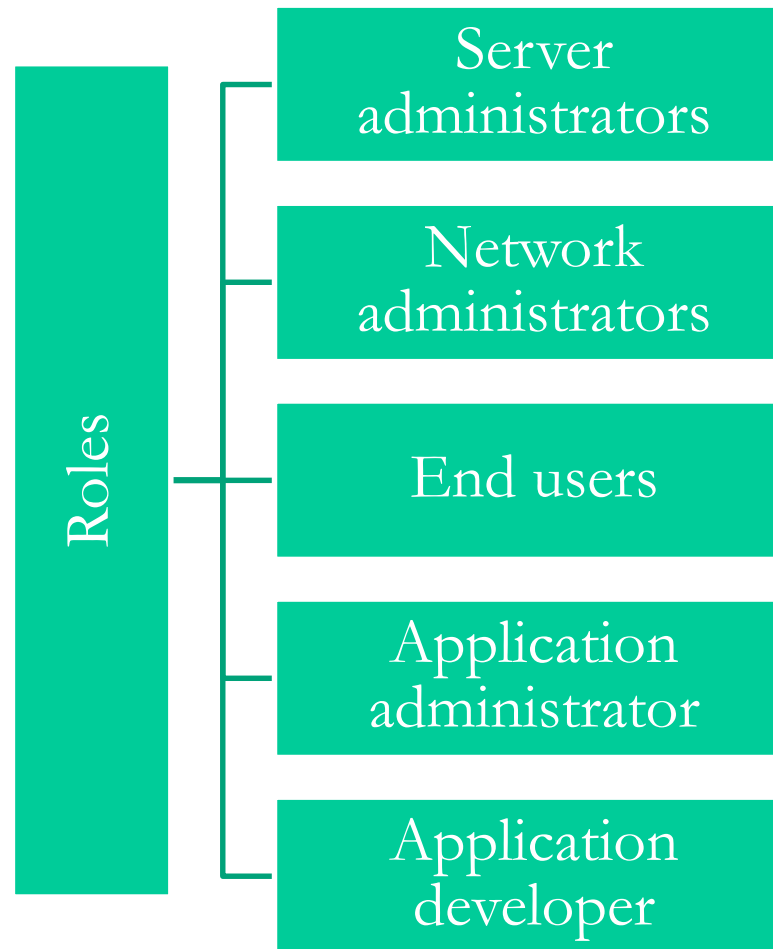




Web Servers and Applications

Chapter 13

Client and Server



A Closer Look at Web Servers

Web server delivers content over HTTP or other protocols.

Files are delivered in response to requests.

Web servers can support different types of content.

Multiple web server platforms exist from different vendors.

The top three popular web servers are Apache, Internet Information Services (IIS), and nginx.



Apache for Linux and UNIX



Security features

- Authentication
- SSL/TLS support
- Proxy support
- URL rewriter
- HTTP request filtering
- Intrusion detection
- Enhanced logging

Application support

- Python and Perl support
- PHP
- Compression support

Microsoft Internet Information Services (IIS)

Security features

- Certificate support
- Authentication support
- Security support and management

Application development

- Process management
- Server-side language
- Database support
- Protocol listeners

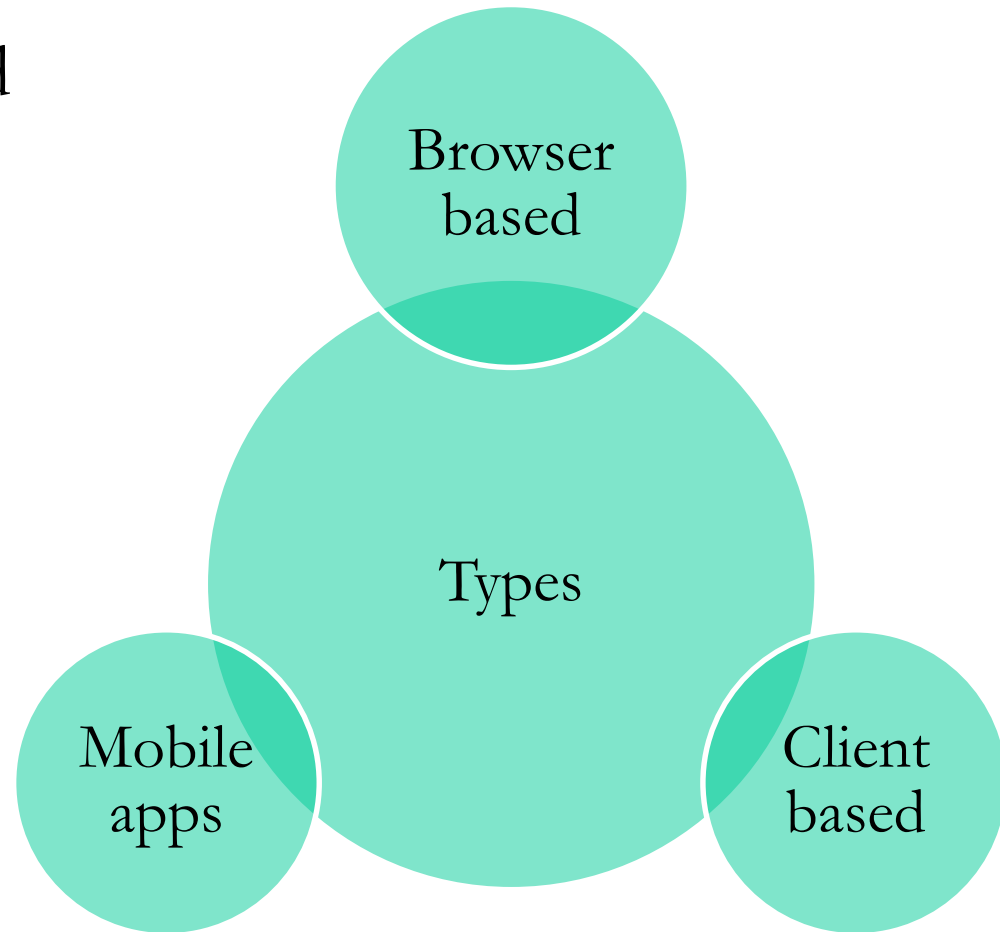
Compatibility

- Support for legacy technologies



Web Applications

A web application is software that is installed on top of a web server and is designed to respond to requests, process information, store information.



Client and Server Web Applications

A server application is hosted on a web server and is designed to be accessed remotely via a web browser or web-enabled application.

The server application is on the web server.

The client is a web browser or web-enabled application.

Information is stored on the server.

Processing is done on the server.

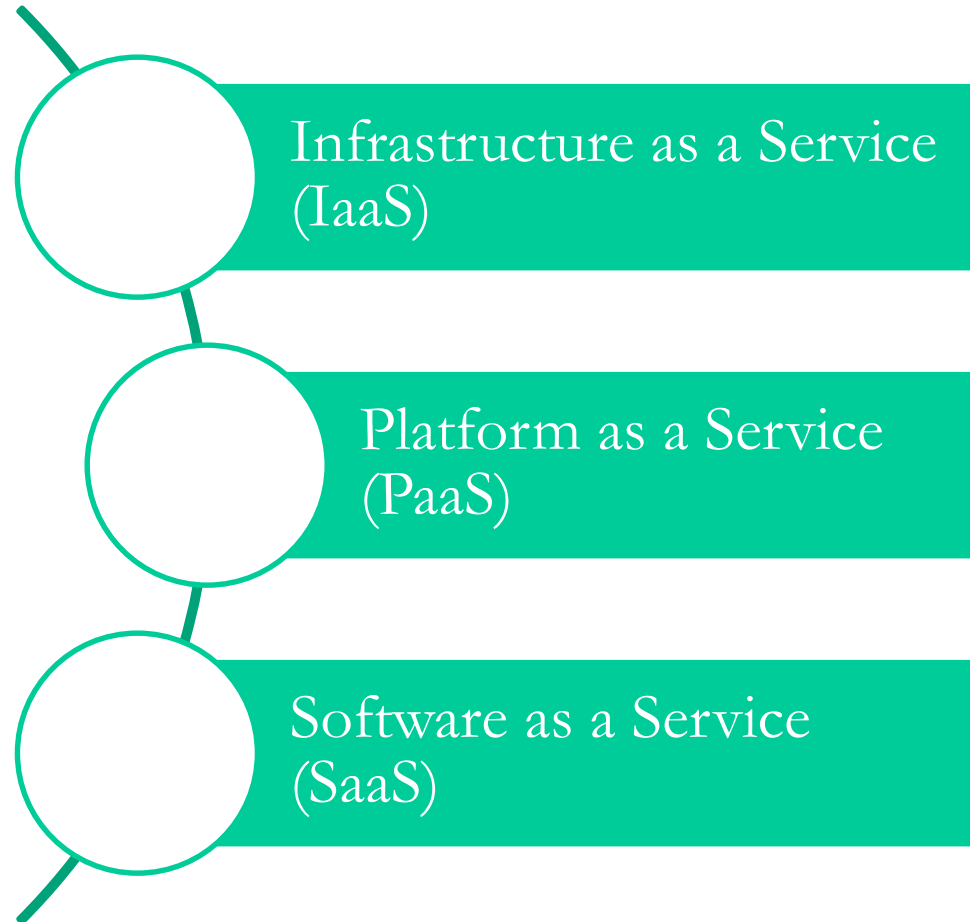
The end result is delivered to the user.

Applications can be made for one platform.



Cloud Services

The cloud is a model for creating shared resources that can be dynamically allocated and shared on demand.



A Closer Look at Web Applications

- **Presentation layer**
- **Logic layer**
- **Data layer**

All of these layers depend on the technology brought to the table in the form of the World Wide Web, HTML, and HTTP.



What Is a Cookie?

Cookies are used to store data.

The file holds state information.

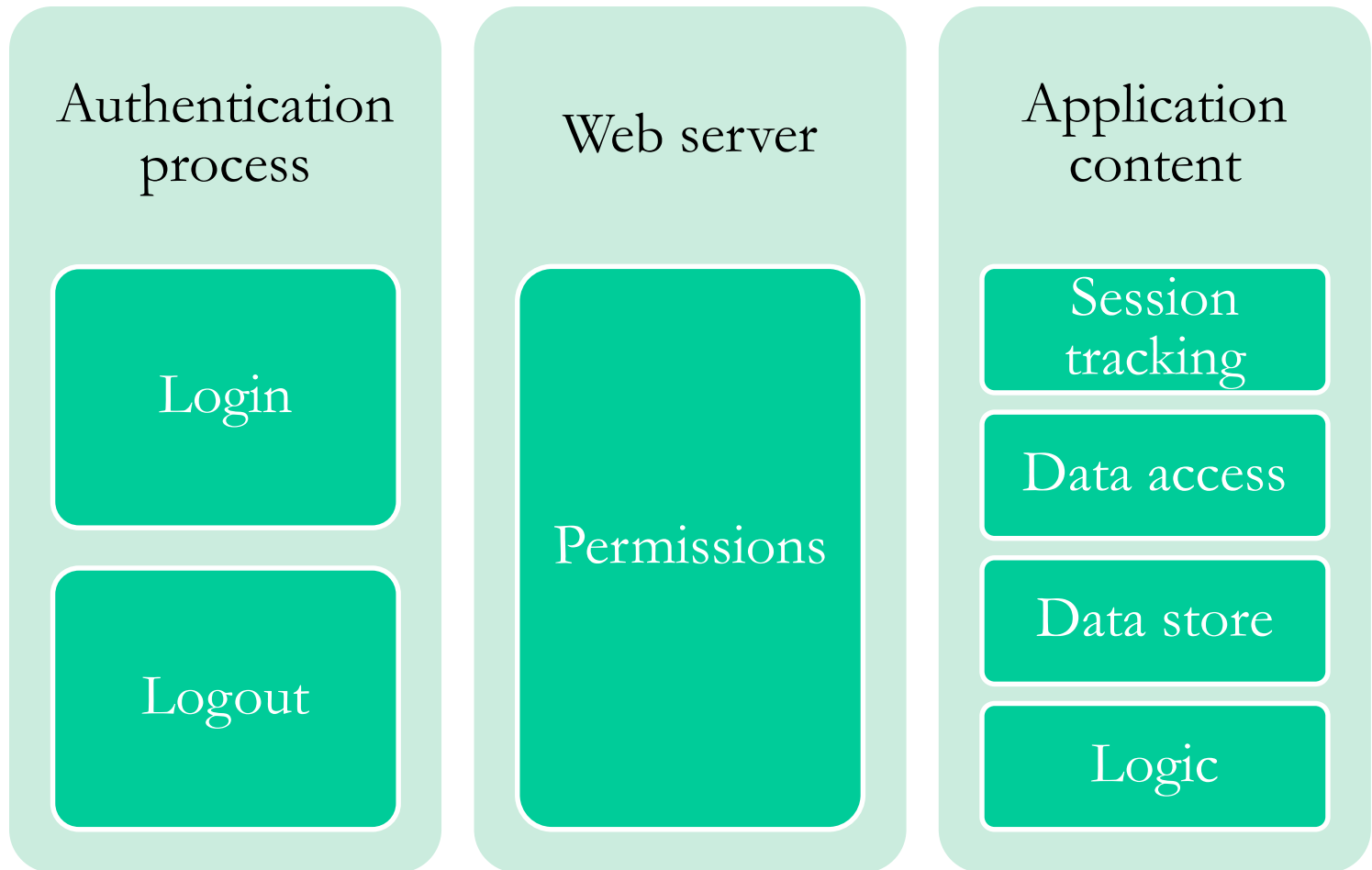
Information can be exposed to a hacker.

Insecure cookies could allow theft.

It's a commonly used technique.



Pieces of the Web Application Puzzle



Common Problems with Web Applications

- **Flawed Web Design**
 - Too much revealed in code
 - Presence of server information
 - Presence of connection information
- **Buffer Overflow**
 - Software-based issue
 - Common vulnerability
 - Can cause numerous issues



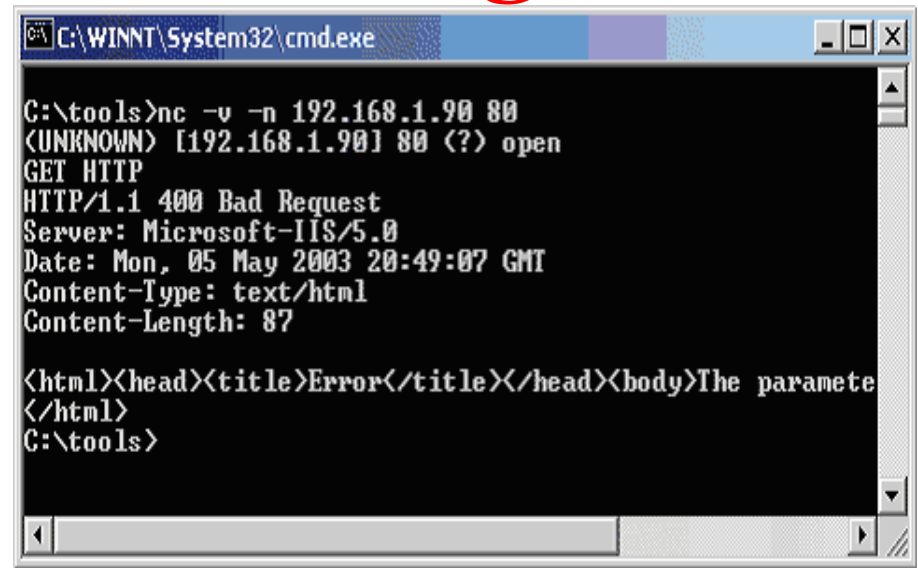
Other Attacks Against Web Applications

- Denial-of-service attack
- Distributed denial-of-service attack
 - Ping or ICMP flooding attack
 - Smurf attack
 - SYN flooding
 - Fragmentation attack



Banner Grabbing

Banner grabbing is an activity that is used to determine information about services that are being run on a remote computer.



```
C:\WINNT\System32\cmd.exe

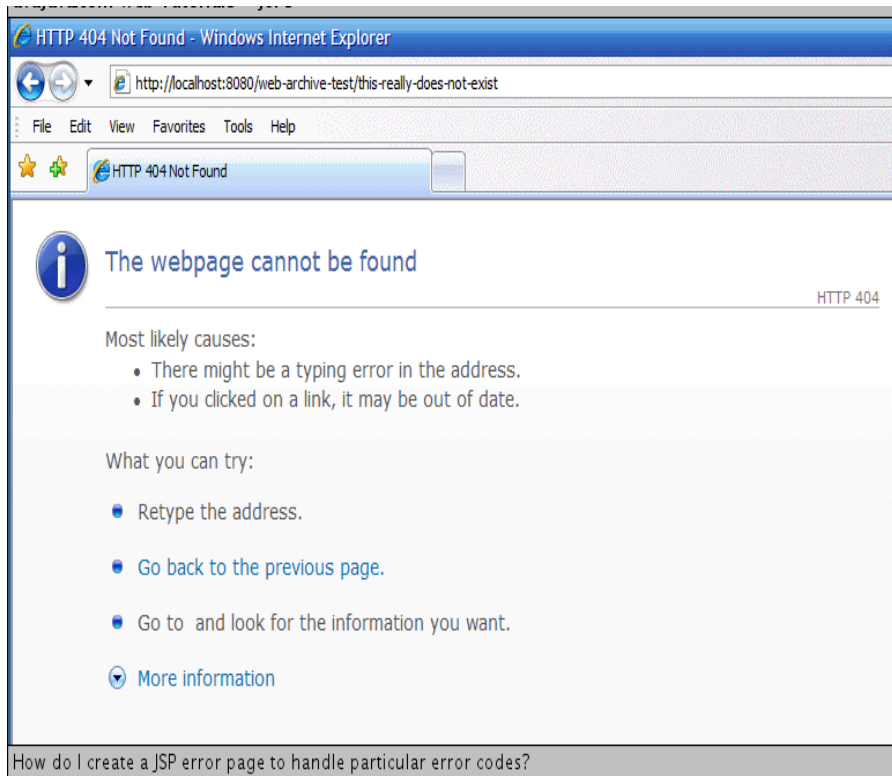
C:\tools>nc -v -n 192.168.1.90 80
<UNKNOWN> [192.168.1.90] 80 (?) open
GET HTTP
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Mon, 05 May 2003 20:49:07 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The paramete
</html>
C:\tools>
```

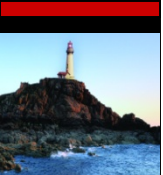
- Banner grabbing is used to identify a system and services.
- It retrieves information from open ports and services.
- Services respond to banner grabs with application-specific information.
- It can use Telnet or SSH to perform this task.



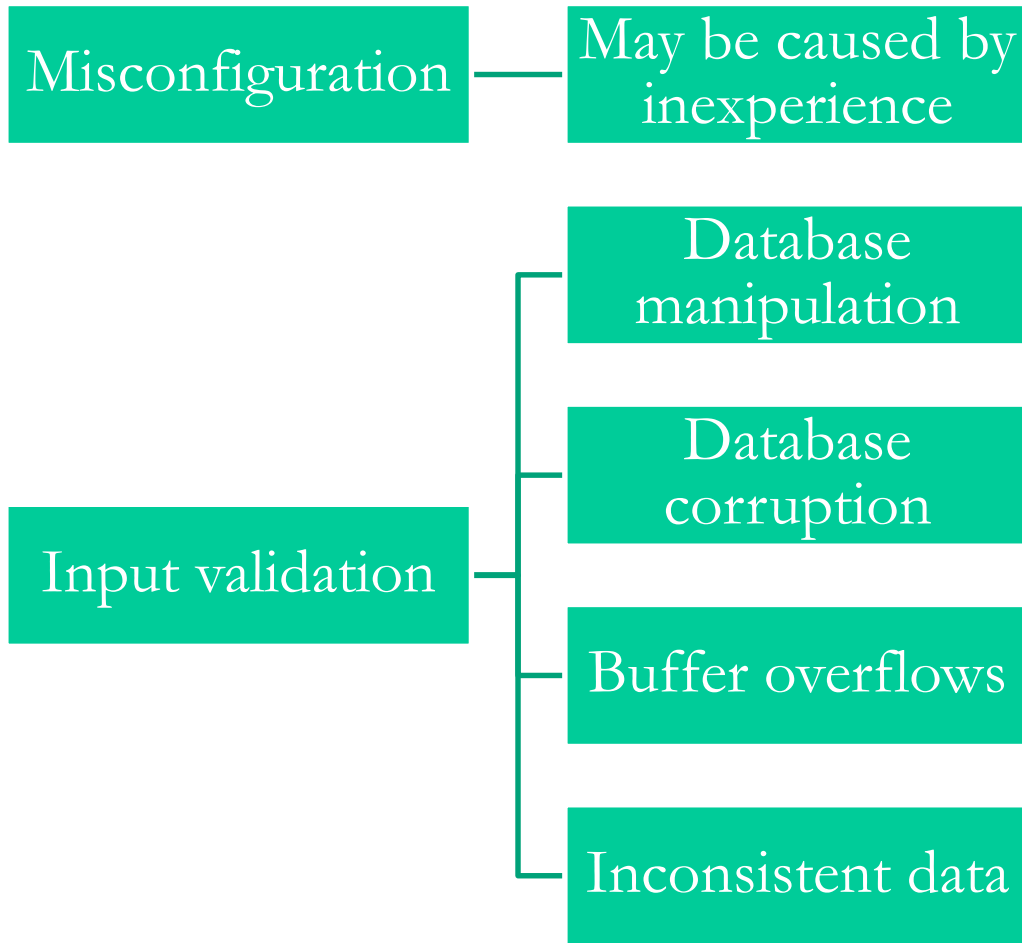
Error Messages



- May reveal too much information
- Should be suppressed or sanitized
- Detailed messages should be accessible only in development
- Custom error message pages may be a solution



Common Flaws and Attack Messages



Cross-Site Scripting

Cross-site scripting (XSS) is a type of attack that can occur in many forms, but in general it occurs when data of some type enters a web application through an untrusted source.



Stored attacks

- The attacker stores malicious code into the vulnerable page.
- The user authenticates in the application.
- The user visits a vulnerable page.
- Malicious code is executed by the user's browser.

Reflected attacks

- This takes the form of an email or via a different web server.
- This occurs when a party injects executable code within an HTTP response.
- Code is not persistent and is not stored.
- It leverages JavaScript, VBScript, or other scripting languages where appropriate.

Coding and Design Flaws

Unvalidated Redirects and Forwards

Caused by bad input validation

Sends user to untrusted location

Insecure Logon Systems

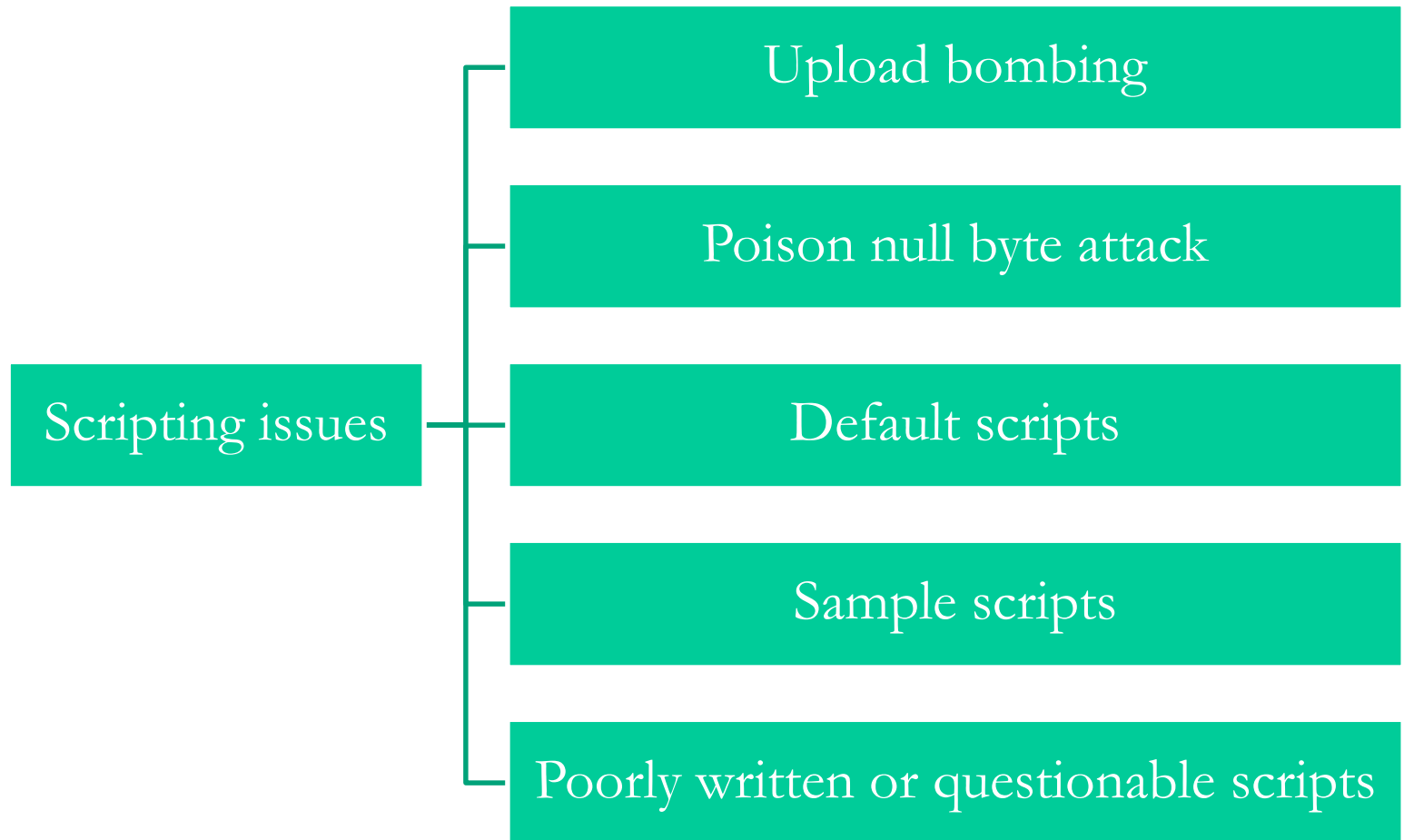
Entry of an invalid user ID with a valid password

Entry of an valid user ID with an invalid password

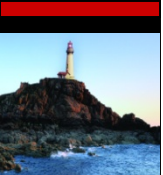
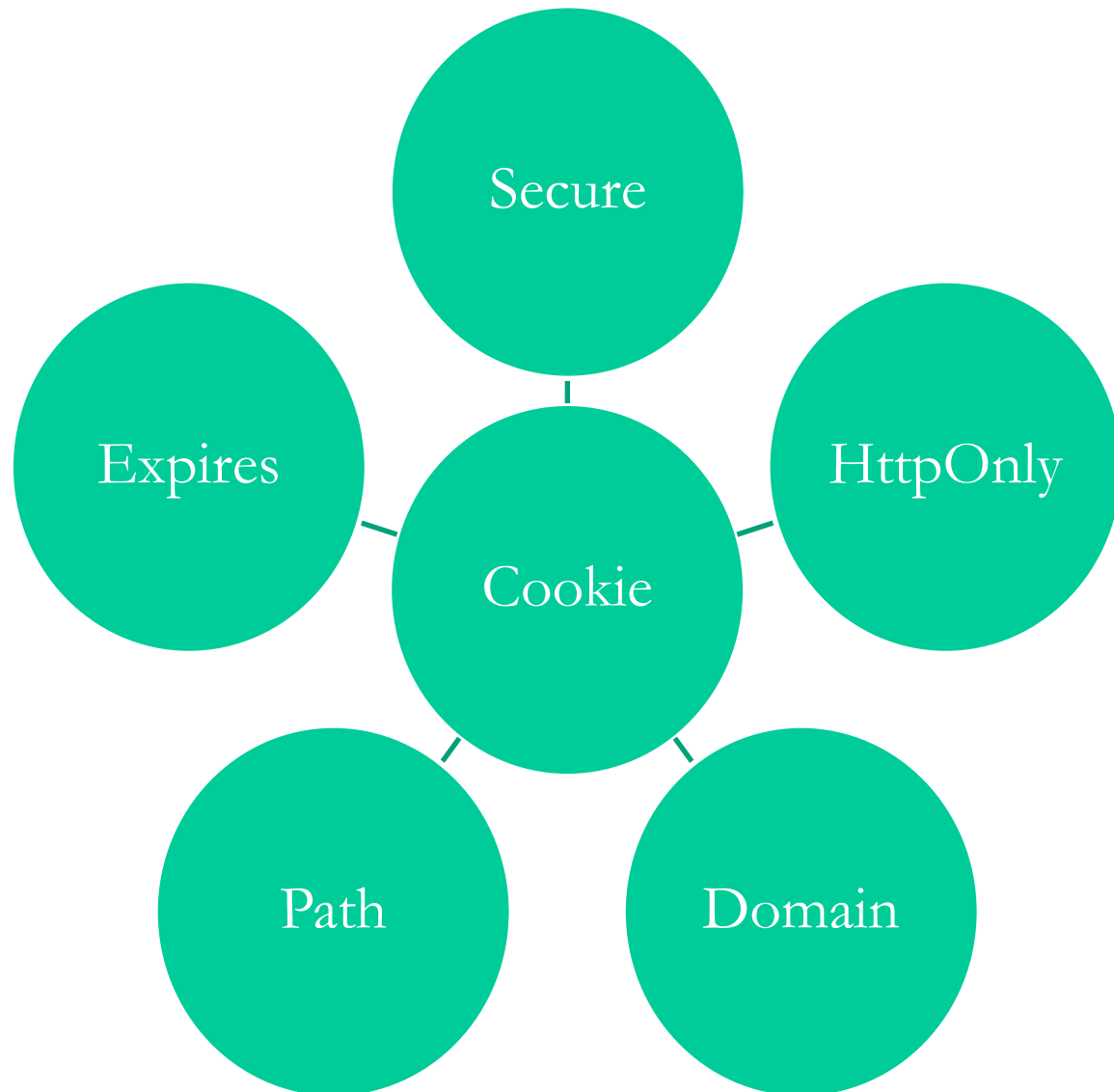
Entry of an invalid user ID and password



Scripting Errors

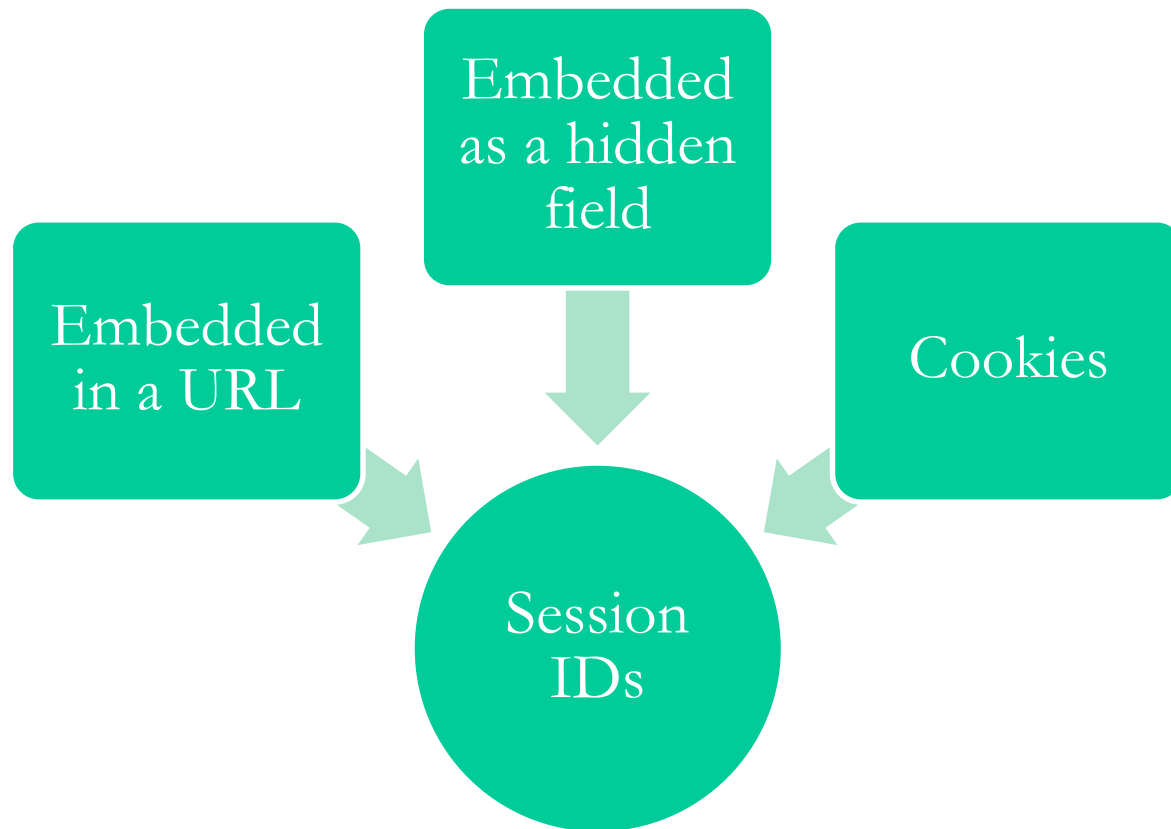


Cookie Issues



Session Hijacking and Web Applications

Session hijacking at the application level focuses on gaining access to a host by obtaining legitimate session IDs from the victim.



Summary

- Definition of a web server
- Definition of a web application
- Can take many forms
- Process and store data on server

