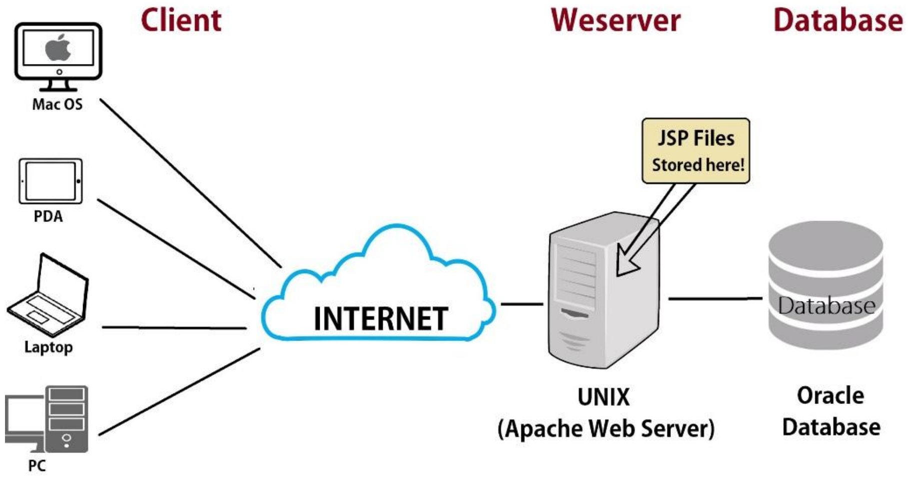
What is Webserver

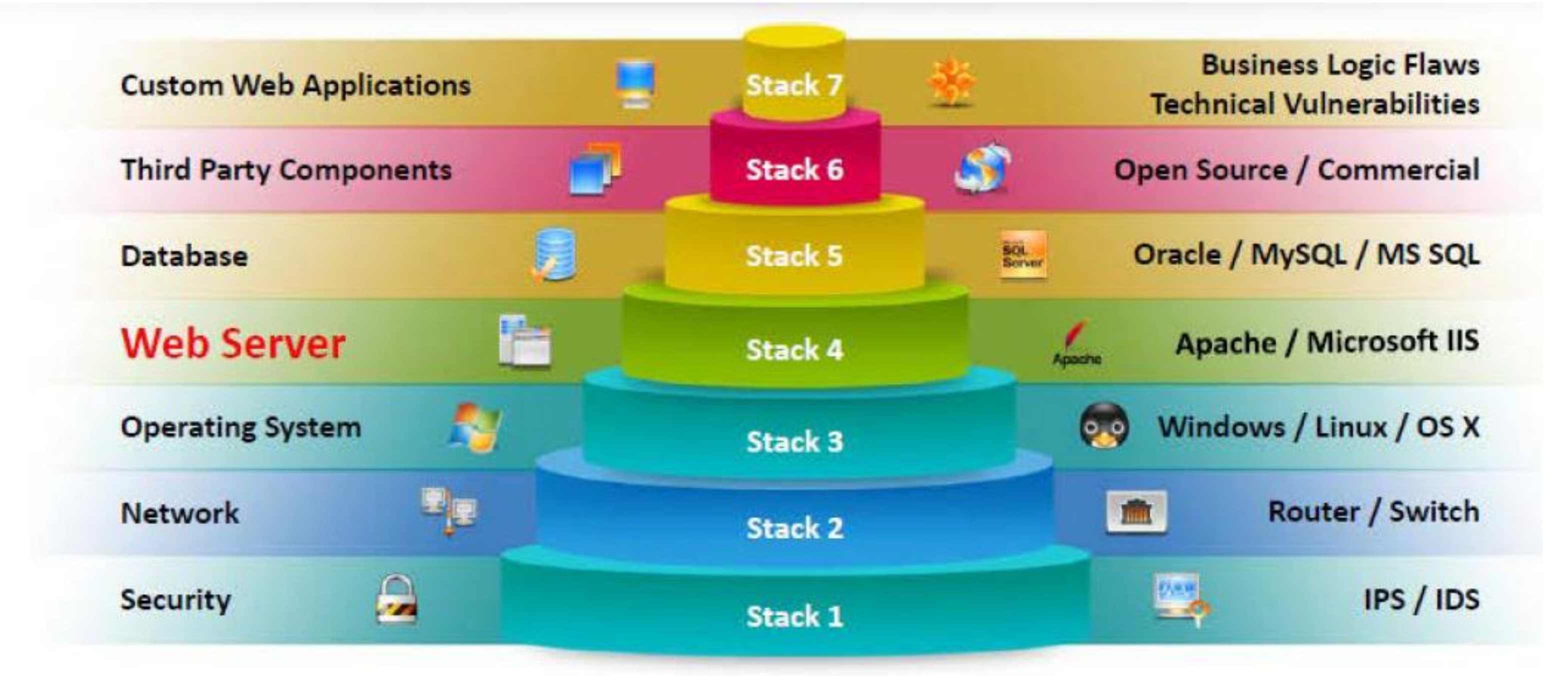
Web Server may be a program that hosts internet sites , supported both Hardware & software. It delivers files and other content on the web site over Hyper Text Transfer Protocol (HTTP). As we all know , use of internet and intranet has raised, web services became a serious a part of the web . it's used for delivering files, email communication, and other purposes. Web server supports differing types of application extensions whereas all of them support HTML for basic content delivery. Web Servers are often differentiated by the safety models, operating systems and other factors.



What is Webserver

Web Server is a program (both hardware & Software) that hosts websites; attackers usually target software vulnerabilities and configurations errors to compromise web servers

Nowadays, network and OS level attacks can be well defended using proper network security measures such as firewalls,IDS however, web servers are accessible from anywhere on the web, which makes them less secured and more vulnerable to attacks

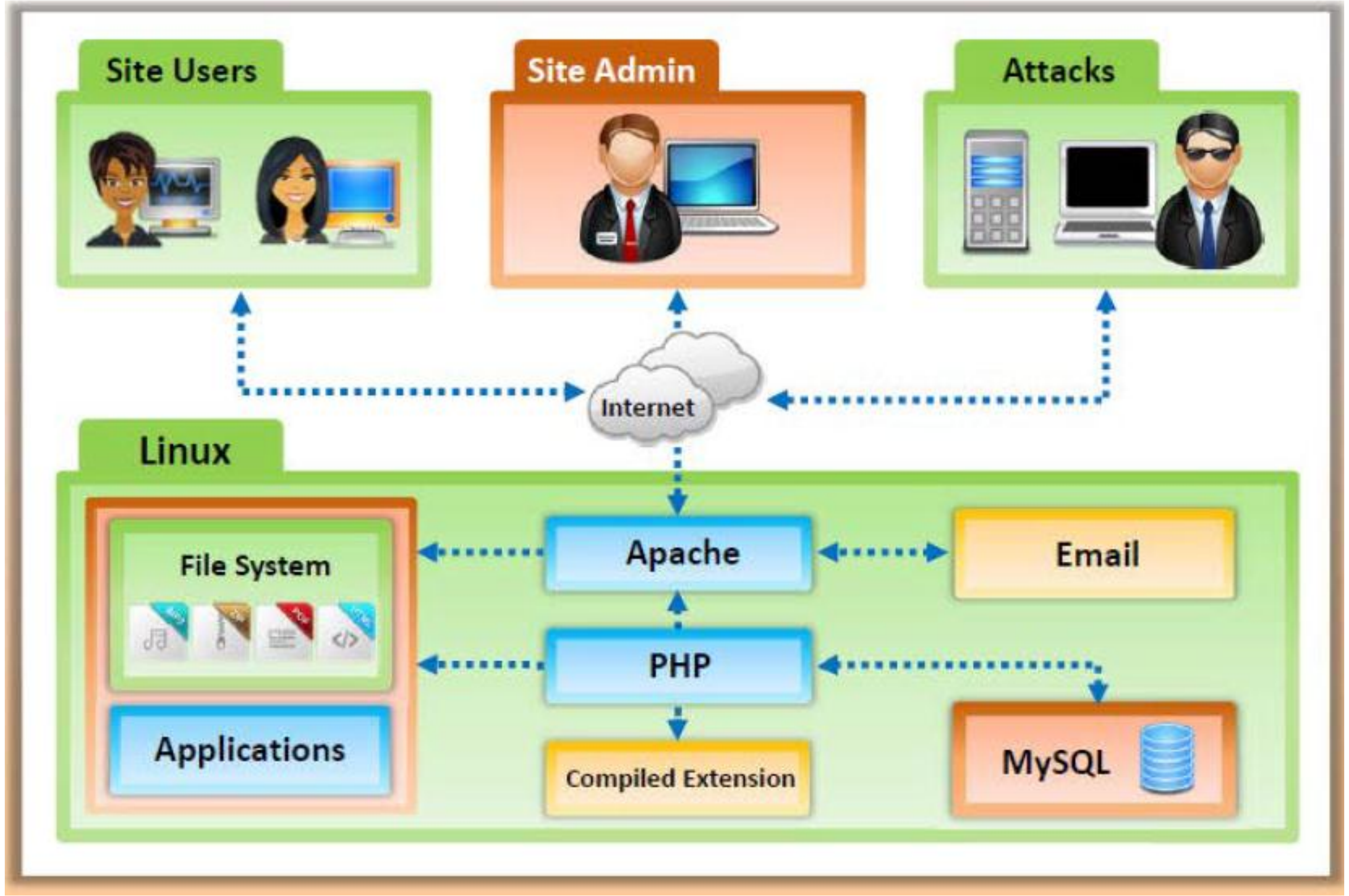


Why Web Servers are Compromised

- Improper file and directory permissions
- Installing the server with default settings
- Unnecessary services are enabled, including content management and remote administration
- Security conflicts with business ease-of-use case
- Lack of proper security policy, procedures & maintenance
- Improper authentication with external systems
- Default accounts with their default passwords or no passwords
- Misconfigurations in web server, operating systems & networks
- Bugs in server software, OS & web applications
- Misconfigured SSL certificates and encryption settings
- Use of self-signed certificates and default certificates

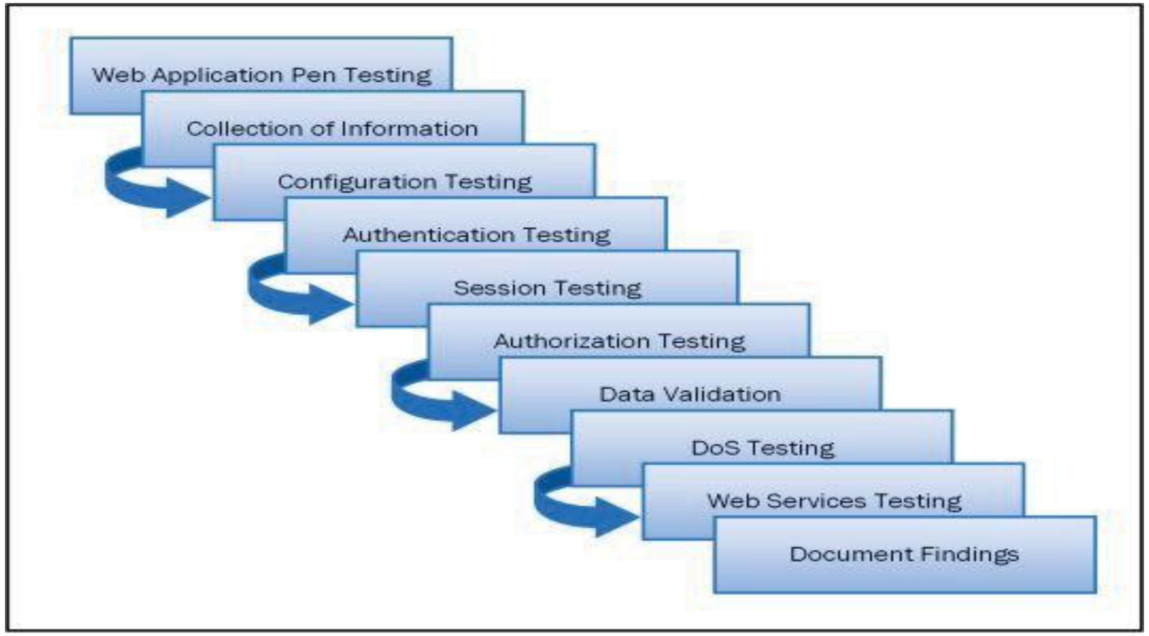
Open Source Webserver Architecture

Open source web server architecture is that the Web server model during which an open source web server is hosted on either an internet server or a third-party host over the web .

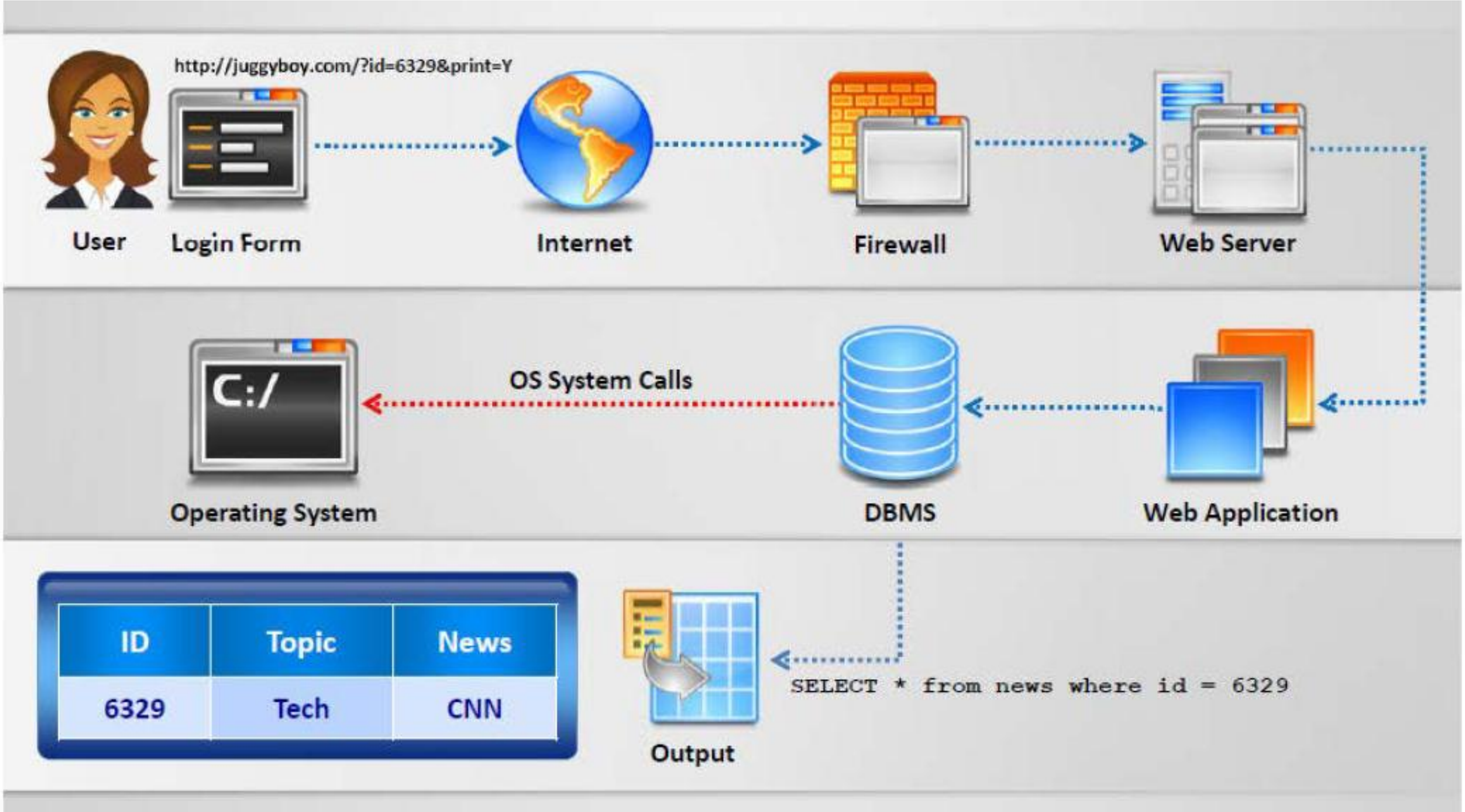


Introduction to Web Applications

Web Applications are that application that's running on a foreign application server and available for clients over the web . These web applications are often available on different platforms like Browser or Software to entertain the clients. Use of Web application has been increased in previous couple of years. Web Application is essentially depending upon Client-Server relationship. Sites could also be generated on the server or containing scripting to be executed on the client browser dynamically.



How Web Applications Work

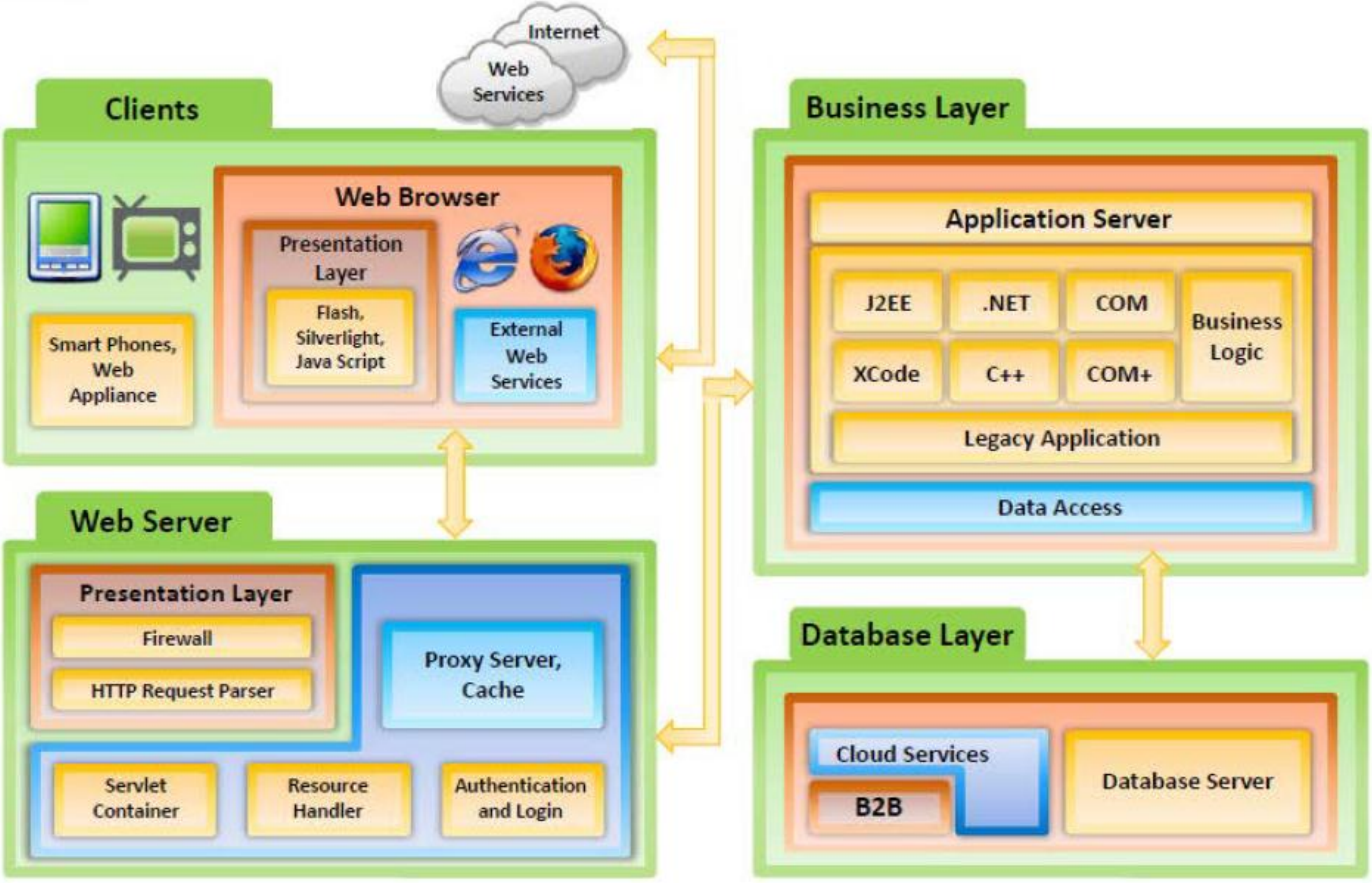


http://juggyboy.com/?id=6329&print=Y

```
SELECT * from news where id = 6329
```

ID	Topic	News
6329	Tech	CNN

Web Application Architecture



Web Application Threats

The Threats to Web Applications are:

- Cookie Poisoning
- Insecure Storage
- Information Leakage
- Directory Traversal
- Parameter/Form Tampering
- DOS Attack
- Buffer Overflow
- Log tampering
- SQL Injection
- Cross-Site (XSS)
- Cross-Site Request Forgery
- Security Misconfiguration
- Broken Session Management
- Session Hijacking
- Network Access Attacks

How to Defend against Web Server Attacks

- Apply restricted ACL's and block remote registry administration
- Secure the SAM (Stand alone Servers only)
- Ensure that security related settings are configured properly and access to the meta base file is restricted with hardened NTFS permissions
- Remove unnecessary ISAPI filters from the webservers
- Remove all unnecessary IIS scripts mappings for optional file extensions to avoid exploiting any bugs within the ISAPI extensions that handle these sorts of files
- Enable a minimum level of auditing on web server and use NTFS permissions to guard the log files

Countermeasures for WebApplication

- Each parameter should be checked against a white list that specifies exactly what input are going to be allowed
- Do server-side validation
- Re-authentication for critical functions
- Simply avoid using redirects and forwards
- Use HTML / URL Encoding
- Filter input for any special characters
- Use tools like XSS Me for Firefox or XSS Rays for Chrome to check your website for any XSS vulnerability
- Minimize user ability to predict object IDs/Names
- Applying the newest security patches (OS, DBMS, Web server and code libraries)
- Setting up roles, permissions, and accounts, including disabling all default accounts or changing their passwords
- Strong encryption algorithms are used for encryption