Analisis Hasil Uji Penetrasi menggunakan metode Information Systems Security Assessment Framework (ISSAF) pada Website = Analysis of Penetration Testing Result using Information Systems Security Assessment Framework (ISSAF) method in a Website

Marcella Cinninthya Putri, author

Abstrak

Pengujian penetrasi merupakan suatu langkah penting yang diambil untuk meningkatkan keamanan sebuah website, terutama bagi suatu perusahaan. Terdapat beberapa kerangka kerja dan metodologi untuk uji penetrasi, salah satunya adalah Information Systems Security Assessment Framework (ISSAF). ISSAF merupakan sebuah kerangka kerja yang komprehensif dengan keunggulan pada domain coverage sehingga memungkinkan pengujian bukan hanya dari luar sistem, namun juga masuk ke dalam sistem. Penelitian ini menunjukan tahapan uji penetrasi menggunakan kerangka kerja ISSAF dan memanfaatkan beberapa tools yang umum digunakan untuk mengidentifikasi kerentanan website bagi perusahaan. Hasil dari penelitian ini ditemukan 7 kerentanan, diantaranya yaitu Clickjacking, Brute-force Attack pada Login Page, HSTS Missing From HTTP Server, Content Security Policy (CSP) Header Not Set , Cookie without SameSite Attribute, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s),serta X-Content-Type-Options Header Missing. Dari hasil pengujian penetrasi ini dapat dijadikan rekomendasi untuk mengatasi kerentanan keamanan pada perusahaan-perusahaan di bidangnya.

.....

Penetration testing is an important step taken to improve the security of a website, especially for a company. There are several frameworks and methodologies for penetration testing, one of which is the Information Systems Security Assessment Framework. (ISSAF). ISSAF is a comprehensive framework with advantages on domain coverage that allows testing not only from outside the system, but also into the system. This research demonstrates the stage of penetration testing using the ISSAF framework and utilizes several commonly used tools to identify website vulnerabilities for companies. This study we found seven vulnerabilities in the target website, including Clickjacking, Brute-force Attack on Login Page, HSTS Missing from HTTP Server, Content Security Policy (CSP) Header Not Set, Cookie without SameSite Attribute, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), and X-Content-Type-Options Header Missing. From this penetration test results, a recommendation to address security vulnerabilities in companies can be conducted.