INOTEK, Vol.7 Agustus 2023
ISSN: 2580-3336 (Print) / 2549-7952 (Online)
Url: https://proceeding.unpkediri.ac.id/index.php/inotek/

Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui Kali Linux

Diterima:
10 Mei 2023
Revisi:
10 Juli 2023
Terbit:
1 Agustus 2023

[1]Firda Nurelia Syah Putri, [2*]Yudo Bismo Utomo, [3]Harso Kurniadi
[1-3]Universitas Islam Kadiri

Abstrak—Pada era serba digital saat ini, setiap warga mancari informasi terbaru dari manapun melalui website. Website juga merupakan kebutuhan yang sangat penting di instansi pemerintah, khususnya di Kabupaten Kediri. Dengan adanya website tersebut, aliran informasi dan komunikasi antara warga dengan pemerintah dapat dilakukan dengan mudah. Akan tetapi, dibalik kelebihan dari website terdapat juga beberapa kelemahan, yaitu terdapat celah keamanan yang bisa diretas oleh warga yang tidak bertanggung jawab. Jika tidak segera ditanggulangi, akan mengakibatkan kerusakan pada data yang ada pada website Pemerintah Kabupaten Kediri. Untuk mengatasi masalah tersebut, digunakan metode *penetration testing* untuk menganalisa celah keamanan pada website Pemerintah Kabupaten Kediri melalui Kali Linux. Hasil yang diperoleh, ditemukan beberapa port terbuka yang memungkinkan *attacker* mengekspos data sensitive berupa *username* dan *password* yang bisa digunakan untuk akses login ke halaman cp panel admin, sehingga pelaporan CVSS Base Score pointnya 5.5 berada di level medium.
Kata Kunci—Penetration Testing; Website; Kali Linux

Abstract— *Every citizen seeks the most recent information through the website in the current all-digital era from any location. at government organizations, especially in Kediri Regency, the website is also a critical requirement. The website makes it simple for residents and the government to exchange information and communicate. However, there are a number of drawbacks to the website that outweigh its benefits, including security flaws that can be exploited by careless users. It will harm the information of Kediri Regency website if it is not handled right away. In order to solve this issue, Kali Linux was used to examine security flaws on the Kediri Regency official website. The collected results revealed a number of open ports that enable hackers to reveal sensitive information in the form of usernames and passwords that may be used to log in to the admin panel cp page, resulting in a CVSS Base Score point reporting of 5.5 being at the medium level.*
Keywords— *Penetration Testing; Website; Kali Linux*

Penulis Korespondensi:

Yudo Bismo Utomo
Program Studi Teknik Komputer
Universitas Islam Kadiri
Email: yudobismo@uniska-kediri.ac.id
ID Orcid: [https://orcid.org/0009-0009-5601-435X]

I. PENDAHULUAN

Pada era serba digital saat ini, setiap warga mancari informasi terbaru dari manapun melalui website, sehingga website merupakan salah satu platform yang paling sering diakses oleh setiap warga dalam mencari berbagai informasi [1][2]. Penerapan website di instansi pemerintah sangat penting, khususnya di Pemerintah Kabupaten Kediri yang mempunyai beberapa kelebihan dan manfaat, yaitu sebagai media penyampaian informasi secara resmi dari pemerintah Kabupaten Kediri kepada warga, sebagai media interaksi dengan warga, menjadi tolak ukur bagaimana aktif atau tidaknya kegiatan di pemerintahan, sebagai tempat menyampaikan aspirasi warganya, memudahkan warga untuk mengenal pemimpinnya serta sebagai media promosi.

Website Pemerintah Kabupaten Kediri dibangun dan dikembangkan oleh Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Kediri yang bekerja sama dengan dinas terkait sebagai *leading sector*. Dengan adanya website tersebut, aliran informasi dan komunikasi antara warga dengan pemerintah dapat dilakukan dengan mudah. Akan tetapi dibalik banyaknya kelebihan dan manfaat, website juga terdapat beberapa kelemahan, yaitu terdapat celah keamanan yang bisa diretas oleh warga yang tidak bertanggung jawab. Hal ini dapat berbahaya, dikarenakan data dan informasi yang dimiliki suatu instansi di pemerintahan tidak semuanya bersifat terbuka. Jika tidak segera ditanggulangi, akan mengakibatkan kerusakan pada data yang ada di website tersebut.

Untuk mengatasi masalah tersebut, digunakan metode *penetration testing* untuk menganalisa celah keamanan pada website Pemerintah Kabupaten Kediri melalui *kali linux*. Metode *penetration testing* merupakan suatu metode yang dilakukan seseorang untuk menemukan celah keamanan pada suatu sistem yang berpotensi dapat diserang oleh pihak yang tidak bertanggungjawab. Orang yang melakukan *penetration testing* adalah *pentester*. Tujuan dari metode *penetration testing* ini adalah untuk mengetahui macam-macam serangan yang terjadi karena adanya kelemahan di dalam sistem[3][4][5].

Sedangkan *kali linux* merupakan sistem operasi *open-source* berbasis *linux debian* yang dikembangkan oleh *Offensive Security*, yang dapat digunakan untuk memenuhi keperluan dalam melakukan *penetrasi* dan juga *testing* di sebuah sistem keamanan pada komputer. *Kali linux* mempunyai tampilan yang sederhana dan penggunaannya yang cukup mudah, yang membuat *kali linux* banyak dicari oleh pemula yang sedang belajar dalam melakukan *penetrasi* dan juga *testing* pada sistem, jaringan dan aplikasi[6][7][8].

Penelitian ini mengacu pada penelitian sebelumnya yang dilakukan oleh Sulis Andriyani, dkk pada tahun 2023 tentang penggunaan metode *penetration testing* dalam menganalisis celah keamanan pada website SMK Al-Kautsar Purwokerto menggunakan framework ISSAF[9]. Hasil yang didapatkan dari penelitian tersebut adalah jenis serangan yang dijadikan *penetration testing*

meliputi seangan XSS Injection, derangan DDoS dan serangan Port 21. Namun, penelitian ini belum membahas cvss base score yang meliputi penilaian, detail dari celah keamanan dan saran perbaikan dari *pentester*.

Pada penelitian kedua yang dilakukan oleh Yum Thurfah Afifah Rosalia, dkk pada tahun 2021 tentang pengujian celah keamanan pada website dengan metode OWASP dilakukan testing terhadap 10 standar keamanan yang ada pada OWASP TOP 10[10]. Hasilnya adalah dari pengujian terhadap 10 standar keamanan pada OWASP TOP 10, ditemukan celah keamanan yang ditemukan adalah *Broken Authentication, Sensitive Data Exposure, dan Security Misconfiguration.* Namun, penelitian ini belum membahas tentang cvss base score yang meliputi penilaian, detail dari celah keamanan dan saran perbaikan dari *pentester*.

Penelitian ketiga yang dilakukan oleh Stefanus Eko Prasetyo, dkk pada tahun 2021 tentang analisa keamanan pada Pay2home dengan metode *penetration testing* [11]. Hasilnya adalah website tersebut masih mempunyai celah pada bagian port service yang memungkinkan terjadinya penyerangan oleh orang yang tidak bertanggung jawab. Namun, penelitian ini belum membahas tentang cvss base score yang meliputi penilaian, detail dari celah keamanan dan saran perbaikan dari *pentester*.

Penelitian keempat yang dilakukan oleh Arif Kurniadi, dkk pada tahun 2021 tentang analisis keamanan jaringan WPA2-PSK menggunakan metode *penetration testing* [12]. Hasilnya adalah metode pengujian *penetration testing* pada TP-Link Archer A6 masih banyak kelemahan sistem, dikarenakan masih menggunakan konfigurasi default dari vendor. Meskipun sama-sama menggunakan kali linux saat melakukan *penetration testing*, namun penelitian ini belum membahas tentang cvss base score yang meliputi penilaian, detail dari celah keamanan dan saran perbaikan dari *pentester*.

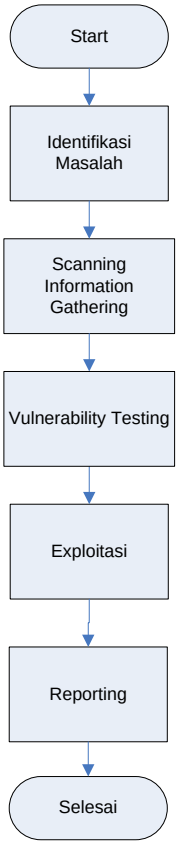
Penelitian kelima yang dilakukan oleh Mochmad Adhari Adiguna, dkk pada tahun 2022 tentang analisa keamanan jaringan WPA2-PSK menggunakan metode *penetration testing* [13]. Hasilnya adalah hampir mirip dengan penelitian keempat yang dilakukan oleh Arif Kurniadi, dkk. Namun, penelitian ini belum membahas tentang cvss base score yang meliputi penilaian, detail dari celah keamanan dan saran perbaikan dari *pentester*.

Dari pemaparan kelima penelitian sebelumnya diatas, maka pembaruan ataupun pembeda antara penelitian ini dengan penelitian sebelumnya adalah penelitian ini akan membahas tentang cvss base score yang meliputi penilaian, detail dari celah keamanan dan saran perbaikan dari *pentester*.

ISSN: 2580-3336 (Print) / 2549-7952 (Online)
Url: https://proceeding.unpkediri.ac.id/index.php/inotek/

II. METODE

Penelitian ini menggunakan metode experimental, dimana kinerja dari metode ini berpangkal dari suatu kasus permasalahan yang kemudian akan dicari solusinya [14][15]. Visualisasi dari *work flow* metode experimental pada penelitian ini dapat dilihat pada gambar 1 berikut ini.



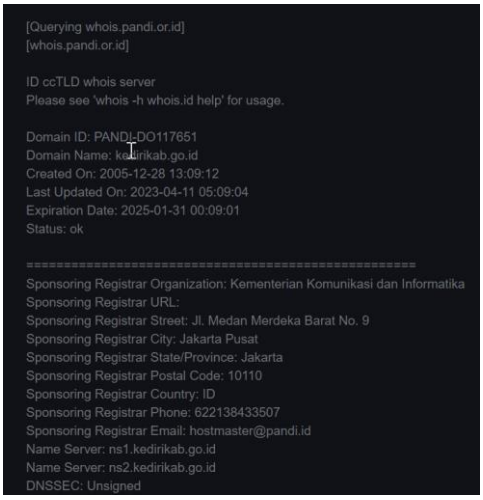
Gambar 1. *Work Flow* Metode Experimental

Tahap awal dari penelitian ini adalah melakukan identifikasi masalah terlebih dahulu yang bertujuan untuk menganalisa celah keamanan pada website dinas Pemerintah Kabupaten Kediri. Dilanjutkan dengan *scanning information gathering*, yaitu mengumpulkan informasi sebanyak mungkin mengenai target yang dituju, seperti IP Address, topology network, network resources dan lain-lain. Setelah itu dilakukan *vulnerability testing* untuk melihat apakah website tersebut bisa dieksploitasi atau tidak. Jika terdapat celah, maka lanjut ke tahap selanjutnya yaitu eksploitasi. Setelah itu, tahap terakhir dari penelitian ini adalah reporting yang memungkinkan *attacker* bisa mendapatkan data sensitive berupa *user*, *password*, *kode enskripsi*, dan lain-lain.

III. HASIL DAN PEMBAHASAN

3.1 Information Gathering

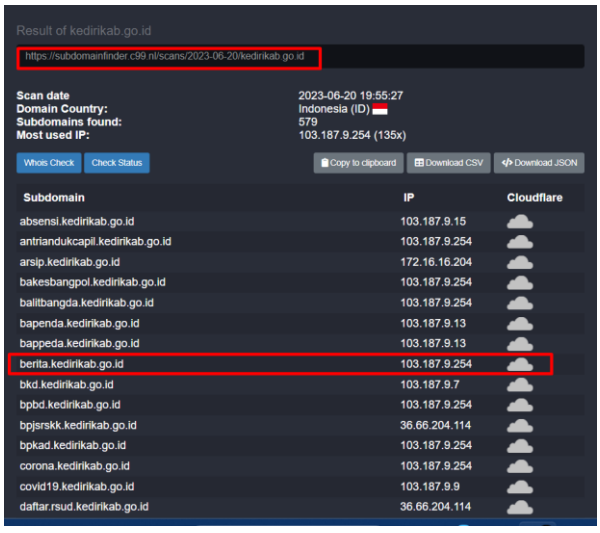
Langkah pertama dalam melakukan analisa celah keamanan website menggunakan metode *penetration testing* adalah dengan melakukan *information gathering* yang bertujuan untuk menggali data dan informasi dari target yang dituju, yaitu website kedirikab.go.id. Dalam menemukan penggalian data dan informasi, penelitian ini menggunakan *tools* yang bernama *whois*. Untuk hasil *information gathering*, dapat dilihat pada gambar 2 berikut ini.



Gambar 2. Hasil *Information Gathering*

3.2 Scanning and Enumeration

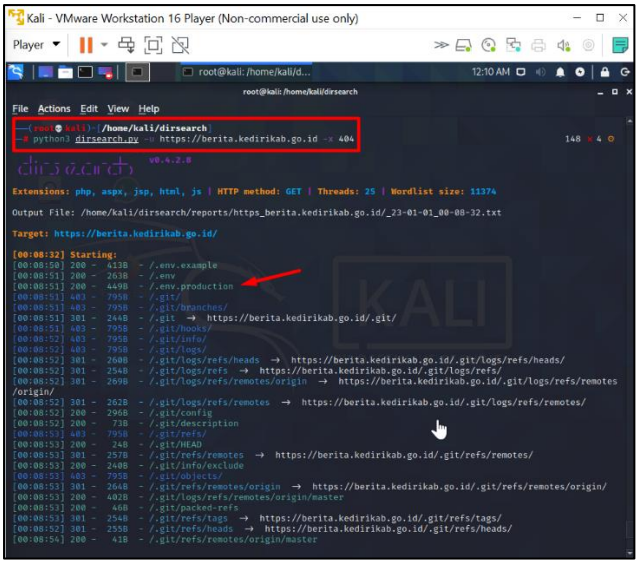
Langkah yang kedua, dilakukan *scanning and enumeration*, yang bertujuan untuk menemukan sub domain yang dimiliki oleh target. Dalam melakukan *scanning and enumeration*, penelitian ini menggunakan *tools sub finder* yang dijalankan di sistem operasi *kali linux*. Hasil dari *scanning and enumeration*, dapat dilihat pada gambar 3 berikut ini.



Gambar 3. Hasil *Information Gathering*

3.3 Vulnerability Testing

Langkah ketiga, dilakukan *vulnerability testing*, yang bertujuan untuk melakukan *testing* apakah ada port yang terbuka atau direktori tersembunyi. Dalam melakukan *vulnerability testing*, penelitian ini menggunakan *tools dirsearch* yang dijalankan di sistem operasi *kali linux*. Hasil dari *vulnerability testing*, dapat dilihat pada gambar 4 berikut ini.



Gambar 4. Hasil *Vulnerability Testing*

Dari hasil tersebut, peneliti berhasil mendapat informasi direktori yang *accessable* yang ditandai dengan response code 200 dan peneliti mendapatkan direktori ***/.env.production,*** yang artinya ada celah yang rentan untuk dimasuki.

3.4 Exploitasi

Langkah keempat, dilakukan exploitasi dengan mencoba akses https://berita.kedirikab.go.id/.env.production dan peneliti menemukan ada sensitive information berupa nama db, user, dan password. Untuk hasil exploitasi dapat dilihat pada gambar 5 berikut ini.

Gambar 5. Hasil *Vulnerability Testing*

3.5 Reporting

Pada tahap terakhir ini, penulis membuat *report cvss base score*, yang berisi *jenis bug, severity, level cvss base score, URL Vulnerability* dan *impact*. Untuk hasil *report*, dapat dilihat pada tabel 1 berikut ini.

Tabel 1. Report CVSS base Score

Report	Hasil
Jenis Bug	Exposure of Sensitive Information (DB Credentials) to Unauthorized Actor
Severity	Major
Level CVSS Base Score	5.5 (Medium)
URL Vulnerability	https://berita.kedirikab.go.id/.env.production
Impact	Memungkinkan attacker bisa mendapatkan data sensitive seperti user, password, kode enskripsi, hingga detail database

IV. KESIMPULAN

Kesimpulan yang diperoleh dari penelitian ini adalah berdasarkan pengujian mengunakan metode penetration testing pada website Pemerintah Kabupaten Kediri melalui Kali Linux, ditemukan beberapa port terbuka yang memiliki akses 200. Kemudian setelah dilakukan *attacking* untuk masuk ke directory environment ditemukan Exposure of Sensitive Information (DB Credentials) to Unauthorized Actor yang memungkinkan untuk mengekspos data sensitive berupa *username* dan *password* yang bisa digunakan untuk akses login ke halaman cp panel admin.

DAFTAR PUSTAKA

[1] A. Nurkholis and Y. B. Utomo, "RANCANG BANGUN SISTEM INFORMASI FAFA (FACTORY FIREWALL ADMINISTRATIVE) BERBASIS WEBSITE (Studi Kasus : PT Lotus Indah Textile Industries)," *Jurnal Teknik Informatika Kaputama (JTIK)*, vol. 6, no. 2, 2022.

[2] A. Nuryansyah *et al.*, "Pengembangan Sistem Informasi Sekolah Berbasis Website Di SMK Taman Karya Madya Ngemplak," 2020. doi: https://doi.org/10.22373/jintech.v1i2.593.

[3] B. Adhi Prakosa, "Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method," 2020. [Online]. Available: https://iocscience.org/ejournal/index.php/mantik

[4] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," 2021. [Online]. Available: http://jurnal.itg.ac.id/

[5] Y. A. Pohan, "Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar," *Jurnal Sistim Informasi dan Teknologi*, pp. 1–6, Mar. 2021, doi: 10.37034/jsisfotek.v3i1.36.

[6] F. Setyawan and H. Amnur, "Keamanan Jaringan Wireless Dengan Kali Linux," 2022. [Online]. Available: http://jurnal-itsi.org

[7] A. Wahid, I. Juliady, S. G. Zain, and J. M. Parenreng, "Secure Wireless Sensor Network using Cryptography for Smart Farming Systems," *Internet of Things and Artificial Intelligence Journal*, vol. 2, no. 4, pp. 248–262, Nov. 2022, doi: 10.31763/iota.v2i4.554.

[8] R. Hermawan, "STRING (Satuan Tulisan Riset dan Inovasi Teknologi) TEKNIK UJI PENETRASI WEB SERVER MENGGUNAKAN SQL INJECTION DENGAN SQLMAP DI KALILINUX," 2021. doi: http://dx.doi.org/10.30998/string.v6i2.11477.

[9] S. Andriyani, M. Fajar Sidiq, and B. Parga Zen, "Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar," 2023.

[10] Y. Thurfah Afifa Rosaliah and B. Hananto, *Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM xxx*. 2021.

[11] S. E. Prasetyo and R. C. Lee, "Analisis Keamanan Jaringan Pada Pay2home Menggunakan Metode Penetration Testing," 2021. [Online]. Available: https://journal.uib.ac.id/index.php/combines

[12] A. Kurniadi, "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : TP-Link Archer A6)," 2021. [Online]. Available: https://journal.uib.ac.id/index.php/combines

[13] M. A. Adiguna and B. W. Widagdo, "Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r)," 2022.

[14] A. M. Aziz, Y. B. Utomo, D. E. Yuliana, I. Kadiri, and K. Kediri, "Implementasi Metode Certainty Factor Berbasis Android Pada Sistem Pakar Diagnosa Kecanduan Smartphone," 2022. doi: https://doi.org/10.36526/ztr.v4i1.1813.

[15] B. Rohmi Khalida and G. Astawan, "Penerapan Metode Eksperimen untuk Meningkatkan Hasil Belajar IPA Siswa Kelas VI SD," vol. 4, 2021, doi: 10.23887/jippg.v4i2.