

BAB V

PENUTUP

5.1 KESIMPULAN

Berdasarkan hasil penelitian dan analisis keamanan website Karkoon Group Asia menggunakan metode penetration testing yang mengacu pada standar OWASP Top 10, maka dapat ditarik beberapa kesimpulan sebagai berikut:

1. Metode penetration testing berbasis OWASP Top 10 terbukti efektif dalam mengidentifikasi dan mengevaluasi tingkat keamanan aplikasi web Karkoon Group Asia. Pendekatan ini mampu memberikan gambaran kondisi keamanan website secara sistematis melalui tahapan information gathering, vulnerability scanning, proof of concept (PoC), hingga analisis risiko.
2. Ditemukan tiga jenis kerentanan keamanan pada website Karkoon Group Asia dengan tingkat keparahan yang berbeda, yaitu:
 - 1) Kerentanan Access Restriction Bypass via Origin Spoof dengan tingkat risiko High, yang diklasifikasikan ke dalam kategori A01 – Broken Access Control. Secara teori berbahaya karena bisa membuat attacker melewati kontrol akses. Namun PoC membuktikan tidak terjadi bypass, sehingga tidak berbahaya pada sistem yang diuji (*False Positive*).
 - 2) Kerentanan Missing Strict-Transport-Security (HSTS) Header dengan tingkat risiko Medium, yang termasuk dalam kategori A05 – Security Misconfiguration. Jika benar ada, bisa menyebabkan downgrade attack HTTP. Namun karena header sudah ada di server, maka risiko tidak ada.

HSTS terbukti telah diterapkan dan berfungsi pada sisi klien (*False Positive*).

- 3) Kerentanan Missing X-Frame-Options Header dengan tingkat risiko Low, yang juga termasuk dalam kategori A05 – Security Misconfiguration. Kerentanan ini berpotensi clickjacking, Tetapi karena sudah ada mitigasi, maka risikonya rendah.

3. Secara keseluruhan, rekomendasi perbaikan difokuskan pada penguatan kontrol akses dan konsistensi konfigurasi keamanan, dengan mempertimbangkan hasil verifikasi manual agar tindakan perbaikan yang dilakukan bersifat tepat sasaran. Pendekatan ini diharapkan dapat meningkatkan tingkat keamanan aplikasi web sekaligus mengurangi potensi kesimpulan keliru akibat keterbatasan konteks pada alat pemindaian otomatis.

5.2 SARAN

Berdasarkan hasil penelitian dan kesimpulan yang telah diperoleh, maka beberapa saran yang dapat diberikan adalah sebagai berikut:

1. Bagi Pengelola Website Karkoon Group Asia

- 1) Disarankan untuk memperbaiki mekanisme kontrol akses, khususnya dengan tidak mengandalkan validasi berbasis HTTP header yang dapat dimanipulasi oleh klien.
- 2) Menerapkan header keamanan tambahan seperti Strict-Transport-Security (HSTS) dan X-Frame-Options secara konsisten untuk meningkatkan perlindungan komunikasi data dan antarmuka pengguna.

- 3) Melakukan pengujian keamanan secara berkala, baik melalui penetration testing internal maupun audit keamanan eksternal, guna mendeteksi potensi kerentanan sejak dini.
- 4) Memastikan seluruh komponen website, termasuk CMS, plugin, dan library pendukung, selalu diperbarui untuk meminimalkan risiko dari komponen rentan atau usang.

2. Bagi Penelitian Selanjutnya

- 1) Penelitian selanjutnya dapat memperluas ruang lingkup pengujian tidak hanya pada sisi aplikasi web, tetapi juga mencakup aspek keamanan jaringan, server, dan infrastruktur pendukung.
- 2) Disarankan untuk menggunakan lebih banyak tools penetration testing atau pendekatan manual yang lebih mendalam guna memperoleh hasil analisis yang lebih komprehensif.
- 3) Penelitian berikutnya juga dapat mengkaji perbandingan efektivitas beberapa standar keamanan, seperti OWASP Top 10, PTES, atau ISSAF, dalam pengujian keamanan website.

Dengan adanya penelitian ini, diharapkan hasil yang diperoleh dapat menjadi referensi akademik serta acuan praktis bagi pengelola website dalam meningkatkan keamanan aplikasi web secara berkelanjutan