Sistematis : Jurnal Ilmiah Sistem Informasi
E-ISSN: 3063-041X
https://ejournal.rizaniamedia.com/index.php/sistematis
DOI: 10.69533
Vol.1 No.1 Oktober 2024

Pengujian Keamanan Sistem Mengunakan Metode Penetration Testing di Website Diskominfostandi Kota Bekasi

[1]Marcell Dwi Purnomo; *[2]Ahmad Chusyairi;

[1,*2]Universitas Bina Insani, Jl Raya Rawa Panjang No.6, RT.001/RW.003, Sepanjang Jaya, Kec. Rawalumbu, Kota Bekasi, Jawa Barat 17114

[1]Email : marcelldwipurnomo@gmail.com
[2*]Email : ahmadchusyairi@binainsani.ac.id

A B T R A C T
The Communication, Informatics, Statistics, and Coding Office of Bekasi City is one of the government agencies that utilizes its website as an important service for the public. The researcher aims to conduct an in-depth analysis of reports from bug hunters regarding vulnerabilities on the website dpppa.bekasikota.go.id, which belongs to the Diskominfostandi of Bekasi City, using the Penetration Testing method based on the NIST SP 800-115 standard. Through Penetration Testing according to the NIST SP 800-115 standard, with the stages of planning, discovery, attack, and reporting, two main vulnerabilities were identified: sensitive information disclosure and SQL Injection. After identifying these two vulnerabilities, the severity of each vulnerability was measured using the Common Vulnerability Scoring System (CVSS) Calculator version 3.1. This tool is used to determine the severity of each vulnerability on the website and prioritize fixes based on CVSS scores, from highest to lowest. Based on this assessment, appropriate corrective actions are then proposed to enhance the security of the DPPPA website to better protect it from potential threats in the future.

Keywords: *Penetration Testing; SQL Injection; SQLmap; System Security; Website.*

A B S T R A K S
Dinas Komunikasi, Informatika, Statistik, dan Persandian Kota Bekasi merupakan salah satu instasi yang memanfaatkan website sebagai layanan penting bagi publik. Peneliti bertujuan untuk melakukan analisis mendalam terhadap laporan dari bug hunter terkait celah kerentanan pada website dpppa.bekasikota.go.id milik Diskominfostandi Kota Bekasi menggunakan metode Penetration Testing berdasarkan standar NIST SP 800-115. Melalui Penetration Testing berdasarkan standar NIST SP 800-115 dengan tahapan planning, discovery, attack, dan reporting mendapatkan dua kerentanan yaitu kerentanan sensitive information disclosure dan kerentanan SQL Injection. Setelah mengidentifikasi dua kerentanan tersebut, dilakukan pengukuran tingkat kerentanannya menggunakan alat bantu Common Vulnerability Scoring System (CVSS) Calculator version 3.1. Alat ini digunakan untuk menentukan tingkat keparahan masing-masing kerentanan pada website dan memprioritaskan perbaikan berdasarkan nilai CVSS dari yang tertinggi hingga terendah. Berdasarkan hasil penilaian ini, memberikan solusi perbaikan yang tepat kemudian untuk meningkatkan keamanan website DPPPA agar lebih terlindungi dari ancaman di masa mendatang.

Kata Kunci: *Keamanan sistem; Penetration Testing; SQL Injection; SQLmap; Website.*

1. Pendahuluan

Perkembangan teknologi informasi mengalami peningkatan yang sangat cepat dan membawa banyak perubahan di dunia. Dengan kemajuan teknologi yang terus meningkat, banyak ditemukan inovasi-inovasi baru yang memudahkan kehidupan manusia, salah satunya adalah situs web. Situs web adalah kumpulan halaman yang berada dalam sebuah *domain* atau *subdomain* yang dapat diakses melalui internet di seluruh dunia [1].

Berdasarkan observasi yang dilakukan pada Dinas Komunikasi, Informatika, Statistik, dan Persandian Kota Bekasi, yang disingkat Diskominfostandi Kota Bekasi, merupakan bagian dari instansi pemerintahan yang bertanggung jawab membantu Wali Kota dalam pelaksanaan urusan pemerintahan terkait teknologi dan komunikasi, statistik, serta persandian di Kota Bekasi. Diskominfostandi Kota Bekasi mempunyai tugas yaitu memberikan layanan kepada semua perangkat daerah di Kota Bekasi di bidang teknologi informasi dan komunikasi, salah satunya yaitu mengelola *server* yang berisi *website* Pemerintah Kota Bekasi, baik yang bersifat profil *website* maupun aplikasi berbasis *website*. Terdapat 231 *website* menggunakan *subdomain* .bekasikota.go.id

yang ter*update* pada tahun 2024, dimana salah satunya terdapat *website* Dinas Pemberdayaan Perempuan dan Perlindungan Anak (DPPPA) Kota Bekasi.

Website DPPPA Kota Bekasi merupakan *website* yang berisi informasi tentang pemberdayaan perempuan serta memberikan upaya perlindungan bagi perempuan dan anak didalam masyarakat. Agar lebih terarah, efektif, dan efisien untuk mencapai tujuan, maka diperlukan pelaksanaan program-program yang matang, yang tentunya DPPPA kota bekasi memiliki kepala dinas yang bertugas membantu walikota dalam melaksanakan tugasnya. DPPPA memiliki tiga bidang dalam melaksanakan tugasnya yaitu bidang pemenuhan hak anak, bidang pencegahan dan penanganan kekerasan terhadap perempuan dan anak, dan bidang pengarusutamaan gender.

Namun, Permasalahan muncul karena terdapat laporan dari *bug hunter* terkait celah kerentanan pada *website* DPPPA. Kerentanan ini meliputi *SQL Injection* yang memungkinkan penyerang dapat mengakses dan mengambil data dari isi *database website* dan mengetahui *form login* untuk mengakses *backend website* DPPPA. Maka adanya laporan dari *bug hunter* menjadikan sebuah ancaman bahwa *website* DPPPA masih memiliki celah kerentanan dan belum sepenuhnya aman dari serangan pihak luar. Setelah mengetahui adanya laporan celah kerentanan pada *website* DPPPA, dilakukan pengujian lebih lanjut untuk mengkonfirmasi kebenaran celah kerentanan yang ditemukan. Pengujian ini menggunakan metode *penetration testing* untuk memvalidasi kerentanan yang ditemukan. Meskipun telah dilakukan pengujian, tingkat risiko dari celah kerentananya belum diketahui dan akan dinilai *menggunakan Common Vulnerability Scoring System* (CVSS) versi 3.1. Karena *website* DPPPA berisi informasi yang dikonsumsi untuk masyarakat, sehingga perlu memberikan solusi perbaikan agar lebih meningkatkan keamanan *website* DPPPA.

"Metode *penetration testing* berwenang untuk melakukan pengujian penetrasi untuk mengeksploitasi sistem dan mencari tahu kemungkinan adanya celah keamanan yang dapat dimanfaatkan untuk eksploitasi. Keduanya merupakan metode yang baik digunakan untuk menguji keamanan sistem. Namun, *penetration testing* memiliki kelebihan dan disarankan untuk melakukan pengujian keamanan sistem [2]."

Terdapat penelitian terdahulu yang relevan seperti penelitian yang dilakukan oleh Andria dan Ridho Pamungkas hasil *penetration testing* tersebut mendapatkan celah kerentanan *SQL Injection* yang dapat melihat stuktur *database* pada *web server*nya, tetapi pada penelitian ini tidak dieksploitasi lebih lanjut untuk mencari adanya informasi sensitif pada isi *database* tersebut[3]. Adapun juga penelitian yang dilakukan oleh Rudi Hermawan menjelaskan bagaimana cara mengeksploitasi kerentanan dalam aplikasi *web server* yang terkena *SQL Injection*, tetapi pada penelitian ini tidak menggunakan *Common Vulnerability Scoring System* (CVSS) untuk menentukan nilai tingkat keparahan pada kerentanannya [4].

Berdasarkan uraian diatas, maka dilakukan penelitian dengan judul "Pengujian Keamanan Sistem Menggunakan Metode *Penetration Testing* di *Website* Diskomifostandi Kota Bekasi". Penelitian ini dilakukan untuk mengidentifikasi lebih lanjut untuk keamanan pada *website* sehingga dapat dilakukan pencegahan agar terhindar dari ancaman akses orang yang tidak bertanggung jawab maupun pencurian data.

2. Tinjauan Pustaka

2.1. Dinas Pemberdayaan Perempuan dan Perlindungan Anak (DPPPA)

Dinas Pemberdayan Perempuan dan Perlindungan Anak sebagai *leading sector* dalam penanganan kasus kekerasan anak telah melakukan program pencegahan maupun dalam hal penangnan kasus yang terjadi. Dalam tupoksi yang sudah dijalankan selama ini sudah ada program-program pencegahan maupun penangan kasus, namun dalam menghasilkan sebuah manageman penangan yang baik perlu juga melibatkan Universitas dalam menciptakan sistem penangnan kasus yang lebih holistik, dalam hal ini manajemen komunikasi dalam penanganan kasus kekerasan seksual pada anak menjadi salah satu fokus

dalam kegiatan pengabdian masyarakat. Salah satu bentuk kegiatannya adalah penguatan tim penanganan kasus dan penyadaran masyarakat dalam bentuk sosialisasi seminar kepada masyarakat. Dalam pengabdian ini diharapkan dapat menghasilkan Jurnal Nasional yang menjadi rujukan bagi penanganan kekerasan seksusal pada anak khususnya melalui pendekatan manejemen komunikasi[5].

2.2. Keamanan Informasi

Keamanan informasi merupakan perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, dan meningkatkan return of investment (ROI) serta peluang bisnis. Dalam merancang sistem keamanan sistem informasi terdapat aspek-aspek keamanan informasi yang perlu di perhatikan. Aspek-aspek tersebut antara lain Confidentiality, Integrity, Availability. Informasi merupakan salah satu aset yang penting untuk dilindungi keamanannya. Perusahaan perlu memperhatikan keamanan aset informasinya, kebocoran informasi dan kegagalan pada sistem dapat mengakibatkan kerugian baik pada sisi finansial maupunn produktifitas perusahaan[6].

2.3. *Website*

Website merupakan sebuah media yang memiliki banyak halaman yang saling terhubung (*hyperlink*), dimana *website* memiliki fungsi dalam memberikan informasi berupa teks, gambar, video, suara dan animasi atau penggabungan dari semuanya[7].

2.4. *Penetration Testing*

Penetration testing adalah praktik pengujian aset teknologi informasi untuk menemukan kerentanan keamanan yang dapat dieksploitasi oleh penyerang. Pengujian penetrasi dapat diotomatisasi dengan perangkat lunak atau dilakukan secara manual[8].

2.5. NIST SP 800-115

National Institute of Standards and Technology atau NIST adalah sebuah perusahaan keamanan informasi yang dikembangkan oleh pemerintah Amerika Serikat untuk membuat dan mendorong pengukuran, standar, dan teknologi. Peneliti menggunakan NIST SP 800-115 sebagai metodologi dalam penelitian ini. NIST SP 800- 115 adalah dokumen yang menunjukan metode dan teknik yang digunakan untuk menguji kerentanan situs dalam *penetration testing* dan rekomendasi solusi dalam menangani kerentanan pada situs[9].

2.6. *Common Vulnerability Scoring System* (CVSS)

Common Vulnerability Scoring System cara ini bisa digunakan untuk dapat menentukan tingkat kerentanan dan menghasilkan skor yang mencerminkan tingkat kerentanan pada *webserver* dan CVSS terdapat kualifikasi ke dalam representasi rendah, sedang, tinggi, dan kritis untuk membantu sebuah organisasi menilai dengan benar dan memprioritaskan proses manajemen kerentanan *website*[10].

2.7. *SQL Injection*

Serangan *SQL injection* adalah teknik yang dapat mengeksploitasi kueri dari *structured query language* (SQL) untuk bisa menembus menuju *back-end* dari *database*, jika sudah menembus *database*, penyerang mendapat keleluasaan dalam mendapatkan informasi sensitif yang terdapat pada *database* tersebut, seperti *username*, *password*, nama, alamat, nomor telepon, dan lain-lain[11].

2.8. *Black Box Testing*

Pengujian *black box* biasanya digunakan untuk menguji pekerjaan internal aplikasi tanpa pengetahuan pemrograman. Pengujian *black box* digunakan untuk menguji fungsional maupun *input output* pada aplikasi. Teknik pengujian ini ditujukan kepada para penguji yang tidak memiliki pemahaman dalam pemrograman[12].

2.9. *Kali Linux*

Kali Linux, yang merupakan turunan tingkat lanjut dari keluarga *Linux*, secara luas digunakan untuk keperluan *penetration testing* dan audit keamanan jaringan komputer. Dikembangkan oleh *Offensive Security*, sistem operasi ini merupakan penyempurnaan dari *Back Track Linux* yang lebih matang dan stabil. *Kali Linux* telah diadaptasi sesuai dengan standar pengembangan *Debian* dan diperkenalkan dalam rilis sekitar tahun 2014[13].

2.10. *SQLmap*

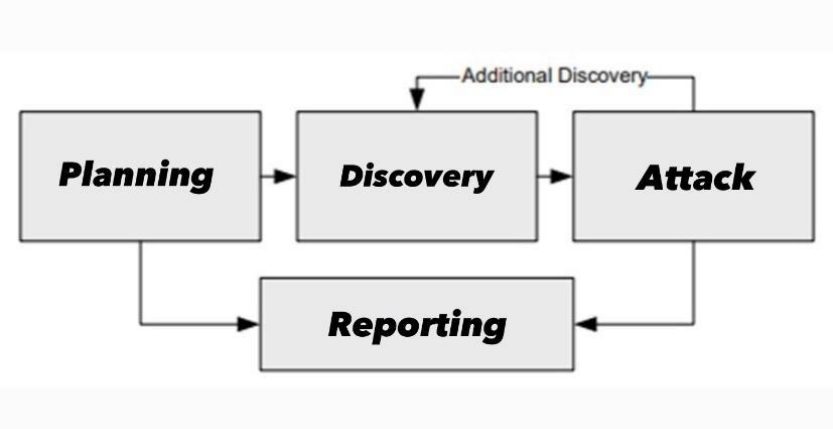
SQLmap adalah alat *open source* yang mampu menganalisis, mendeteksi, dan melakukan eksploitasi (kode yang secara khusus dapat menyerang keamanan sistem komputer) pada kesalahan injeksi *SQL*[14].

2.11. *Directory Buster* (*Dirb*)

Brute force directory adalah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terdiri dari penyerang yang mengonfigurasi nilai yang telah ditentukan, membuat permintaan ke *server* menggunakan nilai tersebut dan kemudian menganalisis responnya[15].

3. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah *Penetration Testing* yang mengacu pada dokumen yang dikeluarkan oleh *National Institute of Standar and Technology* (NIST) dengan kode dokumen NIST SP 800-115, mempunyai tahapan yang terdiri dari *planning*, *discovery*, *attack*, dan *reporting*.



Gambar 1. *Penetration Testing*

Adapun tahapan dalam metode *penetration testing* berdasarkan NIST SP 800-115 pada gambar 1 sebagai berikut:

1. *Planning*

Pada tahap *planning*, peraturan dan hasil yang diharapkan akan didiskusikan dan disetujui oleh kedua pihak, yaitu peneliti dan target. Contoh peraturan yang akan didiskusikan adalah tujuan dilakukannya *penetration testing*, *scope* atau ruang lingkup, rentang waktu pengujian, serta hasil yang diharapkan. Tidak ada pengujian yang dilakukan pada tahap ini.

2. *Discovery*

Tahap *Discovery* mempunyai dua bagian, yaitu mengumpukan informasi tentang target seperti nama *host* dan informasi mengenai alamat IP, sistem, dan *service* dengan cara *scanning* terhadap target. Bagian kedua adalah *vulnerability analysis* atau menganalisis kerentanan yang sudah didapat ketika mengumpulkan informasi.

3. *Attack*

Pada tahap ini, peneliti membuktikan kerentan yang sudah ditemukan pada *discovery* dengan cara menyerang kerentanan tersebut. Pada tahap *attack* atau penyerangan kemungkinan penguji tidak berhasil menyerang, tetapi penguji menemukan informasi yang lebih dalam mengenai target sehingga penguji kembali ke tahap sebelumnya yaitu *discovery*. Jika ini terjadi, perlu diadakan penambahan analisis dan pengujian untuk menentukan tingkat kerentanan yang sebenarnya.

4. *Reporting*

Tahap *reporting* atau laporan adalah tahap yang menjelaskan tentang kerentanan melalui skala dan solusi penanganan kerentanan. Hasil pengujian harus didokumentasikan dan dijelaskan secara lengkap.

4. Hasil dan Pembahasan

4.1. *Planning*

Dalam tahapan *planning*, peneliti menentukan perencanaan dan persiapan

penetration testing. Tahap ini harus dilakukan sesuai metode NIST SP 800-155. Maka dari itu, dibutuhkan pemaparan mulai dari perencanaan dan persiapan sebagai berikut:

a. Ruang lingkup

Wawancara dengan pegawai Diskominfostandi yaitu Zaky Ismail S. Kom. di bidang Teknologi Informasi dan Komunikasi (TIK) bagian keamanan informasi dan staf DPPPA untuk menentukan ruang lingkup pengujian yang akan dilakukan didalam penelitian ini. Adapun kesepakatan yang di hasilkan pada tahap ini adalah:

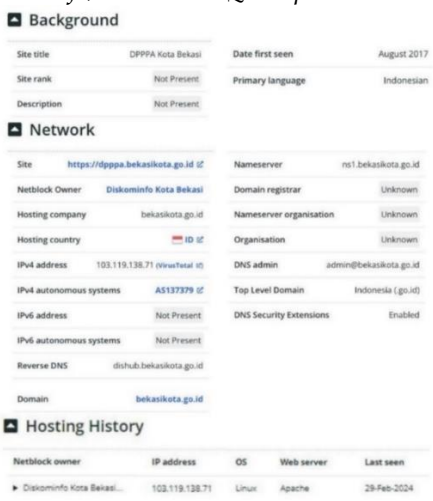
1) Konfirmasi terkait pendekatan dan penjelasan metode *penetration testing* berdasarkan NIST SP 800-155 yang akan digunakan dalam melakukan pengujian kerentanan sistem pada *website* dpppa.bekasikota.go.id.
2) Persetujuan penggunaan teknik *Black box Testing* dalam melakukan *penetration testing*.
3) Target pengujian pada menu *form login* dan terdepat kerentanan *SQL Injection* didalamnya.
4) Persetujuan beberapa *tools* untuk melakukan *penetration testing*.
5) Penyerahan hasil *report* kepada pihak Diskominfostandi Kota Bekasi.

b. Analisis alat kebutuhan pengujian

Dalam penelitian ini dibutuhkan alat yang digunakan untuk melakukan pengujian dengan metode *penetration testing* yaitu terdiri dari perangkat keras (*hardware*), perangkat lunak (*software*), dan *tools* yang digunakan seperti *netcraft*, *dirb*, dan *SQLmap*.

4.2. *Discovery*

Pada tahap ini peneliti memfokuskan upayanya pada *tools*, yaitu *netcraft*, *dirb* dan *SQLmap* untuk melakukan *scanning* terhadap *website* dpppa.bekasikota.go.id. Berikut adalah hasil dari *tools netcraft*, *dirb* dan *SQLmap*:



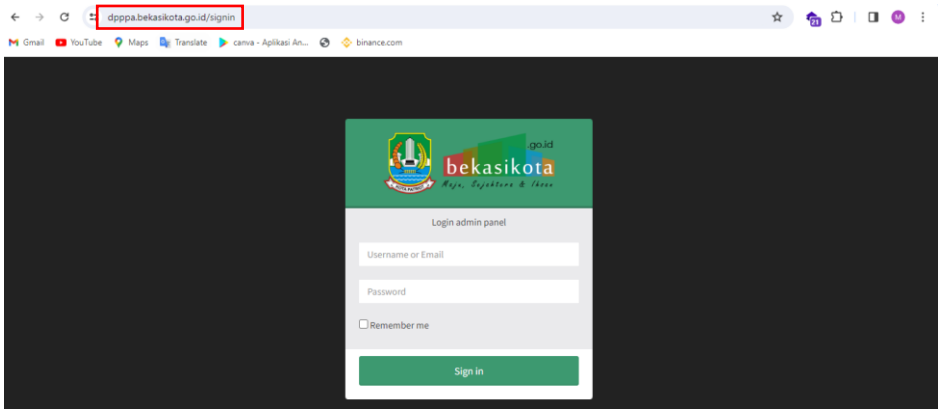
Gambar 2. Hasil *Scanning Netcraft*

Pada gambar 2 terdapat hasil *scanning* dari *tool Netcraft* kegunaannya untuk memberikan informasi *background*, *network*, dan *hosting history* mengenai *site title*, *date first seen*, *IP address*, *domain*, *nameserver*, *Operating System* (OS), *web server* yang digunakan oleh *website* DPPPA.

```
---- Scanning URL: https://dpppa.bekasikota.go.id/ ----
+ https://dpppa.bekasikota.go.id/@ (CODE:400|SIZE:1134)
==> DIRECTORY: https://dpppa.bekasikota.go.id/application/
==> DIRECTORY: https://dpppa.bekasikota.go.id/asset/
==> DIRECTORY: https://dpppa.bekasikota.go.id/banner/
+ https://dpppa.bekasikota.go.id/dashboard (CODE:307|SIZE:0)
+ https://dpppa.bekasikota.go.id/demo (CODE:200|SIZE:17656)
+ https://dpppa.bekasikota.go.id/id (CODE:200|SIZE:37266)
+ https://dpppa.bekasikota.go.id/index.php (CODE:200|SIZE:37266)
+ https://dpppa.bekasikota.go.id/json (CODE:200|SIZE:813668)
+ https://dpppa.bekasikota.go.id/lost+found (CODE:400|SIZE:1134)
+ https://dpppa.bekasikota.go.id/rss (CODE:200|SIZE:1175877)
+ https://dpppa.bekasikota.go.id/server-status (CODE:403|SIZE:199)
+ https://dpppa.bekasikota.go.id/signin (CODE:200|SIZE:2703)
==> DIRECTORY: https://dpppa.bekasikota.go.id/system/
==> DIRECTORY: https://dpppa.bekasikota.go.id/uploads/
==> DIRECTORY: https://dpppa.bekasikota.go.id/wp-admin/
```

Gambar 3. Hasil *Scanning Dirb*

Pada gambar 3 terdapat hasil *scanning directory buster* menggunakan *tool dirb* pada terminal di *kali linux*. Saat *scanning* peneliti menemukan *directory login* dengan *code* 200 berarti bahwa halaman atau *directory* yang ditemukan dapat diakses.



Gambar 4. *Form Login Website*

Pada gambar 4 peneliti memastikan hasil *scanning directory buster* yang didapatkan sebelumnya, saat melakukan pengecekan *directory* dpppa.bekasikota.go.id/*signin* ada halaman *form login* yang muncul dan bisa menjadi informasi yang sangat penting.

```
got a 302 redirect to 'https://dpppa.bekasikota.go.id/signin/checkLogin'. Do you want to follow? [Y/n] Y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY
 clause
    Payload: username=1' RLIKE (SELECT (CASE WHEN (1538=1538) THEN 1 ELSE 0x28 E
ND))-- mATb&password=pass&Submit=Submit

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY cla
use (FLOOR)
    Payload: username=1' OR (SELECT 4629 FROM(SELECT COUNT(*),CONCAT(0x716a6b627
1,(SELECT (ELT(4629=4629,1))),0x7162627171,FLOOR(RAND(0)*2))x FROM INFORMATION_S
CHEMA.PLUGINS GROUP BY x)a)-- HEJe&password=pass&Submit=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=1' AND (SELECT 5716 FROM (SELECT(SLEEP(5)))YwzG)-- RIRF&pa
ssword=pass&Submit=Submit
```

Gambar 5. Hasil *Scanning SQLmap*

Pada gambar 5 tedapat hasil *scanning* kerentanan *SQL Injection* menggunakan *tool SQLmap*. Terlihat terkena *parameter "username"* yang terdapat pada *endpoint /signin*, yang berfungsi sebagai inputan berupa *username* pada saat melakukan *login* ke dalam aplikasi.

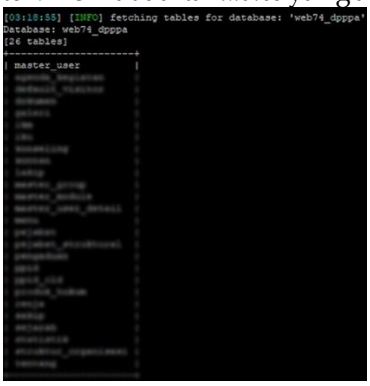
Gambar 6. Hasil *Scanning SQLmap*

Pada gambar 6 hasil *scanning* lanjutan dan terdeteksi ada 11 *database* yang terlihat salah satunya *database* milik *website* DPPPA yaitu web74_dpppa.

4.3. *Attack*

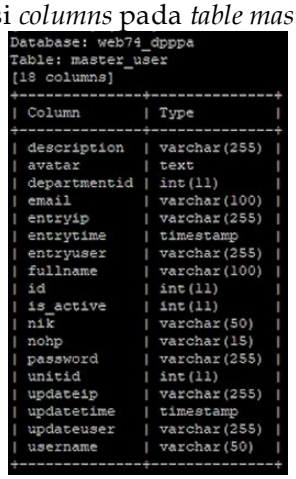
Pada tahap ini, peneliti akan melakukan simulasi penyerangan terhadap *website* dengan informasi yang didapat pada tahap *discovery* guna melihat apakah kerentanan yang ditemukan pada tahap *discovery* dapat dieksploitasi menggunakan *SQLmap* pada terminal *kali linux*. Berikut adalah tahapan eksploitasi kerentanan yang akan dilakukan pada kerentanan *SQL Injection*:

Pada tahapan *discovery* ada suatu kerentanan *SQL Injection* yang terlihat pada *parameter username* dan terdeteksi ada salah satu *database* milik *website* dpppa.bekasikota.go.id yaitu web74_dpppa. Setelah itu dilanjutkan dengan mengeksploitasi kerentanan yang ada pada *database* web74_dpppa untuk melihat daftar *tables* yang ada pada *database* web74_dpppa.



Gambar 7. Daftar *Tables Database* web74_dpppa

Pada Gambar 7 terdapat daftar *tables* dari *database* web74_dpppa. Peneliti melihat daftar tables salah satunya *master_user* yang memungkinkan adanya informasi sensifif seperti *account* seperti *username* dan juga *password*. Lalu peneliti melanjukan eksploitasi pada *table master_user* untuk melihat isi *columns* pada *table master_user*.

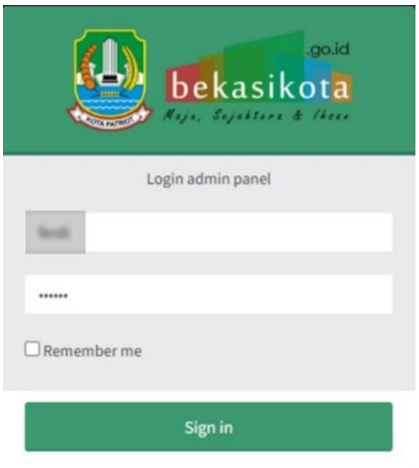


Gambar 8. Daftar *Columns Table master_user*

Pada Gambar 8 terdapat daftar *columns* pada *table master_user*. Pada *columns* tersebut banyak informasi sensitif seperti *username*, *password*, nohp, nik, dll. Peneliti mencoba mengekstrak data dari *database* yang terkena dampak oleh serangan *SQL injection*. Dengan opsi ini, *SQLMap* akan mencoba menampilkan isi dari *table* dan *columns* tersebut.

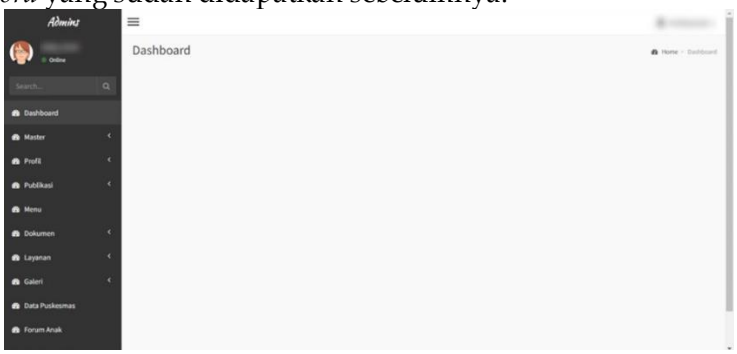
Gambar 9. Informasi *table* dari *master_user*

Pada Gambar 9 peneliti dapat melihat informasi sensitif seperti *username* dan *password* untuk masuk ke *form login* yaitu dpppa.bekasikota.go.id/*signin* yang sudah didapatkan sebelumnya menggunakan *dirb* pada hasil tahapan *discovery*. Lalu menggunakan salah satu *account* untuk *login* ke halaman *backend website*.



Gambar 10. Proses *Login*

Pada gambar 10 peneliti mencoba *login* ke halaman *backend* dengan informasi *username* dan *password* yang sudah didapatkan sebelumnya.



Gambar 11. Tampilan Halaman Backend

Pada Gambar 11 menunjukkan bahwa peneliti berhasil masuk ke halaman *backend* pada *website* DPPPA dan bisa dengan mudah mengeksploitasi halaman *backend* tersebut.

4.4. *Reporting*

Tahap *reporting* adalah tahap terakhir berdasarkan standar NIST SP 800-115. Pada tahap sebelumnya, peneliti sudah mengumpulkan temuan kerentanan dan melakukan simulasi penyerangan terhadap kerentanan yang ditemukan. Berikut adalah tabel kerentanan yang telah ditemukan dapat dilihat pada tabel 1:

Tabel 1. Hasil *Reporting*

Nama Kerentanan	CVSS 3.1	Hasil Pengujian	Dampak	Solusi
Sensitive Information Disclosure	5.3 (*Medium*)	Mendapatkan *directory form login* tersembunyi pada *website* DPPPA yaitu dpppa.bekasikota.go.id/*signin*.	Menjadi informasi bagi pihak yang tidak berwenang dan bisa menjadi langkah awal untuk penyerang dalam pencarian kelemahan atau kerentanan lebih lanjut.	Mengganti nama *directory* agar terhindar dari nama *directory* yang umum. Dengan cara ini, serangan otomatis yang berusaha menemukan *form login* pada *directory* yang umum seperti "/*signin*" akan menjadi lebih sulit.
SQL Injection	10.0 (*Critical*)	Mendapatkan informasi *username* dan *password* dari informasi *database* yang terbuka pada kerentanan *SQL Injection*.	Berdampak mengetahui banyak informasi sensitif yang bisa di salahgunakan.	Menggunakan fungsi *escape* untuk membersihkan input pengguna untuk memastikan tidak ada karakter yang mencurigakan atau berbahaya misalnya karakter seperti tanda kutip tunggal (‘), tanda kutip ganda (“), tanda bintang(*) dan karakter *wildcard SQL* harus dihindari atau di *escape*. Menurut Robby Yuli Endra Apabila sebuah input tidak menggunakan fungsi *escape*() maka akan menjadi sasaran yang empuk untuk diserang menggunakan *SQL Injection*. Bukan itu saja serangan melalui format ekstensi, Xsrf, dan Xss belum ada pada PHP *Native* jadi *developer* diharuskan untuk membuat keamanan tersebut[16].

5. Kesimpulan

Kesimpulan

Setelah menerima laporan bug hunter terkait celah kerentanan *website* DPPPA, peneliti mengkonfirmasi kebenarannya melalui pengujian menggunakan metode *penetration testing* berdasarkan standar NIST SP 800-115 dengan tahapan *planning*, *discovery*, *attack*, dan *reporting* berhasil mengidentifikasi dua kerentanan pada *website* DPPPA, yaitu *sensitive information disclosure* dan *SQL Injection*. Dalam menggunakan metode *penetration testing* ini peneliti mendapatkan celah kerentanan *sensitive information disclosure* yang dapat melihat *directory form login* menuju ke *back end* dan celah kerentanan *SQL Injection* yang dapat mengetahui informasi sensitif seperti *username* dan *password* yang bisa di salahgunakan, Penilaian risiko menggunakan CVSS versi 3.1 menunjukkan *SQL Injection* memiliki nilai *critical* dan *sensitive information disclosure* bernilai *medium*, dan dilanjutkan memberi solusi perbaikan yang tepat untuk kedua kerentanan tersebut agar meningkatkan keamanan *website* DPPPA.

Daftar Pustaka

[1] I. M. P. Utama, K. R. Putri, A. A. E. Wirayuda, and V. A. Tyora, “Analisis Perbandingan Kinerja Tool Website Directory Brute Force dengan Target Website DVWA,” *JURNAL INFORMATIK*, vol. 18, no. 3, pp. 1–8, 2022, [Online]. Available: https://www.kali.org/get-kali/#kali-platforms,

[2] I. G. Ary Suta Sanjaya, G. Made arya Sasmita, and D. Made Sri Arsa, “Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF,” *Jurnal Ilmiah Merpati*, vol. 8, no. 2, pp. 1–12, 2020.

[3] Andria and R. Pamungkas, “Penetration Testing Database Menggunakan Metode SQL Injection Via SQLmap di Termux,” *IJAI (Indonesian Journal of Applied Informatics)*, vol. 5, no. 1, pp. 1–10, 2020.

[4] R. Hermawan, "Teknik Uji Penetrasi Web Server Menggunakan SQL Injection Dengan SQLmap di Kalilinux," *STRING (Satuan Tulisan Riset dan Inovasi Teknologi)*, vol. 6, no. 2, pp. 1–7, 2021.

[5] Novrian, R. Sovianti, and M. Husni Mubarok, "Pendampingan dan Sosialisasi Manajemen Komunikasi Penanganan Kasus Kekerasan Seksual Pada Anak di Dinas P3A dan 18 Kelurahan Kota Bekasi," *Jurnal Pengabdian Masyarakat Multidisiplin*, vol. 2, no. 2, pp. 1–9, 2021.

[6] B. Triandi, "Keamanan Informasi secara Aksiologi Dalam Menghadapi Era Revolusi Industri 4.0," *Jurnal Riset Komputer (JURIKOM)*, vol. 6, no. 5, pp. 1–7, 2019, [Online]. Available: http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom|Page477

[7] H. Wangge Lawa, Y. D. D. Y. Kwuta, and E. E. Sala, "Sistem Informasi Pengelolaan Bantuan Dana Desa Hangalande Berbasis Web," *Jurnal Sistem Informasi dan Teknik Komputer*, vol. 8, no. 1, pp. 1–7, 2023.

[8] H. Sofyan, M. Sugiarto, and B. M. Akbar, "Implementation of Penetration testing on Websites to Improve Security of Information Assets UPN 'Veteran' Yogyakarta," *Jurnal Informatika dan Teknologi Informasi*, vol. 20, no. 2, pp. 1–10, 2023, doi: 10.31515/telematika.v20i2.7757.

[9] S. A. Maherza, B. Hananto, and I. W. W. Pradnyana, "Penetration Testing Terhadap Website Sekolah Menengah Atas ABC dengan Metode NIST SP 800-115," *Jurnal Informatik*, vol. 19, no. 1, pp. 1–17, 2023.

[10] B. P. Zen, R. A. G. Gultom, and A. H. S. Reksoprodjo, "Analisis Security Assessment Menggunakan Metode Penetration Testing Dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara," *Jurnal Teknologi Penginderaan*, vol. 2, no. 1, pp. 1–18, 2020.

[11] D. Perdana Putranto, Jayanta, and B. Hananto, "Analisis Keamanan Website Leads UPNVJ Terhadap Serangan SQL Injection & Sniffing Attack," *JURNAL INFORMATIK*, vol. 18, no. 3, pp. 1–9, 2022.

[12] I. R. Dhaifullah, M. Muttanifudin, A. A. Salsabila, and M. A. Yakin, "Survei Teknik Pengujian Software," *Journal Automation Computer Information System*, vol. 2, no. 1, pp. 1–8, 2022.

[13] T. Yusnanto, M. A. Muin, and S. Wahyudiono, "Analisa Infrastruktur Jaringan Wireless dan Local Area Network (WLAN) Meggunakan Wireshark Serta Metode Penetration Testing Kali Linux," *Journal on Education*, vol. 04, no. 04, pp. 1–7, 2022.

[14] M. A. W. Wardhana, K. D. P. Pratama, and S. Muryani, "Aplikasi Informasi Pemeliharaan Alat Produksi Pada PT. Teguh Karya Perima," *Jurnal Infortech*, vol. 4, no. 2, pp. 1–8, 2022, [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/infortech148

[15] W. Linggih Jaelani, Yanto, and F. Khoirunnisa, "Penetration Testing Website Dengan Metode Black Box Testing Untuk Meningkatkan Keamanan Website Pada Instansi (Redacted)," *Jurnal Ilmiah Nasional Riset Aplikasi dan Teknik Informatika*, vol. 05, no. 01, pp. 1–8, 2023.

[16] R. Y. Endra, Y. Aprilinda, Y. Y. Dharmawan, and W. Ramadhan, "Analisis Perbandingan Bahasa Pemrograman PHP Laravel dengan PHP Native pada Pengembangan Website," *Jurnal Manajemen Sistem Informasi dan Teknologi*, vol. 11, no. 1, pp. 1–8, Jun. 2021, doi: 10.36448/expert.v11i1.2012.