**DEPARTMENT: COMPUTER SCIENCE**

**COURSE CODE: CSC 413**

**COURSE TITTLE: INTERNET TECHNOLOGY & WEB DESIGN**

**AN ASSIGNMENT ON THE TOPIC: WEB SECURITY**

**BY:**

GROUP D

**MEMBERS**

U18/FNS/CSC/1132 ABUBAKAR IDRIS BAKO

U19/FNS/CSC/2101 SALIHU MUHAMMAD BELLO

U19/FNS/CSC/2103 MARAFA BATHOLOMEW

U18/FNS/CSC/1011 DAVID CEPHAS GAZA

U18/FNS/CSC/1012 SAMSON ENDURANCE LAMIGNI

**SUBMITTED ON**

4th May, 2023

**ABSTRACT**

Web security is important to keeping hackers and cyber-thieves from accessing sensitive information. Without a proactive security strategy, businesses risk the spread and escalation of malware, attacks on other websites, networks, and other IT infrastructures. If a hacker is successful, attacks can spread from computer to computer, making it difficult to find the origin.

Web security is a broad category of security solutions that protect your users, devices, and wider network against internet-based cyberattacks—malware, phishing, and more—that can lead to breaches and data loss. It reduces the security risk to your organization when your users accidentally access malicious files and websites through some combination of firewall inspection, intrusion prevention system (IPS) scanning, sandboxing, URL filtering, and various other security and access controls.

**INTRODUCTION**

web security refers to the protective measures and protocols that organizations adopt to protect the organization from cyber criminals and threats that use the web channel. Web security is critical to business continuity and to protecting data, users and companies from risk. It's also refers to protecting networks and computer systems from damage to or the theft of software, hardware, or data. It includes protecting computer systems from misdirecting or disrupting the services they are designed to provide.

Web security is synonymous with cybersecurity and also covers website security, which involves protecting websites from attacks. It includes cloud security and web application security, which defend cloud services and web-based applications, respectively. Protection of a virtual private network (VPN) also falls under the web security umbrella.

Web security is crucial to the smooth operation of any business that uses computers. If a website is hacked or hackers are able to manipulate your systems or software, your website—and even your entire network—can be brought down, halting business operations.

**METHODOLOGY**

Secondary data analysis is the methodology used in this assignment. The secondary data analysis refers to the use of existing research data to find answer to a question that was different from the original work Secondary data can be large scale surveys or data collected as part of personal research. In other word, Secondary analysis is a form of research that uses existing data, or secondary data, collected previously to perform a new study. Researchers might use quantitative or qualitative data another research team or agency gathered or produced for different reasons and analyze it in a new way. That data might be publicly available or the researcher or analyst might need permission to access and use it. The data they use typically comes from trusted government and research sources.

**TECHNOLOGIES OF WEB SECURITY**

Various technologies are available to help companies achieve web security, including web application firewalls (WAFs), security or vulnerability scanners, password-cracking tools, fuzzing tools, black box testing tools, and white box testing tools.

**Web Application Firewalls (WAFs):** Protects web applications by monitoring and filtering internet traffic that flows between an application and the internet. In this way, a WAF works as a secure web gateway (SWG). It provides protection for web applications against attacks, including cross-site scripting, file inclusion, cross-site forgery, Structured Query Language (SQL) injection, and other threats.

In the Open Systems Interconnection (OSI) model, a WAF works within Layer 7. Even though it works against many internet threats, it is not intended to defend against all kinds of threats. A WAF often works within a suite of protective tools meant to defend a network, computer, or application.

**Security or Vulnerability Scanners**

**Vulnerability Scanners**: Refers to tools that organizations use to automatically examine their systems, networks, and applications to check for weaknesses in their security. Once a vulnerability scanner has finished checking the target system, security teams can use the results to address critical vulnerabilities.

**Password Cracking Tools**: With password cracking tools, you can still gain access to your system even if you have lost or forgotten your password. This helps maintain web security for business in a couple of different ways.

First, if you need to reset your password but cannot remember the original one, a password-cracking tool allows you to gain access. Second, if someone has penetrated your system and changed the password, you can use a password-cracking tool to get back in and change the password to something harder to figure out, thereby regaining control.

**Fuzzing Tools**: Are used to check software, networks, or operating systems for coding errors that may result in security weaknesses. Once an error is found, a fuzzer pinpoints the potential causes of the problem.

Fuzzing tools can be valuable at various stages of the software development process as well. Whether implemented during initial testing, before final deployment, or somewhere in between, developers can use them to gain insights into vulnerabilities so they can be addressed.

**WEB SECURITY VULNERABILITIES**

* **SQL Injection**: This type of flaw enables an attacker to tamper with an application’s database queries by injecting code. In most attacks, hackers can retrieve data belonging to other users or related to the application itself, such as passwords, credit card details, and cookies.

When an SQL injection attack goes awry, an attacker may attempt a denial-of-service attack or compromise the underlying web server or other back-end infrastructure.

* **Cross-site Scripting (XSS):** It is a widely used technique to execute code, most commonly JavaScript, in the targeted website or application. A successful cross-site scripting grants attackers access to the entire application. An example of an XSS attack is when a hacker exploits an input field’s vulnerability and uses it to inject malicious code into another website.

Hackers have complete control over what happens once their targets click on the infected link. The main reason why XSS is considered a high-risk security flaw is that it allows an attacker to view data stored in LocalStorage, SessionStorage, or cookies on the target system. Hence, no personal data should be stored in these systems.

* **Cross-site Request Forgery (CSRF):** A CSRF attack employs social engineering techniques to convince a user to modify application data such as the username or password. A CSRF attack requires an application that uses session cookies solely to identify the user making a request. These cookies are then used to track or validate user requests. Depending on the action the user is forced to complete, the attacker can steal money, accounts, or perform other web application attacks.

**DEFENSE STRATEGIES FOR DEVELOPER FOR WEB SECURITY**

**Resource Assignment:** With a resource assignment strategy, a developer designates the needed resources in a way that lets the developer know about new issues as they arise. With constant updates, the developer can identify and take action against threats before security actually gets breached.

**Web Scanning:** Web scanning involves using an application to crawl a website in search for vulnerabilities that can leave it open to a bot, spyware, root kit, Trojan horse, or distributed denial-of-service (DDoS) attack. The scanner checks all the pages on the website, forming a diagram complete with a structure representing the layout of the site. It then systematically checks the entire site for potential weaknesses.

**LITERATURE REVIEW ON WEB SECURITY**

This paper focuses on a literature review on the vulnerability of web security and defense strategies to mitigate the web threats.

**REFERENCE**

Why Web Security Is So Important - Strategy Marketing Agency. www.strategynewmedia.com

Web Security - Definition, Benefits, Technologies - Zscaler. www.zscaler.com

What is web security? - Minecast. www.minecast.com

Web Application Security: Best Practices and Tools - Hostinger. www.hostinger.com

Web Security and Website Security - Fortinet. www.fortinet.com