Website Development - Security

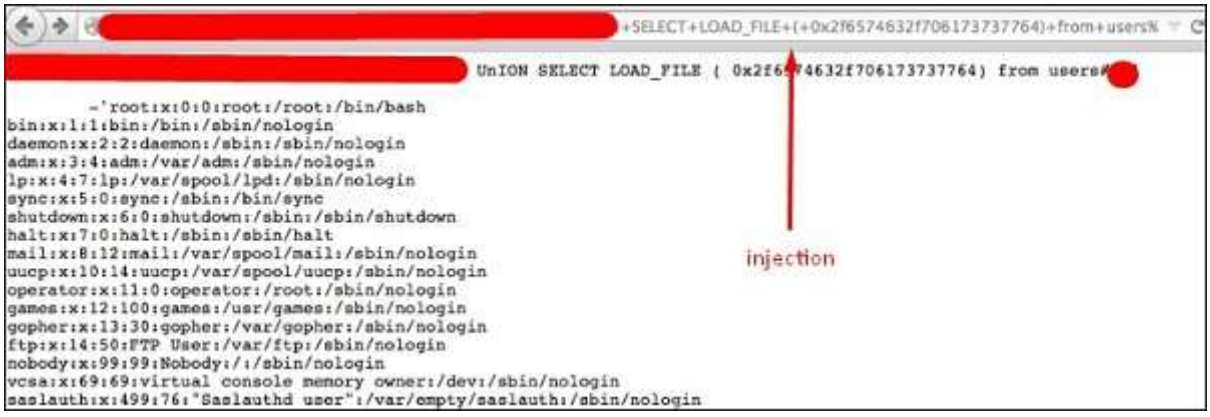
Securing your webpages is as important as developing it, because any threat which can compromise the security can harm your business reputation, damage you financially (by stealing your online deposits), damage your clients that visit your website, etc.

As per security experts, they will suggest to do the website security check based on the **OWASP TOP 10**, which is a powerful awareness document for web application security. The OWASP Top 10 represents a broad consensus about what the most critical web application security flaws are.

SQL Injections

Injection flaws, such as SQL, OS and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or a query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

Solution − To secure your webpage from iSQL, you must validate inputs and filtering symbols.



Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, which allows attackers to compromise passwords, keys, session tokens or even to exploit other implementation flaws to assume other users' identities.

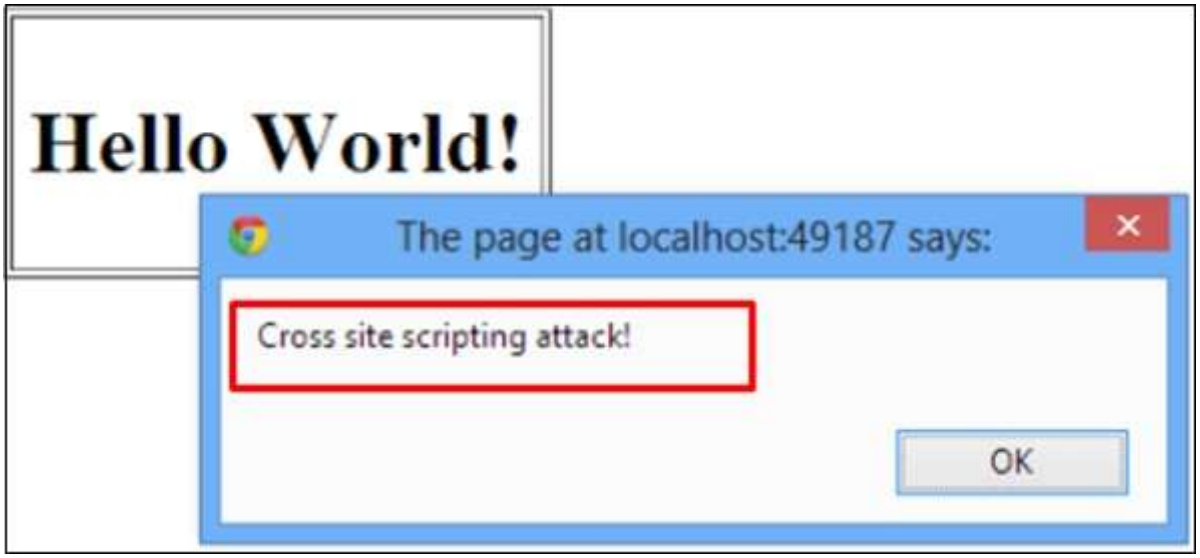
Solution − To secure your site from this flaw, you must make cookies and sessions with expiration time.

Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's

browser, which can then hijack user sessions, deface websites or redirect the user to malicious sites.

Solution − Protection from this is on the same lines as it is for iSQL.



Insecure Direct Object Reference

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory or a database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

Solution − You should implement specific protection mechanisms such as passwords to safeguard such files.

Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server and the platform. Secure settings should be defined, implemented and maintained, as the defaults are often insecure.

Solution − Software should be kept up to date.

Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft or other crimes.

Solution − Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

Missing Function Level Access Control

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests to access functionality without proper authorization.

Solution − You should check the levels of authentication.

Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests which the vulnerable application thinks are legitimate requests from the victim.

Solution − The most commonly used prevention is to attach some unpredictable challenge based tokens to each request that comes from a website and associate them with the user's session.

Using Components with Known Vulnerabilities

Components, such as libraries, frameworks and other software modules almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

Solution − Check if that component version has vulnerabilities and try to avoid or change with another version.

Invalidated Redirects and Forwards

Web applications frequently redirect and forward users to other pages and websites. These applications use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites or use forwards to access unauthorized pages.

Solution − Always validate a URL.

Secure Used Protocols

This is the case where you have a VPS plan and you manage everything on your own. When the services are installed they use default ports. This makes the job easier to a hacker because he knows where to look at.

Some of the main service ports which are used in hosting of websites are given below −

- SSH – port 22
- FTP – port 21
- MySQL – port 3306

- DNS – port 53
- SMTP – port 25

The port changing of those services varies depending on the Operating System and its different versions. In addition to this, you have to install a firewall. If it is a Linux OS, we will recommend **IPtables** and block all the other unneeded ports. In case your OS is Windows, you can use its incorporated firewall.

To block brute force logins in your services, you can use **Fail2ban**, which is a Linux based software and block all the IP addresses which makes many failed login attempts.

Useful Video Courses

Create A WordPress Website In 24 Hours Or Less Guaranteed

23 Lectures 1.5 hours

Zach Miller

More Detail

The Ultimate Guide To Building Your WordPress Website

45 Lectures 2 hours

Zach Miller

More Detail

Google Maps SEO: The 4 Pillars To Rank Your Website Page 1

21 Lectures 2.5 hours

Zach Miller

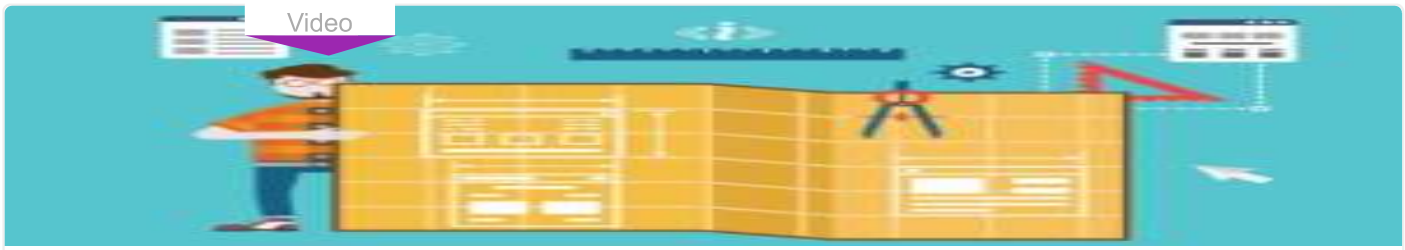
More Detail

Complete CSS Flexbox Course & A Real World Website Project

21 Lectures 2.5 hours

DigiFisk (Programming Is Fun)

More Detail



CSS Grid - Build Modern Real World Websites Fast (+Projects)

52 Lectures 4 hours

DigiFisk (Programming Is Fun)

More Detail

E Commerce Website Development In PHP With PDO

100 Lectures 34 hours

Azaz Patel

More Detail