iNURTURE
Education Solutions
TOMORROW'S HERE

Chapter 2.1

Web Server hacking and Applications

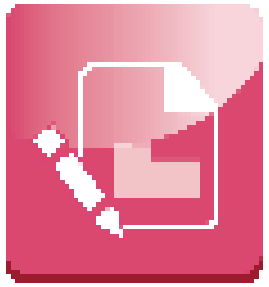
Aim

To describe the students with various attacks on a web server and web applications and enrich them with the steps that must be taken to counter measure the attacks.

Instructional Objectives

After completing this chapter, you should be able to:

- Explain how Web server and application work
- List the types of Web server vulnerabilities
- Identify the attacks against web servers
- Outline the objective of Web application hacking
- List various web application threats along with their countermeasures
- Explain how a web-based password cracker works



Learning Outcomes

At the end of this chapter, you are expected to:

- Explain various ways to increase the security of the web server against attacks
- Summarise the stages of web application attacks
- Discuss how various web application threats can be avoided

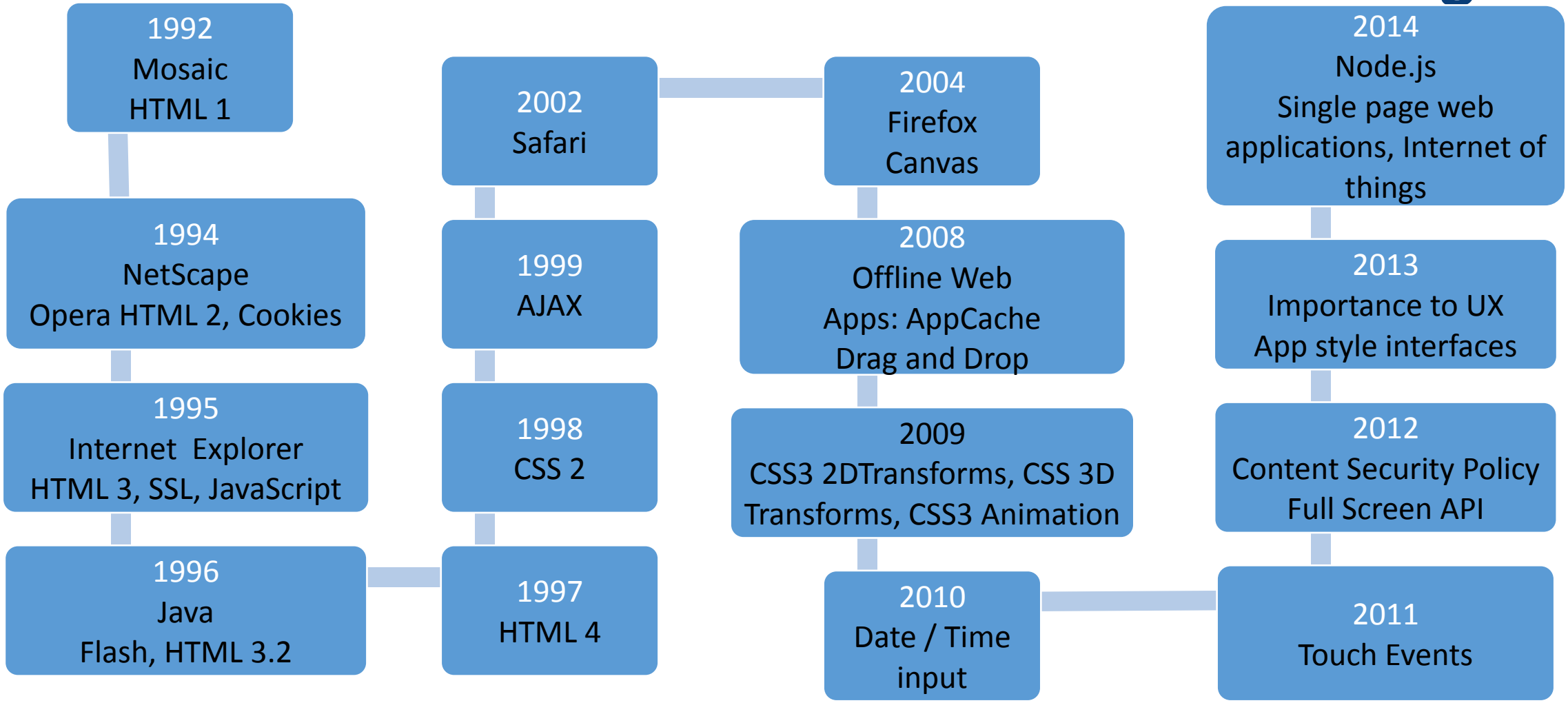
Web Server Hacking

Introduction to Web Server Hacking

Web has become vulnerable component

Unbelievable transformation in terms of visuals, content, design and user-experience

Evolution of Web browser and related Technologies



Nmap (Network Mapper)

- Nmap is a free network security scanner
- Compatible for Windows, Linux and Mac
- Functions of Nmap are
  - Discovers network components like hosts and servers
  - Determines open ports and services running on a host machine
  - Determines the operating system on the host machine

Nmap (Network Mapper) Commands

Objective	Syntax
Scan a single host	nmap 192.168.1.1
Scan an IP address	nmap www.yahoo.com
Scan multiple a host for additional information	nmap –v www.yahoo.com
Scan multiple IP addresses	nmap 192.168.1.1 192.168.1.2 192.168.1.3 nmap 192.168.1.1,2,3
Scan range of IP addresses	nmap 192.168.1.1-20
Scan range of IP addresses with a wildcard	nmap 192.168.1.*
Scan an entire subnet	nmap 192.168.1.0/24
To detect if the host is protected by firewall	nmap –sA/ 192.168.1.254
To scan a host behind a firewall	nmap –PN 192.168.1.1
Scan a network to detect servers and devices running on it (Also known as host discovery or ping scan)	nmap –sP 192.168.1.0/ 24
To display only open ports of the network	namp – open192.168.1.1

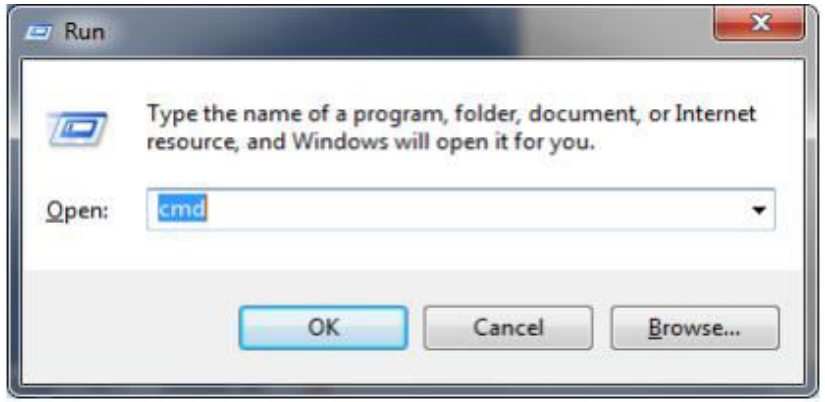
Details of Nmap with different switches and their functions

To detect if the host is protected by firewall	**nmap –sA/ 192.168.1.254**
To scan a host behind a firewall	nmap –PN 192.168.1.1
Scan a network to detect servers and devices running on it (Also known as host discovery or ping scan)	nmap –sP 192.168.1.0/ 24
To display only open ports of the network	namp – open192.168.1.1

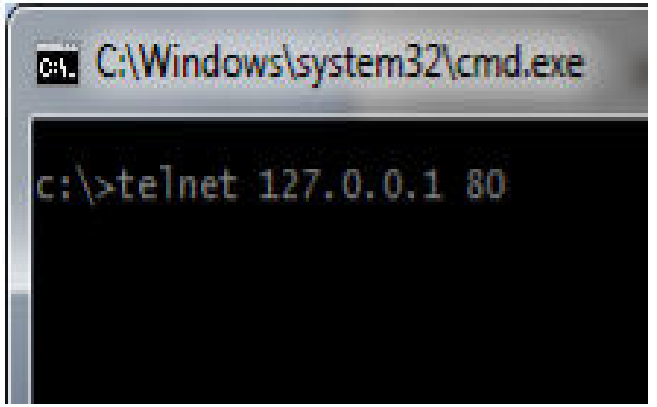
Nmap for Specific Port Numbers

```
nmap -p [port] hostName
## Scan port 80
nmap -p 80 192.168.1.1

## Scan TCP port 80
nmap -p T:80 192.168.1.1

## Scan UDP port 53
nmap -p U:53 192.168.1.1

## Scan two ports ##
nmap -p 80,443 192.168.1.1

## Scan port ranges ##
nmap -p 80-200 192.168.1.1

## Combine all options ##
nmap -p U:53,111,137,T:21-25,80,139,8080 192.168.1.1
nmap -p U:53,111,137,T:21-25,80,139,8080 server1.cyberciti.biz
nmap -v -sU -sT -p U:53,111,137,T:21-25,80,139,8080 192.168.1.254

## Scan all ports with * wildcard ##
nmap -p "*" 192.168.1.1

## Scan top ports i.e. scan $number most common ports ##
nmap --top-ports 5 192.168.1.1
nmap --top-ports 10 192.168.1.1
```

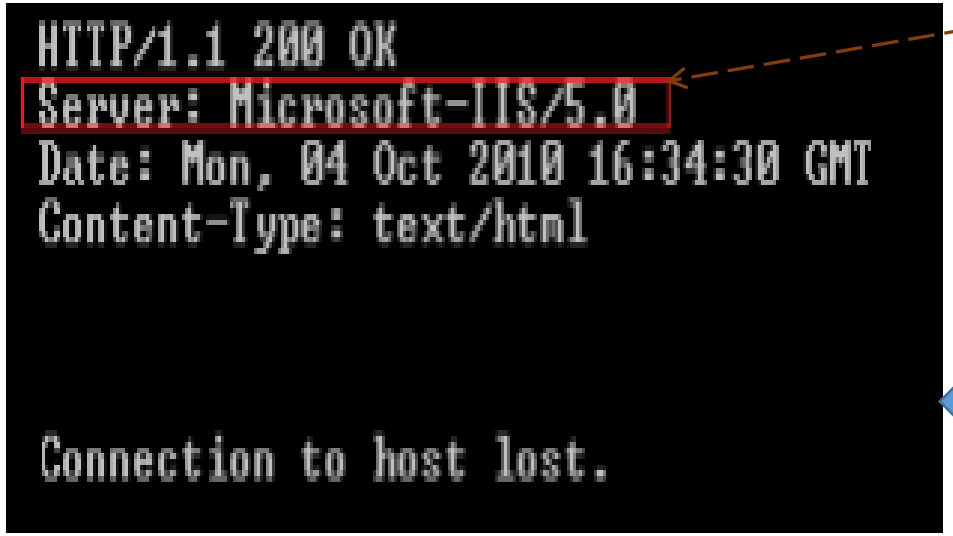
Banner grabbing and Enumeration



1. Access the command prompt



2. Type telnet (host address) (port number) as shown here.



Server Version

3. The command windows will turn to be a blank display a blinking cursor. Now, type “HEAD /HTTP/1.0” and hit enter key

Banner grabbing using Netcat

"Netcat is a featured networking utility which reads and writes data across network connections, using the TCP/IP protocol."

Features of Netcat:

- Can create both inbound and outbound connection to and from any TCP or UDP ports
- Establish a tunnel between UDP and TCP protocols
- Has a built-in port scanning facility.
- Able to read command-line arguments from any standard input

Syntax for running the Netcat tool

1. ~# nc -v target_IP_address 80

   Nc denotes the program name

   -v indicated that we are running Netcat command in verbose mode

   Target_IP_address is the IP address of the target computer

   80 is the open TCP port on the target computer

2. GET /index.html HTTP/1.0

   Press the ENTER button few times. Note: try with HTTP/1.1

3. The result will include the web server name and version number

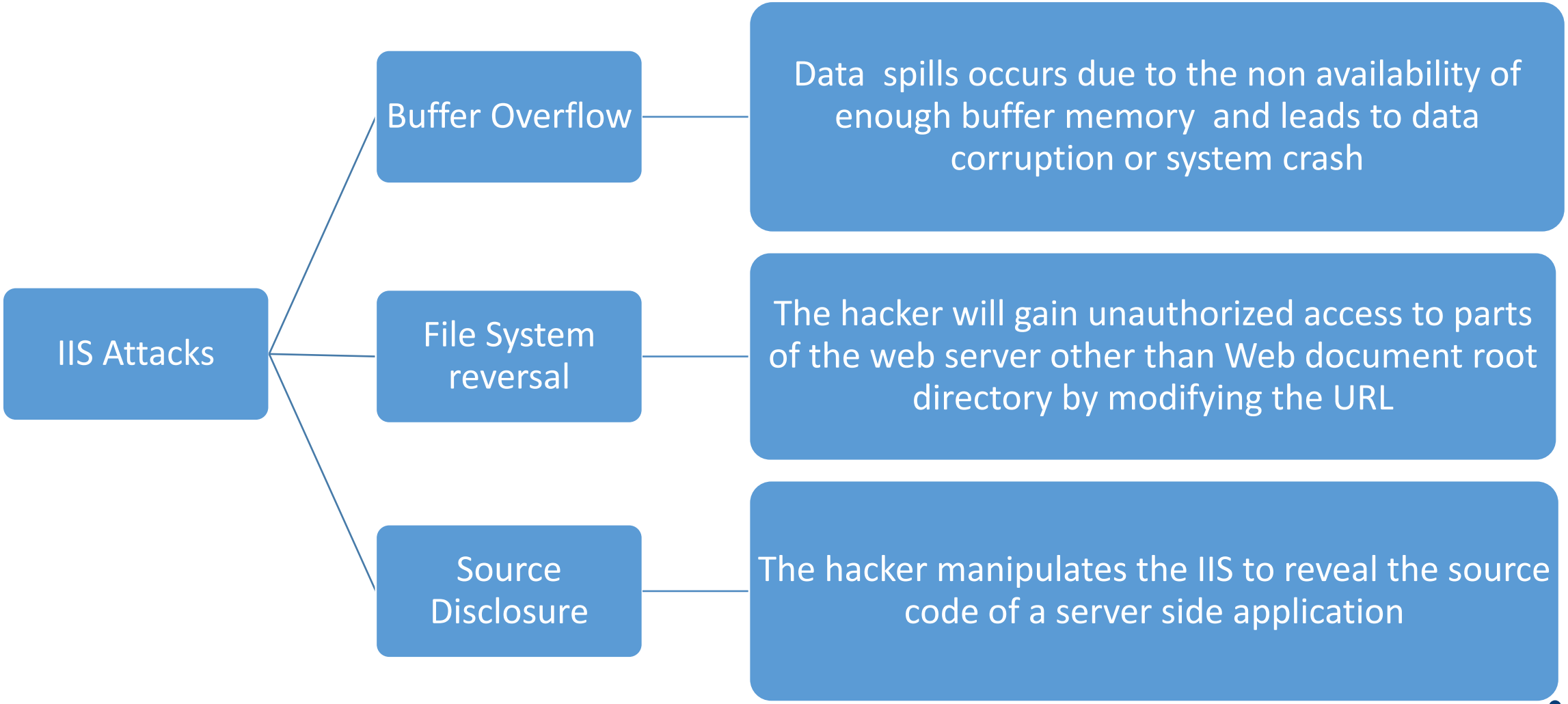
Server vulnerability

- Most popular web servers used are Microsoft IIS, Apache, lighttpd and IBM lotus

common vulnerabilities

- Injection flaws
  - occurs due to non-filtering of the user input
- Broken authentication
  - due to problems like passwords either stored or transmitted in an unencrypted fashion
  - session hijacking or stealing session IDs
- Cross Site Scripting
- Misconfiguration in security

Attacks on Web Server



Buffer Overflow

IPP Printer over-flow attack

- The major player in this attack is the mws3ptr.dll
- which is an ISAPI filter that talks with the printer files and user requests.
- The hacker exploits the vulnerability in this DLL

ISAPI Buffer overflow attack

- Microsoft's IIS Indexing Service DLL or ida.dll and
- Microsoft Data Query file or idg.dll

WebDAV/ntdll.dll

- a standard for collaborative authoring on the web as defined by Internet Engineering Task Force
- remotely located on the internet, to collaboratively edit and manage files

Attack by ISSHack.exe

- The hacker will cause the IIS http daemon buffer to overflow and then will execute a malicious code

File System Reversal

- Users access only a partition of server file system namely Web document root directory,
- This contains web server application software and the files that are accessible to public users
- Attacker does this by inserting special characters in the website URL like, . . / (dot dot slash).
- This attack is also called by the same name.

Source Disclosures

- The attack reveals to the hacker, information like database organizations source code vulnerabilities, application parameters and privileges and so on.

Apache Attacks

Brute-Force Attacks

- Used to perform simple attacks against your own server

Programming Model Attacks

- An attack of a more severe nature than Brute Force attack
- Any traces of the attack in the log will be erased by the hacker and requires limited bandwidth

Apache chunked encoding vulnerability

- A mistake in Apache software misinterprets the size of chunks yet to be received and this results in buffer overflow and there may also be possibilities of malicious code execution.

Other Apache Attacks

Mod_proxy buffer overflow

- It configures a proxy server for both HTTP and FTP protocols
- Results in a buffer overflow in a web server and enables execution of malicious code, which in turn causes a Denial of Service attack.

Long URLs

- Lengthy URLs result in the risk to the servers exposing their directory listings.
- The default limit for the length of the request line is 8190 bytes

PHP Scripting

- Can also be used in conjunction with HTML for web page development
- Opens the doors to hackers to run malicious code on web server

URL trailing slashes

- If the trailing slashes in a URL are not limited, it may expose the original directory listing

Quiz / Assessment

1) The actual process of 'retrieving information about the type and version of the web server' is called			
a) Three-way-handshake method	**b) Banner grabbing**	**c) Port scanning**	**d) None of the above**
2) Three basic types of attacks against ISI are buffer overflow, file system reversal and _____			
a) PHP Scripting	**b) Long URLs**	**c) Source disclosure**	**d) Cross-site Scripting**

Web Application hacking

- Web is a repository of static information that can be shared to anyone who seek.
- Hacking into a web application may serve as a means to steal
    - Personal information like usernames and passwords
    - Credit card information, to purchase things on the internet
    - Target's identity to engage in harmful or criminal activities
- Some of the common web application attacks include the following
    - Cross Site Scripting or XSS
    - Remote code execution
    - SQL injection
    - Cookie/ Session poisoning
    - Parameter / form tampering
    - User name enumeration

Cross Site Scripting or XSS

- Amongst the most threatening web vulnerabilities.
- In this attack, the hacker sends a request to a website in such a way that the website sends a malicious web or email code to another user who is a victim in this scenario

Non-Persistent

- The attack will only be executed when the user visits the link specifically crafted link by the hacker

Persistent

- In this type of attack, the code crafted by the hacker will be stored on a database and the implications of this attack are more severe in nature.

After a successful XSS attack, the hacker may be able to

- Hijack an account
- Access victim's browser history and data on clipboard
- Remotely control victim's browser
- Scan victim's intranet applications an even exploit any vulnerabilities present

Remote code execution

- Here, attacker gains authority to execute his own system level code on a target web server, thereby gaining highest level access to files
- It occurs at server system software level

SQL Injection

- The hacker mainly focuses on the database application of a web server like SQL, Oracle Net listener and MySQL.
- The hacker gains access to sensitive information residing on the DB before he executes a remote code.

Cookie poisoning

- It presents as a vulnerability to a hacker who may modify the data carried by the cookie for transferring data from one step to another step in a web program
- It identifies the current session of the browser and is called '*Session token*'
- The hacker attempts to modify this session token and upon success, can take over another session and the process is called Session poisoning

Parameter tampering

- occurs when a programmer decided to store any information needed for the next step in a process in a variable that uses a <hidden> tag.
- By resubmitting the saved html file, he could hijack someone's session depending on the data in the hidden variable

Username enumeration

- The hacker may determine the precise username by deciphering the error messages.

Un-validated Input

- It is entirely the responsibility of the web developers and programmers to evaluate and edit the data received at the web-based program
- This vulnerability could be held in control using firewalls, Intrusion detection systems and installing software or hardware patches on the server

SQL Injection

- The hacker mainly focuses on the database application of a web server like SQL, Oracle Net listener and MySQL.
- The hacker gains access to sensitive information residing on the DB before he executes a remote code.

Improper error handling

- when you are on a website, it simply says ‘there has been an error’ or says ‘your request cannot be processed at the moment. Please try later’.
- Following are some of the precautionary steps could be taken by the system administrator to handle errors effectively
  - Any part of the default error page template should be removed
  - Eliminate any template parameters from web applications
  - Provide attention towards customized error templates created by the web programmer.
  - It is a must for the system administrator to maintain a complete log file.

Insecure Storage

- It is recommended for a web programmer to use one of the available API packages that come with encryption schemes rather develop one of this.

Countermeasures

Attack type	Countermeasures
IIS buffer overflow	Scan the IIS server regularly to detect vulnerabilities Installing Microsoft patches without fail Configuring firewalls Disabling IPP printing options Scan the URL's using URLScan and Use IIS Lockdown tool to turn off any unnecessary features on the server
File System traversal	Restricting access to executables like cmd.exe Placing system software separately from website software and content folders. Installing IIS Lockdown, which screens all web server requests to identify any characters that indicate the possibilities of an attack
Remote code execution	By limiting the usage if execution of commands using shell Avoid processing of data input by the user which is not pre-scanned.

Countermeasures

Attack type	Countermeasures
SQL injection	Send customized error messages from the server, which do not contain any useful information Grant least privilege to the user by not having him on the DB that host highest privilege given to a DB owner
Cross Site Scripting (XSS)	Lay constraints on the input data by verifying its format, range and any other irregularities. There are tools available, like Range Validator that does this job. By encoding output that may contain user input data and any other information from the DB. HTML Encode is one such tool that can help you do this.
Username enumeration	Deliver customized error messages to valid users, that do not contain any valuable keys Deactivate any feature that indicate password prediction by any means

Hidden Fields

- A hidden field is dynamic field that is hidden within a HTML form using the tag <hidden>
- Hidden fields are mostly used by websites related to financial transactions and e-commerce platform

Example shows lines of vulnerable HTML code

```
<form method="post" action="page.aspx">
<input type="hidden" name="PRICE" value="200">
Product name : <input type="text" name="product" value="shop" name="product" value="Shirt"><br>
Product price:200.00"><br>
<input type="submit" value="submit">
</form>
```

When a user sends a normal request in this web page,

```
http://www.shop.com/page.aspx?product=Shirt&price=200
```

The hacker may change the above code to alter the price of the shirt as 2, like given below

```
http://www.shop.com/page.aspx?product=Shirt&price=2
```

- Some of the steps mentioned below, help in preventing hidden field manipulation attack
  - By adapting ‘Steps of the wizard’ approach in web application development.
  - Installing application firewall
  - Design web applications such that the dynamic information will be stored in an encrypted cookie.

Web-based Authentication

'the process of verifying that the credentials provided by the user holds good on that resource and belong to that individual only'.

Common methods		
Password: Ideally, a combination of alphabets, numerals and special characters, known only to the users	Debit card or a credit card, especially for e-commerce and banking applications	Biometrics like finger print scanning and retina scan

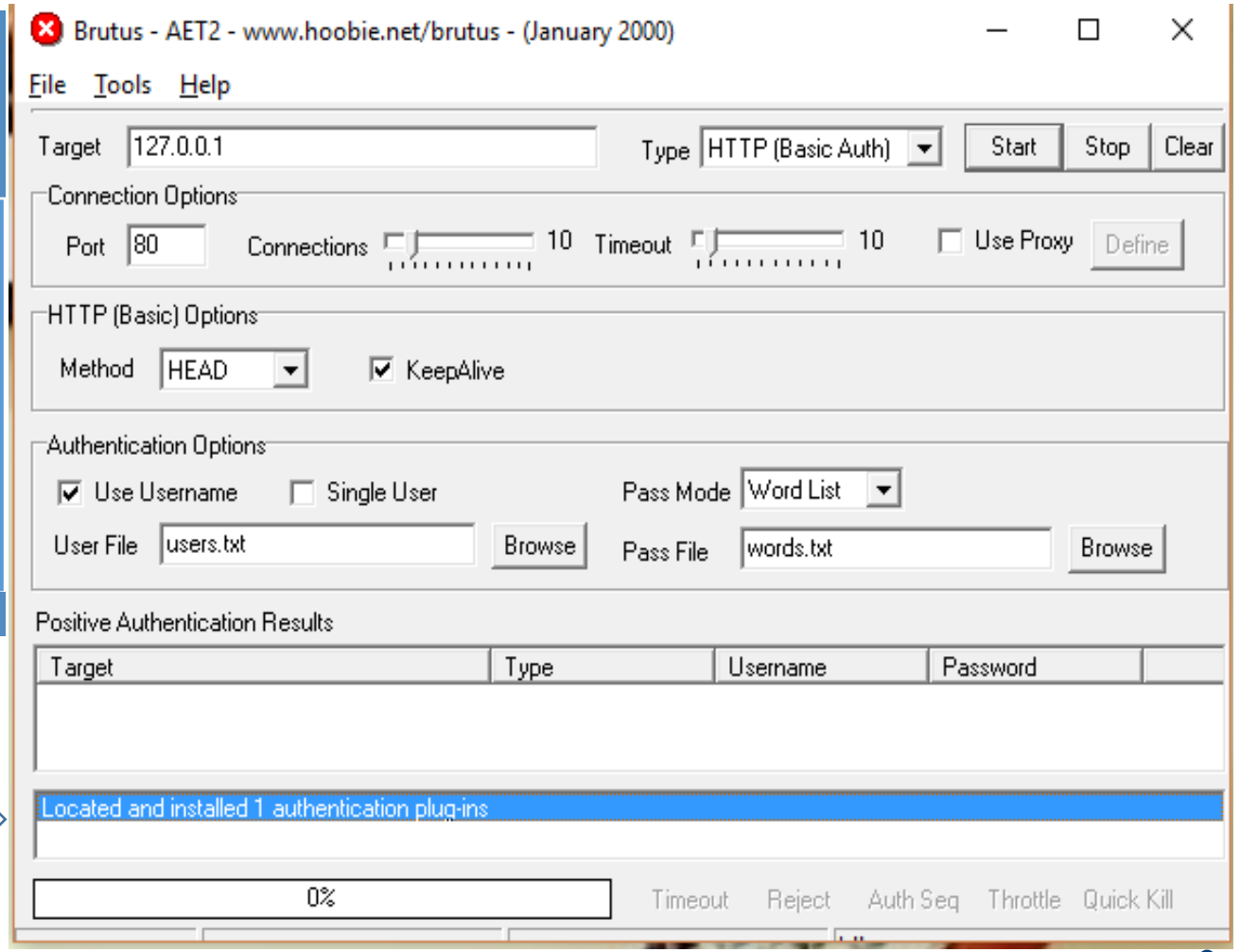
Web-based Authentication methods

HTTP Basic Authentication	HTTP Digest Authentication	HTTPS Client Authentication	Form Based Authentication
• Based on Username and Password • offers minimum level security	• Identical to HTTP Basic authentication • Based on a username and password authentication wherein, the password is encrypted	• A stronger authentication protocol compared to others • This method is based on Certificate based authentication using the user's Public Key Certificate or PKC	• Commonly used authentication type where the user enters his username and password in a HTML form and sends it to the server via SSL or HTTP

Web-based password cracking

Important terms regarding password types are		
A static password is one that is same in each logon	A dynamic password is one that is changed at every logon	A one-time password can be used only once and then discarded.

Installation and password cracking using Brutus



Quiz / Assessment

3) Which one of the below options is not a web application attack?

a) Cross-site Scripting	b) SQL injection	c) Cookie poisoning	d) File system reversal

4) In _____ type of web-based authentication, the entire process is stored in a cookie and hence need not be repeated each time the client has to authenticate his credentials on the server

a) Digest authentication	b) Basic authentication	c) Form based authentication	d) None of the above

e-References & External Resources

- It is very interesting to know how web has evolved over the past decades and what better way for this than understanding it by a visually appealing timeline? http://www.pewinternet.org/2014/03/11/world-wide-web-timeline/ and http://www.evolutionoftheweb.com/ are two good sources in this context.
- Here is a pdf on how to use Namp for different network scenarios. https://nmap.org/docs/discovery.pdf
- Read an article about how to identify vulnerabilities in a web server https://www.giac.org/paper/gsec/3729/web-server-vulnerabilities-defense-in-depth-strategy-squid-proxy/105970
- Download a copy of the application developer's handbook from https://leaksource.files.wordpress.com/2014/08/the-web-application-hackers-handbook.pdf
- How to prevent web server vulnerabilities? http://eqinc.com/blog/166-how-to-prevent-common-web-server-vulnerabilities
- Web-based authentication methods explained https://blog.risingstack.com/web-authentication-methods-explained/
- How to select the most appropriate web based application method http://www.techrepublic.com/article/understanding-and-selecting-authentication-methods/

External Resources

1. The CEH Prep Guide, the comprehensive guide to Certified Ethical Hacking by Ronald L. Krutz and Russell Dean Vines
2. The Basics of Hacking and Penetration Testing, second edition, by Patrick Engebretson
3. Official Certified Ethical Hacker Review Guide by Kimberly Graves
4. Unofficial Guide to Ethical Hacking by Ankit Fadia

Activity

Brief description of activity

Online Activity
(30min)

Description:
Open a telnet connection to various TCP ports on the target system and make a note of the banner information that you get out of this activity in the below format, beginning with port number 80 (TCP Port)

Port number	Banner information
80	

Repeat the above exercise by replacing TCP by other port numbers like FTP

Also, note down which are the web server applications that are running on the target systems.

Thank You