UJI KERENTANAN KEAMANAN PADA APLIKASI *WEBSITE* APOTEK XYZ MENGGUNAKAN OWASP *(Open Website Application Security Project)*

Aldio Rasyid

ABSTRAK

Seiring dengan perkembangan teknologi digital, keamanan aplikasi website menjadi isu yang semakin krusial. Aplikasi website telah menjadi salah satu sarana utama komunikasi dan transaksi di era digital. Namun, pertumbuhan ini juga membawa peningkatan risiko keamanan. Aplikasi website yang rentan dapat menyebabkan pencurian data, hilangnya privasi pengguna, atau konsekuensi serius bagi bisnis. Oleh karena itu, pengujian kerentanan keamanan aplikasi website menjadi langkah esensial untuk melindungi dari ancaman. Dalam penelitian ini, aplikasi website Apotek XYZ menjadi objek kajian untuk mengidentifikasi dan menganalisis kerentanan keamanannya menggunakan panduan *OWASP Top 10*. Proses penelitian dilakukan melalui tiga tahap utama: pengumpulan informasi, pemindaian, dan pengujian. Tahap pengumpulan informasi menggunakan alat seperti *Netcraft*, *Subfinder*, *Whois*, *Httprint*, *Whatweb*, dan *Nmap* untuk mengidentifikasi data terkait *IP address*, subdomain, alamat hosting, server, *HTTP headers*, dan port yang terbuka. Pada tahap pemindaian, *OWASP ZAP* mengidentifikasi delapan celah keamanan, termasuk lima dengan kategori risiko *medium* dan tiga dengan kategori risiko *low*. Kemudian dilakukan *penetration testing* dari total 8 celah keamanan yang termasuk dalam kategori *OWASP Top 10* dengan perhitungan *risk severity*. Di antara temuan ini, satu celah berisiko tinggi yaitu *Parameter Tampering*, menonjol sebagai ancaman signifikan. Kesimpulan dari penelitian ini menyoroti berbagai kerentanan keamanan yang ditemukan pada aplikasi website Apotek XYZ dan memberikan rekomendasi praktis untuk memperbaiki celah-celah tersebut guna meningkatkan keamanan aplikasi. Rekomendasi yang dapat diberikan untuk memperbaiki celah keamanan website Apotek XYZ yaitu mengimplementasikan validasi *server-side* sebelum memberikan akses kepada pengguna, mengkonfigurasi *cookie* dengan flag *HttpOnly* dan *attribute SameSite*, menggunakan *parameterized queries* untuk mencegah *SQL Injection*, menerapkan mekanisme otorisasi yang kuat dan melindungi terhadap manipulasi URL, menyertakan header *X-Frame-Options* untuk mencegah *clickjacking*, mengonfigurasi *error handling* dengan tepat untuk menyembunyikan informasi sensitif, menghapus header *X-Powered-By* untuk menyembunyikan informasi server, memperbarui libraries *JavaScript* secara berkala, menyertakan *csrf_token* dalam form untuk melindungi form secara otomatis, dan mengimplementasikan header *Content-Security-Policy* untuk membatasi jenis resource yang diperbolehkan. Implementasi rekomendasi tersebut diharapkan dapat meningkatkan keamanan dan keandalan website Apotek XYZ terhadap serangan siber.

Kata kunci : *Website, Penetration Testing,* OWASP, OWASP Top 10

Security Vulnerability Testing on XYZ Pharmacy Website Application Using OWASP (Open Web Application Security Project)

Aldio Rasyid

ABSTRACT

As technology advances, the security of web applications has become an increasingly crucial issue. Websites have become a primary means of communication and transactions in the digital era. However, this growth also brings increased security risks. Vulnerable web applications can lead to data theft, loss of user privacy, or serious business consequences. Therefore, vulnerability testing of web applications is an essential step in protecting against threats. This study focuses on the Apotek XYZ website to identify and analyze its security vulnerabilities using the OWASP Top 10 guidelines. The research process was carried out in three main stages: information gathering, scanning, and testing. The information gathering stage used tools such as Netcraft, Subfinder, Whois, Httprint, Whatweb, and Nmap to identify data related to IP addresses, subdomains, hosting addresses, servers, HTTP headers, and open ports. In the scanning stage, OWASP ZAP identified eight security vulnerabilities, including five medium-risk and three low-risk categories. Penetration testing revealed a total of 8 security vulnerabilities falling into OWASP Top 10 categories with risk severity calculation. Among these findings, one high-risk vulnerabilities, Parameter Tampering, stood out as significant threats. The conclusion of this study highlights the various security vulnerabilities found on the Apotek XYZ website and provides practical recommendations to fix these issues to enhance the application's security. The recommendations for improving the security of the Apotek XYZ website include implementing server-side validation before granting user access, configuring cookies with the HttpOnly flag and SameSite attribute, using parameterized queries to prevent SQL Injection, enforcing strong authorization mechanisms and protecting against URL manipulation, including the X-Frame-Options header to prevent clickjacking, properly configuring error handling to hide sensitive information, removing the X-Powered-By header to obscure server information, regularly updating JavaScript libraries, including csrf_token in forms to protect them automatically, and implementing the Content-Security-Policy header to restrict allowed resource types. Implementing these recommendations is expected to improve the security and reliability of the Apotek XYZ website against cyber attacks.

Keywords : ***Website, Penetration Testing*****, OWASP, OWASP Top 10**