2024

Rabu, 8 Mei

TUGAS

La Ode Muhammad Yudhy Prayitno
NIM E1E122064

Analisis Keamanan Website BPJS Kesehatan Menggunakan Metode Vulnerability Asesement

Mata Kuliah
Cyber Security

Dosen Pengajar
L. M. Fid Aksara S.Kom., M.Kom.

A. Latar Belakang

Di era digital saat ini, keamanan website menjadi aspek krusial yang harus diperhatikan, terutama bagi lembaga publik seperti Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan yang mengelola data sensitif dari jutaan peserta. Meskipun BPJS Kesehatan telah menerapkan standar keamanan ISO 27001, potensi peretasan dan kebocoran data tetap mengancam. Oleh karena itu, analisis keamanan website BPJS Kesehatan dengan menggunakan metode vulnerability assessment sangat diperlukan untuk mengidentifikasi celah keamanan yang ada dan meningkatkan kerahasiaan, integritas, serta ketersediaan layanan data bagi peserta.

Oleh karena itu, sebagai respons terhadap permasalahan tersebut, penulis menawarkan solusi dengan melakukan analisis keamanan website menggunakan tool Open Web Application Security Project (OWASP). Melalui analisis ini, berbagai kerentanan yang memungkinkan terjadinya serangan pada website BPJS Kesehatan dapat diidentifikasi secara sistematis. Dengan demikian, langkah-langkah perlindungan yang sesuai dapat diimplementasikan untuk mengurangi risiko serangan dan meningkatkan keamanan sistem secara keseluruhan.

B. Vulnerability Assessment

Vulnerability Assessment adalah sebuah kerangka kerja konseptual yang komprehensif, yang mencakup definisi kerentanan untuk mengukur risiko. Dengan tergantung pada tujuan penggunaan hasil penilaian, penggunaan kerangka kerja ini dapat bervariasi, mulai dari keinginan untuk memberikan informasi kepada politik internasional hingga mengambil tindakan di tingkat masyarakat. Vulnerability Assessment digunakan untuk melakukan pengujian terhadap titik-titik yang berpotensi sebagai pintu masuk serangan. Selain itu, kerangka kerja ini juga berguna dalam mengidentifikasi masa berlakunya versi perangkat lunak, mendeteksi port-port yang terbuka, dan bahkan mengenali aplikasi-aplikasi yang sedang berjalan.

C. OWASP

Open Web Application Security Project (OWASP) adalah sebuah kerangka kerja sumber terbuka yang difokuskan pada peningkatan keamanan perangkat lunak aplikasi, khususnya aplikasi web. OWASP merupakan sebuah organisasi yang didedikasikan untuk menemukan dan mengatasi kerentanan dalam aplikasi web.

Meskipun OWASP tidak memiliki afiliasi dengan perusahaan teknologi tertentu, namun mereka mendukung penggunaan teknologi keamanan komersial. OWASP menghasilkan berbagai jenis proyek melalui kolaborasi terbuka, termasuk Web Security Testing Guide (WSTG), OWASP Top Ten, WSTG Checklist v4.2, dan lain sebagainya.

Ada sebelas langkah yang dapat dilakukan untuk mengevaluasi dan menguji keamanan situs web sesuai standar yang diterbitkan oleh OWASP. Langkah-langkah ini meliputi pengumpulan informasi, manajemen konfigurasi, transmisi aman, otentikasi, manajemen sesi, otorisasi, enkripsi, serta validasi data. Selain itu, langkah-langkah juga mencakup penanganan penolakan layanan dan penanganan kesalahan. Dengan mengikuti langkah-langkah ini, pengembang dapat memperbaiki dan meningkatkan keamanan situs web mereka sesuai dengan standar keamanan yang ditetapkan oleh OWASP.

D. OWASP-ZAP

OWASP ZAP (Zed Attack Proxy) adalah sebuah aplikasi yang digunakan untuk melakukan pengujian penetrasi guna menemukan celah keamanan pada aplikasi website. Secara otomatis, ZAP menyediakan pemindai yang membantu dalam proses ini (Guntoro et al., 2020). ZAP juga merupakan salah satu proyek unggulan dari OWASP. Selain menyediakan fitur pemindai otomatis, ZAP juga dilengkapi dengan seperangkat program yang memungkinkan pengguna untuk mendeteksi celah keamanan secara manual. Selain itu, ZAP juga mampu menghasilkan laporan mengenai temuan keamanan dalam format HTML dan XML. Dengan demikian, ZAP menjadi alat yang sangat berguna dalam upaya meningkatkan keamanan aplikasi web.

E. Pembahsan

1. Planning

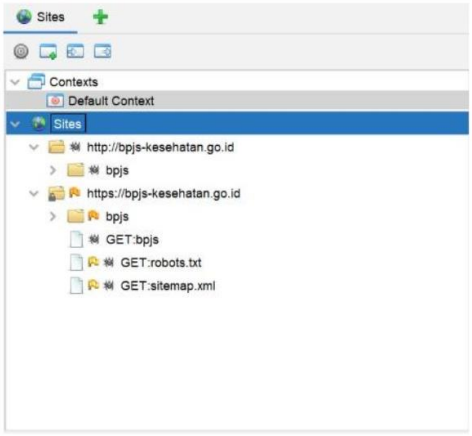
Pada tahap ini, persiapan kebutuhan untuk melakukan pengujian celah keamanan pada website BPJS Kesehatan telah disiapkan. Berikut adalah beberapa hal yang diperlukan:

Table 1 Peralatan yang dibutuhkan

Peralatan	*Spesifikasi*
Laptop	OS : Windows 10 Home 64-bit Processor : Intel(R) Core(TM) i7-8565U Memory : 8192MB RAM
OWASP ZAP	OWASP ZAP versi 2.11.0
Koneksi Internet	Up to 20 Mbps
Web Browser	Chrome

2. Information Gathering

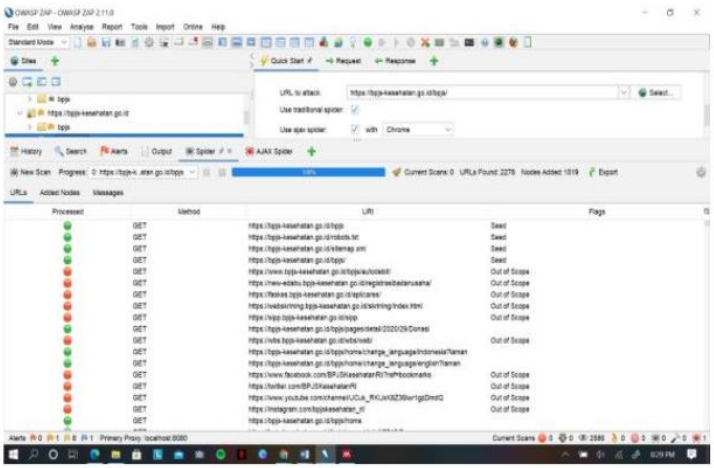
Di tahap ini, peneliti mengumpulkan informasi yang terdapat pada website BPJS Kesehatan. Situs yang sedang dipindai akan disimpan langsung pada sesi OWASP ZAP. Pemindaian yang dilakukan menggunakan OWASP ZAP tidak hanya bertujuan untuk menemukan kelemahan, tetapi juga untuk mendeteksi keberadaan file tertentu.



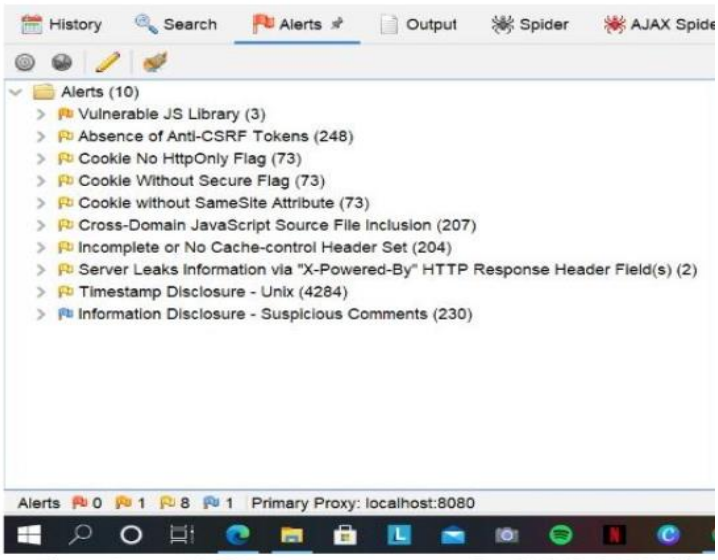
Gambar 1 Sites BPJS Kesehatan

3. Operasi Pengujian Kerentanan

Proses pengujian atau pendeteksian kerentanan pada website BPJS Kesehatan dilakukan menggunakan tool OWASP ZAP, sesuai dengan penjelasan sebelumnya.



Gambar 2 Proses Pemindaian Website BPJS Kesehatan



Gambar 3 Kerentanan pada Web BPJS Kesehatan

Proses awal pengujian dilakukan dengan melakukan pemindaian pada website BPJS Kesehatan. Proses pemindaian ini bertujuan untuk mendeteksi kerentanan pada website tersebut, seperti yang terlihat pada Gambar 4. Hasil dari pemindaian ini ditampilkan pada Gambar 5, yang menunjukkan kerentanan pada website BPJS Kesehatan dengan berbagai tingkat risiko yang berbeda.

Table 2 Kerentanan pada website BPJS Kesehatan

Type	*URL*	*Risk*	*Confidence*
Vulnerable JS Library	https://bpjs-kesehatan.go.id/bpjs/themes/admin/js/jquery-1.7.2.js	Medium	Medium
Absence of Anti-CSRF Tokens	https://bpjs-kesehatan.go.id/bpjs/	Low	Medium
Cookie No HttpOnly Flag	https://bpjs-kesehatan.go.id/bpjs/	Low	Medium
Cookie Without Secure Flag	https://bpjs-kesehatan.go.id/bpjs/	Low	Medium
Cookie without SameSite Attribute	https://bpjs-kesehatan.go.id/bpjs/	Low	Medium
Cross-Domain JavaScript Source File Inclusion	https://bpjs-kesehatan.go.id/bpjs/	Low	Medium
Incomplete or No Cache-control Header Set	https://bpjs-kesehatan.go.id/bpjs/	Low	Medium
Secure Pages Include Mixed Content	https://bpjs-kesehatan.go.id/bpjs/multimedia/index/114	Low	Medium
Server Leaks Information via "X-Powered-By" HTTP Response Header	https://bpjs-kesehatan.go.id/robots.txt	Low	Medium
Timestamp Disclosure - Unix	https://bpjs-kesehatan.go.id/bpjs/	Low	Low
Information Disclosure - Suspicious Comments	https://bpjs-kesehatan.go.id/bpjs/	Informational	Low

Dalam penelitian ini, ditemukan sebelas kerentanan pada website BPJS Kesehatan, dengan rincian informasi sebagai berikut: terdapat 9 kasus dengan tingkat risiko rendah (low), 1 kasus dengan tingkat risiko menengah (medium), dan 1 kasus lainnya hanya bersifat informatif, seperti yang terdokumentasikan dalam Tabel 2.

4. Deskripsi Kerentanan dan Solusi Penanganan Kerentanan

Berdasarkan hasil analisis menggunakan tool OWASP ZAP terhadap kerentanan pada website BPJS Kesehatan yang telah dijelaskan sebelumnya, berikut adalah rekomendasi solusi penanganan untuk setiap kerentanan:

a) Jquery library yang diidentifikasi, versi 1.7.2 rentan. Solusinya adalah meningkatkan versi jquery ke yang terbaru.
b) Tidak ada token Anti CSRF yang ditemukan dalam formulir pengiriman HTML. Solusinya adalah menggunakan perpustakaan atau kerangka kerja yang tidak memungkinkan serangan CSRF terjadi.
c) Cookie disetel tanpa tanda HttpOnly, yang berarti cookie dapat diekspos ke JavaScript. Solusinya adalah mengatur tanda HttpOnly pada cookie untuk mencegah akses melalui JavaScript.
d) Cookie disetel tanpa tanda aman, yang berarti cookie dapat diakses melalui koneksi yang tidak terenkripsi. Solusinya adalah pastikan cookie yang sensitif selalu diteruskan melalui saluran terenkripsi.
e) Cookie disetel tanpa atribut SameSite, yang berarti cookie dapat dikirim sebagai permintaan 'lintas situs'. Solusinya adalah pastikan atribut SameSite diatur dengan benar pada semua cookie.
f) Halaman berisi file skrip dari domain pihak ketiga. Solusinya adalah pastikan file sumber JavaScript dimuat hanya dari sumber tepercaya.
g) Header kontrol cache belum disetel dengan benar atau tidak ada. Solusinya adalah pastikan header HTTP kontrol-cache disetel dengan benar.
h) Halaman mencakup konten campuran, yaitu konten yang diakses melalui HTTP, bukan HTTPS. Solusinya adalah pastikan halaman yang tersedia melalui SSL/TLS terdiri dari konten yang dikirimkan melalui SSL/TLS.
i) Server web/aplikasi membocorkan informasi melalui header respons HTTP "X-Powered-By". Solusinya adalah pastikan konfigurasi server web Anda untuk menekan header "X-Powered-By".
j) Stempel waktu diungkapkan oleh aplikasi/server web – Unix. Solusinya adalah pastikan data stempel waktu tidak sensitif dan tidak dapat digabungkan untuk mengungkapkan pola yang dapat dieksploitasi.
k) Tanggapan tampaknya berisi komentar mencurigakan yang dapat

membantu penyerang. Solusinya adalah hapus semua komentar yang dapat memberikan informasi yang dapat dimanfaatkan oleh penyerang.

Dengan menerapkan solusi-solusi di atas, diharapkan dapat mengurangi risiko kerentanan pada website BPJS Kesehatan dan meningkatkan keamanannya.

F. Kesimpulan

Hasil pengujian ini mengungkapkan sebelas celah kerentanan pada website BPJS Kesehatan yang ditemukan melalui pemindaian menggunakan tool OWASP ZAP versi 2.11.0. Selain itu, solusi-solusi untuk menangani kerentanan tersebut juga diperoleh. Penelitian ini bertujuan untuk melakukan uji penetrasi menggunakan OWASP ZAP versi 2.11.0 dengan tujuan menguji keamanan website BPJS Kesehatan. Dari hasil penelitian, dapat disimpulkan bahwa website BPJS Kesehatan tergolong aman untuk digunakan, dan penggunaan OWASP ZAP terbukti sangat efektif dalam mendeteksi kerentanan.