INNOVATIVE: Journal Of Social Science Research
Volume 3 Nomor 4 Tahun 2023 Page 9192-9203
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

# Penanganan Celah Keamanan *Website* dengan *Ethical Hacking* dan *Issaf* Menggunakan *Acunetix Vulnerability* (Studi Kasus di Bkpsdmd Kabupaten Kerinci)

Lusi Kestina[1✉], Yuhandri[2], Gunadi Widi Nurcahyo[3]
Universitas Putra Indonesia YPTK Padang
Email: lusikestina@gmail.com[1✉]

Abstrak

Permasalahan keamanan pada dunia pemerintahan menjadi salah satu sasaran praktik peretas jahat. Kepentingan *hacker* pada sektor pemerintahan tidak hanya berfokus pada kepentingan ekonomi, tetapi juga kepentingan politik. Salah satu serangan yang sering terjadi adalah *web defacement*. Badan Kepegawaian dan Pengembangan Sumber Daya Manusia Daerah (BKPSDMD) Kabupaten Kerinci merupakan instansi yang aktif dalam menggunakan teknologi *website* dalam aktifitasnya. Penelitian ini dilakukan untuk mengukur tingkat keamanan *website* BKPSDMD dengan menerapkan *Ethical Hacking* dan ISSAF. Hasil dari penelitian ini akan merekomendasikan dan menerapkan tindakan optimalisasi berdasarkan hasil analisa dari penerapan *Ethical Hacking* dan ISSAF.
Kata Kunci :

Abstract

Security issues in the world of government are one of the targets of malicious hacker practices. Hackers' interests in the government sector are not only focused on economic interests, but also political interests. One attack that often occurs is web defacement. The Kerinci Regency Personnel and Human Resources Development Agency (BKPSDMD) is an agency that is active in using website technology in its activities. This research was conducted to measure the security level of the BKPSDMD website by applying Ethical Hacking and ISSAF. The results of this study will recommend and implement optimization actions based on the results of the analysis of the application of Ethical Hacking and ISSAF.
Keywords :

## PENDAHULUAN

Keamanan siber telah menjadi isu prioritas seluruh negara di dunia [1]. Pada dunia pemerintahan, hal ini disebabkan oleh telah banyaknya instansi pemerintah menerapkan sistem informasi untuk menunjang segala aktivitasnya. Namun para pengembang sistem informasi tersebut tidak maksimal dalam mengantisipasi adanya celah keamanan. Seiring perkembangannya, serangan siber makin sering dirasakan. Beberapa kalangan mengingatkan bahwa serangan siber juga mulai beralih dari mendapatkan keuntungan ekonomi ke kepentingan politik [2]. Semua organisasi baik pemerintah maupun swasta perlu memiliki manajemen risiko yang kuat untuk mengurangi kemungkinan terjadinya serangan siber [3].

Berdasarkan data dari Lanskap Keamanan Siber Indonesia 2022 yang dirilis oleh Badan Siber dan Sandi Negara (BSSN) menyebutkan bahwa total trafik anomali di Indonesia selama tahun 2022 adalah 976.429.996 terdapat 2.348 kasus yang merupakan jenis serangan *Web Defacement*.

*Web Defacement* merupakan salah satu celah keamanan pada *website* inilah yang dimanfaatkan oleh seseorang untuk menyerang sebuah *website* [4]. Hal ini berawal dari permasalahan keamanan yang menjadi bagian yang penting dari sebuah sistem informasi [5]. Organisasi menghadapi tantangan terbesar bagaimana mengamankan aplikasi *Website* mereka dari ancaman kejahatan siber [6]. Banyak instansi pemerintah yang belum mengelola keamanan informasi dengan baik, sehingga rentan terhadap serangan siber. Hal ini terlihat dari masih banyaknya instansi pemerintah yang menggunakan aplikasi atau instalasi bajakan sehingga masih mudah dimanfaatkan oleh serangan siber di organisasi pemerintah [7]. *Ethical Hacking* atau biasa disebut dengan Penyerang Topi Putih adalah alat penting untuk menguji sistem komputer dan aplikasi jaringan atau Website untuk menemukan kelemahan keamanan [8].

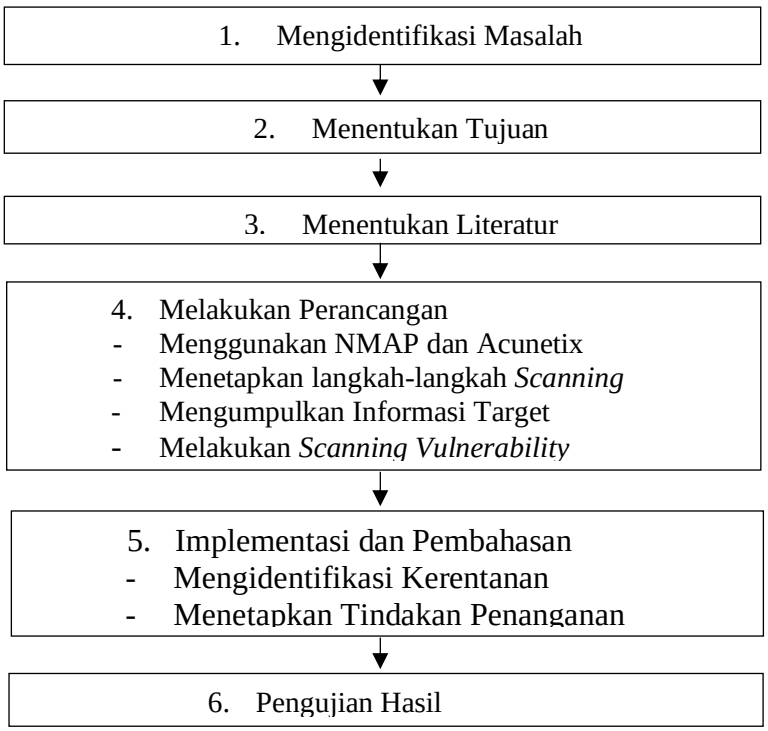
Badan Kepegawaian dan Pengembangan Sumber Daya Manusia Daerah (BKPSDMD) Kabupaten Kerinci adalah salah satu instansi di lingkungan pemerintah kabupaten Kerinci yang menggunakan *Website* sebagai media penyampaian informasi. *Website* BKPSDMD Kabupaten Kerinci juga tak lepas dari resiko ancaman keamanan.

Berdasarkan kondisi diatas, diperlukan adanya penanganan celah keamanan pada *Website* BKPSDMD Kabupaten Kerinci. Penelitian ini akan menggunakan *Ethical Hacking* dan ISSAF (*Information System Security Assesment Framework*). *Ethical Hacking* merupakan suatu aktifitas melakukan penetrasi ke suatu sistem [9], sedangkan ISSAF digunakan untuk menganalisa keamanan sistem dengan metode *Penetration Testing* [10]. Hasil penelitian ini diharapkan dapat memberikan manfaat bagi kepala BKPSDMD terkait penanganan celah

keamanan pada *Website* BKPSDMD yang ditemukan dan memberikan rekomendasi tindakan pengamanan sehingga dapat meminimalisir ancaman serangan siber.

## METODE PENELITIAN

Metodologi penelitian merupakan cara atau langkah ilmiah yang digunakan dalam melakukan penelitian. Adapun kerangka kerja penelitian sebagai berikut:




Gambar 2.1 Kerangka Kerja Penelitian

1. Mengindentifikasi Masalah

   Identifikasi masalah merupakan proses mengidentifikasi permasalahan yang akan dijadikan fokus pada penelitian. Masalah yang menjadi fokus pada penelitian ini adalah penanganan celah keamanan pada *Website* BKPSDMD Kabupaten Kerinci
2. Menentukan Tujuan

   Menentukan tujuan adalah langkah yang sangat penting dalam proses penelitian. Tujuan penelitian ini adalah menguji keamanan, menganalisis celah keamanan dan memperbaiki celah keamanan pada *Website* BKPSDMD Kabupaten Kerinci
3. Menentukan Literatur

   Studi Literatur adalah sebuah proses mencari, mengevaluasi dan menyatukan sumber-sumber informasi yang relevan dengan topik penelitian. Studi literatur yang dilakukan menghasilkan data seperti pada Tabel 1.

Tabel 1. Data Website BKPSDMD Kab.Kerinci

| Setting | Value |
|---|---|
| *PHP Built On* | *Native* |
| *Database Type* | *myqsl* |
| *Database Version* | *5.2.1* |
| *Database Collation* | *Latin_swedish_ci* |
| *Database Connection Collation* | *mysqli* |
| *PHP Version* | *7.4* |
| *Web Server* | *Apache* |
| *Web Server to PHP Interface* | *cpanel* |

4. Melakukan Perancangan

   Perancangan adalah proses merancang dan mengatur langkah-langkah untuk mencapai tujuan tertentu. Perancangan dimulai dari mengumpulkan informasi menggunakan *tools* NMAP dan Whois.com. Setelah informasi awal didapatkan, kemudian dilakukan *scanning* pada *website* target menggunakan *Acunetix Web Vulnerability*.
5. Implementasi dan Pembahasan

   Tahapan implementasi dilakukan dengan menguji kerentanan yang ada pada *Website* BKPSDMD Kabupaten Kerinci dengan *Ethical Hacking* dan ISSAF kemudian memperbaiki celah yang telah ditemukan.
6. Pengujian Hasil

   Setelah semua tahapan selesai, selanjutnya akan dilakukan pengujian kembali terhadap perbaikan celah yang telah dilakukan.

## HASIL DAN PEMBAHASAN

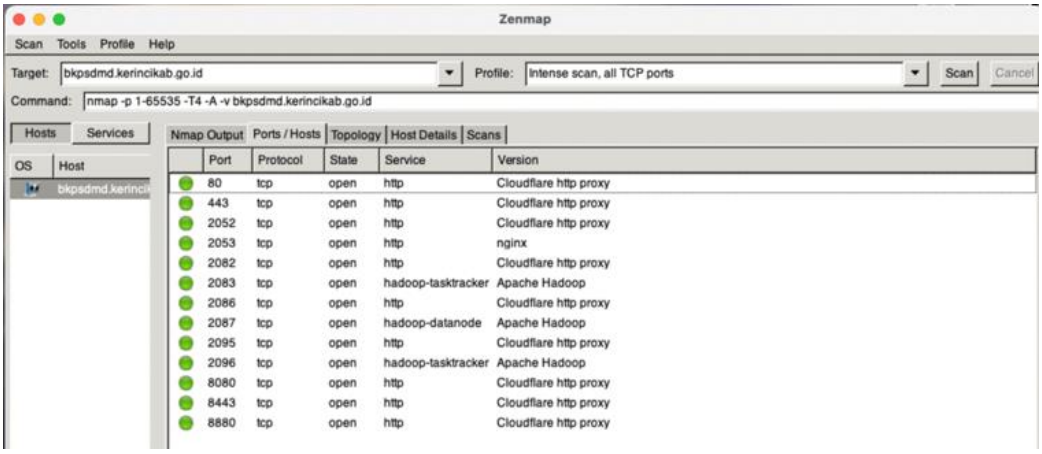
### Hasil

### Ethical Hacking

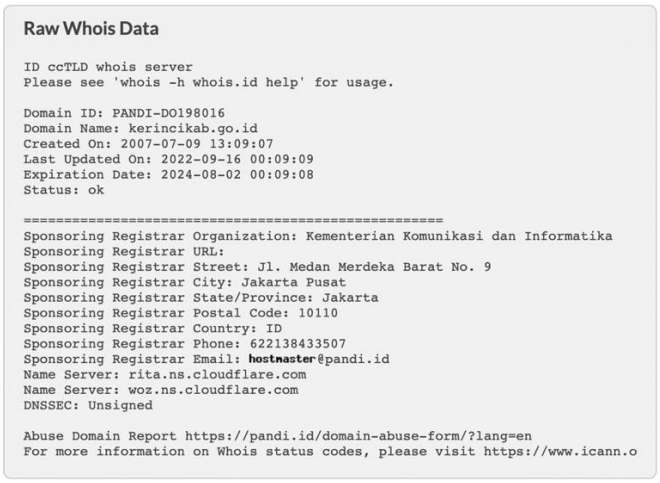
*Ethical hacking* juga dikenal sebagai *white hat hacking*. Pelaku *Ethical Hacking* disebut juga dengan *ethical hacker*. Terdapat 3 tahapan utama pada praktik Ethical Hacking yaitu *Reconnaissance*, *Scanning* dan *Assessment* dan *Exploitation*.

a. *Reconnaissance*

Tahap awal ini dilakukan pengumpulan sebanyak mungkin informasi tentang target seperti alamat IP, nama *domain*, informasi DNS dan detail lainnya. Pengumpulan informasi menggunakan *tools* NMAP dan Whois.com seperti pada Gambar 3.1 dan 3.2 dibawah ini




Gambar 3.1 Hasil *Scanning* menggunakan NMAP

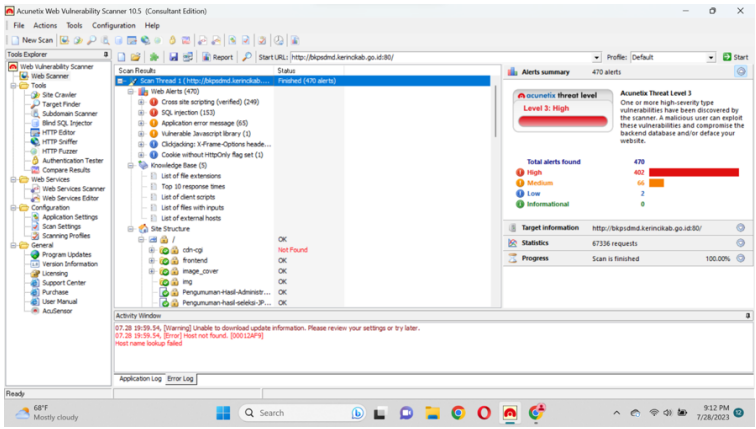



Gambar 3.2 Hasil *Scanning* menggunakan Whois.com

Pada hasil *scan* dari *tools* NMAP memperlihatkan *port-port* yang terbuka yang dapat dimanfaatkan oleh penyerang. Sedangkan pada hasil *scan* menggunakan *Whois.com* menampilkan informasi bahwa https://bkpsdmd.kerincikab.go.id menggunakan *Domain* ID: PANDI- DO198016. *Domain* ini berasal dari sebuah layanan Pengelola Nama *Domain* Internet Indonesia (PANDI) yang dibuat pada 09 Juli 2007 dan akan *expired* pada tanggal 02 Agustus 2024.

b. *Scanning* dan *Assessment*

Proses *scanning* pada tahap ini dilakukan dengan menggunakan *tools Acunetix Web Vulnerability Scanner* seperti yang terlihat pada Gambar 3.3



Gambar 3.3 Hasil *Scanning*

Selanjutnya, pada proses *assessment* terhadap prioritas kerentanan, perlu diperhatikan tingkat kerentanan dan dampaknya pada sistem. Kerentanan yang memiliki tingkat dan dampak yang tinggi harus diprioritaskan terlebih dahulu untuk diatasi.

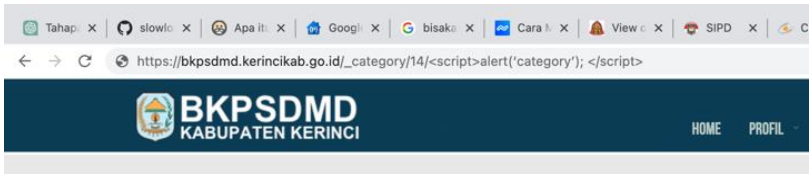
c. Exploitation

Tahapan *Ethical Hacking* berikutnya adalah *Exploitasi*. Pada penelitian ini, exploitasi dilakukan dengan melakukan percobaan penyerangan dengan Teknik *Distributed Denail of Service* (DDOS) dengan memanfaatkan tools *Slowloris*. Seperti pada Gambar 3.4

```
lusikestina@MacBook-Air-Lusi ~ % cd slowloris
lusikestina@MacBook-Air-Lusi slowloris % python3 slowloris.py bkpsdmd.kerincikab.go.id
[26-08-2023 12:29:58] Attacking bkpsdmd.kerincikab.go.id with 150 sockets.
[26-08-2023 12:29:58] Creating sockets...
[26-08-2023 12:30:09] Sending keep-alive headers...
[26-08-2023 12:30:09] Socket count: 150
[26-08-2023 12:30:24] Sending keep-alive headers...
[26-08-2023 12:30:24] Socket count: 150
[26-08-2023 12:30:24] Creating 149 new sockets...
[26-08-2023 12:30:48] Sending keep-alive headers...
[26-08-2023 12:30:48] Socket count: 150
[26-08-2023 12:30:48] Creating 149 new sockets...
[26-08-2023 12:31:16] Sending keep-alive headers...
[26-08-2023 12:31:16] Socket count: 150
```

Gambar 3.4. Percobaan *Exploitasi* dengan DDOS

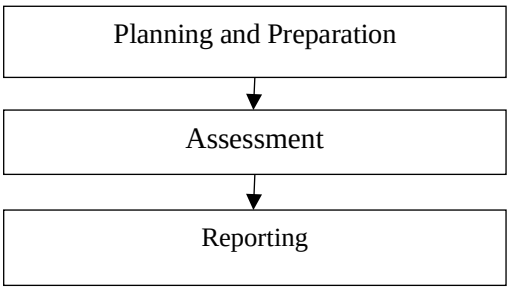
Exploitasi berikutnya pada celah *Cross Site Script* dengan menyisipklan kode khusus pada URL atau *Browser* agar kode tersebut dieksekusi oleh *web browser* ketika diakses oleh pengguna lain. Pada kasus ini, *website* target selalu merespon apa saja *script* yang *diinputkan* padanya.




Gambar 3.5.Penyisipan Kode asing pada URL

ISSAF

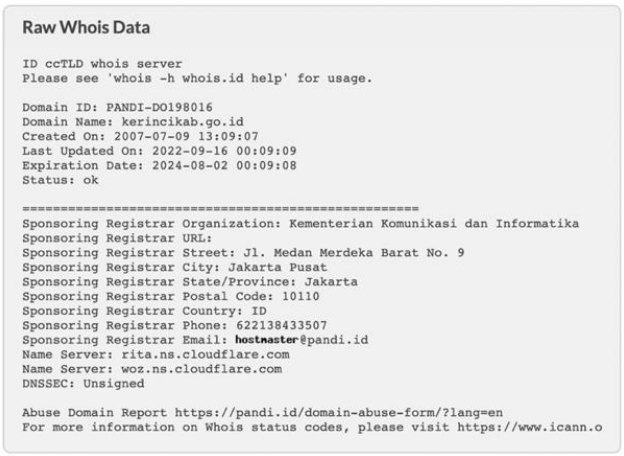
ISSAF adalah kerangka kerja yang digunakan untuk melakukan penilaian keamanan sistem informasi.




Gambar 3.6 Tahap Pengujian menggunakan ISSAF

1. *Planning and Preparation*

Pada tahap ini, dilakukan kesepakatan Kerjasama yang tertuang dalam Surat Pernyataan Perjanjian Kerahasiaan (*Non Disclousure Agreement*) *IT Security Assessement* antara Lusi Kestina, S.Kom (sebagai peneliti) dengan Efrawadi, SP, M.Si (Kepala BKPSDMD Kabupaten Kerinci) pada tanggal 1 Juni 2023. Setelah kesepakatan dibuat, dilakukan *scanning* pada *website* target seperti yang terlihat pada Gambar 3.7



**Raw Whois Data**

```
ID ccTLD whois server
Please see 'whois -h whois.id help' for usage.

Domain ID: PANDI-DO198016
Domain Name: kerincikab.go.id
Created On: 2007-07-09 13:09:07
Last Updated On: 2022-09-16 00:09:09
Expiration Date: 2024-08-02 00:09:08
Status: ok

================================================
Sponsoring Registrar Organization: Kementerian Komunikasi dan Informatika
Sponsoring Registrar URL:
Sponsoring Registrar Street: Jl. Medan Merdeka Barat No. 9
Sponsoring Registrar City: Jakarta Pusat
Sponsoring Registrar State/Province: Jakarta
Sponsoring Registrar Postal Code: 10110
Sponsoring Registrar Country: ID
Sponsoring Registrar Phone: 622138433507
Sponsoring Registrar Email: hostmaster@pandi.id
Name Server: rita.ns.cloudflare.com
Name Server: woz.ns.cloudflare.com
DNSSEC: Unsigned

Abuse Domain Report https://pandi.id/domain-abuse-form/?lang=en
For more information on Whois status codes, please visit https://www.icann.o
```

Gambar 3.7 Hasil Whois.com BKPSDMD Kabupaten Kerinci

2. *Assessment*

Tahap *Assessment* pada ISSAF tidak jauh berbeda dengan tahap *Assessment* pada *Ethical Hacking*. Pada tahap ini dilakukan *Scanning* terhadap *website* dengan tujuan mencari celah kerentanan pada *website* BKPSDMD Kabupaten Kerinci seperti terlihat pada Tabel 2.

Tabel 2 Data Hasil Scanning BKPSDMD Kabupaten Kerinci

| No | *Thread Level* | *Jenis Web Alert* | *Level Severity* | Jumlah Alert |
|---|---|---|---|---|
| 1 | *3 (High)* | *Cross site scripting :* | *High* | 249 |
| 2 | | *SQL Injection* | *High* | 153 |
| 3 | | *Application Error Message* | *Medium* | 65 |
| 4 | | *Vulnerable Javascript Library* | *Medium* | 1 |
| 5 | | *Clickjacking: X-Frame-Options header missing* | *Low* | 1 |
| 6 | | *Cookie without HttpOnly flag set* | *Low* | 1 |

3. *Reporting*

Tahap *reporting* pada ISSAF merupakan pelaporan hasil penilaian keamanan sistem, menyusun laporan dan rekomendasi perbaikan berdasarkan celah yang ditemukan. Laporan disampaikan dengan tujuan agar pemilik *website* target dapat mengambil keputusan untuk memutuskan langkah lebih lanjut agar segera dilakukan penanganan.

Tabel 3. Data Resiko kerentanan

| No | Jenis *Web Alert* | *Level / Severity* | Resiko |
|---|---|---|---|
| 1 | *Cross site scripting* | *High* | *Cross-Site Scripting* (XSS) adalah jenis serangan keamanan pada aplikasi web di mana penyerang menyuntikkan skrip berbahaya (biasanya dalam bentuk *JavaScript*) ke dalam halaman web yang kemudian dieksekusi oleh *browser* pengguna akhir. Kerentanan ini dapat dimanfaatkan oleh penyerang untuk mencuri informasi pengguna dan menyebabkan perubahan yang tidak diinginkan pada halaman *web*, atau mengarahkan pengguna ke situs *web* palsu. |

| | | | |
|---|---|---|---|
| 2 | *SQL Injection* | *High* | Penyerang dapat memasukkan input yang dirancang secara khusus untuk memanipulasi pernyataan SQL yang dieksekusi oleh *database*. Serangan ini terjadi ketika aplikasi *web* tidak memvalidasi atau menyaring input yang dimasukkan oleh pengguna sebelum menggunakannya dalam pernyataan SQL. Serangan ini dapat mengakibatkan akses yang tidak sah ke *database*, pengungkapan informasi sensitif, perubahan data, atau bahkan penghapusan data. |
| 3 | *Application Error Message* | *Medium* | *Application Error Message* dapat dieksploitasi oleh penyerang untuk mendapatkan informasi sensitive untuk merencanakan serangan lebih lanjut. |
| 4 | *Vulnerable Javascript Library* | *Medium* | Kerentanan ini dapat dimanfaatkan oleh penyerang untuk melancarkan serangan seperti serangan injeksi kode, pencurian data sensitif, eksekusi skrip berbahaya, dan manipulasi alur aplikasi. |
| 5 | *Clickjacking: X-Frame-Options header missing* | *Low* | Penyerang dapat memasukkan konten berbahaya dari situs eksternal ke dalam iframe tersembunyi di halaman yang tampaknya sah, mengelabui pengguna untuk mengklik atau berinteraksi dengan elemen yang tidak disadari mereka. |
| 6 | *Cookie without HttpOnly flag set* | *Low* | Celah ini dapat membuka jalan bagi serangan *cross-site scripting* (XSS), di mana penyerang dapat mencuri *cookie* pengguna dan meretas sesi, mengakses informasi pribadi, atau melakukan tindakan tidak sah atas nama pengguna |

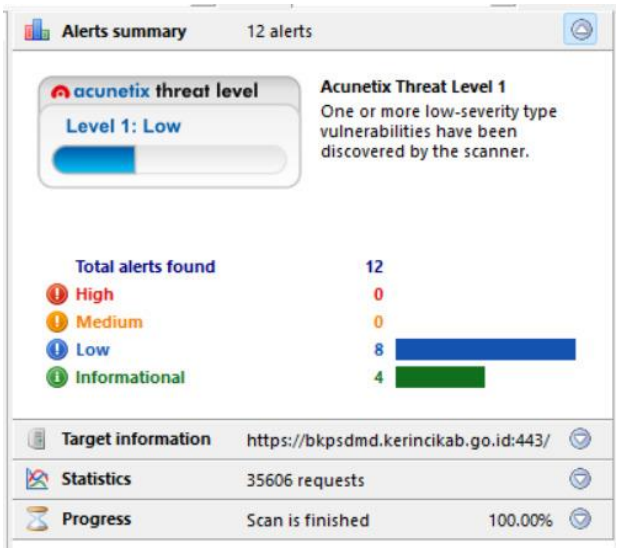
Optimalisasi

Optimalisasi merupakan perancangan dalam mengatasi kerentanan yang telah ditemukan dan telah di-*exploitasi* sebelumnya.

Tabel 4 Hasil Perbaikan dari penerapan *Ethical Hacking* dan ISSAF

| No | Jenis *Web Alert* | Rekomendasi Perbaikan | Hasil |
|---|---|---|---|
| 1 | *Port* terbuka | Memutuskan koneksi pada *port* yang tidak diperlukan, penggunaan *firewall* untuk mengontrol akses, pembaruan perangkat lunak secara teratur, segmentasi jaringan, kontrol akses yang tepat, penerapan protokol keamanan dan pemantauan pada log aktivitas | Berhasil |
| 2 | *Cross site scripting* | Memfilter karakter asing pada URL, diperlukan modifikasi *script* pada /home/u4525527/public_html/bkpsdmd/frontend/template4/page.php dengan menghapus script berikut ini : ‘ include 'post-category.php'; ‘ | Berhasil |
| 3 | *SQL Injection* | Memfilter metakarakter dari setiap *input* pengguna | Berhasil |
| 4 | *Application Error Message* | Mengatur pesan kesalahan agar tidak mengungkapkan informasi sensitif atau rincian teknis yang berlebihan, | Berhasil |
| 5 | *Vulnerable Javascript Library* | Mengupdate Javascript *Library* | Berhasil |

Setelah optimalisasi pada *website* dilakukan dengan mengacu pada rekomendasi perbaikan, dilakukan uji *website* kembali dengan hasil kerentanan Level 1 : Low seperti Gambar 3.8 berikut :




Gambar 3.8 Hasil *Scanning* setelah optimalisasi

## SIMPULAN

Penerapan Ethical Hacking dan ISSAF dapat menangani masalah pada *Website* https://bkpsdmd.kerincikab.go.id dengan baik. Berdasarkan penelitian yang dilakukan, penerapan *Ethical Hacking* lebih mendetail dalam pengumpulan informasi karena *Ethical Hacking* menempuh tahap *Exploitasi* / percobaan penyerangan sehingga peneliti mengetahui lebih dalam mengenai tingkat bahaya celah keamanan tersebut.

## DAFTAR PUSTAKA

Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara. Dinamika Global: Jurnal Ilmu Hubungan Internasional, 7(02), 295-316.

Sanjaya, B. R., Efrianti, D., Ali, M., Prasetyo, T., Mukhtadi, M., Widasari, Y. K., & Khumairoh, Z. (2022). Pengembangan Cyber Security dalam Menghadapi Cyber Warfare di Indonesia. Journal of Advanced Research in Defense and Security Studies, 1(1), 19-34.

Mahendra, V., & Soewito, B. (2023). Penerapan Kerangka Kerja NIST Cybersecurity dan CIS Controls sebagai Manajemen Risiko Keamanan Siber. Techno. Com, 22(3), 527-538.

Herawati, N., & Budiyanto, V. (2023). ANALISIS KEAMANAN SEBUAH DOMAIN MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP) Zap. JURNAL TEKNOLOGI TECHNOSCIENTIA, 27-36.

Rahayu, S. F., Prawira, D., & Rusi, I. (2021). PENGUKURAN TINGKAT KEAMANAN INFORMASI MENGGUNAKAN METODE INDEKS KAMI. Coding Jurnal Komputer dan Aplikasi, 9(03), 468-477.

Patel, K. (2019, April). A survey on vulnerability assessment & penetration testing for secure communication. In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 320-325). IEEE.

Rai, I. N. A. S., Heryadi, D., & Kamaluddin, A. (2022). The Role of Indonesia to Create Security and Resilience in Cyber Spaces [Peran Indonesia dalam Membentuk Keamanan dan Ketahanan di Ruang Siber]. Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional, 13(1), 43-66.

Devi, R. S., & Kumar, M. M. (2020, June). Testing for security weakness of web applications using ethical hacking. In 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184) (pp. 354-361). IEEE.

Muhyidin, Y., Totohendarto, M. H., & Undamayanti, E. (2022). Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto Dengan Metode Ethical Hacking. Jurnal Teknologika, 12(1), 80-89.

Umar, R., Riadi, I., & Elfatiha, M. I. A. (2023). Analisis Keamanan Sistem Informasi Akademik Berbasis Web Menggunakan Framework ISSAF. Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi, 12(1)