ANALISIS RESIKO KEAMANAN TERHADAP WEBSITE DINAS PENANAMAN MODAN DAN PELAYANAN TERPADU SATU PINTU PEMERINTAHAN XYZYZ MENGGUNAKAN STANDAR PENETRATION TESTING *EXECUTION* STANDARD (PTES)

ANALYSIS OF OROS MODELER DATA REPORTING PROCESS TO SAP HANA IN ACTIVITY BASED COSTING FOR INDONESIA TELECOMMUNICATION INDUSTRY

Dennis Nigel Cunong[1], Muhardi Saputra[2], Warih Puspitasari[3]

[1,2,3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]denniscunong@student.telkomuniversity.ac.id, [2]muhardi@telkomuniveristy.co.id,
[3]warihpuspitasari@telkomuniversity.ac.id

Abstrak

Perkembangan teknologi yang pesat dapat mempengaruhi setiap individu, organisasi, bahkan pemerintahan dalam penyampaian informasi secara akurat, efektif, dan efisien. Pemerintahan daerah XYZ adalah instansi yang bertugas melayani masyarakat dalam pengurusan administrasi di daerah XYZ. Informasi pemerintahan dikelola oleh Dinas Komuniasi, Informatika dan Statistika (Diskominfo) daerah XYZ sebagai instansi yang bergerak dibidang teknologi informasi. Diskominfo memanfaatkan kemajuan teknologi untuk menyampaikan informasi kepada masyarakat daerah XYZ dan di luar daerah XYZ melalui website dengan tujuan mempermudah dalam penyampaian informasi. Seiring perkembangan teknologi, keamanan terhadap suatu website menjadi sesuatu hal yang penting karena dapat mencegah serangan dari orang yang tidak bertanggung jawab, karena dapat merusak sistem atau merugikan proses bisnis yang berjalan. Dengan begitu, kita perlu melakukan pengujian terhadap kerentanan yang dimiliki oleh website tersebut yaitu dengan cara melakukan *Vulnerability Assessment dan Penetration Testing*. Sebelum melakukan pengujian kita perlu melakukan analisis terhadap celah keamanan yang ditemukan. Pada proses analisis ini dimana seorang penguji mesimulasikan dirinya sebagai cracker yang berusaha melakukan analisis celah keamanan untuk dapat masuk kedalam sistem. Saat ini tandar *Penetration Testing Execution Standard* (PTES). Standar ini dipilih karena memiliki tahapan yang jelas dan mudah untuk dipahami.

Kata kunci: analisis celah kemanan, website, PTES.

Abstract

The rapid development of technology can affect every individual, organization, and even government in conveying information accurately, effectively and efficiently. Local government XYZ is a body in charge of serving the public in administrative management in the XYZ field. Government information is managed by the Office of Communication, Information and Statistics (Diskominfo) region XYZ as an institution engaged in information technology. Diskominfo utilizes technological advances to convey information to people in Region XYZ and outside Region XYZ through the website with the aim of facilitating the transmission of information. As technology develops, website security becomes important because it can prevent attacks from irresponsible people, because it can damage the system or endanger ongoing business processes. That way, we need to test the vulnerability of the website by conducting a Vulnerability Assessment and Penetration Testing. Before conducting the test, we need to do a vulnerability analysis that is found. In this analysis process, where a tester simulates himself as a cracker who tries to do a security vulnerability analysis to enter the system. Currently Penetration Testing Execution Standards (PTES) are standard. This standard was chosen because it has stages that are clear and easy to understand.

Keywords: Vulnerability Analysis, website, PTES

1. Pendahuluan

Website merupakan suatu media yang dapat menyampaikan dan memperoleh informasi kapanpun dan dimanapun. *Website* menggunakan protokol *Hypertext Transfer Protocol* (HTTP) untuk dapat diakses melalui *web browser*, sedangkan dokumen pada *website* disimpan dalam *web server* [1]. *Web server* diterapkan agar *website* dapat komunikasi dengan *client* (*web browser*) [2]. Peretasan *website* bertujuan untuk mendapatkan informasi rahasia atau penting tanpa seizin pemilik *website* dan ada juga yang mengubah tampilan dari *website* tersebut dengan tujuan tertentu [3]. Sebagian *website* masih kurang memperhatikan keamanannya sehingga masih terdapat beberapa celah untuk *cracker* memperoleh informasi penting atau merubah informasi pada *website* tersebut. Pengelolaan kemanan *website* dilakukan secara berkala dengan tujuan mengantisipasi celah keamanan yang terdapat pada *website* tersebut. Beberapa celah keamanan pada umumnya ditemukan seperti *cross-site, scripting, information leakage, authentication and authorization, session management,* SQL, CSRF, dan masih banyak lainnya. Mengontrol kerentanan keamanan *website* dapat dilakukan dengan *vulnerability assessment and penetration testing*. Tujuan dilakukannya VAPT adalah menemukan celah keamanan dan penanganan celah kemanan tersebut agar *website* tersebut dapat dioptimalkan dalam pemeliharaannya [4].

2. Dasar Teori

2.1 *Website* Pemerintahan Daerah XYZ

Website XYZ merupakan salah satu *website* yang dikelola langsung oleh pemerintahan daerah XYZ. *Website* XYZ merupakan platform penyelenggaraan layanan perizinan dan non perizinan Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kabupaten XYZ. Pada *website* ini ada beberapa layanan yang dapat diberikan kepada pengguna yaitu *online single submission*, SILONCER sistem layanan online cetak sendiri, Monitoring perizinian, dan pengaduan.

2.2 *Vulnerability Assessment*

Vulnerability Assessment adalah salah satu cara untuk melakukan pengukuran terhadap keamanan sistem dengan menemukan kerentanan. *Vulnerability assessment* dapat menjadi suatu acuan untuk bagaimana strategi pengelolaan sistem yang benar dan pengawasan terhadap keamanan sistem informasi melalui kerentanan yang ditemukan. Kerentanan pada saat sekarang sangat sering terjadi sehingga membutuhkan operasional seperti manajemen tambahan. Insiden terhadap kerentanan yang terjadi pada setiap sistem sangat berpengaruh terhadap kinerja sistem selama masih berjalan berjalan. Analisis *vulnerability* dapat memperkirakan tindakan yang efektif untuk dilakukan agar dapat melakukan pencegahan secara efektif dan aktual setelah mengetahui kerentanan dalam sistem [5].

Langkah-langkah yang dapat dilakukan untuk melakukan analisis *vulnerability* adalah:
1. Menentukan dan mengklasifikasikan jaringan atau sistem
2. Menetapkan tingkat kepentingan
3. Mengidentifikasi potensi ancaman
4. Mengembangkan strategi untuk menghadapi masalah
5. Menentukan dan menerapkan solusi untuk pencegahan terjadinya penyerangan

Setelah selesai melakukan analisis, maka tentukan apakah termasuk dalam faktor ancaman tinggi atau tidak, jika merupakan ancaman tinggi maka sistem harus dihentikan sementara waktu untuk melakukan perbaikan [5].

3. Metode yang Digunakan

PTES adalah standar yang dikembangkan pada tahun 2010 dan dapat digunakan untuk melakukan analisis dan audit sistem keamanan *website* [6]. Celah keamanan pada *website* biasanya terjadi dalam prosedur keamanan, perangkat lunak, kontrol sistem internal, atau saat melakukan pemasangan infrastruktur yang dapat meningkatkan ingritas, kerahasiaan, akuntabilitas atau mengguanakn data atau layanan.*vulnerability assessment* dapat melakukan analisis celah keamanan terhadap serangan dan memberikan saran untuku dapat mengurangi resiko terhadap *website* target. Tujuan pada metode ini yaitu memberikan hasil pengujian celah keamanan pada aplikasi *website*, hasil pengujian akan menjadi tolak ukur untuk melakukan peningkatan keamanan pada *website*. Hasil laporan celah keamanan akan membantu perusahaan atau organisasi dalam meningkatkan keamanan *website* target. PTES memiliki 7 tahapan untuk melakukan implemantasi, mulai dari *Pre-engagement Interactions* hingga *reporting*. Berikut merupakan tahapan-tahapan PTES [7]:

3.1 *Pre-engagement Interactions*

Pada bagian ini bertujuan untuk menyediakan dan menjelaskan alat dan teknik yang membantu dalam langkah persiapan dari *pen testing*. Informasi dapat diperoleh dari berbagai sumber termasuk dari pengalaman penguji yang telah melakukan pentesting bertahun-tahun. Langkah ini sangat penting sebelum memulai langkah pentesting.

Pentesting tidak harus konfrontatif, karena seharusnya kegiatan pentesting bukan mengenai berhasil diretas atau tidak, tetapi tentang mengidentifikasi resiko bisnis yang dapat diserang [1].

3.2 *Intelligence Gathering*

Pada tahapan ini melakukan pengumpulan informasi tentang pentesting. Tujuan dari informasi yang diperoleh adalah untuk menyediakan dan merancang tindakan yang akan dilakukan sesuai dengan kesepakatan dari target [1].

3.3 *Threat Modeling*

Tahapan ini akan melakukan identifikasi terhadap pendekatan pemodelan ancaman yang diperlukan untuk melakukan pentesting. Fokus standar ini bergantung pada proses bisnis dan aset bisnis perusahaan. Fase pemodelan ancaman sangat penting untuk penguji dan perusahaan, karena pada pemodelan ini dapat memberi kejelasan terhadap resiko dan prioritas target [1].

3.4 *Vulnerability Analysis*

Tahapan ini akan melakukan identifikasi terhadap pendekatan pemodelan ancaman yang diperlukan untuk melakukan pentesting. Fokus standar ini bergantung pada proses bisnis dan aset bisnis perusahaan. Fase pemodelan ancaman sangat penting untuk penguji dan perusahaan, karena pada pemodelan ini dapat memberi kejelasan terhadap resiko dan prioritas target [1].

3.5 *Exploitation*

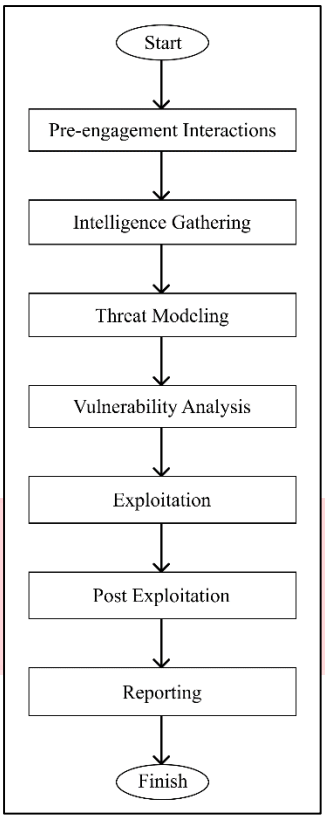
Pada tahapan ini tidak hanya berfokus kepada pembangunan akses ke sistem. Karena pada tahapan ini sangat diperlukan perencanaan yang baik dan pengambilan keputusan yang tepat. Fokus utama melakukan *exploitation* adalah mengidentifikasi titik masuk ke dalam *website* target yang memiliki nilai tinggi (penting). Jika tahapan *vulnerability analysis* selesai dengan benar, daftar target bernilai tinggi seharusnya dipenuhi. Pada akhir serangan harus mempertimbangkan probabilitas keberhasilan dan dampak tertinggi pada target [1].

3.6 *Post Exploitation*

Tujuan dari *post exploitation* adalah untuk menentukan nilai dari *website* dan melakukan konsultasi agar dapat memberikan saran terhadap pertahanan *website*. *Website* dinilai dari data yang memiliki sensitifitas tinggi berupa data identitas, data keuanagan dan data perencanaan. Metode yang dijelaskan dalam tahapan ini dimaksudkan untuk membantu tester mengidentifikasi dan mendokumentasikan data sensitif, mengidentifikasi pengaturan konfigurasi, saluran komunikasi, dan hubungan dengan perangkat jaringan lain yang dapat digunakan untuk mendapatkan akses lebih lanjut ke jaringan, dan mengatur satu atau lebih metode mengakses *website* [1].

3.7 *Reporting*

Tujuan dari tahapan ini adalah menentukan nilai kerentanan dan mempertahankan untuk dapat mengontrol saat digunakan. Tingkatan nilai ditentukan dari tingkat sensitivitas data yang tersimpan di dalamnya dan kegunaannya. Tahapan ini dimaksudkan untuk membantu penguji mengidentifikasi dan mendokumentasikan data sensitif, mengidentifikasi hasil konfigurasi, saluran komunikasi, dan hubungan dengan perangkat jaringan lain yang dapat digunakan untuk memperoleh akses lebih lanjut [1].



Gambar 1: Tahapan PTES

4. Pengujian dan Analisis

Penelitian ini berfokus pada penemuan celah keamanan dalam aplikasi *website* pemerintahan daerah XYZ, sehingga dapat memberikan rekomendasi keamanan yang dapar diberikan untuk meningkatkan sistem aplikasi *website*. Sebelum melakukan pengujian celah keamanan terhadap *website* target, perlu mengumpulkan informasi untuk menentukan tindakan pengujian. Pada panalitian ini menggunakan satu *tool information gathering* untuk informasi dasar yaitu Zenmap dan dua *tools vulnerability assessment* untuk melakukan pengujian kerentanan yaitu Nikto dan OWASP-ZAP. Proses pengujian menggunakan *virtual machine* dengan sistem operasi kali linux. Tujuan dari penelitian ini adalah menemukan celah keamanan pada *website* pemerintahan daerah XYZ.

4.1 *Information Gathering* dengan *Tool* Zenmap

Zenmap merupakan aplikasi berbasis GUI dan multi platform sebagai interface sederhana untuk nmap. Zenmap merupakam salah satu tools untuk eksploitasi jaringan dan audit keamanan secara gratis (*open source*) [2]. Zenmap digunakan untuk mendapatkan *information gathering* berupa port dan sistem yang digunakan oleh *website* target. Penelitian ini, pengujian akan dilakukan terhadap *website* pemerintahan daerah XYZ. Berikut merupakan hasil pengujian menggunakan *tool* Zenmap:

1. IP Address Pemerintahan daerah XYZ yaitu 220.XXX.XXX.XXX
2. Port 443 merupakan port yang tebuka pada *website* pemerintahan daerah XYZ. Port tersebur digunakan untuk menjalankan *web server web server* yang aman atau SSL.
3. Port 1723 merupakan port yang terbuka pada *website* pemerintahan daerah XYZ.Port tersebut digunakna untuk melakukan pengaturan PPTP VPN (*Point-to-Point Tunneling Protocol Virtual Private Networking*).

4.2 *Vulnerability Assessment* dengan *tool* Nikto

Nikto adalah aplikasi *open source* yang digunakan untuk melakukan pengujian kerentanan pada *website* dengan CLI (*Command Line Interface*) [2]. Pada aplikasi Nikto terdapat 6700 potensi kerentanan file atau program untuk pengujian [3]. Berikut hasil pengujian menggunakan *tool* Nikto.

Risk Level	Detail of Alert
High	XSS-Protection
Medium	X-Frame-Option
Low	Strict-Transport-Security HTTP
	Expect-CT
	The X-Content-Type-Options header
	Content-Encoding header

4.3 *Vulnerability Assessment* dengan *tool* OWASP-ZAP

OWASP-ZAP adalah aplikasi *vulnerability scanner* yang dapat digunakan secara gratis (*open source*), aplikasi ini dikembangkan oleh organisasi OWASP. Fitur yang terdapat pada OWASP-ZAP antaralain *Active and passive scanner, Dynamis SSL Certificates, Anti CSRF token handling, Brute Force, Fuzzing, Smart card support, Parameter analysis, Intercepting Proxy, Spider scan, Extensibility, Report Generation, Auto tagging, Session Comparison, Port Scanner, Invoke external apps, Api + headless mode* [4]. Berikut merupakan hasil pengujian menggunakan OWASP-ZAP.

Risk Level	Detail of Alerts
High	Cross Site Scripting
	SQL Injection
	Remote OS Command Injection
Medium	X-Frame-Options Header Not Set
	Application Error Disclosure
	Buffer Overflow
	Format String Error
Low	Incomplete or No Cache-control and Pragma HTTP Header Set
	Cookie No HttpOnly Flag
	X-Content-Type-Options Header Missing
	Web Browser XSS Protection Not Enabled
	Password Autocomplete in Browser
	Cookie Without Secure Flag

5. Kesimpulan

Kesimpulan dari penelitian yang telah dilakukan, bahwa *website* pemerintahan daerah XYZ masih memiliki banyak celah keamanan yang dapat dimanfaatkan oleh peretas untuk melakukan penyerangan terhadap *website*. Terdapat 1 celah keamanan dengan resiko tinggi, 4 celah keamanan dengan resiko sedang, dan 9 celah keamanan dengan celah keamanan dengan resiko rendah. Dengan ditemukannya semua celah keamanan dapat membentu pemerintahan daerah XYZ untuk mengembangkan *website* degan mudah.

Untuk penelitian lebih lanjut, disarankan untuk menggunakan berbagai *tools* dan metode yang berbeda untuk menemukan celah keamanan yang berbeda. Penelitian ini juga dapat menjadi referensi untuk semua orang dalam melakukan audit keamanan suatu *website*, baik dari segi metode maupun *tools* yang digunakan.

6. Referensi

[1] The PTES Team, "The Penetration Testing *Execution* Standard Documentation," p. 3, 2017.

[2] E. B. Setiawan and A. Setiyadi, "Web vulnerability analysis and implementation," *IOP Conference Series: Materials Science and Engineering*, p. 4, 2018.

[3] J. Ruhiyat and A. Setiyadi, "Sistem Monitoring Website dengan Metode ISSAF di Dinas Komunikasi dan Informatika Kabupaten Tanggerang," *Jurnal Ilmiah Komputer dan Informatika (KOMPUTA) UNIKOM*, p. 3, 2019.

[4] A. P. Dewanto, "Penetration Testing Pada Domain uii.ac.ic Menggunakan OWASP 10," *Tugas Akhir Universitas Islam Indonesia*, p. 14, 2018.

[5] T. Evi and Malabay, "Analisis Pengembangan Aplikasi Web Untuk Profil Perusahaan," *Seminar Nasionl Informatika*, pp. E-123, 2009.

[6] A. Aziz and T. Tanpati, "Analisis Web Server untuk Pengembangan Hosting Server Institusi: Pembandingan Kinerja Web Server Apache dengan NginXYZ," *Jurnal Multinetics Vol. 1 No. 2*, p. 13, 2015.

[7] N. WK, Network Hacking Dengan LinuXYZ BackTrack, Semarang: Penerbit Andi, Wahana Komputer, 2012.

[8] L. M. Gultom and H. Mawaddah, "Analisis Celah Keamanan Website Instansi Pemerintah Di Sumatera Utara," *Teknovasi*, p. 1, 2015.

[9] A. Gupta, K. and K. Kaur, "Vulnerability Assessment and Penetration Testing," *Journal of Engineering Trends and Technology*, p. 328, 2013.

[10] A. Aziz and T. Tanpati, "Analisis Web Server untuk Pengembangan Hosting Server Institusi: Pembandingan Kinerja Web Server Apache dengan NginXYZ," *JURNAL MULTINETICS VOL. 1 NO. 2*, p. 13, 2015.

[11] N. WK, Network Hacking Dengan LinuXYZ BackTrack, Semarang: Penerbit ANDI, WAHANA KOMPUTER, 2012.

[12] K. M. F, S. Saadati and A. Ahmadi, "Vulnerability Assessment and Risk Reduction of Water Supply Systems," *World Environmental and Water Resources Congress 2010: Challenges of Change*, p. 4414, 2010.

[13] F. A. Dabaseh and E. Alshammri, "Automated Penetration Testing: an Overview," *Dhinaharan Nagamalai et al. (Eds)* , pp. 124-125, 2018.