JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 2, No. 1, Juni 2024
ISSN 3025-0919 (media online)
Hal 30-37

Analisis Keamanan Aplikasi Web Menggunakan Metode Penetration Testing

Dimastito Prasetyo[1], Parhan Yuspandi[1], July Rimaza Putra[1], Yoel Michael Sihombing[1]

[1]Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Indonesia
[1]titodimas188@gmail.com , [2]parhan.ypd@gmail.com, [3]julyrimazaa@gmail.com,
[4]yoel9736@gmail.com

Abstrak- Keamanan aplikasi web saat ini menjadi perhatian utama bagi organisasi dan pengembang perangkat lunak. Ancaman keamanan yang terus berkembang memerlukan pendekatan yang komprehensif untuk mengidentifikasi dan memitigasi kerentanan pada aplikasi web. Dalam penelitian ini, kami melakukan analisis keamanan aplikasi web dengan cara melakukan metode *penetration testing.*

Metode *penetration testing* melibatkan serangkaian teknik, alat, dan prosedur untuk menguji kemampuan sistem dalam menangkal serangan potensial. Kami menerapkan tahapan-tahapan dalam proses penetration testing, seperti *reconnaissance*, *scanning*, *gaining access*, *maintaining access*, dan *reporting*. Selama proses tersebut, kami mengidentifikasi berbagai jenis kerentanan, seperti SQL *injection*, *cross-site scripting* (XSS), *insecure direct object references*, dan lainnya, Melalui penerapan penetration testing yang sistematis, penelitian ini bertujuan untuk menunjukkan bagaimana organisasi dapat secara signifikan meningkatkan ketahanan keamanan aplikasi web mereka.

Kata kunci: keamanan aplikasi web, *penetration testing*, kerentanan, mitigasi.

Abstract- *Web application security is currently a major concern for organizations and software developers. Ever-evolving security threats require a comprehensive approach to identifying and mitigating vulnerabilities in web applications. In this research, we carry out web application security analysis using the penetration testing method.*

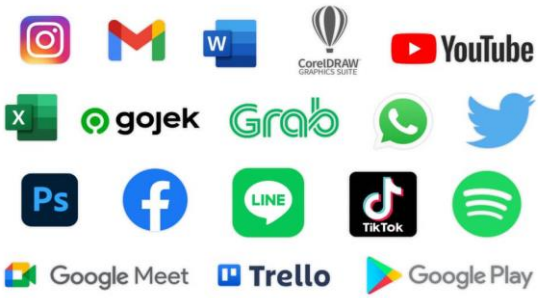
The penetration testing method involves a series of techniques, tools, and procedures to test a system's ability to ward off potential attacks. We apply stages in the penetration testing process, such as reconnaissance, scanning, gaining access, maintaining access, and reporting. During the process, we identified various types of vulnerabilities, such as SQL injection, cross-site scripting (XSS), insecure direct object references, and others, Through the systematic application of penetration testing, this research aims to show how organizations can significantly improve the security resilience of their web applications.

Keywords: web application security, penetration testing, vulnerabilities, mitigation.

I. PENDAHULUAN

Aplikasi web adalah sebuah program yang dapat diakses melalui jaringan internet menggunakan browser web. Aplikasi ini berjalan di server web dan tidak perlu diunduh atau diinstal pada perangkat pengguna. Contoh dari aplikasi web adalah situs media sosial, *e-commerce*, email berbasis web, dan banyak lagi. Aplikasi web umumnya dibangun menggunakan berbagai teknologi seperti HTML, CSS, JavaScript untuk antarmuka pengguna, dan bahasa pemrograman server seperti Python, PHP, Ruby, atau Node.js untuk logika di sisi server. Selain itu, aplikasi web juga sering memanfaatkan database untuk menyimpan dan mengelola data.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 2, No. 1, Juni 2024
ISSN 3025-0919 (media online)
Hal 30-37



Gambar 1. Contoh Aplikasi Web

Keamanan jaringan menjadi aspek yang sangat penting dipertukarkan di internet. Keamanan jaringan adalah praktik dan teknologi yang dirancang untuk melindungi integritas, kerahasiaan, dan ketersediaan data serta sumber daya jaringan dari ancaman dan akses yang tidak sah. Setiap organsiasi/perusahaan dituntut untuk menjaga kerahasiaan, integritas dan otentikasi data pada sebuah *web server* sesuai standar keamanan internasional. Karna itu dibutuhkan cara untuk menemukan kerentanan pada *web server*, salah satunya adalah melakukan *penetration testing.*

A. Pengertian *Penetration Testing*

Penetration testing, yang sering disingkat sebagai "pen testing," adalah proses evaluasi keamanan yang dilakukan secara aktif terhadap sistem komputer, jaringan, atau aplikasi untuk mengidentifikasi potensi kerentanan yang dapat dieksploitasi oleh penyerang. Tujuan utama dari penetration testing adalah untuk menilai keamanan suatu sistem dengan cara mensimulasikan serangan dunia nyata oleh penyerang yang berpotensi memiliki niat jahat. Proses ini bertujuan untuk mengidentifikasi dan mengeksploitasi kerentanan dalam sistem sehingga organisasi dapat mengetahui dan memperbaiki kelemahan tersebut sebelum penyerang nyata dapat memanfaatkannya. Penetration testing adalah langkah penting dalam strategi keamanan siber yang proaktif, membantu organisasi mengidentifikasi dan memperbaiki kelemahan sebelum dapat dieksploitasi oleh penyerang. Penetration testing merupakan praktik kritis dalam upaya mempertahankan keamanan sistem informasi di era digital yang penuh tantangan ini. Dengan pendekatan yang tepat, organisasi dapat mengidentifikasi dan mengatasi potensi ancaman keamanan sebelum mereka dieksploitasi oleh penyerang.

B. Pengertian *Web Server*

Web server adalah perangkat lunak atau perangkat keras yang bertugas untuk menerima permintaan *(requests)* dari klien melalui protokol HTTP *(Hypertext Transfer Protocol)* atau HTTPS (HTTP Secure) dan mengirimkan kembali respon dalam bentuk halaman web atau konten lain yang diminta. *Web server* berperan sebagai perantara antara pengguna dan sumber daya web yang dihosting, seperti halaman HTML, gambar, video, dan aplikasi web. *Web server* adalah komponen penting dari infrastruktur internet, memungkinkan distribusi dan akses ke konten web secara global. Komponen utama *web server* adalah :

- Server Perangkat Keras: Komputer fisik atau perangkat yang menjalankan perangkat lunak *web server*.

- Perangkat Lunak Web Server: Program yang menjalankan layanan web, seperti Apache, Nginx, Microsoft Internet Information Services (IIS), dan LiteSpeed.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 2, No. 1, Juni 2024
ISSN 3025-0919 (media online)
Hal 30-37

2. METODE

Penetration Testing Execution Standart (PTES) merupakan penyedia servis keamanan menggunakan bahasa yang umum dengan cakupan yang dalam. Penetration testing, atau sering disebut sebagai pen testing, adalah proses evaluasi keamanan yang aktif dan sistematis terhadap sistem komputer, jaringan, atau aplikasi untuk mengidentifikasi dan mengeksploitasi kelemahan yang mungkin ada. Tujuan utama dari penetration testing adalah untuk menilai keamanan suatu sistem dengan cara mensimulasikan serangan yang mungkin dilakukan oleh penyerang potensial. Proses ini melibatkan penggunaan berbagai teknik dan alat untuk menemukan, mengevaluasi, dan memanfaatkan kerentanan keamanan yang ada dalam lingkungan yang diuji.

Komponen penting dalam penetration testing :

- Identifikasi Target**:** Penetration testing dimulai dengan mengidentifikasi target yang akan diuji, seperti aplikasi web, jaringan komputer, atau sistem operasi.
- Reconnaissance (Pengintaian)**:** Tahap ini melibatkan pengumpulan informasi tentang target yang akan diserang, seperti sistem yang digunakan, teknologi yang ada, dan struktur jaringan.
- Scanning**:** Penguji melakukan pemindaian terhadap target untuk mengidentifikasi port yang terbuka, layanan yang berjalan, dan kerentanan yang mungkin ada.
- Fingerprinting**:** Teknik ini digunakan untuk mengidentifikasi versi perangkat lunak dan layanan yang berjalan di dalam target, yang dapat membantu dalam menentukan kerentanan yang dapat dieksploitasi.
- Penetration (Eksploitasi)**:** Pada tahap ini, penguji mencoba mengeksploitasi kerentanan yang ditemukan untuk memperoleh akses yang tidak sah ke sistem atau data yang sensitif.
- Maintaining Access**:** Jika penguji berhasil mendapatkan akses yang tidak sah, mereka dapat mencoba untuk mempertahankan akses tersebut untuk jangka waktu yang lebih lama, memungkinkan mereka untuk melakukan lebih banyak aktivitas berbahaya atau mendapatkan informasi tambahan.

  Penetration testing merupakan bagian penting dari strategi keamanan informasi yang komprehensif, membantu organisasi untuk melindungi data sensitif mereka dan mengurangi dampak dari serangan yang potensial. Dengan menggunakan metode dan alat yang tepat, penguji dapat memberikan wawasan berharga tentang kelemahan yang mungkin ada dan membantu dalam meningkatkan tingkat keamanan keseluruhan suatu sistem.

Berikut adalah langkah atau proses yang di lakukan untuk *Penetration Testing Execution* :

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 2, No. 1, Juni 2024
ISSN 3025-0919 (media online)
Hal 30-37

Gambar 2. Proses *Penetration Testing*

Gambar diatas merupakan tahapan penelitian yang akan dilakukan. Adapun Keterangannya sebagai berikut :

1. ***Pre-Engagement Interaction***

   Memnjelaskan kegiatan apa saja yang akan dilakukan kepada client mulai dari hal pertama yang akan dinlakukan hingga tujuan akhir yang akan di capai dengan menggunakan *Penetration Testing* ini.

2. ***Intelligence Gathering***

   Melakukan pengumpulan informasi yang akan digunakan dalam melakukan uji *penetration testing*. Informasi yang perlu didapatkan adalah informasi domain, IP address, host.

3. ***Threat Modelling***

   proses sistematis untuk mengidentifikasi dan menilai potensi ancaman terhadap sistem, aplikasi, atau jaringan, serta menentukan tindakan mitigasi untuk mengurangi risiko tersebut.

4. ***Vulnerabillity Testing***

   proses untuk mengidentifikasi, mengklasifikasikan, dan menganalisis kelemahan atau kerentanan dalam sistem komputer, jaringan, aplikasi, atau infrastruktur lainnya.

5. ***Exploitation***

   proses memanfaatkan kerentanan yang ditemukan dalam sistem komputer, jaringan, aplikasi, atau perangkat keras untuk mendapatkan akses yang tidak sah, merusak sistem, atau mencuri data. Eksploitasi ini sering kali dilakukan oleh

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 2, No. 1, Juni 2024
ISSN 3025-0919 (media online)
Hal 30-37

penyerang untuk mencapai tujuan tertentu, seperti mengakses data sensitif, menginstal malware, atau mengambil alih kendali sistem.

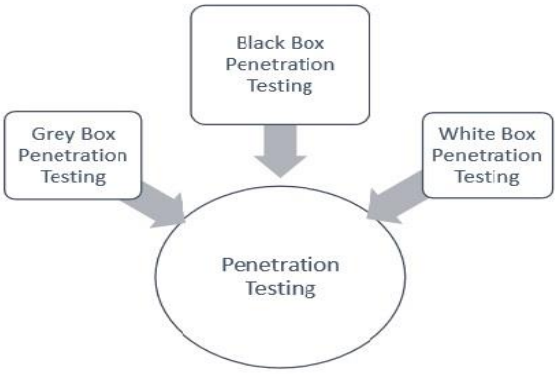
6. ***Post Exploitation***

   Fase dalam proses penetration testing atau serangan siber yang terjadi setelah penyerang berhasil mengeksploitasi kerentanan dan mendapatkan akses awal ke sistem target. Pada tahap ini, penyerang atau penguji keamanan berfokus pada tujuan spesifik mereka, seperti mempertahankan akses, mengumpulkan informasi, mengeskalasi hak akses, dan menginstal perangkat lunak tambahan.

7. ***Reporting***

   Langkah terakhir adalah menganalisa hasil tes tadi dan menyusun laporan berisi temuan celah, potensi dampak serangan, dan saran untuk memperbaiki sistem keamanan.

Ada tiga metode *penetration testing* yaitu sebagai berikut :



Gambar 3. Metode *Penetration Testing*

1. ***Black Box***

   Black Box tidak memiliki pengetahuan sebelumnya tentang sistem atau jaringan yang akan diuji dan kadang dikenal sebagai tes eksternal. Prosesnya Pen tester melakukan pengumpulan informasi, pemindaian (scanning), eksploitasi, dan penilaian kerentanan dari nol. Tujuannya Mensimulasikan serangan oleh pihak luar yang tidak memiliki akses ke informasi internal.

2. *White Box* memiliki pengetahuan penuh tentang sistem atau jaringan yang akan diuji, termasuk informasi tentang infrastruktur, kode sumber, dan arsitektur jaringan dan kadang dikenal sebagai tes internal. Tujuan dari metode ini adalah mengidentifikasi kerentanan internal yang mungkin tidak terlihat dalam pendekatan black box. Prosesnya Pen tester menganalisis kode sumber, melakukan pemindaian kerentanan mendalam, dan menggunakan informasi internal untuk mengeksploitasi kelemahan.

3. ***Grey Box***

   Gary Box memiliki sebagian pengetahuan tentang sistem atau jaringan yang akan diuji. Tujuannya mensimulasikan serangan oleh pihak dalam yang memiliki akses

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 2, No. 1, Juni 2024
ISSN 3025-0919 (media online)
Hal 30-37

terbatas atau pihak luar yang memiliki informasi tertentu tentang sistem. Dan prosesnya menggunakan informasi yang diketahui untuk melakukan eksploitasi, namun tetap melakukan pengumpulan informasi dan pemindaian tambahan.

3. HASIL DAN PEMBAHASAN

A. Tahap *Penetration Testing*

1. *Pre-Engagement Interaction*

   Pre-Engagement interaction ini meliputi pengecekan

   - Identifikasi
   - Konfirmasi Ruang Lingkup, dan
   - Data.

   Tujuan dari tahapan ini adalah penyajian dan penjelasan alat beserta teknik yang akan dilakukan kepada pihak yang akan di pentest.

2. *Intelligence Gathering*

   Tahapan *Intelegence Gathering* ini pertama kali adalah melakukan pengecekan informasi Domain.

   Threat Modelling

   Tahap ini bertujuan untuk mengurangi kerentanan dengan mengevaluasi setiap komponen dan interaksi yang terjadi dalam sistem *software* atau aplikasi

3. *Vulnerability Analysis*

   Tahapan ini adalah proses yang dilakukan adalah Scanning terhadap Aplikasi Web yang akan di cek.

4. *Exploitatiton*

Gambar 4. SQL Map

5. *Post Exploitation*

   Tahap ini bertujuan untuk menentukan suatu nilai dari sistem guna untuk mempertahankan *control* dari sistem tersebut.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 2, No. 1, Juni 2024
ISSN 3025-0919 (media online)
Hal 30-37

6. *Reporting*

proses dokumentasi dan penyampaian temuan, analisis, dan rekomendasi kepada pemangku kepentingan. Tujuan utama dari pelaporan ini adalah untuk memberikan gambaran lengkap tentang keamanan sistem, menunjukkan kerentanan yang ditemukan, dan memberikan panduan untuk mitigasi dan perbaikan.

B. Metode *Penetration Testing*

1. *Black Box*

Black Box adalah salah satu metode pengujian yang digunakan dalam berbagai disiplin ilmu, termasuk pengujian perangkat lunak, pengujian keamanan (penetration testing), dan lainnya. Dalam konteks pengujian keamanan siber, *Black Box Testing* merujuk pada pendekatan di mana penguji tidak mempunyai pengetahuan sebelumnya tentang arsitektur internal, kode sumber, atau desain sistem yang diuji. Penguji hanya mengetahui spesifikasi umum dan fungsionalitas yang seharusnya ada, mirip dengan perspektif seorang penyerang yang tidak memiliki akses ke informasi internal.

2. *White Box*

Pada cara *penetration testing* metode *white box*, *pentester* akan diberi tahu semua informasi terkait dengan *software* yang akan diuji. *Pentester* akan diberi akses penuh untuk mencari tahu seperti apa sistem keamanan yang diterapkan. Pada metode ini, *pentester* 'ditantang' untuk mempelajari semua informasi tersebut dan menentukan di mana titik keamanan yang dianggap lemah. Nantinya, *penetration testing* akan dilakukan di titik-titik yang dianggap rentan itu.

3. Gray Blok

Cara *penetration testing* terakhir adalah melalui metode *grey box*. Metode ini merupakan gabungan antara metode *black box* dan *white box*. Dalam artian, *pentester* akan mendapatkan informasi yang diperlukan untuk melakukan *penetration testing*. Akan tetapi, informasi yang diberikan tidak menyeluruh seperti pada metode *white box*.

Dengan metode *grey box*, *pentester* bisa melakukan pengujian secara lebih terfokus karena sudah bisa memperkirakan titik-titik rentan yang perlu diuji. Alhasil, uji kerentanan bisa dilakukan dengan waktu yang lebih cepat dibandingkan metode *black box*.

4. KESIMPULAN

Dari penelitian tersebut, maka dapat diambil kesimpulan bahwa :

- *Penetration testing* membantu dalam mengungkap kerentanan yang tidak terdeteksi oleh metode pengujian tradisional lainnya, seperti code review atau *static analysis*, dengan mensimulasikan serangan dunia nyata.
- Proses *penetration testing* meningkatkan kesadaran tentang pentingnya keamanan aplikasi di kalangan pengembang dan pemangku kepentingan lainnya, mendorong budaya keamanan yang lebih proaktif dalam pengembangan perangkat lunak.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 2, No. 1, Juni 2024
ISSN 3025-0919 (media online)
Hal 30-37

REFERENSI

Marzuki Hasibuan, A. M. (2022). Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux Untuk Mengetahui Kerentanan Keamanan Server Dengan Metode Black Box. *VOL. 1 NO. 4 (2022) EDISI DESEMBER*, *1*, 172-177.

Clarke, B., & Dayton, T. (2015). *Hacking Exposed Web Applications: Web Security Secrets and Solutions (3rd Edition)*. McGraw-Hill Education.

Pathan, A. K., & Islam, M. S. (2019). A Survey on Penetration Testing: Tools, Methods, and Challenges. *Journal of Cyber Security Technology*, 3(1), 20-39.

Rana, A. A., & Balaji, S. (2016). Penetration Testing of Web Applications. *International Journal of Advanced Research in Computer Science and Software Engineering*, 6(4), 1-7.

Kennedy, D., O'Gorman, J., Kearns, D., Aharoni, M., & Hartman, B. (2011). *Metasploit: The Penetration Tester's Guide*. No Starch Press.

OWASP (Open Web Application Security Project). (2021). *OWASP Testing Guide*. Diakses dari: https://owasp.org/www-project-web-security-testing-guide/

PortSwigger. (2021). *Web Security Academy*. Diakses dari: https://portswigger.net/web-security

Ibrahim, A. M., Defisa, T., & Seta, H. B. (2022, October). Analisis Keamanan Sistem pada Website Perusahaan CV. Kazar Teknologi Indonesia dengan Metode Vulnerability Assesment and Penetration Testing (VAPT). In *Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer dan Aplikasinya* (Vol. 3, No. 1, pp. 312-325).

Hanafi, T. A., Iswayudi, C., & Rachmawati, R. Y. (2019). APLIKASI PENDETEKSI CELAH KEAMANAN APLIKASI WEB DENGAN PENETRATION TESTING MENGGUNAKAN METODE INPUT VALIDATION TESTING. *Jurnal SCRIPT*, 132-141.