

Analisis Hasil Uji Penetrasi dengan Menggunakan Framework Penetration Testing Execution Standard (PTES) pada Website Redstorm. = Penetration Test Results Analysis using the Penetration Testing Execution Standard (PTES) Framework on the Redstorm Website.

Chusnul Nabilah, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=9999920525775&lokasi=lokal>

Abstrak

Ancaman keamanan terhadap *website* biasa dihasilkan melalui celah yang memungkinkan pengguna lain melakukan tindak kejahatan. Untuk pemeliharaan keamanan *website* yang baik, deteksi kerentanan *website* dapat dilakukan dengan prosedur *vulnerability identification* dan *penetration testing*. *Penetration Testing Execution Standard* (PTES) digunakan pada penelitian ini sebagai kerangka kerja atau *framework* *penetration testing* dengan tujuan untuk mendapatkan hasil akhir berupa kerentanan yang dapat mengganggu keamanan *website*. Terdapat tujuh tahapan yang akan dilakukan pada *framework* PTES yaitu *Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation,* dan *Reporting*. *Penetration testing* ini juga menerapkan metode *blackbox testing*. *Blackbox testing* adalah metode pengujian yang dilakukan tanpa mengetahui informasi apa pun mengenai sistem *website*. Ditemukan tiga kerentanan dengan tingkat risiko tinggi pada *website* redstorm setelah melakukan *penetration testing* dengan *framework* PTES dan metode *blackbox* *testing*, yaitu PII *Disclosure*, SQL *Injection*, dan SQL *Injection*-SQLite. Hasil ini menekankan perlunya penguatan keamanan *website* dan penerapan langkah-langkah mitigasi yang sesuai untuk melindungi data sensitif dan melawan potensi serangan. Selain itu, penelitian ini menegaskan efektivitas dan relevansi kerangka kerja PTES dalam mengidentifikasi kerentanan keamanan sistem. Implikasi dari temuan ini memberikan kontribusi bagi pengembangan kebijakan keamanan informasi dan penelitian tentang keamanan siber yang lebih lanjut.

.....

Security threats to common websites are generated by gaps that allow other users to commit criminal acts. For good website security maintenance, website vulnerability detection can be done with vulnerability identification and penetration testing procedures. The Penetration Testing Execution Standard (PTES) is used in this research as a framework for penetration testing with the aim of obtaining the final result of vulnerabilities that can interfere with the operation of the website. There are seven stages that will be performed on the PTES framework: Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-exploitation, and Reporting. The penetration test also uses the blackbox testing method. Blackbox testing is a test method that is performed without knowing any information about the website system. Three high-risk vulnerabilities were found on Redstorm websites after performing penetration testing with the PTES framework and blackbox testing methods, namely PII Disclosure, SQL Injection, and SQL injection-SQLite. The results emphasize the need to strengthen website

security and implement appropriate mitigation measures to protect sensitive data and counter potential attacks. In addition, the study confirms the effectiveness and relevance of the PTES framework in identifying system security vulnerabilities. The implications of these findings contribute to the development of information security policies and further research on cybersecurity.