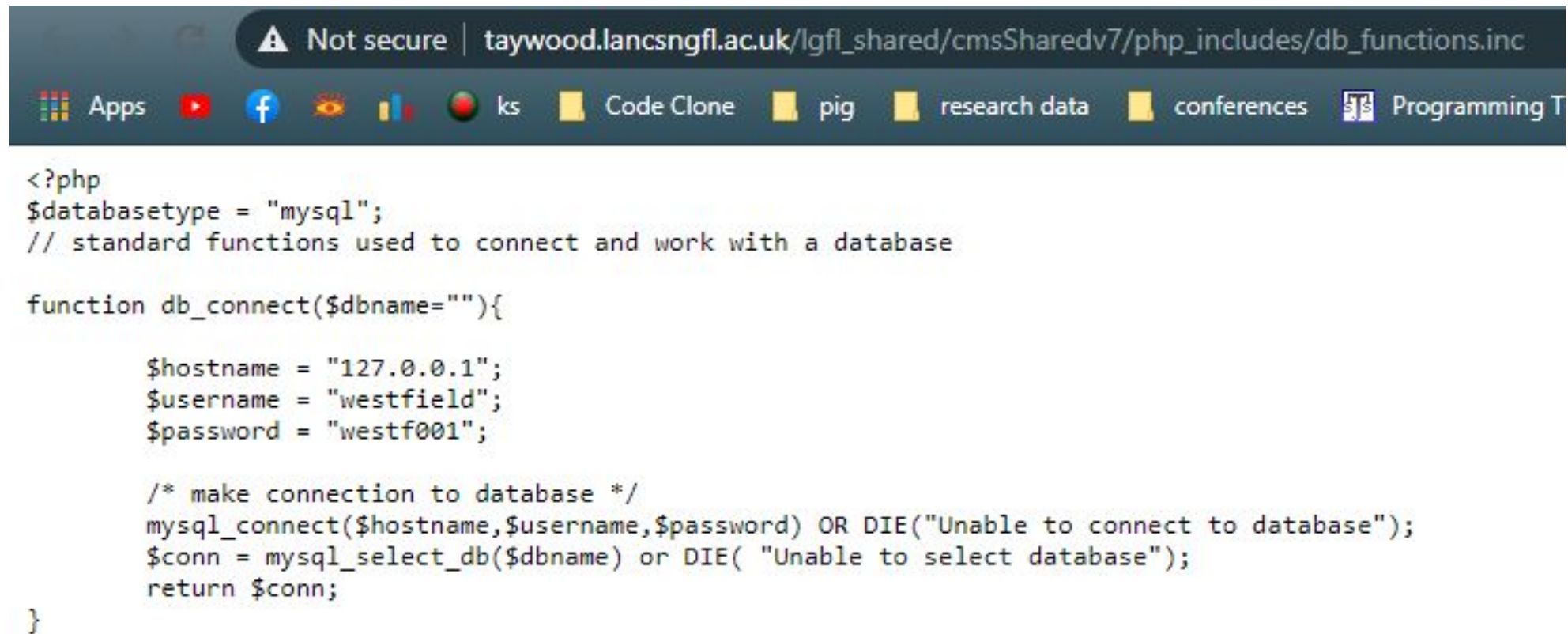
Information Gathering (Google hacking)

There are many ways to find the same page. These individual queries could all help find the same page.



Information Gathering (SQL Passwords)

Query filetype:inc intext:mysql_connect



The screenshot shows a web browser window with the address bar displaying "taywood.lancsngfl.ac.uk/lgfl_shared/cmsSharedv7/php_includes/db_functions.inc". The browser's address bar also shows a "Not secure" warning. Below the address bar, there is a navigation bar with several icons and labels: "Apps", "YouTube", "Facebook", "Eye", "Bar chart", "ks", "Code Clone", "pig", "research data", "conferences", and "Programming T". The main content area of the browser displays the following PHP code:

```
<?php
$databasetype = "mysql";
// standard functions used to connect and work with a database

function db_connect($dbname=""){

    $hostname = "127.0.0.1";
    $username = "westfield";
    $password = "westf001";

    /* make connection to database */
    mysql_connect($hostname,$username,$password) OR DIE("Unable to connect to database");
    $conn = mysql_select_db($dbname) or DIE( "Unable to select database");
    return $conn;
}
```



Information Gathering

- Use the website / web application
- Information is revealed in ...
 - HTML Text (form names, parameters, comments)
 - URLs
- Parameters
 - HTTP Request and Response Headers



Tricks of Pen tester

A pen tester approaches a target knowing ..

- The workings of the target domain (e.g., the web)
- How systems are built in that domain
 - Protocols (e.g., HTTP, TCP, ...)
 - Languages (e.g., PHP, Java, Python,...)
 - Frameworks (e.g., Laravel, Rails, .Net, Spring)
- Common weaknesses in the software/system
 - Bugs (e.g., SQL injections, XSS, CSRF,...)
 - Misconfiguration, bad design (e.g., default passwords, hidden files,...)



Fuzzing

- Fuzzing or fuzz testing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program.
- The program is then monitored for exceptions such as crashes, failing built-in code assertions, or potential memory leaks.
- For example: In authentication
 - Password:
you can try a lots of known password automatically to find the password.



Tools

- Pen testers use tools to
 - Probe a target
 - Gather information and test hypotheses about it
 - Exploit a vulnerability (or attempt to)
- Which tools depends on the **goal**, and the **target**
 - If an enterprise network, want to find, probe, and exploit machines, routers, topology, etc.
 - If a single machine, want to consider installed software, running programs, interesting files
 - If a single program, want to explore and exploit possible inputs and interactions



Tools overview

- Nmap for network scanning
- Zap web proxy for probing, exploitation
- Metasploit for general-purpose exploitation
- Kali Linux



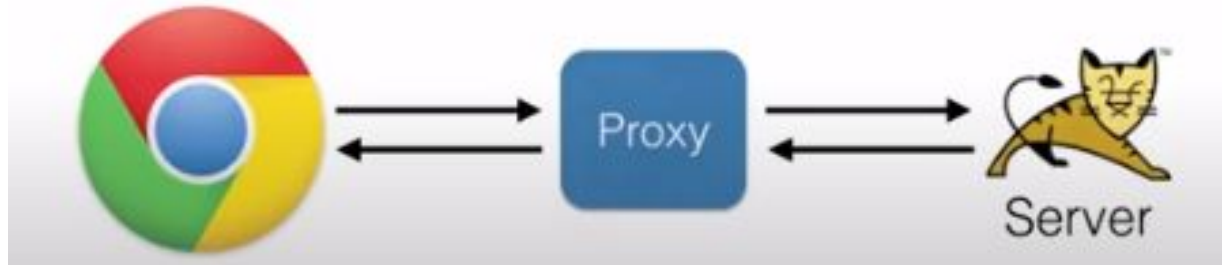
Nmap for network probing

- Nmap stands for “network mapper”. Figures out
 - What **hosts** are available on the network,
 - What **services** (application name and version) those hosts are offering,
 - What **operating systems** (and OS versions) they are running,
 - What type of **packet filters/firewalls** are in use
 - ... and more
- Works by **sending raw IP packets** into the network and **observing the effects**
- Free, open source <https://nmap.org/>



Web Proxies

- Web applications are common pen testing targets
- Web proxies sit between the browser and server
 - Displaying exchanged packets
 - Modifying them as directed by the testing



- Some proxies have additional features for vulnerability scanning/exploitation, site probing, etc.

Zap for proxy

OWASP Zed Attack Proxy (Zap)

- A GUI-based inspection/modification of captured packets
- Can set “breakpoints” to allow packets through until a certain condition is met
- Additional features
 - Active scanning: attempts XSS, SQL injection, etc.
 - Fuzzing: context-specific payloads
 - **Spider**: explores a site to construct a model of its structure
- Free, Open-source <https://www.zaproxy.org/>
- commercial tool like **Burp suite**



Zap for proxy

Untitled Session - 20200807-114155 - OWASP ZAP 2.9.0

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites + Quick Start Request Response +

Header: Text Body: Text

Contexts
Default Context
Sites

POST http://localhost/dvwa/login.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
Referer: http://localhost/dvwa/login.php
Cookie: security=impossible; PHPSESSID=7e1ca3jdccdbn031d6h9cp9ce7
Host: localhost

username=ZAP&password=ZAP&Login=Login&user_token=%3C%21--%23EXEC+cmd%3D%22ls+%2F%22--%3E

History Search Alerts Output Spider Active Scan Fuzzer +



Metasploit

Metasploit advanced open-source **platform** for **developing, testing, and using exploit code**.

- Boasts and **extensible model** through which payloads, encoders, no-op generators, and exploits can be integrated.
- Scripting attacks
 - **Probe** remote site looking for vulnerable services
 - **Construct** payload based on versions, other features
 - **Encode** payload to avoid detection
 - **Inject** payload
 - **Wait** for shellcode to connect back; **command prompt!**
- **msfconsole** --- **interactive console** for executing metasploit commands
- **msfpayload, msfencode** --- generate (stealthy) shellcode



Kali

- Kali is a Linux distribution with many open-source pen testing tools installed and configured
- The ones we have already mentioned
 - Nmap, Zap, Metasploit, Burp Suite
- And dozens more
 - John the Ripper for password cracking
 - Valgrind for dynamic binary analysis
 - Reaver for wifi password cracking
 - Peepdf for scanning PDF files for attack vectors
 - ... and more

<https://www.kali.org/>

These tools can be used for nefarious purposes



Vulnerabilities Exploited by Penetration Testing

- Misconfigurations
- Buffer Overflows
- Insufficient Input Validation
- File Descriptor Attacks
- Race Conditions
- Incorrect File and Directory Permissions



Report Writing

Pen testing report should contain the following information

- Executive summary
- Engagement Highlights
- Vulnerabilities summary
- Details of performed attacks
- Remediation of vulnerabilities



Suggested books

- ETHICAL HACKING AND PENETRATION TESTING GUIDE
RAFAY BALOCH
- PENETRATION TESTING A Hands-on Introduction to Hacking
Georgia Weidman



References

- Ernest Lopez & Matt Linton, NASA – Penetration Testing and Vulnerability Assessment, August 2010
- Kali: <https://www.kali.org/>
- Google Hacking for Penetration Testers:
https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Lon_g.pdf
- Google Hacking Database: <http://www.hackersforcharity.org/ghdb/>
- OWASP Testing Guide, V4:
https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf
- OWASP Zed Attack Project:
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

