Network Security June 2022 B

Unit 3

Assignment on Vulnerability Audit and Assessment - Baseline Analysis and Plan

Introduction:

Website is chosen: **https://tigertek.org.uk**

The following website vulnerability scanner tools were used to scan the website and were very helpful to run the business as per security standards. It helps to find vulnerabilities like SQL Injection, XSS, OS Command Injection, Directory Traversal, and many more.

- Qualys SSL Labs - Website scanner
- Mozilla Observatory
- Pen-test tools - Website Vulnerability Scanner

Identifying and Analysis of Vulnerabilities:

Following vulnerabilities were identified in the above website using these vulnerability scanning tools.

Insecure cookie setting: Missing Secure flag

The secure flag is not set for cookies containing such sensitive information on this website. If such a request is made and the cookie's secure flag is not set, the browser will deliver the data over an unencrypted channel (plain HTTP). As a result, there is a chance that an attacker will eavesdrop on the browser's clear-text connection with the server and steal the user's cookie.

Insecure cookie setting: Missing HttpOnly flag

The HttpOnly flag is not set for all cookies. A cookie has been set without the HttpOnly flag, allowing the JavaScript code executing on the web page to access it. The cookie will be accessible and can be sent to another website if an attacker is successful in inserting malicious JavaScript code on the page (for example, using an XSS attack). This could result in session hijacking in the case of a session cookie.

Missing security header: Content-Security-Policy

Cross-Site Scripting vulnerabilities are prevented from being exploited by web browsers thanks to the Content-Security-Policy (CSP) header (XSS). The absence of this header makes the target application easy exploitable by attackers if it is an XSS-vulnerable application. Identified that Content-Security-Policy is not configured for this website.

Missing security header: X-XSS-Protection

X-XSS-Protection header not implemented. When a browser detects reflected Cross-Site Scripting (XSS) attacks, it is told to cease loading web pages by the X-XSS-Protection HTTP header. In the event that the online application has such a vulnerability, the absence of this header exposes application users to XSS attacks.

Missing security header: Referrer-Policy

Referrer-Policy, a new header that should be set by all sites, enables a site to manage the amount of information the browser includes with navigations away from a document. This referral policy is not configured.

Missing security header: Permissions-Policy

A new header called Permissions Policy enables a site to manage which browser features and APIs can be utilised. It is not enabled on the server-side.

Security.txt file is missing:

The security.txt file has been found to be missing on the server. Not making a proper Security.txt file for your server has no special danger. However, this file is crucial since it

provides a specific mechanism for reporting security flaws and vulnerabilities. The security file is not enabled on the server side.

DNS CAA is not enabled:

Certification Authority Authorization (CAA) record is recommended for any public website. Public key pinning (HPKP) and CAA have comparable goals, however, HPKP's implementation is completely different. First, HPKP is a run-time client-side control that stops already-issued certificates from being regarded as legitimate, whereas CAA inhibits certificate issuance. In other words, HPKP is for browsers, whereas CAA is for CAs. In contrast to CAA, which is mostly an administrative control, HPKP, which operates by whitelisting public keys, is a powerful technical control.

SNI is not enabled:

Server Name Indication (SNI) is not enabled. When a client (user) device connects to the correct IP address for a website but the name on the SSL certificate doesn't match the name of the website, this is referred to as a "common name mismatch error" and is prevented by SNI. This type of issue frequently causes the user's browser to display the warning "Your connection is not private."

Weak Ciphers enabled on TLSv1.2:

Following weak ciphers are enabled on the TLS1.2 version on this website.

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

References:

J. Fonseca, M. Vieira and H. Madeira, "Testing and Comparing Web Vulnerability Scanning Tools for SQL Injection and XSS Attacks," 13th Pacific Rim International Symposium on Dependable Computing (PRDC 2007), 2007, pp. 365-372, doi: 10.1109/PRDC.2007.55.

Y. Makino and V. Klyuev, "Evaluation of web vulnerability scanners," 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2015, pp. 399-402, doi: 10.1109/IDAACS.2015.7340766.

https://pentest-tools.com/website-vulnerability-scanning/website-scanner [Accessed on 2nd Jul 2022]

https://observatory.mozilla.org/ [Accessed on 1st Jul 2022]

https://www.ssllabs.com/projects/index.html [Accessed on 1st Jul 2022]