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

SKRIPSI

Disusun Oleh :

Aldio Rasyid

1910511008

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2024

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

SKRIPSI

Diajukan Kepada Fakultas Ilmu Komputer

Universitas Pembangunan Nasional Veteran Jakarta

Untuk Memenuhi Syarat Memperoleh Gelar Sarjana Strata Informatika

Disusun Oleh :

Aldio Rasyid

1910511008

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2024

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri dan sumber yang dikutip maupun yang dirujuk telah saya nyatakan benar:

Nama : **Aldio Rasyid**

NIM 1910511008

Tanggal : 16 Juli 2024

Judul Skripsi : **Uji Kerentanan Keamanan Pada Aplikasi *Website* Apotek XYZ Menggunakan OWASP (*Open Web Application Security Project*)**

Bilamana pada kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Bekasi, 16 Juli 2024

Yang menyatakan,

Aldio Rasyid

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademika Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Aldio Rasyid
NIM : 1910511008
Fakultas : Ilmu Komputer
Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan karya ilmiah saya kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non-Eksklusif (*Non-Exchange Royalty Free Right*) untuk dipublikasikan dengan judul:

Uji Kerentanan Keamanan Pada Aplikasi *Website* Apotek XYZ Menggunakan OWASP (*Open Web Application Security Project)*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media atau memformatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasi skripsi saya selama tetap mencantumkan nama saya sebagai penulis atau pencipta data sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Bekasi
Pada tanggal : 16 Juli 2024

Yang Menyatakan,

Aldio Rasyid

LEMBAR PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama : Aldio Rasyid

NIM 1910511008

Program Studi : S1 Informatika

Judul Tugas Akhir : Uji Kerentanan Keamanan Pada Aplikasi *Website* Apotek XYZ Menggunakan OWASP (*Open Web Application Security Project*)

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Dr. Widya Cholil, S.Kom., MIT.
Penguji I

Rio Wirawan, S.Kom., MMSI.
Penguji II

Henki Bayu Seta, S.Kom., MTI.
Pembimbing

Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM.
Dekan

Dr. Widya Cholil, S.Kom., MIT.
Kepala Program Studi

Ditetapkan di : Jakarta
Tanggal Ujian : 10 Juli 2024

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**

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan judul "Uji Kerentanan Keamanan pada Aplikasi Website Apotek XYZ Menggunakan OWASP (Open Website Application Security Project)". Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer pada Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Penulis menyadari bahwa tanpa dukungan, bimbingan, dan dorongan dari berbagai pihak, penyusunan skripsi ini tidak akan berjalan dengan baik dan selesai tepat pada waktunya. Oleh karena itu, penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Allah Yang Maha Esa, yang telah memberikan kesehatan serta ilmu kepada penulis sehingga dapat menyelesaikan skripsi ini dengan baik.
2. Orang tua dan keluarga penulis yang selalu memberikan dukungan moral dan material serta doa yang tiada henti.
3. Bapak Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM selaku Dekan Fakultas Ilmu Komputer UPN Veteran Jakarta beserta jajarannya.
4. Ibu Dr. Widya Cholil, M.I.T. selaku Kepala Program Studi Informatika UPN Veteran Jakarta.
5. Bapak Henki Bayu Seta, S.Kom., MTI., selaku dosen pembimbing yang telah memberikan bimbingan, saran, dan motivasi kepada penulis dalam menyusun skripsi ini.
6. Ibu Nurul Afifah Arifuddin, S.Pd., M.T. selaku dosen pembimbing akademik.
7. Seluruh jajaran Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta yang telah membantu dalam perizinan dan administrasi.
8. Teman-teman dan sahabat penulis yang telah memberikan semangat, bantuan, serta kebersamaan yang berarti selama proses penyusunan skripsi ini.
9. Teman-teman Informatika angkatan 2019 selama berkuliah di UPN Veteran Jakarta. Terima kasih atas pengalaman, dan bantuannya ketika mengalami kesulitan.

10. Semua pihak yang tidak dapat penulis sebutkan satu per satu yang telah membantu dan memberikan dukungan dalam bentuk apapun.

Penulis menyadari bahwa penyusunan skripsi ini jauh dari sempurna. Oleh karena itu, penulis harap kepada para peneliti selanjutnya untuk memberikan saran dan kritik yang bersifat membangun untuk kesempurnaan skripsi ini. Akhir kata penulis berharap semoga skripsi ini mampu bermanfaat untuk semua pihak.

Bekasi, 13 Juni 2024

Aldio Rasyid

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL