JURNAL RISTEC : Research in Information Systems and Technology
Vol. 4 No. 2 Tahun. 2023

Conducting Penetration Testing to Identify Vulnerabilities in a Bank Company Information Technology

Nava Gia Ginasta[1*], Krisnawanti[2], Fikri Fahru Roji[3]
[1]Program Studi Bisnis Digital, Fakultas Logistik Teknologi dan Bisnis, Universitas Logistik dan Bisnis Internasional, Jalan Sariasih No. 54, Bandung, Jawa Barat, 40151, Indinesia
[2]Manajemen Rekayasa, Fakultas Logistik Teknologi dan Bisnis, Universitas Logistik dan Bisnis Internasional, Jalan Sariasih No. 54, Bandung, Jawa Barat, 40151, Indinesia
[3]Program Studi Bisnis Digital, Fakultas Ekonomi, Universitas Garut, Garut, Jawa Barat, Indonesia
*Penulis koresponden, *e-mail* : *navgia@ulbi.ac.id*

Abstract: Company XYZ is a regional business entity that manages finances and provides credit to small businesses. However, their e-banking applications have vulnerabilities that hackers can exploit. This research aims to identify and understand potential attacks on these vulnerabilities, assess the impact of exploitation by attackers, and provide recommendations for securing computer systems and networks based on penetration testing results. The XYZ e-banking application web server can be tested using five methods: Vulnerability Scanning, Apache Tomcat Sample Directory Vulnerabilities, Cross-Site Request Forgery (CSRF), Weak Cryptographic Testing, and Header Security. The application is in the Warning to High category, which indicates that it requires follow-up action. To mitigate the vulnerability, developers can take steps such as deleting the /examples directory, limiting the validity of cookies, using SSL and enabling Mod Security.

Keywords: Applications; e-Banking; Vulnerability; Penetration Test; Webserver

Abstrak: Perusahaan XYZ merupakan badan usaha daerah yang mengelola keuangan dan memberikan kredit kepada usaha kecil. Namun, aplikasi e-banking mereka memiliki kerentanan yang dapat dieksploitasi oleh peretas. Penelitian ini bertujuan untuk mengidentifikasi dan memahami potensi serangan terhadap kerentanan tersebut, menilai dampak eksploitasi yang dilakukan penyerang, dan memberikan rekomendasi untuk mengamankan sistem dan jaringan komputer berdasarkan hasil pengujian penetrasi. Web server aplikasi e-banking XYZ dapat diuji menggunakan lima metode: Vulnerability Scanning, Vulnerabilities Direktori Contoh Apache Tomcat, Cross Site Request Forgery (CSRF), Weak Cryptographic Testing, dan Header Security. Aplikasi tersebut masuk dalam kategori Peringatan hingga Tinggi yang menandakan memerlukan tindakan tindak lanjut. Untuk mengurangi kerentanan, pengembang dapat mengambil langkah-langkah seperti menghapus direktori /examples, membatasi validitas cookie, menggunakan SSL, dan mengaktifkan Keamanan Mod.

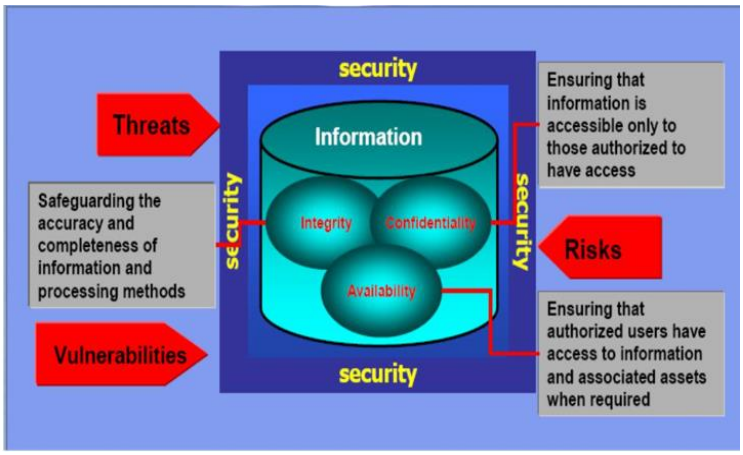
Kata kunci: Aplikasi; e-Banking; Kerentanan; Penetration Test; Web server

PENDAHULUAN

Perkembangan teknologi informasi yang demikian cepat, disatu sisi memberikan dampak positif terhadap kesejahteraan manusia, namun disisi lain teknologi informasi dapat dimanfaatkan untuk hal-hal negatif yang menjurus kearah kriminalitas (*cyber crime*), mulai dari aktifitas hacker seperti *scanning port, cracking password, web defacement*, sampai DDOS. Aktifitas kenakalan *user*, seperti *enumerasi, sniffers, gaining access* dan *escalating privilage.* Atau yang menjurus kearah kriminal seperti *carding*, dan *phising.* Dengan banyak beredarnya *exploit* atau *tools hackinng* melalui jaringan internet, yang memacu kegiatan instrusi terhadap jaringan public (internet) dan

bahkan sudah mampu memasuki jaringan private yang memiliki kelemahan *(vulnerability*) pada sistem jaringannya (*Network vulnerability*).

Informasi merupakan aset terpenting sebuah Organisasi/Perusahaan yang tidak bisa diukur dengan nilai finansial (Krisnawanti et al., 2023). Gambar 1 menunjukkan data harus dilindungi dengan berbagai cara, karena kepercayaan customer dan keberlanjutan operasional Teknologi Informasi organisasi (Business Continuity) serta ketersediaan (Availability) data supaya tidak jatuh ke tangan pesaing atau bahkan ke pihak yang lebih merugikan. Oleh karena itu, informasi sebuah Organisasi/Perusahaan mutlak untuk dikelola dan diproteksi dengan baik sehingga menjadikannya sebagai competitive advantages bagi organisasi/perusahaan.



Gambar 1. Ancaman Terhadap Informasi Milik Organisasi/Perusahaan

Perusahaan XYZ merupakan Badan Usaha Milik Daerah (BUMD) yang bergerak dibidang perbankan. Perusahaan tersebut bertugas mengelola keuangan daerah yaitu sebagai pemegang Kas Daerah dan membantu meningkatkan ekonomi daerah dengan memberikan kredit kepada perusahaan kecil. Saat ini perusahaan telah menggunakan Teknologi Informasi berupa Aplikasi untuk mempermudah proses bisnisnya. Namun aplikasi tersebut memungkinkan *user* dapat mengakses informasi penting yang apabila disalahgunakan akan merugikan perusahaan (Supriady et al., 2023). Selain itu, sistem yang memiliki tingkat keamanan yang rendah dapat berpotensi mempermudah masuknya *hacker* ke dalam sistem yang berdampak pada kerusakan atau beralihnya fungsi sistem yang telah dibangun (Fachri et al., 2021). Sehingga perlu upaya untuk mengamankan aplikasi tersebut baik dari sisi infrastruktur maupun aplikasi. Ketangguhan organisasi dalam melawan serangan daat diamati untuk mengevaluasi sikap keamanan informasi organisasi. Salah satu cara untuk memastikan sistem tersebut aman adalah dengan melakukan pengujian penetrasi untuk menemukan kerentanan baru pada suatu sistem (Riandhanu, 2022).

Beberapa penelitian telah melakukan pengujian keamanan *web server* dengan menggunakan metoode *penetration testing* (Fachri, 2023; Fachri et al., 2021; Hidayatulloh & Saptadiaji, 2021; Pohan, 2021; Santoso et al., 2022) Terdapat tiga jenis *penetration testing* yang dapat dilakukan yaitu

External Penetration Testing (Black Box Testing) (Teguh Yuwono et al., 2021), Pengujian kotak abu-abu, dan *Internal Penetration Testing* (*White Box Testing)*. Penelitian ini bertujuan untuk menentukan dan mengetahui serangan-serangan yang bisa terjadi terhadap kerentanan yang ada pada sistem, mengetahui dampak bisnis yang diakibatkan dari hasil eksploitasi yang dilakukan oleh penyerang atau *hacker.* Sehingga dapat memberikan rekomendasi dan langkah-langkah pengamanan sistem dan jaringan komputer terhadap hasil *penetration testing.*

KAJIAN PUSTAKA

Pengertian *Penetration Testing*

Penetration testing merupakan metode untuk mengevaluasi keamanan sistem dan teknologi informasi termasuk di dalamnya komputer dab atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya (Fachri et al., 2021). Tujuan dari pengujian ini adalah untuk memperoleh semua kemungkinan kerentanan keamanan yang ada. Kerentanan dipahami sebagai risiko bahwa penyerang dapat mengganggu atau mendapatkan akses resmi ke sistem atau data yang terkandung di dalamnya. Kerentanan biasanya ada secara tidak sengaja. Kererntanan umum adalah kesalahan desain, kesalahan konfigurasi, kesalahan perangkat lunak, dan lain sebagainya. Momen kerentanan diantaranya pengembangan prangkat lunak, implementasi perangkat lunak, mengkonfigurasi perangkat lunak, pengenalan infrastruktur baru, dan mengkonfigurasi komponen jaringan.

Pengujian penetrasi berfokus pada pengujian potensi kerentanan yang terkait sistem yang ada (Fauzan & Syukhri, 2021). Pengujian ini dilakukan dengan lengkap sebelum sistem Teknologi Informasi diterapkan, dan diulang secara teratur baik secara rutin maupun saat sistem dikonfigurasi ulang untuk memastikan perlindungan dari kerentanan baru.

Klasifikasi Risk Level

Untuk mengetahui bagian-bagian dari temuan yang terdapat kemungkinan kelemahan yang dapat mempengaruhi ruang lingkup bisnis, klasifikasi Risk Level dibagi menjadi dua kategori:

1. *Likelihood*

   Likelihood adalah kemungkinan terhadap Risiko yang akan muncul dilihat dari kemunngkinan terhadap risiko yang akan muncul *likelihood* dibagi menjadi 5 kategori, yaitu:

   - Definite (Sering) adalah risiko yang akan muncul setiap kali kegiatan dilakukan jika presentasi kemunculan terhadap risiko tersebut lebih dari 80% maka kategori tersebut masuk ke dalam Definite (Sering)

- *Likely* (Beberapa) adalah risiko yang muncul 60%-80% pada saat kegiatan assesment dilakukan, risiko ini dimasukkan ke dalam kategori *Likely* (beberapa).
- *Occasional (*Jarang*)* adalah risiko yang muncul 50/50 pada kegiatan assesment dilakukan, risiko ini dimasukkan ke dalam kategori Occasional (jarang).
- *Seldom* (Sangat Jarang) adalah risiko yang memiliki tingkat kemunculan yang rendah masuk ke dalam kategori ini.
- *Unlikely* (Langka) adalah risiko yang muncul hampir di bawah 10% tingkat kemunculannya pada saat kegiatan assessment berjalan, termasuk ke dalam kategori unlikely.

2. *Consequences*

Tingkat dari dampak yang terjadi atau tingkat kerusakan yang terjadi dari risiko tersebut, Consequenses pun terdapat tingkatan, tingkatan tersebut adalah sebagai berikut:

- Insignificant adalah risiko yang akan menyebabkan masalah yang tidak perlu dalam sebuah kegiatan.
- Marginal adalah jika risiko akan menyebabkan kerusajan tapi kerusakannya tidak begitu besar dan tidak akan menyebabkan perbedaan pada kegiatan.
- Moderate adalah jika risiko yang muncul tidak terlalu menyebabkan ancaman yang besar.
- Critical adalah risiko yang muncul dapat menyebabkan kehilangan beberapa proses fungsional.
- Catastrophic adalah risiko yang muncul dapat menyebabkan proses dan functional bisnis tidak produktif ataupun kerusakan yang sangat fatal.

3. Penggunaan Klasifikasi Risiko

Untuk penggunaan Klasifikasi risiko dibuat table matrix, selanjutnya dibuat kategori untuk menentukan level risiko tersebut.

- High, Risiko yang masuk ke dalam kategori High yang diberi warna hitam pekat adalah risiko dengan level paling tinggi dimana risiko tersebut harus segera mendapatkan action karena risiko ini dapat memengaruhi ruang lingkup bisnis.
- Medium to Hight (M2H), risiko level di bawah high level yang harus tetap mendapatkan action karena Level Medium to High ini dapat mempengaruhi beberapa infrastruktur.
- Medium, Risiko level ini dampak terhadap infrastruktur tidak terlalu parah dan masih dapat di handle dengan mudah.
- Medium to Low (M2L) risiko level ini masih sering ditemukan, biasanya risiko ini tidak berpengaruh terhadap infrastruktur.
- Low, risiko level ini biasanya hanya berupa innformasi mengenai infrastruktur.

Matriks untuk menentukan risiko level ditunjukkan oleh Gambar 2.

Risk rating (CVSS 3)

Pada penelitian ini terdapat sistem scoring, sistem *scoring* ini digunakan untuk menunjukkan seberapa rentan suatu kelemahan yang ditemukan. Tidak semua kelemahan itu memiliki nilai kerentanan yang sama jika dilihat dari ruang lingkup dan dampak yang dihasilkan. Sehingga dibutuhkan suatu standar untuk melakukan scoring terhadap seluruh kelemahan yanng ditemukan. *Common Vulnerability Scoring System version 3* atau biasa disebut CVSS V3 adalah salah satu standar yang telah diakui internasional untuk melakukan hal tersebut. Dipilih CVSS V3 sebagai sistem scoring pada laporan ini karena kemudahan yang ditawarkan CVSS V3 dalam melakukan kalkulasi perhitungan.

C / L	Insignificant	Marginal	Moderate	Critical	Catastrophic
Definite	M2H	M2H	H	H	H
Likely	M	M2H	M2H	H	H
Occasional	M2L	M	M2H	H	H
Seldom	L	M2L	M	M2H	H
Unlikely	L	M2L	M	M2H	M2H

C = Consequences

L = Likelihood

Gambar 2. Matriks Risiko Level

METODE PENELITIAN

Ruang Lingkup Kegiatan

Untuk mencapai tujuan yang telah ditetapkan atas kebutuhan tim IT Perusahaan XYZ untuk melakukan pengujian keamaan teknologi informasi, maka lingkup kegiatan konsultan adalah sebagai berikut:

1. External Network Penetration testing (Black Box Testing)

   Pada proses ini, dilakukan Penetration Testing terhadap Domain dan aplikasi e-banking perusahaan XYZ. Tahap ini dilakukan dengan tujuan untuk mengetahui peluang kerentanan keamanan (*security hole*) yang mungkin dapat dieksploitasi melalui jaringan internet, dan merekomendasikan untuk menutup *security hole* yang ditemukan. Ruang lingkupnya antara lain:

   a. Domain perusahaan.co.id yang tercakup di dalamnya terkait konfigurasi dasar dan kemungkinan celah keamanan pada:
      - DNS server
      - Email server
      - Web server

   b. Aplikasi e-banking Perusahaan XYZ.

2. Internal Network Penetration testing (White Box Testing)

   Pada proses ini, dilakukan pengujian terhadap aplikasi e-Banking dari sisi jaringan internal dengan hak akses yang diberikan *user* ke dalam aplikasi. Ruang lingkupnya adalah Aplikasi e-Banking perusahaan XYZ.

Langkah-Langkah Penelitian

Penelitian ini dibagi menjadi 2 (dua) kelompok kegiatan sebagai berikut, dimana secara keseluruhan telah dapat mengakomodasi kebutuhan pengujian keamanan teknologi informasi e-banking perusahaan XYZ:

1. External Penetration Testing

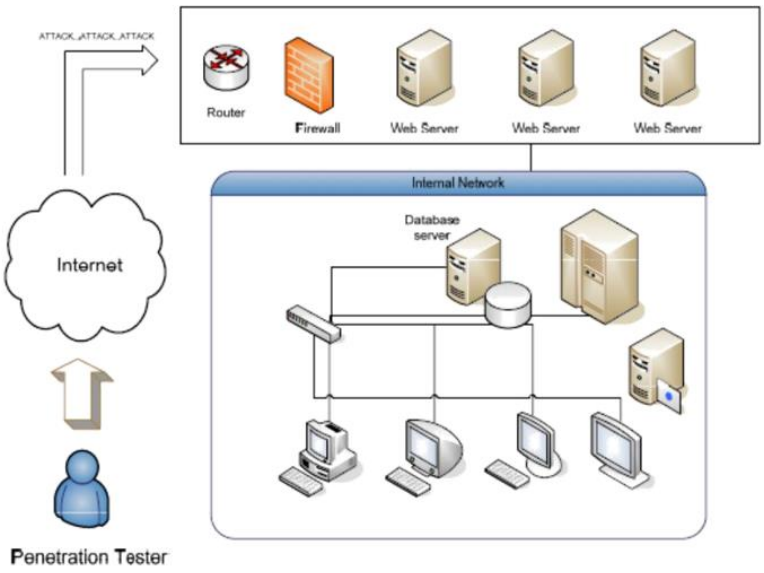
   Pada kegiatan ini, dilakukan uji guna mengetahui tingkat keamanan suatu aplikasi berbasis web. Teknik Black Box yang digunakan mengikuti prosedur standar dari:

   - INDONESE (Internet Domain dan Network Security) Assesmen Framework.
   - OWASP (Open Web Applications Security Project)

   Kegiatan ini dilakukan dengan tujuan untuk mengetahui vurnerability pada Doain dan aplikasi berbasis web Perusahaan XYZ yang mungkin dapat dieksploitasi dan merekomendasikan untuk menutup vulnerability yang ditemukan. Web application penetration test akan dilakukan dari eksternal untuk mensimulasikan serangan dari luar, seperti yang ditunjukkan oleh Gambar 3. Uji ini bertujuan untuk mendapatkan akses kepada informasi yang berharga dengan meng-exploit kelemahan pada web *application*.

   Semua ini dilakukan tanpa informasi awal dari perusahaan XYZ mengenai Domain dan aplikasi berbasis web. Pendekatan ini disebut dengan *black box testing* untuk mengidentifikasi celah keamanan aplikasi berbasis web (W et al., 2016), karena jika terdapat

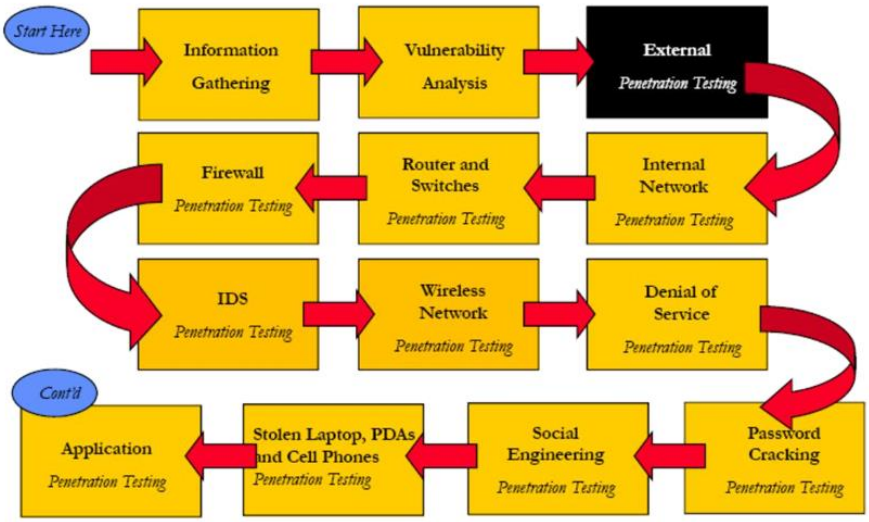
celah keamanan maka dapat digunakan oleh penyerang untuk melakukan *database quiries* atau bahkan mengaktifkan *remote cimmand line* akses menuju server. Gambar 4 dan 5 menyajikan *penetration Testing Roadmap* yang dilalui oleh penelitian ini hingga memperoleh hasil yang diinginkan.



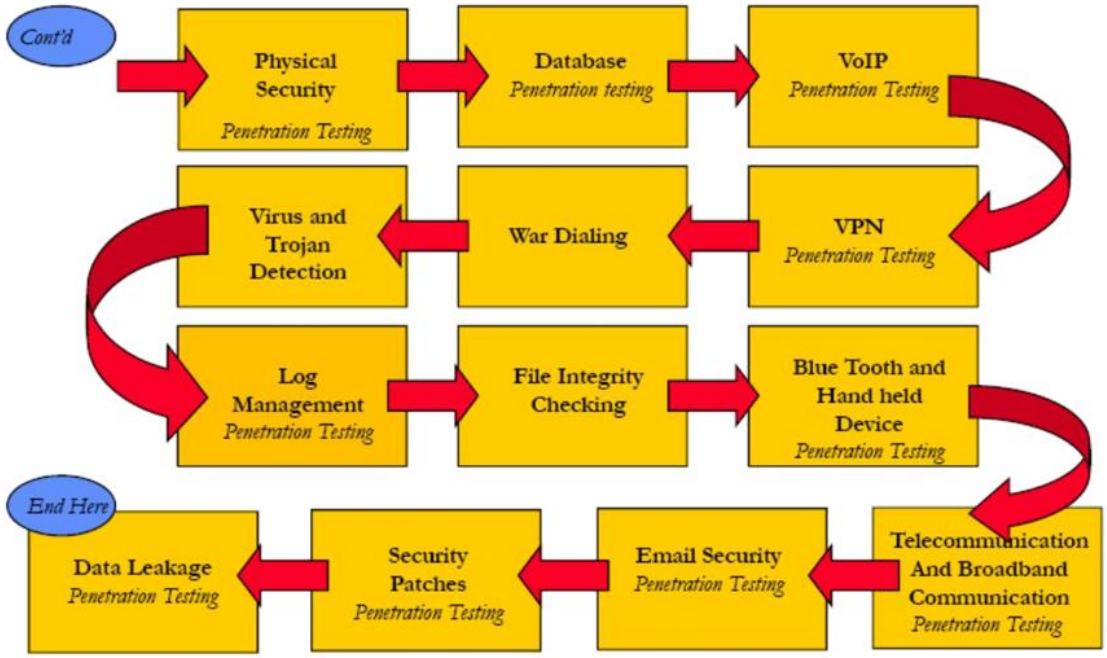
Gambar 3. Eksterna *Penetration Testing*

2. Application Penetration Testing

Pada langkah ini, dilakukan test guna mengetahui tingkat keamanan aplikasi e-Banking yang digunakan perusahaan XYZ. Kegiatan ini dilakukan dengan mengetahui vulnerability pada aplikasi e-Banking yang mungkin dapat dieksploitasi dan merekomendasikan untuk menutup vulnerability yang ditemukan.



Gambar 4. Eksternal *Penetration Test Roadmap*



Gambar 5. ***Penetration Test Roadmap***

Tools yang Digunakan

Pada penelitian ini, terdapat beberapa *tools* yang digunakan oleh pentester (Daniswara et al., 2020). Beberapa *tools* tersebut diantaranya:

- Google Hacking Data Base
- Drsearch
- Wireshark
- Nmap
- Metasploit Framework
- Basic Command Line
- Basic SMTP Command

HASIL DAN PEMBAHASAN

Pembanding Tools & Metodologi

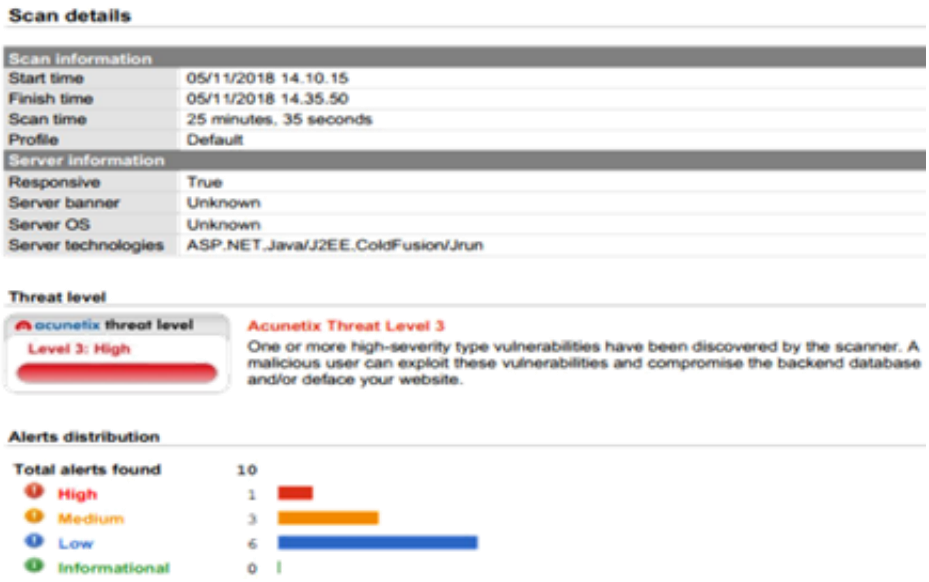
Pada bab metode penelitian telah dipaparkan *tools* yang digunakan. Sebelum *tools* tersebut digunakan, dilakukan perbandingan terhadap *tools* yang tersedia pada umumnya. Pembanding dari *tools* yang digunakan adalah dengan metasploit framework. Metasploit framework adalah *enterprise penetration testing tools* dimana *tools* ini sudah mencakup dari semua *tools* yang sedang pretester gunakan. Pembandign dari metodologi yang digunakan adalah CEH, dan OWASP scoring sistem.

Metode pembanding yang digunakan adalah *best practice* dari lapangan dari pengalaman selama melakukan penetration testing, metode CEH sangat tidak efektif untuk digunakan karena metode tersebut sangat mengandalkan *tools* dan cara penggunaan *tools hacking.* Pembangunan b*est practice* juga dibutuhkan untuk membuat proses *penetration test* lebih efektif karena dibutuhkan dalam pengatuuran manajemen *penetration testing.*

OWASP scoring sistem menggunakan alur scoring yang sangat sulit untuk dipahami dan sangat tidak praktis dalam pengerjaan *penetration test* saat memilih nilai skoring dari sebuah kelemahan, maka dari itu CVSS v3 digunakan sebagai scoring sistem. Hal tersebut disebabkan oleh CVSS v3 sangat mudah dimengerti bagi orang awam yang cukup tidak paham dengan dunia keamanan karena *point-point* dan variabel yang dijelaskan pada CVSS v3 adalah *point* variabel manajemen.

Proses Vulnerability Scanning

Pada hasil scanning dengan Acunetix ditemukan 1 High level vulnerability. Selanjutnya dilakukan proses Proof of Concept padaannualal Testing. Hasil scan pada aplikasi e-banking dengan Acunerix ditunjukkan oleh Gambar 6.



Gambar 6. Hasil Scan dengan Acunetix pada Aplikasi e-Banking Perusahaan XYZ

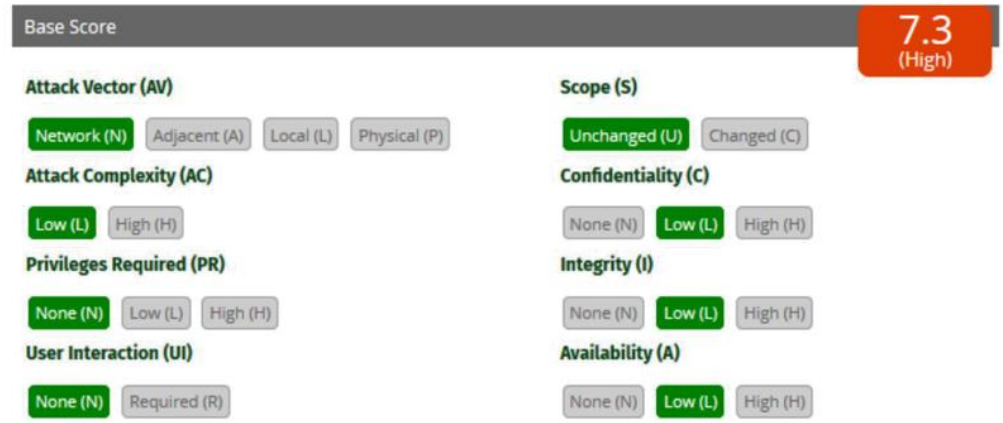
Proses Manual Testing

Apache Tomcat Examples Directory Vulnerabilities

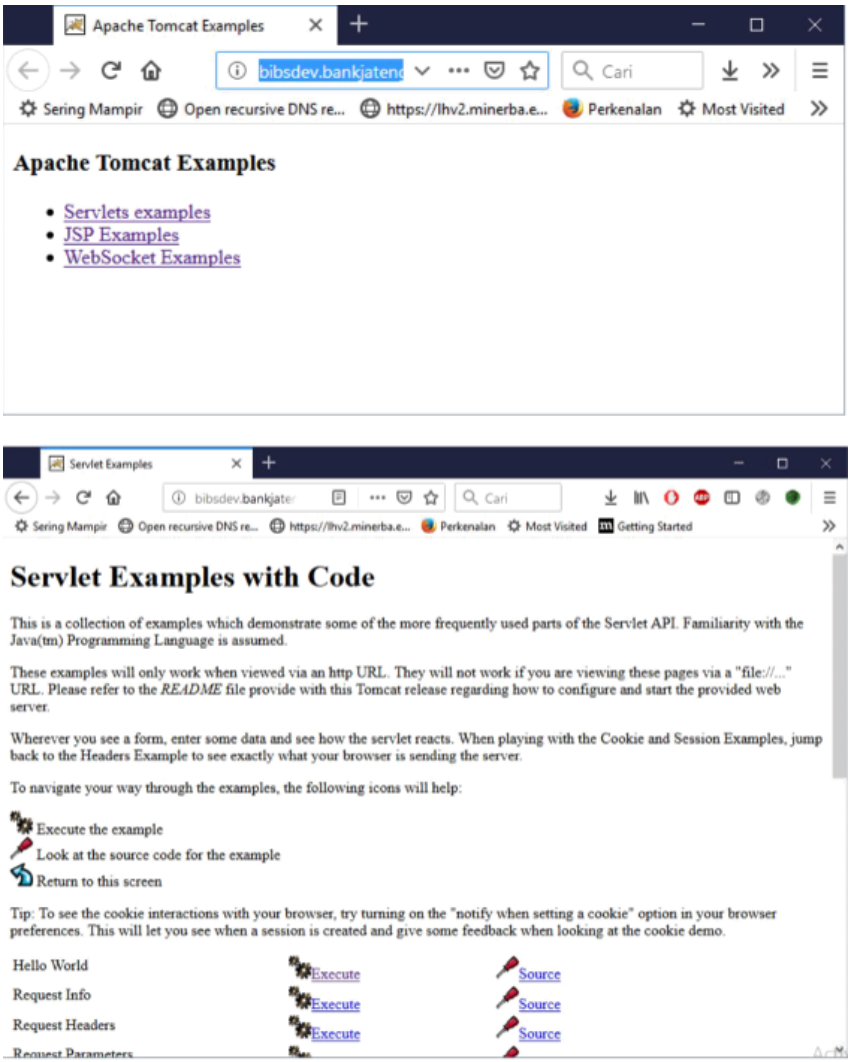
Proses manual testing dilakukan dengan menggunakan Apache Tomcat examples directory vulnerabilities. Instalasi default Apache Tomchat berisi direktori "/examples" di dalamnya terdapat banyak contoh servlets dan JSPs. Beberapa contoh ini merupakan risiko keamanan dan tidak boleh digunakan di server produksi.

Beberapa contoh servlet memungkinkan manipulasi sesi. Karena sesi global inilah servlet menimbulkan risiko keamanan yang besar, sehingga penyerang dapat berpotensi menjadi

administrator dengan memanipulasi sesi. Gambar 7 menunjukkan hasil pembuktian kerentanan menyebutkan bahwa skor 7.3 dan jenis kerentanan dalam kategori High.



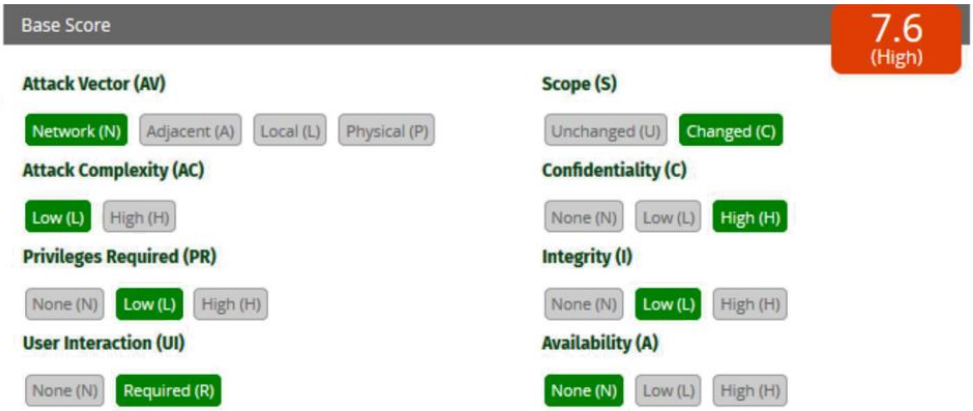
Gambar 7. Hasil Apache Tomcat Examples Directory Vulnerabilities



Gambar 8. Hasil Pembuktian Kerentanan

Cross Site Request Forgery (CSRF)

*Cross Site Request Forgery (*CSRF) adalah serangan pada website yang dieksekusi atas wewenang korban, tanpa dikehendakinya. Pada pengujian, penguji mencoba mengubah password dan berhasil. Hal tersebut menunjukkan sistem memiliki kerentanan. Gambar 9 menunjukkan hasil pembuktian kerentanan menyebutkan bahwa skor 7.6 dan jenis kerentanan dalam kategori High.

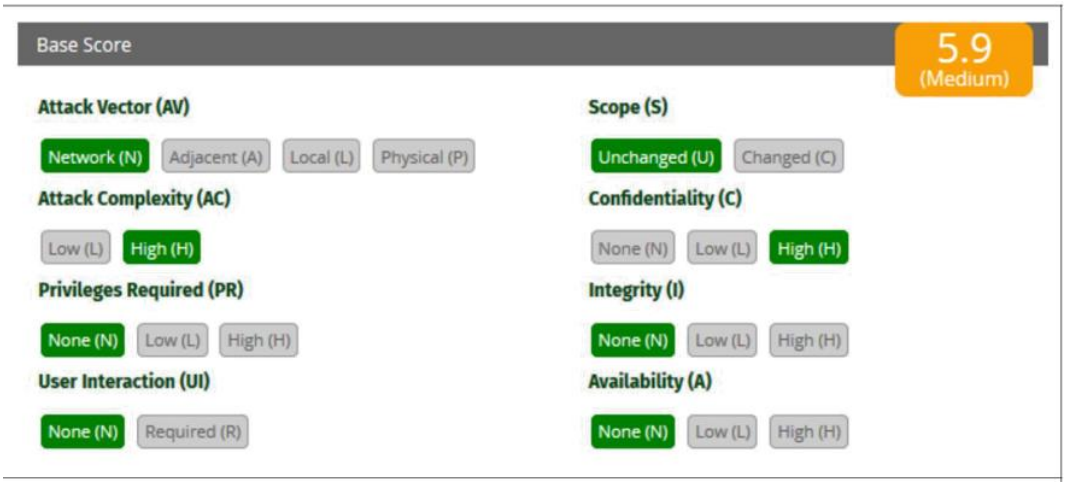


Gambar 9. Hasil Cross Site Request Forgery (CSRF)

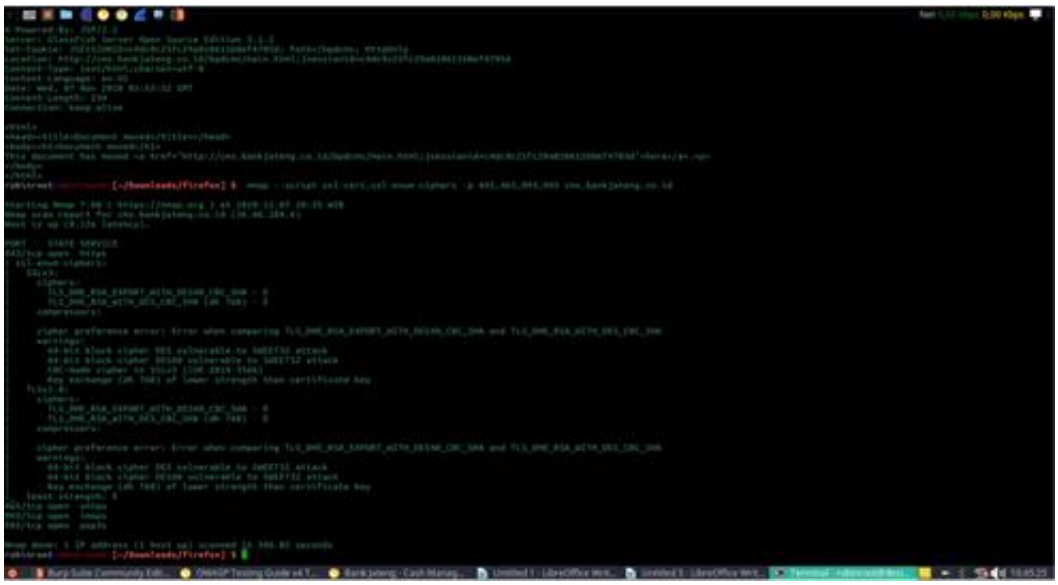
Gambar 10. Proses pembuktian dengan Mengganti Password

Testing for Weak Cryptography

Pengujian ini dilakukan untuk mengetahui proses transisi akses (terutama username dan password) ke aplikasi dilindungi oleh “Secure Protocol”, dan pengguna “Secure Protocol” seperti telah sesuai dengan best practice. Pengujian ini menggunakan tools Nmap. Gambar 11 menunjukkan hasil pembuktian kerentanan menyebutkan bahwa skor 5.9 dan jenis kerentanan dalam kategori Meidum.



Gambar 11. Hasil pengujian Testing for Weak Cryptography

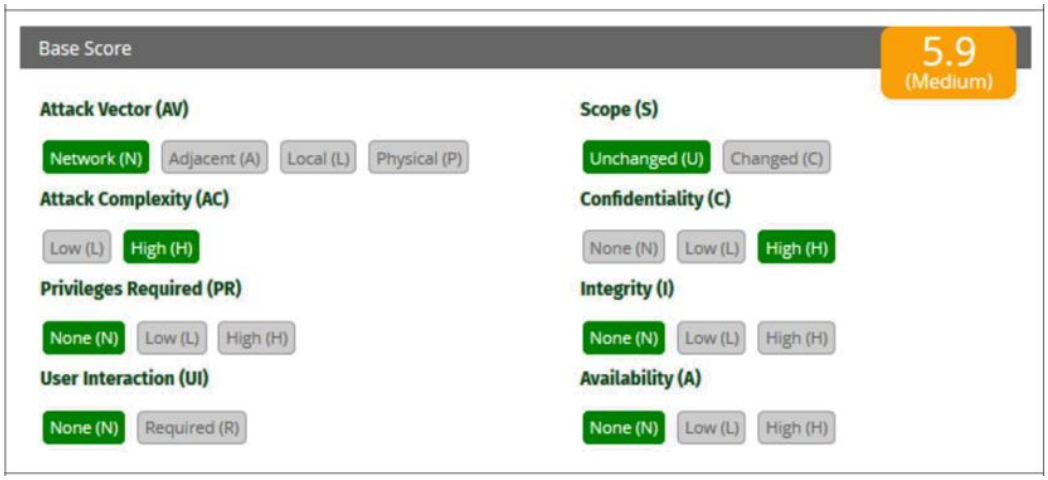


Gambar 12. Pembuktian Kerentanan

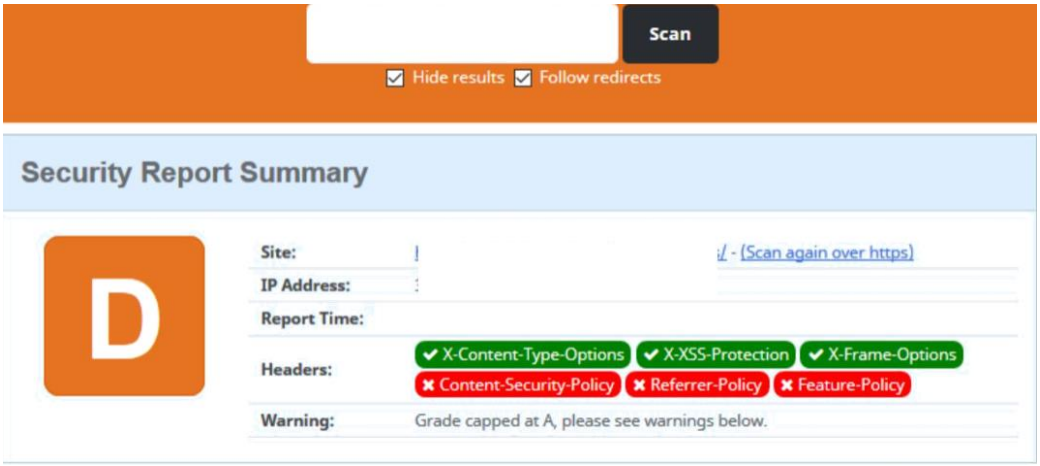
Security Header

Security header adalah tren *security* pada tahun 2017 dimana cara kerja security header ini adalah memberikan perintah kepada user agar browser yang akan menjada user tetap aman, karena header ini dibaca oleh browser, browser dapat melakukan pengecekan dan pembenahan jika user melakukan aktifitas hacking.

Security header ini biasanya pada saat user melakukan request kepada server, web server ini akan merespon dengan memberikan variable header yang akan di eksekusi oleh Browser, seperti contohnya X-XSS-Protection dimana header ini akan meproteksi website dari serangan XSS dimana jika user melakukan hacking terhadap website yang menggunakan security header ini tidak akan dieksekusi oleh browser. Pengujian ini menggunakan tools https://securityheaders.com. Gambar 13 menunjukkan hasil pembuktian kerentanan menyebutkan bahwa skor 5.9 dan jenis kerentanan dalam kategori Meidum.



Gambar 13. Hasil Pengujian Security Header



Gambar 14. Hasil Pembuktian Kerentanan

KESIMPULAN DAN SARAN

Metode *Penetration testing* dapat diterapkan pada *webserver* aplikasi e-banking perbankan perusahaan XYZ. Menurut lima jenis pengujian yaitu Proses Vulnerability Scanning, Apache Tomcat Examples Directory Vulnerabilities, Cross Site Request Forgery (CSRF), Testing for Weak Cryptography dan Security Header kategori aplikasi ini Warning hingga High sehingga perlu ditindaklanjuti. Developer dapat melakukan hal berikut untuk menurunkan tingkat kerentanan aplikasi, sebaiknya directori /examples dihapus di server produksi; *membatasi masa berlaku cookie antara 5 menit atau 10 menit (biasanya ini sudah dilakukan); menggunakan* secure protocol (ssl) sesuai dengan best practice dan mengaktifkan Mod Security pada konfigurasi *webserver*. Penelitian selanjutnya diharapkan Penetration Testing dapat dilakukan untuk menganalisis keamanan jaringan yang lebih kompleks.

DAFTAR PUSTAKA

Daniswara, R. R., Made, G., Sasmita, A., Agus, P., & Pratama, E. (2020). Testing for Information Gathering Using OWASP Testing Guide v4 (Case Study : Udayana University SIMAK-NG Application). In *JITTER-Jurnal Ilmiah Teknologi dan Komputer* (Vol. 1, Issue 1).

Fachri, F. (2023). OPTIMASI KEAMANAN WEB SERVER TERHADAP SERANGAN BRUTE-FORCE MENGGUNAKAN PENETRATION TESTING. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIK)*, *10*(1), 51–58. https://doi.org/10.25126/jtiik.2023105872

Fachri, F., Fadlil, A., Riadi, I., Dahlan, A., Jln Soepomo, Y., & Artikel, I. (2021). Analisis Keamanan Webserver Menggunakan Penetration Test. *JURNAL INFORMATIKA*, *8*(2). http://ejournal.bsi.ac.id/ejurnal/index.php/ji

Fauzan, F. Y., & Syukhri. (2021). Analisis Model Web Security PTES (Penetration testing Execution and Standart) Pada Aplikasi E-Learning Universitas Negeri Padang. *Jurnal Vocational Teknik Elektronika Dan Informatika*, *9*(2), 105–111. http://ejournal.unp.ac.id/index.php/voteknika/

Hidayatulloh, S., & Saptadiaji, D. (2021). Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP). *Jurnal Algoritma*, *19*(1), 77–86. http://jurnal.itg.ac.id/

Krisnawanti, Gia Ginasta, N., Faisal Nasrudin, M., & Anis Nasution, A. (2023). Inventory Control at The Perintis Cimaung Pharmacy Using Open Source Enterprise Resource Planning System: Odoo 14.0. *JURNAL RISTEC:Research in Information System and Technology*, *4*(1), 12–25.

Pohan, Y. A. (2021). Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar. *Jurnal Sistim Informasi Dan Teknologi*, 1–6. https://doi.org/10.37034/jsisfotek.v3i1.36

Riandhanu, I. O. (2022). Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi. *Jurnal Informasi Dan Teknologi*. https://doi.org/10.37034/jidt.v4i3.236

Santoso, N. A., Ainurohman, M., & Kurniawan, R. D. (2022). PENERAPAN METODE PENETRATION TESTING PADA KEAMANAN JARINGAN NIRKABEL. *JURNAL RESPONSIF*, *4*(2), 162–167. https://ejurnal.ars.ac.id/index.php/jti

Supriady, Ginasta, N. G., & Hanum, R. (2023). AUDIT SISTEM INFORMASI OPERASIONAL MENGGUNAKAN FRAMEWORK COBIT 5 (STUDI KASUS : BANK XYZ). *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*, *4*(1), 157–163. https://doi.org/10.35870/jimik.v4i1.147

Teguh Yuwono, D., Raya Olat Maras, J., Alang, B., Hulu, M., Moyohulu, P., Sumbawa, K., & Tenggara Barat, N. (2021). DETEKSI SERANGAN VULNERABILITY PADA OPEN JURNAL SYSTEM MENGGUNAKAN METODE BLACK-BOX. In *Jurnal Informatika & Rekayasa Elektronika)* (Vol. 4, Issue 1). http://e-journal.stmiklombok.ac.id/index.php/jireISSN.2620-6900

W, Y., Riadi, I., & Yudhana, A. (2016). Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST). *Prosiding Annual Research Seminar 2016*, *2*(1), 300–304. http://ars.ilkom.unsri.ac.id300