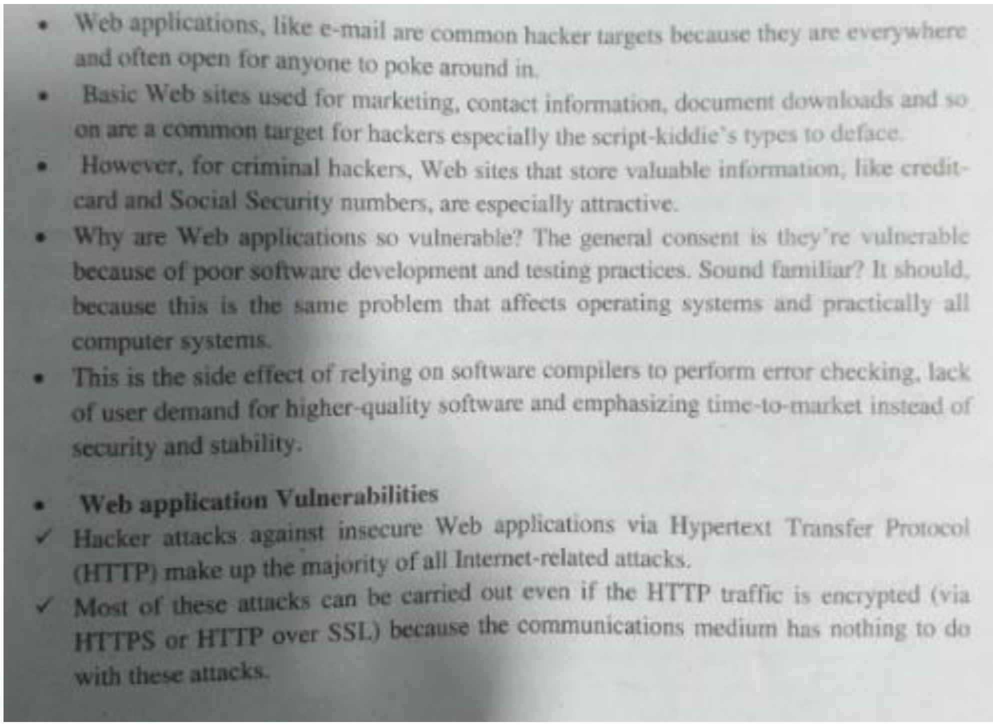


- Web applications, like e-mail are common hacker targets because they are everywhere and often open for anyone to poke around in.
- Basic Web sites used for marketing, contact information, document downloads and so on are a common target for hackers especially the script-kiddie's types to deface.
- However, for criminal hackers, Web sites that store valuable information, like credit-card and Social Security numbers, are especially attractive.
- Why are Web applications so vulnerable? The general consent is they're vulnerable because of poor software development and testing practices. Sound familiar? It should, because this is the same problem that affects operating systems and practically all computer systems.
- This is the side effect of relying on software compilers to perform error checking, lack of user demand for higher-quality software and emphasizing time-to-market instead of security and stability.

- **Web application Vulnerabilities**

✓ Hacker attacks against insecure Web applications via Hypertext Transfer Protocol (HTTP) make up the majority of all Internet-related attacks.

✓ Most of these attacks can be carried out even if the HTTP traffic is encrypted (via HTTPS or HTTP over SSL) because the communications medium has nothing to do with these attacks.

- ✓ Many attacks against Web applications are just minor nuisances or may not affect confidential information or system availability.
- ✓ However, some attacks can cause destruction on your systems. Whether the Web attack is against a basic brochure ware site or against the company's most critical customer server, these attacks can hurt your organization.
- ✓ Some other **web application security vulnerabilities** are as follows

SQL Injection

- Injection is a security vulnerability that allows an attacker to alter backend SQL statements by manipulating the user supplied data.
- Injection occurs when the user input is sent to an interpreter as part of command or query and trick the interpreter into executing unintended commands and gives access to unauthorized data.

Cross site scripting

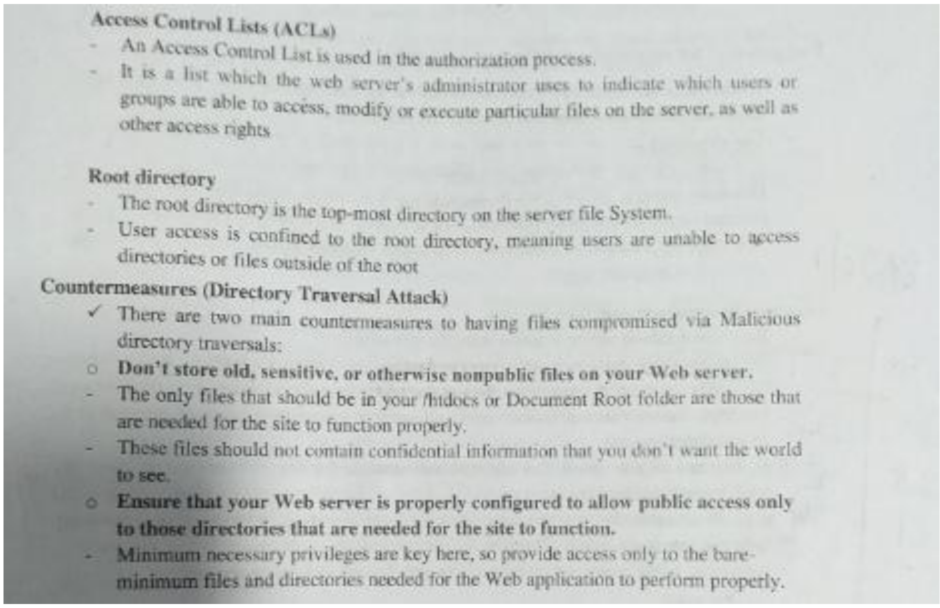
- Cross Site Scripting is also shortly known as XSS.
- XSS vulnerabilities target scripts embedded in a page that are executed on the client side i.e. user browser rather than at the server side. These flaws can occur when the application takes untrusted data and send it to the web browser without proper validation.
- Attackers can use XSS to execute malicious scripts on the users in this case victim browsers. Since the browser cannot know if the script is trusty or not, the script will be executed, and the attacker can hijack session cookies, deface websites, or redirect the user to an unwanted and malicious websites.
- XSS is an attack which allows the attacker to execute the scripts on the victim's browser.

Security Misconfiguration

- Security Configuration must be defined and deployed for the application, frameworks, application server, web server, database server, and platform. If these are properly configured, an attacker can have unauthorized access to sensitive data or functionality.
- Sometimes such flaws result in complete system compromise. Keeping the software up to date is also good security.

Directory Traversals

- ✓ A directory traversal is a really basic attack, but it can turn up interesting information about a Web site.



Access Control Lists (ACLs)

- An Access Control List is used in the authorization process.
- It is a list which the web server's administrator uses to indicate which users or groups are able to access, modify or execute particular files on the server, as well as other access rights

Root directory

- The root directory is the top-most directory on the server file System.
- User access is confined to the root directory, meaning users are unable to access directories or files outside of the root

Countermeasures (Directory Traversal Attack)

✓ There are two main countermeasures to having files compromised via Malicious directory traversals:

○ **Don't store old, sensitive, or otherwise nonpublic files on your Web server.**

- The only files that should be in your /htdocs or Document Root folder are those that are needed for the site to function properly.
- These files should not contain confidential information that you don't want the world to see.

○ **Ensure that your Web server is properly configured to allow public access only to those directories that are needed for the site to function.**

- Minimum necessary privileges are key here, so provide access only to the bare-minimum files and directories needed for the Web application to perform properly.