**Jurnal Pendidikan dan Konseling**
Volume 4 Nomor 4 Tahun 2022
E-ISSN: 2685-936X dan P-ISSN: 2685-9351
**Universitas Pahlawan Tuanku Tambusai**

# Analisis Vulnerability Terhadap Website Lembaga Bahasa LIA Palembang Menggunakan Nessus, Netsparker dan Acunetic

**Aristian[1*], Widya Cholil[2]**
[1,2]Program Studi Teknik informatika, Fakultas Ilmu Komputer, Universitas Bina Darma
E-mail: aristian2310@gmail.com[1], cholilwdya@gmail.com[2]

**Abstrak**

Website merupakan salah satu media informasi yang sangat penting di era perkembangan pesat teknologi dan informasi. Aspek keamanan dan mengetahui celah Kerentanan mempunyai peranan sangat penting dalam sebuah website. Analisis keamanan dapat dilakukan dengan melakukan evaluasi guna melindungi website dan mencegah serangan. Evaluasi keamanan bertujuan untuk mendeteksi celah kerentanan dan tingkat keparahan yang ada pada website LBPP-LIA Palembang. Metode yang digunakan adalah penelitian tindakan (*action research*) yang terdiri dari 5 tahapan yaitu *diacnosing, action planning, action taking, evaluation* dan *learning*. Analisis dan evaluasi dilakukan dengan teknik *scanning* dan tingkat kerentanan dikategorikan berdasarkan standar *Common Vulnerability Scoring System (CVSS)* versi.3 untuk menentukan tingkat keparahan serta memperhitungkan resiko kerentanan yang direpresentasikan dalam bentuk angka. *Tools* analisis *vulnerability scanner* menggunakan *tools* Nessus, Netsparker dan Acunetic. Proses *scanning* yang telah dilakukan pada website LBPP-LIA Palembang berjalan dengan lancar dengan menemukan kelemahan dan kerentanan yang ada. *Tools* Nessus menemukan 9 *alerts*, pada *tools* Netsparker menemukan 14 *alerts*, sedangkan *tools* Acunetic menemukan 88 *alerts*. Data *vulnerability* hasil analisis ini dapat dijadikan acuan bagi pengelola atau administrator website LBPP-LIA Palembang untuk segera melakukan perbaikan dan menutup celah kerentanan yang ada.
**Kata Kunci:** *Analisis Vulnerability, website, Nessus, Netsparker, Acunetic*

**Abstract**

Website is one of the most important information media in the era of rapid development of technology and information. Security aspects and knowing vulnerabilities have a very important role in a website. Security analysis can be done by evaluating to protect the website and prevent attacks. The security evaluation aims to detect vulnerabilities and the severity of the existing LBPP-LIA Palembang website. The method used is action research which consists of 5 stages, namely diagnosing, action planning, action taking, evaluation and learning. Analysis and evaluation is carried out by scanning techniques and the level of vulnerability is categorized based on the Common Vulnerability Scoring System (CVSS) version.3 standard to determine the severity and take into account the risk of vulnerability which is represented in the form of numbers. The vulnerability scanner analysis tools use the Nessus, Netsparker and Acunetic tools. The scanning process that was carried out on the LB LIA Palembang website went smoothly by finding existing weaknesses and vulnerabilities. The Nessus tools found 9 alerts, the Netsparker tools found 14 alerts, while the Acunetic tools found 88 alerts. The vulnerability data from this analysis can be used as a reference for the manager or administrator of the LBPP-LIA Palembang website to immediately make repairs and close existing vulnerabilities.
**Keywords:** *Vulnerability Analysis, website, Nessus, Netsparker, Acunetic*

## PENDAHULUAN

Perkembangan media informasi saat ini semakin canggih, guna mempermudah pekerjaan serta meningkatkan efisiensi waktu. Salah satu media informasi yang efektif dan efisien, yang dapat menyampaikan informasi kepada masyarakat adalah website.(Hasugian, 2018)

Menurut (Romadhon et al., 2021) Website adalah kumpulan informasi/kumpulan *page* yang biasa diakses lewat jalur internet. Setiap orang di berbagai tempat dan segala waktu bisa menggunakannya selama terhubung secara online di jaringan internet. Secara teknis, website adalah kumpulan dari *page*, yang tergabung kedalam suatu domain atau subdomain tertentu. Website merupakan informasi yang bersifat global dan terbuka sehingga kebutuhan dalam berkomunikasi, bertukar informasi ataupun mencari informasi mudah di dapat oleh siapapun, dimanapun dan kapanpun. Dengan kemudahan akses internet tersebut maka website semakin rentan

terjadinya kerusakan terhadap sistem dan pencurian data atau informasi yang bersifat privasi. Maka Keamanan dalam sebuah website adalah hal yang mutlak, karena dalam perkembangannya sebuah website dapat melakukan transaksi, memasukkan data pribadi, dan sebagainya. Aktivitas-aktivitas tersebut terdapat data penting seperti nomor identitas, nomor rekening, hingga data pribadi.(Hanafi et al., 2019)

Guna melindungi website dari kerusakan sistem dan kehilangan data akibat eksploitasi dari pihak yang tidak bertanggung jawab. Berbagai cara dapat digunakan untuk mendeteksi serangan atau penyusupan, dengan cara mengevaluasi seperti packet *sniffing, scanning, dan* monitoring layanan. Teknik-teknik tersebut dapat memblok, mengizinkan, atau menyaring paket yang mencoba masuk ke dalam jaringan dan mengakses sumberdaya atau layanan tertentu. Serangan terjadi biasanya adanya kelemahan pada website seperti kesalahan pemrograman, penggunaan autentikasi atau *password* yan lemah, *sensitive* data tidak terenkripsi atau mengijinkan koneksi dari berbagai alamat IP dan lain sebagainya.(Bayu Rendro & Nugroho Aji, 2020)

Sejarah berdirinya Lembaga Bahasa dan Pendidikan Profesional LIA (LBPP-LIA), adapun nama LIA merupakan singkatan dari Lembaga Indonesia Amerika pada periode 1959-1978. LIA berdirinya pada tahun 1961 yang berlokasi di jalan Segara (Perpustakaan USIS) lalu LIA di tutup pada tahun 1968, kemudian di buka kembali pada tahun 1970. Pada tahun 1978 LIA di kelola secara mandiri dengan mendirikan gedung di jalan Pramuka sehingga terjadi perubahan nama LIA dan terbentuknya yayasan LIA, lalu pada tahun 1981 LIA berubah nama menjadi PPIA yang bergerak dibidang pendidikan dan kebudayaan, kemudian pada tahun 1986 yayasan LIA terpisah dengan PPIA dan nama LIA bukan akronim dari singkatan Lembaga Indonesia Amerika.

Lembaga Bahasa dan Pendidikan Profesional LIA (LBPP-LIA) Palembang merupakan intansi swasta yang bergerak di bidang pendidikan. LBPP-LIA Palembang adalah salah satu unit dari Yayasan LIA Jakarta, berdiri pada tanggal 4 Januari 1996 berdasarkan SK No. 21. Tanggal 30 Agustus 1995 dan diresmikan langsung oleh Bapak Walikota kota Palembang serta didampingi Direktur Yayasan LIA pada masanya. Pada awal berdirinya LBPP-LIA Palembang beralamatkan di jalan Veteran Kota Palembang. Guna meningkatkan pelayanan yang maksimal kepada siswa, kemudian pada tahun 2000 LBPP-LIA pindah ke JL. Jendral Sudirman No 2953 RT 013 RW 015 Kelurahan 20 Ilir Kecamatan Ilir Timur 1 Kota Palembang Provinsi Sumatra Selatan. LBPP-LIA Palembang merupakan salah satu lembaga pendidikan kursus bahasa Inggris terbaik di Indonesia dengan kualitas dan mutu yang terjamin. Demi kenyamanan dan kepuasan pelangggan, Lembaga Bahasa LIA Palembang menggunakan situs website sebagai media informasi yang terhubung langsung dengan para pengguna yang dapat diakses melalui alamat URL *www.liapelambang.com.*

Berdasarkan hasil observasi dan wawancara yang dilakukan pada website LBPP-LIA Palembang dalam website terdapat beberapa fasilitas seperti pendaftaran online, *test (exam), call center* dan lainnya yang menggunakan *form* dan menu *login id* dengan menggunakan *username* dan *password* yang diaktifkan biasanya rentan terhadap serangan *password auto-complite* sehingga penyerang dengan mudah memperolah *password* yang beresiko bocornya data pribadi yang bersifat privasi. Lemahnya keamanan website Lembaga Bahasa LIA Palembang juga berpotensi ada *vulnerability* lainya seperti *Cross-site-Scripting (XSS), Cross-site-request-forgery (CSRF), Denial of service (Dos)* ataupun kerentanan lainya. Berdasarkan informasi yang di berikan pihak pengelola, website LBPP-LIA Palembang tidak terlalu sering terjadi ganguan, hanya saja sering lambat saat *login* mungkin dikarenakan sistem yang harus diperbaharui. Perbaikan dilakukan sepenuhnya oleh LBPP-LIA pusat sehingga apabila terjadi serangan dan ganguan maka cabang harus melaporkan segera kepusat. Sedangkan untuk pemeliharaan dilakukan secara bergatian di setiap cabang sedangkan LBPP-LIA mempunyai 64 cabang di seluruh Indonesia.

Berdasarkan uraian permasalahan diatas, maka penulis akan melakukan analisis *vulnerability* atau kerentanan pada website LBPP-LIA Palembang menggunakan *tools* Nessus, Netsparker dan Acunetic dengan menerapkan metode *action research* serta metode *CVSS (Common Vulnerability Scoring System),* adapun tujuannya adalah untuk menemukan celah kerentanan dan melakukan evaluasi terhadap temuan yang diperolah serta mengetahui tingkat keparahan kerentanan tersebut. Diharapkan data hasil penelitian ini dapat memberikan manfaat serta membantu dan mempermudah LBPP-LIA Palembang untuk segera melaporkan ke LBPP-LIA pusat untuk memperbaiki dan menutup celah yang ada serta dapat dijadikan referensi untuk meningkatkan sistem keamanan pada website LBPP-LIA Palembang.

Penelitian serupa juga pernah dilakukan oleh (Saputra Ahad & Akbar, 2015), yang berjudul "Analisis Kerentanan Terhadap Ancaman Serangan Pada Website PDAM Tirta Musi Palembang" . Penelitian ini bertujuan untuk menganalisa dan mengetahui celah kerentanan yang ada pada situs website PDAM Tirta Musi Palembang

yang dapat diakses melalui alamat situs www.tirtamusi.com. Metode penelitian yang digunakan adalah *Action Research (AR)* dan untuk menentukan nilai kerentanan dengan metode *Common Vulnerability Scoring System (CVSS)*, serta dibantu *tools* analisis kerentanan yaitu Acunetic web vulnerability, Netsparker dan Nessus. Hasil penelitian yang telah dilakukan , tools Acunetic web vulnerability menemukan total 28 jenis *alerts* yang terdiri dari 4 jenis bertipe *high*, 3 bertipe *medium*, 5 bertipe *low* dan 16 bertipe *informational* dengan kategori *high thereat level*. Selanjutnya *tools* Netsparker menemukan total 15 *alerts* yang terdiri dari 1 bertipe *critical*, 1 bertipe *important*, 6 bertipe *low* dan 7 bertipe *informational*. Terakhir *tools* Nessus menemukan total 15 jenis *alerts* yang terdiri dari 1 jenis bertipe *critical*, 2 jenis bertipe *medium*, 1 jenis bertipe *low* dan 11 jenis bertipe *informational*. Berdasarakan hasil tersebut terdapat banyak kerentanan yang bertipe *critical, high* ataupun *medium* yang harus segera dilakukan perbaikan dan penutupan celah tersebut, untuk kerentanan jenis *low* dan *informational* tidak dapat diabaikan karena penyerang dapat dengan mudah masuk ke sistem dari server tersebut.

Selanjutnya penelitian yang dilakukan oleh (Wibowo et al., 2019), dalam jurnal informatika, vol.6, No.2, ISSN.2555-6579, E-ISSN.2528-2247, dengan judul " *Vulnerability* pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunkan Open VAS dan Acunetis WVS". Penelitian ini bertujuan melakukan analisis celah kerentanan website jurnal ilmiah yang berbasis OJS versi 2.4.8.0 pada Universitas Muhammadiyah Purwokerto dengan menggunakan tools Open VAS dan Acunetix WVS agar dapat meningkatkan sistem keamanannya. Metode penelitian yang digunakan adalah metode penelitian terapan dan *Vulnerability Assessment* . Hasil penelitian yang telah dilakukan , Open VAS menemukan 9 data kelemahan yang terdiri dari 7 data bertipe *medium* dan 2 bertipe *low* , sedangkan Acunetic WVS memenukan 166 kelemahan data yang terdiri dari 149 jenis bertipe *medium* dan 71 bertipe *low*. Berdasarkan hasil *scanning*, terdapat banyak data kelemahan yang dapat dijadikan masukan bagi administrator untuk segera menutup atau memperbaiki celah kerentanan yang ada pada website jurnal ilmiah Universitas Muhammadiyah Purwokerto.

Sedangkan penelitian yang dilakukan oleh (Aziz, 2021), dalam *jurnal of engineering, computer science and information technology*, vol.1, No.1, dengan judul "Vulnerability Assessment untuk mencari celah keamanan web aplikasi *E-learning* pada Universitas XYZ. Penelitian ini bertujuan untuk mengevaluasi celah keamana pada web aplikasi *E-learning* Univeritas XYZ agar kegiatan belajar mengajar menjadi lebih efektif serta efisien dan menghindari gangguan serangan akibat kegiatan yang dilakukan pihak tidak bertanggung jawab. Penelitian ini menggunakan metode *vulnerability assessment* dan *penetrations testing life cycle* dan pengujian menggunakan bantuan *tools nessus*. Berdasarkan hasil pengujian yang dilakukan Nessus mendeteksi 7 jenis kerentanan yang terdiri dari 1 jenis bertipe *critical*, 2 jenis bertipe *high*, 3 jenis bertipe *medium* dan 1 jenis bertipe *low*. Selanjutnya *scanning service port* yang mempunyai kerentanan, terdeteksi 8 kerentanan *service port* yang terdiri dari 1 jenis bertipe *critical*, 3 jenis bertipe *high*, 3 jenis bertipe *medium* dan 1 jenis bertipe *low*. Berdasarkan hasil penelitian yang telah dilakukan *overall risk level* bereda pada *level high*, sehingga direkomendasikan untuk melakukan perbaikan secepat mungkin dan mengevalusi mendalam terhadap keamanan web aplikasi *E-learning* Universitas XYZ.

## METODE

Penelitian ini menggunakan metode *action research* menurut Zakariah, Alfriani and Zakariah (dalam Kuncoro et al., 2022) metode *action research (AR)* atau penelitian tindakan merupakan suatu bentuk rancangan penelitian dalam penelitian tidakan peneliti mendiskripsikan, menginterpretasi dan menjelaskan suatu situasi sosial pada waktu bersamaan dengan melakukan perubahan atau intervensi dengan tujuan perbaikan atau partisipasi. Terdapat lima tahapan dalam siklus penelitian *action research* yaitu:

a. *Diacnosing*, penulis pada tahap ini melakukan identifikasi masalah sistem keamanan website LBPP-LIA Palembang dengan cara melakukan observasi dan wawancara kepada pihak pengelola website.
b. *Action planning*, tahap ini penulis melakukan pemahaman pokok-pokok permasahan yang telah ditemukan pada tahap sebelumnya dan menentuan tindakan yang harus dilakukan untuk menyelesaikan permasalahan pada website lembaga bahasa lia Palembang.
c. *Action taking*, tahapan ini mengimplementasikannya *action planning* untuk melakukan investigasi guna mendapatkan informasi kelemahan sistem serta melakukan ujicoba pada webserver dengan menggunakan tipe ancaman pada objek penelitian secara langsung.

d. *Evaluating* setelah implementasi tindakan dilakukan tahap ini penulis akan mengevaluasi hasil implementasi dan menyimpulkan hasil sebagai aktivitas yang telah dilakukan.
e. *Learning* tahapan terakhir penulis akan melakukan review kembali teradap masalah-masalah yang telah ditemukan pada tahap sebelumnya guna memberikan solusi yang terbaik untuk menyelesaikan masalah tersebut.

Tingkat keparahan kerentanan ditentukan menggunakan standar *Common Vulnerability Scoring System (CVSS)*. *CVSS* adalah kerangka kerja terbuka untuk mengomunikasikan karakteristik dan tingkat keparahan kerentanan perangkat lunak. *CVSS* terdiri dari tiga grup metrik: Basis,Temporal dan Lingkungan.(FIRST, 2019).

Metrik menghasilkan skor kerentanan mulai dari 0 hingga 10, yang mendefinisikan tingkat resiko dalam tabel 1 berikut :

*Table 1 Category & Vulnerability Scoring*

| ***Category*** | ***Score*** |
|---|---|
| *None* | *0* |
| *Low* | *0,1-3,9* |
| *Medium* | *4,0-6,9* |
| *High* | *7,0-8,9* |
| *Criticial* | *9,0-10* |

Metode pengumpulan data yang digunakan penulis dalam kegiatan penelitian ini antara lain : (Alda & Afifudin, 2020)

A. Observasi

Penulis melakukan observasi langsung di lokasi penelitian di bidan IT management untuk mengamati serangkaian perilaku dan suasana serta mencari permasalahan yang ada pada website LBPP-LIA Palembang.

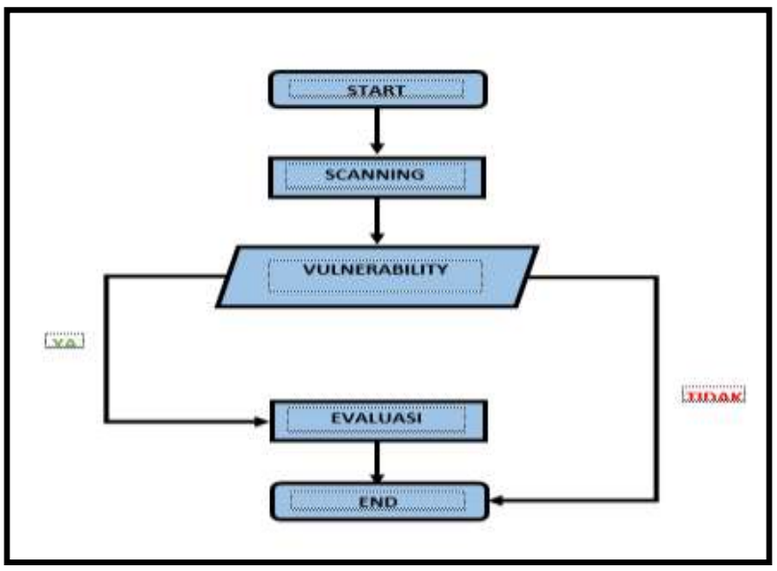
B. Wawancara

Penulis mengajukan pertanyaan dan diskusi kepada tenaga IT serta jajarannya untuk memperoleh informasi sistem keamanan webserver website LBPP-LIA Palembang.

C. Studi Pustaka

Penulis mencari referensi dari teori-teori yang mendukung kegiatan penelitian yang bersumber dari buku, jurnal, internet dan dari sumber lain

Analisis dan evaluasi dilakukan dengan teknik *scanning*. Proses analisis dilakukan dengan cara mengikuti diagram alur kerja yang telah disusun berikut :




Gambar 1 Diagram Alur Kerja

**HASIL DAN PEMBAHASAN**

**HASIL**

Proses *scanning* yang telah dilakukan pada website LBPP-LIA Palembang dengan menggunakan *tools* Nessus, Netsparker dan Acunetic. Dari hasi *scanning* tersebut mendapatkan hasil, Nessus menemukan 8 *vulnerability alerts* yang terdiri dari 3 jenis kategori kerentanan yaitu 1 buah kategori *critical* dengan 2 alerts, 1 buah kategori *medium* dan 1 buah yang kategori *informational* dengan 6 *alerts*.. Sedangkan *tools* kedua penulis menggunakan Netsparker. Hasil *scanning* menggunakan *tools* Netsparker menemukan adanya 3 jenis kategori

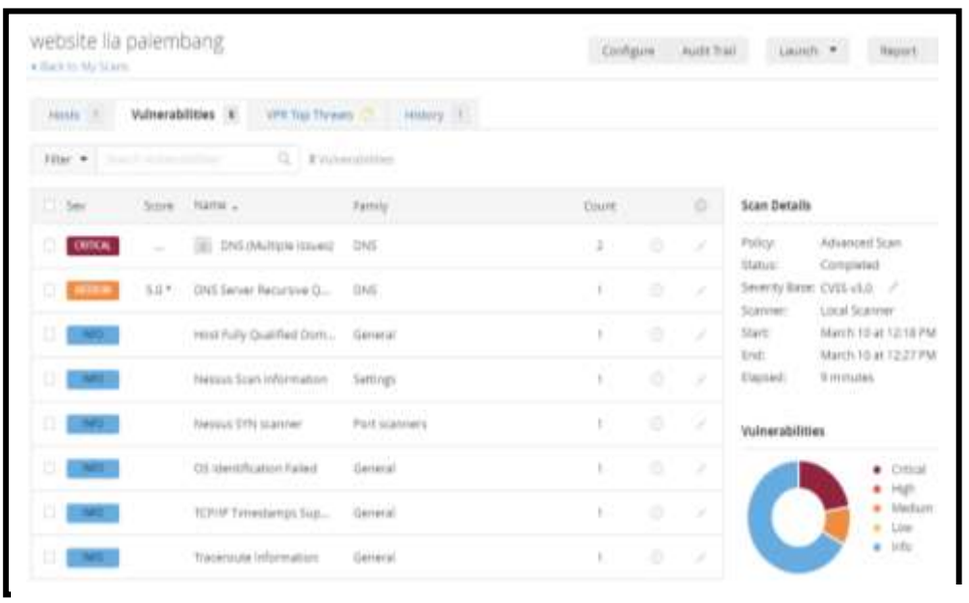
kerentanan yaitu 2 buah kategori *medium* dengan 3 *alerts*, 5 buah kategori *low* dengan 9 *alerts* dan 2 buah kategori *informational* dengan total 14 *vulnerability alerts*. *Scanning* ketiga menggunakan *tools* Acunetic, dari hasil *scanning* yang telah dilakukan *tools* Acunetic menemukan total 88 *vulnerability alerts* yang terdiri 4 jenis kategori kerentanan yaitu dari 1 kategori *high* dengan 75 *alerts*, 2 kategori *medium*, 2 kategori *low* dengan 10 *alerts* dan 1 jenis kategori *informational* dengan *category high threat level 3.*

Hasil data yang diperoleh secara keseluruhan dari tiga *tools* tersebut merupakan data penelitian yang bersifat sementara, karena kerentanan diperolah pada saat penulis melakukan *scanning* berdasarkan jadwal penelitian yang dilakukan sebelumnya, jika terjadi perbedaaan atau perubahan data dikarenakan pihak LBPP-LIA pusat atau administrator telah melakukan perbaikan dan menutup kelemahan sistem tersebut sehingga data dalam pembahasan merupakan data yang di peroleh saat penulis melakukan analisis sesuai jadwal penelitian dan data dapat berubah sewaktu-waktu.

**PEMBAHASAN**

**A. *Scanning* LBPP-LIA Palembang menggunakan Nessus**

Hasil *scanning* menggunakan Nessus menemukan 8 *vulnerability alerts* yang terdiri dari 3 jenis kategori kerentanan yaitu 1 buah kategori *critical* dengan 2 *alerts*, 1 buah kategori *medium* dan 1 buah yang kategori *informational* dengan 6 *alerts*, dapat dilihat pada gambar berikut :



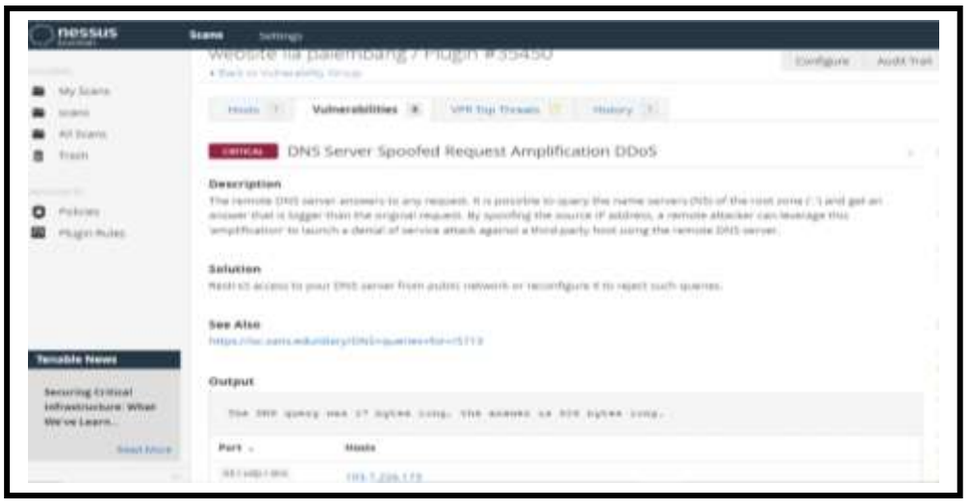

Gambar 2. Hasil *Scanning* Menggunakan Nessus

*Report* hasil *scanning* menggunakan Nessus:

1. Kategori *Critical*

Ditemukan 2 jenis kerantanan dengan kategori *critical* yaitu:

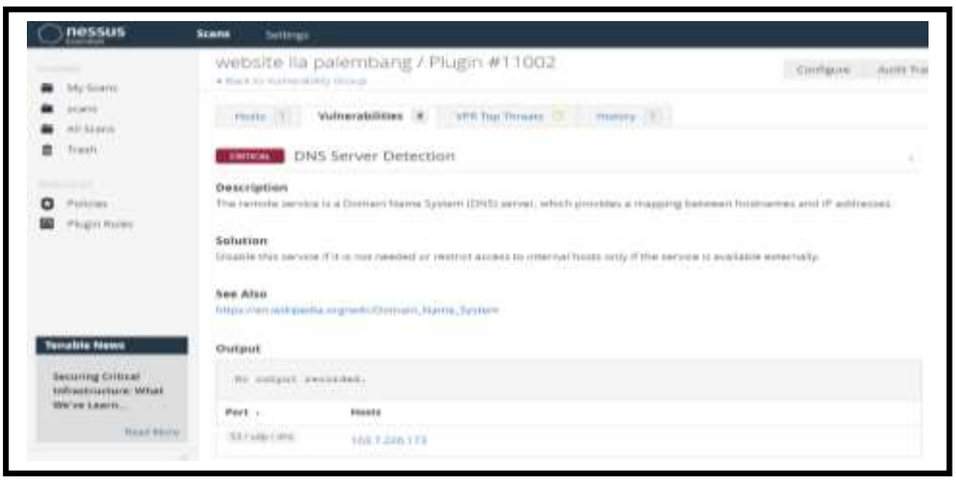
*a. DNS Server Spoofed Request Amplification DDoS*




Gambar 3. *Description DNS Sfoofed Reguest Amplification DDoS*

Merupakan kerentanan yang memungkinkan Server DNS menjawab semua permintaan, Sehingga mendapat informasi yang detail mengenai server sesuai dengan permintaan awal. Penyerang memalsukan alamat IP sumber dengan memanfaatkan amplifikasi untuk meluncurkan serangan penolakan layanan terhadap host pihak ketiga menggunakan server DNS jarak jauh. Solusi perbaikan yang direkomendasikan oleh Nessus adalah membatasi akses ke server DNS dari jaringan publik atau konfigurasi ulang untuk menolak permintaan. Adapun kerentanan ini mempunyai *CVSS V.3 base score 9.5.*

*b. DNS Server Detection*



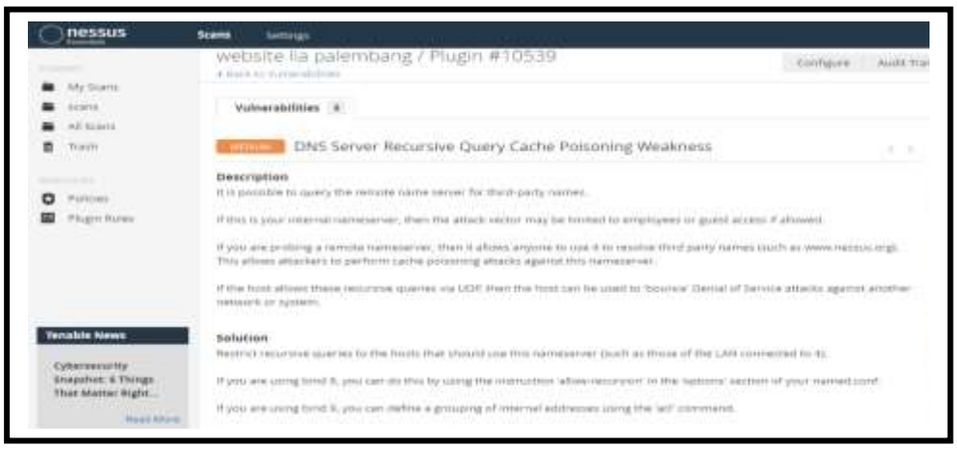

Gambar 4. *Description DNS Server Detection*

Merupakan informasi Layanan jarak jauh berupa *server Domain Name System (DNS),* yang menyediakan pemetaan antara *hostname* dan alamat IP. Informasi *DNS server* dapat dilihat pada *article Wikipedia* yang dapat diakses dengan alamat *URL* https://en.wikipedia.org/wiki/Domain_Name_System. Solusi perbaikan yang direkomendasikan oleh Nessus adalah nonaktifkan layanan ini jika tidak diperlukan atau batasi akses ke *host* internal hanya jika layanan tersedia secara eksternal. Adapun kerentanan ini mempunyai *CVSS V.3 base score 9.3.*

2. Kategori *Medium*

Ditemukan 1 jenis kerantanan dengan kategori *medium* yaitu:

*a. DNS Server Recursive Query Cache Poisoning Weakness*




Gambar 5. *Description DNS Server Recursive Query Chace Poisoning Weakness*

Merupakan kerantanan yang dimungkinkan untuk menanyakan nama server untuk nama pihak ketiga seperti www.nessus.org sehingga memungkinkan penyerang untuk melakukan serangan cache poisoning terhadap nama server ini dan jika host mengizinkan kueri rekursif ini melalui UDP, maka host dapat digunakan untuk memantulkan serangan Denial of Service terhadap jaringan atau sistem lain. Solusi perbaikan yang direkomendasikan oleh Nessus adalah batasi kueri rekursif ke *host* yang harus menggunakan server nama ini. Adapun kerentanan ini mempunyai *CVSS V.3 base score 5.0.*

3. Kategori *Informational*

Ditemukan 6 jenis kerantanan dengan kategori *informational* yaitu:

*a. Host Fully Qualified Domain Name (FQDN) Resolution*

Nessus menjelaskan bahwa dapat menyelesaikan nama domain yang sepenuhnya memenuhi syarat *(FQDN)* dari *host. Host* 103.7.226.173 belum mempunyai *hostname* yang lengkap atau valid untuk memenuhi syarat *(FQDN)* guna menentukan lokasi yang pasti dalam hirarki DNS.

*b. Nessus Scan Information*

Berupa *plugin* yang menampilkan setiap *host* yang diuji serta informasi tentang scanning yang dilakukan berupa versi set *plugin*, jenis pemindai, versi mesin Nessus, Pemindai *port* yang digunakan, rentang *port* dipindai, waktu perjalanan pulang pergi *ping*, tanggal pemindaian, durasi pemindaian dan jumlah *host* yang dipindai secara paralel.

*c. Nessus SYN Scanner*

Nessus SYN scanner adalah pemindai *port* setengah terbuka karena suatu koneksi penuh TCP tidak sampai terbentuk yang dilakukan cukup cepat bahkan terhadap target *firewall*. Pemindaian *SYN* kurang mengganggu dari pada pemindaian TCP (koneksi penuh) terhadap layanan yang rusak, tetapi pemindaian tersebut dapat menyebabkan masalah pada *firewall* yang kurang kuat dan juga meninggalkan koneksi yang tidak tertutup pada target, jika jaringan dimuat.

*d. OS Identification Failed*

Merupakan suatu teknik yang memungkinkan untuk mengumpulkan satu atau lebih sidak jari dengan sistem jarak jauh menggunakan kombinasi remote *probe (TCP/IP, SMB, HTTP, NTP, SNMP dan lain-lain).*

*e. TCP/IP Timestamps Supported*

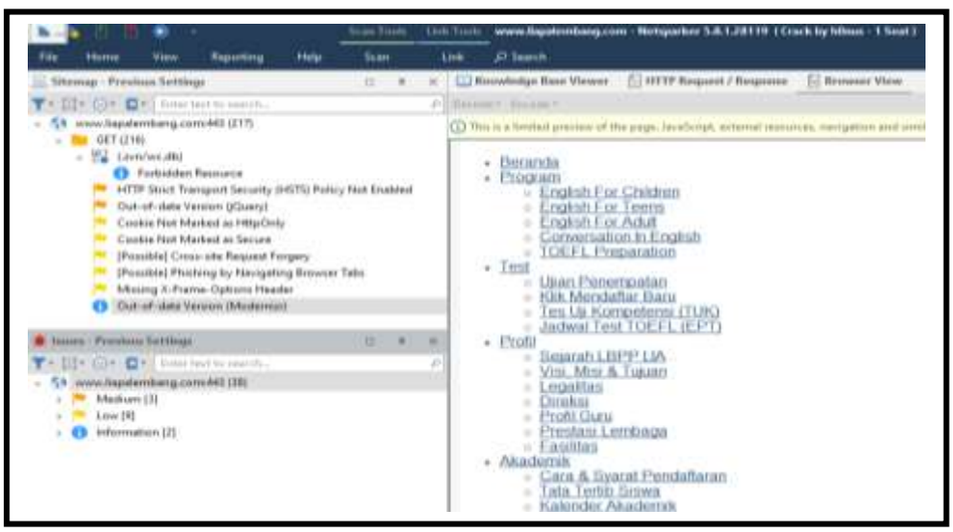
Merupakan *host* yang mengimplementasikan cap waktu TCP, seperti yang didefinisikan oleh RFC1323.

*f. Traceroute Information*

Merupakan sebuah perintah yang di buat untuk menunjukkan rute yang dilewati oleh paket untuk mencapai *host*. Rute yang paling dekat di tampilkan dalam daftar output yang terdapat pada jalur antara *host* dan tujuan

**B. *Scanning* LBPP-LIA Palembang menggunakan Netsparker**

Hasil *scanning* menggunakan Netsparker menemukan adanya 3 jenis kategori kerentanan yaitu 2 buah kategori *medium* dengan 3 *alerts*, 5 buah kategori *low* dengan 9 *alerts* dan 2 buah yang berkategori




Gambar 6. Hasil *Scanning* Menggunakan *Netsperker*

*informational* dengan total 14 *alerts,* dapat dilihat pada gambar berikut :
*Report* hasil *scanning* menggunakan Netsparker:

1. Kategori *Medium*

Ditemukan 2 jenis kerantanan dengan kategori *medium* yaitu:

*a. HTTP Strict Transport Security (HSTS) Policy Not Enabled*


Gambar 7. *Description HTTP Strict Transport Security (HSTS) Policy Not Enabled*

Netsparker mengidentifikasi bahwa kebijakan *HTTP Strict Transport Security (HSTS)* tidak diaktifkan sehingga situs web target dilayani tidak hanya dari *HTTPS* tetapi juga *HTTP* dan tidak memiliki implementasi kebijakan *HSTS*. *HTTP Strict Transport Security (HSTS)* adalah mekanisme kebijakan

keamanan web di mana *server* web menyatakan bahwa agen pengguna yang mematuhi, seperti browser web harus berinteraksi dengannya hanya menggunakan koneksi aman *(HTTPS)*. Solusi perbaikan yang direkomendasikan oleh Netsparker adalah Konfigurasikan server web untuk mengalihkan permintaan *HTTP* ke *HTTPS*. Adapun kerentanan ini mempunyai *CVSS V.3 base score 5.2.*

*b. Out of date (jQuery Version)*

Netsparker mengidentifikasi versi *jQuery* yang digunakan website sudah kedaluwarsa sehingga perangkat lunak rentan terhadap serangan. Terdapat 2 *directory* yang menunjukkkan bahwa *jQuery* telah kadaluwarsa yaitu pada ***/****(Directoy)* dengan alamt *url* *https://www.liapalembang.com/* dan ***/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp*** dengan alamt *url https://www.liapalembang.com/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp.* Solusi perbaikan yang direkomendasikan oleh Netsparker adalah tingkatkan penginstalan *jQuery* ke versi terbaru. Adapun kerentanan ini mempunyai *CVSS V.3 base score 6.2.* Salah satu kerentananya di tampilkan pada gambar berikut:


Gambar 8. *Description Out Of Date (jQuery Version)*

2. Kategori *Low*

Ditemukan 5 jenis kerantanan dengan kategori *low* yaitu:

*a. Cookie Not Marked as HttpOnly*

Netsparker mengidentifikasi *cookie* yang tidak ditandai *HTTPOnly* sehingga skrip tidak dapat di baca dari sisi klien. Menandai *cookie* sebagai *HTTPOnly* dapat memberikan lapisan perlindungan tambahan terhadap serangan *cross-site scripting (XSS)*. Solusi perbaikan yang direkomendasikan oleh Netsparker adalah tandai *cookie* sebagai *HTTPOnly* untuk menjadi lapisan pertahanan ekstra terhadap *XSS*. Adapun kerentanan ini mempunyai *CVSS V.3 base score 1.7.*

*b. Cookie Not Marked as Secure*

Netsparker mendeteksi *cookie* yang tidak tandai aman yang dikirimkan melalui *HTTPS* sehingga *cookie* berpotensi dicuri oleh penyerang dengan cara mencegat dan mendekripsi lalu lintas, atau melakukan serangan *man-in-the-middle* untuk memaksa korban untuk membuat permintaan *HTTP*. Solusi perbaikan yang direkomendasikan oleh Netsparker adalah Kirim informasi tambahan di setiap permintaan HTTP yang dapat digunakan untuk menentukan apakah permintaan tersebut berasal dari sumber resmi. Adapun kerentanan ini mempunyai *CVSS V.3 base score 2.0.*

*c. [Possible] Cross-site Request Forgery*

*Cross-site reguest forgery* adalah teknik serangan yang memaksa pengguna untuk melakukan tindakan yang tidak diinginkan pada aplikasi web pada saat pengguna di autentikasi. *CSRF* dilakukan penyerang dengan cara memasang tindakan apa pun yang dapat dilakukan oleh pengguna seperti menambahkan pengguna, memodifikasi konten dan menghapus data. Solusi perbaikan yang direkomendasikan oleh Netsparker adalah Jika memposting formulir dalam permintaan ajax, tajuk HTTP khusus dapat digunakan untuk mencegah *CSRF* karena browser mencegah situs mengirim tajuk *HTTP* khusus ke situs lain tetapi

memungkinkan situs untuk mengirim tajuk *HTTP* khusus ke diri mereka sendiri menggunakan *XMLHttpRequest*. Adapun kerentanan ini mempunyai *CVSS V.3 base score 3.2.*

*d. [Possible] Phishing by Navigating Browser Tabs*

Netsparker mendeteksi kemungkinan adanya serangan *phishing* dengan menavigasi tab browser tetapi tidak dapat mengonfirmasi kerentanannya. Solusi perbaikan yang direkomendasikan oleh Netsparker adalah tambahkan *"rel=noopener"* ke tautan untuk mencegah laman menyalahgunakan *window.opener.* Ini memastikan bahwa halaman tidak dapat mengakses properti *window.opener* di browser Chrome dan Opera. Adapun kerentanan ini mempunyai *CVSS V.3 base score 1.6.*

*e. Missing X-Frame-Options Header*

Netsparker mendeteksi tidak ada *header X-Frame-Options* yang menandakan bahwa situs website berisiko terkena serangan *clickjacking*. *Clickjacking* merupakan teknik penyerangan dengan menggunakan beberapa lapisan transparan untuk mengelabui pengguna agar mengklik tombol atau tautan pada halaman *frame* tingkat atas, sehingga penyerang membajak klik yang dimaksudkan dan mengarahkannya ke halaman lain. Solusi perbaikan yang direkomendasikan oleh Netsparker adalah mengirim *X-Frame-Options* yang tepat di *header* respons *HTTP* yang menginstruksikan browser untuk tidak mengizinkan pembingkaian dari domain lain. Adapun kerentanan ini mempunyai *CVSS V.3 base score 1.3.*

3. Kategori *Informational*

Ditemukan 2 jenis kerantanan dengan kategori Kategori *Informational*

*informational* yaitu:

a. *Forbidden Resource*

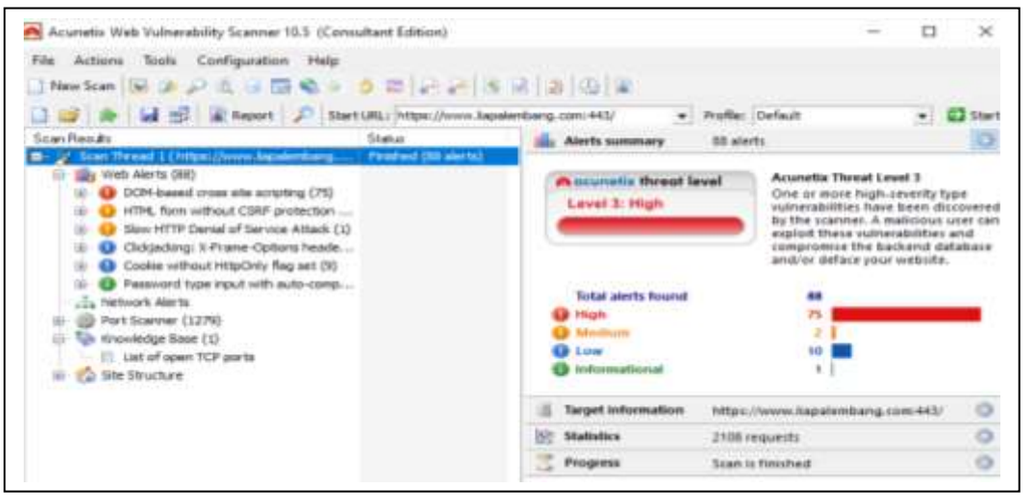
Netsparker memberikan informasi bahwa telah mengidentifikasi sumber daya terlarang yang mana server telah menolak akses ke sumber daya tersebut.

b. *Out-of-date Version (Modernizr)*

Netsparker mengidentifikasi situs website menggunakan Modernizr yang sudah kedaluawarsa sehingga perangkat lunak rentan terhadap serangan. Solusi perbaikan yang direkomendasikan oleh Netsparker adalah harap tingkatkan instalasi Modernizr ke versi stabil terbaru.

### C. *Scanning* LBPP-LIA Palembang menggunakan Acunetic

Hasil *scanning* menggunakan Acunetic menemukan sebayak 88 total *alerts* terdiri dari 4 jenis kategori kerentanan yaitu 1 kategori *high* dengan 75 *alerts*, 2 buah kategori *medium*, 2 buah kategori *low* dengan 10 *alerts* dan 1 buah kategori *informational*, dapat dilihat pada gambar berikut :

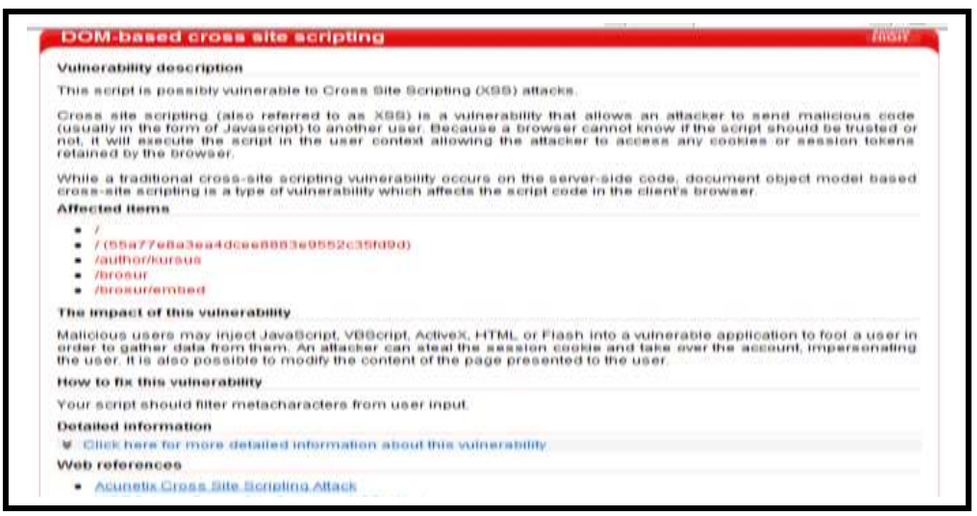



Gambar 9. Hasil *Scanning* Menggunakan Acunetic

*Report* hasil *scanning* menggunakan Netsparker :

1. Kategori High

Ditemukan 1 jenis kerantanan dengan kategori high yaitu:




Gambar 10. *Description DOM-based cross site scripting*

*a. DOM-based cross site scripting*

Acunetic mengindetifikasi adanya serangan *cross-site scripting (XSS)* berbasis *DOM (Document Object Model)* pada *website www.liapalembang.com* dengan mendeteksi 75 total *alerts* yang ditemukan pada 5 *directory* berikut:

*a) /directory)*
*b) / (55a77e8a3ea4dcee8883e9552c35fd9d)*
*c) /author/kursus*
*d) /brosur*
*e) /brosur/embed*

*Cross-site Scripting* merupakan jenis serangan *injection cedo* dengan mengirimkan kode berbahaya ke pengguna lain. Serangan yang dilakukan dengan mengijeksikan kode *script* ke dalam browser (biasanya dalam bentuk *JavaScript, VBScript, ActiveX, HTML,* atau *Flash)* sehingga browser tidak dapat mengetahui

skrip yang dijalankan benar atau tidak dan memungkinkan penyerang mendapat akses *cookie* atau *token sesion* yang ada di dalam browser.

Sementara kerentanan *cross-site scripting berbasis Document Object Modul* merupakan jenis kerentanan yang memengaruhi kode skrip di browser klien. Penyerang dapat mencuri *cookie sesion* dan mengambil alih akun, menyamar sebagai pengguna. Dimungkinkan juga untuk memodifikasi konten halaman yang disajikan kepada pengguna. Solusi perbaikan yang direkomendasikan oleh Acunetic adalah skrip harus memfilter metakarakter yang di input pengguna. Adapun kerentanan ini mempunyai *CVSS V.3 base score 8.3.*

2. Kategori *Medium*

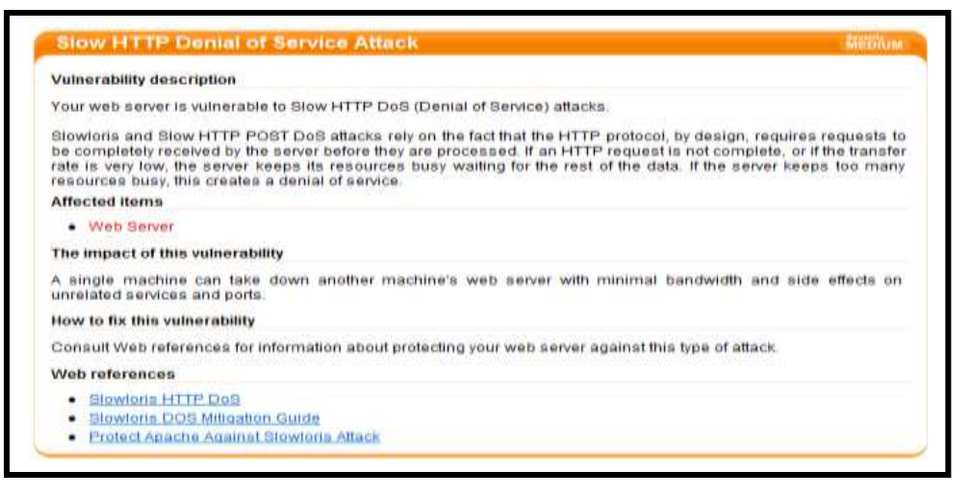
Ditemukan 2 jenis kerantanan dengan kategori *medium* yaitu:

*a. HTML form without CSRF protection*


Gambar 11. *Description HTML from without CSRF protection*

*Cross-site reguest forgery* sering dikenal dengan *one-click attack, session riding* atau *abriviated* yang di singkat *CSRF* atau *XSRF*, merupakan jenis eksploitasi situs web dimana penyerang memaksa pengguna untuk melakukan tindakan yang telah di pilih dengan cara mengirimkan perintah yang tidak sah ke pengguna situs web. Solusi perbaikan yang direkomendasikan oleh Acunetic adalah lakukan pemeriksaan pada formulir ini apakah memerlukan perlindungan *CSRF* atau jika perlu terapkan tindakan pengulangan *CSRF*. Adapun kerentanan ini mempunyai *CVSS V.3 base score 4.3.*

*b. Slow HTTP Denial of Service Attack*




Gambar 12. *Description Slow HTTP Denial of Service Attack*

Acunetic mengidentifikasi server web rentan terhadap serangan *Slow HTTP DoS (Denial of Service).* Serangan *Dos* bergantung pada protokol *HTTP*, secara desain memerlukan permintaan yang diterima sepenuhnya oleh *server* sebelum diproses. Jika permintaan *HTTP* tidak lengkap atau kecepatan transfer sangat rendah maka server membuat sumber dayanya sibuk menunggu sisa data sehingga

menciptakan penolakan layanan. Hal ini di buktikan dengan adanya perbedaan antara waktu dan koneksi sebesar 354553281ms. Solusi perbaikan yang direkomendasikan oleh Acunetic adalah konsultasikan referensi Web untuk informasi tentang melindungi server web dari serangan jenis ini. Adapun kerentanan ini mempunyai *CVSS V.3 base score 4.0.*

3. Kategori *Low*

Ditemukan 2 jenis kerantanan dengan kategori *low* yaitu:

*a. Clickjacking: X-Frame-Options header missing*

*Clickjacking* merupakan teknik berbahaya yang digunakan penyerang untuk mengungkapkan informasi rahasia atau mengambil kendali komputer dengan cara menipu pengguna agar mengklik sesuatu berbeda sehingga pengguna beranggapan meraka sedang mengklik halaman web yang tampaknya tidak berbahaya. website ini berisiko terkena serangan *clickjacking* karena server tidak dapat mengembalikan *header X-Frame-Options*. *Header respons X-Frame-Options* merupakan browser yang mengizinkan atau merender *page* di dalam *frame*. Solusi perbaikan yang direkomendasikan oleh Acunetic adalah konfigurasikan server web untuk menyertakan *header X-Frame-Options* dan konsultasikan referensi web untuk informasi lebih lanjut tentang kemungkinan nilai untuk header ini. Adapun kerentanan ini mempunyai *CVSS V.3 base score 3.8.*

*b. Cookie without HttpOnly flag set*

Acunetic menjelaskan bahwa pada *cookie* tidak memiliki *settingan flag HTTPOnly*. Sehingga ketika *cookie* di *setting* dengan *flag HTTPOnly* sehingga akses *cookie* hanya dapat dilakukan server yang telah diintruksikan oleh browser bukan oleh skrip sisi. Adapun detail serangan terdapat 9 *name cookie* yang ditemukan pada */(directory)* dengan *domain cookie "www.liapalembang.com"* sebagai berikut :

a) Domain Cookie: "wordpress test cookie"
b) Domain Cookie: "wordpress 6a4b94104b90ab1a169088129d01638d"
c) Domain Cookie: "wordpress sec 6a4b94104b90ab1a169088129d01638d"
d) Domain Cookie:"wordpress logged in 6a4b94104b90ab1a169088129d01638d"
e) Domain Cookie: "wp settings 0"
f) Domain Cookie: "wp settings time 0"
g) Domain Cookie: "wordpressuser 6a4b94104b90ab1a169088129d01638d"
h) Domain Cookie: "wordpresspass 6a4b94104b90ab1a169088129d01638d"
i) Domain Cookie: "wp postpass 6a4b94104b90ab1a169088129d01638d"

Solusi perbaikan yang direkomendasikan oleh Acunetic adalah Jika memungkinkan, harus menyetel *flag HTTPOnly* untuk *cookie* ini. Adapun kerentanan ini mempunyai *CVSS V.3 base score 2.0.*

4. Kategori *Informational*

Ditemukan 1 jenis kerantanan dengan kategori *informational* yaitu:

*a. Password type input with auto-complete enabled*

Acunetic memberikan informasi bahwa pada *directory* /wp-login.php*. password auto-complite* diaktifkan sehingga dengan menggunakan akses lokal penyerang dapat memperolah nama dan kata sandi *cleartext* dari *chace* browser tersebut. Solusi perbaikan yang direkomendasikan oleh Acunetic adalah Pelengkapan otomatis kata sandi harus dinonaktifkan di aplikasi sensitif.

**D. Evaluasi Hasil Pembahasan**

Setelah menjalankan proses *scanning* dengan menggunakan *tools* Nessus, Netsparker dan Acunetic, penulis menemukan beberapa kerentanan berbahaya yang teridentifikasi seperti *Cross-site-Scripting (XSS), Cross-site-Request-Forgery (CSRF), HSTS Policy Not Enabled, Clickjacking attack, OS Identification Failed, Out-of-date Version (jQuery & Modernizr)* dan lain-lain. Menemukan adanya *port* yang terbuka sehingga serangan dapat dengan mudah dilakukan. Berdasarkan hasil *scanning* yang telah dilakukan terdapat banyak sekali

kerantanan yang perlu dievaluasi dan diperbaiki oleh administrator atau pengelola situs web *wwwliapalembang.com* sehingga website sangat rentan terhadap serangan. Pengelola diharapkan segera menutup celah kerentanan dan memperbaiki sistem yang bermasalah sebelum terjadi serangan yang mengakibatkan kerugian pihak LBPP- LIA Palembang.

**E. Dokumentasi dan Pelaporan**

Table 2. Hasil *Scanning* Celah Kerentanan secara keseluruhan

| No | *Tools* | *level* | Kerentanan *(vulnerability)* | *CCVSS v.3 Base Score* |
|---|---|---|---|---|
| 1 | Nessus | *Critical* | *DNS Server Spoofed Request Amplification DDoS* | 9.5 |
| | | | *DNS Server Detection* | 9.3 |
| | | *Medium* | *DNS Server Recursive Query Cache Poisoning Weakness* | 5.0 |
| | | *Informational* | *Host Fully Qualified Domain Name (FQDN) Resolution* | - |
| | | | *Nessus Scan Information* | - |
| | | | *Nessus SYN scanner* | - |
| | | | *OS Identification Failed* | - |
| | | | *TCP/IP Timestamps Supported* | - |
| | | | *Traceroute Information* | - |
| | | | | |
| 2 | Netsparker | *Medium* | *HTTP Strict Transport Security (HSTS) Policy Not Enabled* | 5.2 |
| | | | *Out-of-date Version (jQuery)* | 6.2 |
| | | *Low* | *Cookie Not Marked as HttpOnly* | 1.7 |
| | | | *Cookie Not Marked as Secure* | 1.5 |
| | | | *[Possible] Cross-site Request Forgery* | 3.5 |
| | | | *[Possible] Phishing by Navigating Browser Tabs* | 1.6 |
| | | | *Missing X-Frame-Options Header* | 1.3 |
| | | *Informational* | *Forbidden Resource* | - |
| | | | *Out-of-date Version (Modernizr)* | - |
| | | | | |
| 3 | Acunetic | *High* | *DOM-based cross site scripting* | 8.3 |
| | | *Medium* | *HTML form without CSRF protection* | 4.3 |
| | | | *Slow HTTP Denial of Service Attack* | 4.0 |
| | | *Low* | *Clickjacking: X-Frame-Options header missing* | 3.8 |
| | | | *Cookie without HttpOnly flag set* | 2.0 |
| | | *Informational* | *Password type input with auto-complete enabled* | - |

**SIMPULAN**

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan pada website LBPP-LIA Palembang, maka mendapatkan Simpulan bahwa:

1. Hasil scanning menggunakan *tools* Nessus menemukan 8 *vulnerability alerts* yang terdiri dari 3 jenis kategori kerentanan yaitu 1 buah kategori *critical* dengan 2 *alerts*, 1 buah kategori *medium* dan 1 buah yang kategori *informational* dengan *6 alerts* dengan kategori *VPR top thereats level low*
2. Hasil *scanning* menggunakan *tools* Netsparker menemukan adanya 3 jenis kategori kerentanan yaitu 2 buah kategori *medium* dengan 3 *alerts*, 5 buah kategori *low* dengan 9 *alerts* dan 2 buah kategori *informational* dengan total 14 *vulnerability alerts*
3. Hasil *scanning* menggunakan *tools* Acunetic menemukan total 88 *vulnerability alerts* yang terdiri 4 jenis kategori kerentanan yaitu dari 1 kategori *high* dengan 75 *alerts*, 2 kategori *medium*, 2 kategori *low* dengan 10 *alerts* dan 1 jenis berkategori *informational* dengan *category high threat level 3.*
4. Hasil analisis menunjukkan bahwa terdapat celah kerentanan dengan kategori *high, critical* ataupuan *medium*

sangat berbahaya dan harus segera dilakukan perbaikan. Sementara untuk kategori *low* dan *informational* tidak dapat diabaikan karena penyerang dapat dengan mudah masuk ke sistem server.

5. Peneliti memberikan saran untuk segera memperbaiki celah kerantanan yang telah di temukan, melakukan *update* sistem-sistem yang sudah kadaluwarsa serta melakukan evaluasi lebih lanjut terhadap kerentanan yang ada menggunakan tools Nessus, Netsparker, Acunetic ataupun *tools-tools* lainnya.

## DAFTAR PUSTAKA


Alda, M., & Afifudin. (2020). Application of New Student Registration Based on Mobile Application. *JITK (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer)*, *6*(1), 129–136. https://doi.org/10.33480/jitk.v6i1.1382

Aziz, M. (2021). Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning Pada Universitas Xyz. *Jecsit*, *1*(1), 101–109.

Bayu Rendro, D., & Nugroho Aji, W. (2020). Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software Nmap (Studi Kasus Di Smk Negeri 1 Kota Serang). *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *7*(2), 108–115. https://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/view/2522

FIRST. (2019). *Common Vulnerability Scoring System version 3.1 Specification Document Revision 1*. 1–24. https://www.first.org/cvss/

Hanafi, T. A., Iswahyudi, C., Informatika, P. S., & Industri, F. T. (2019). *Jurnal SCRIPT Vol . 7 No . 2 Desember 2019 APLIKASI PENDETEKSI CELAH KEAMANAN APLIKASI WEB DENGAN PENETRATION TESTING MENGGUNAKAN METODE INPUT VALIDATION Jurnal SCRIPT Vol . 7 No . 2 Desember 2019 E- ISSN : 2338-6313*. *7*(2), 132–141.

Hasugian, P. S. (2018). Perancangan Website Sebagai Media Promosi Dan Informasi. *Journal Of Informatic Pelita Nusantara*, *3*(1), 82–86.

Kuncoro, I. D., Widodo, S. A., & Widatama, K. (2022). *UNIVERSITAS MUHAMMADIYAH PURWOREJO EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUDE ( ETSI )*. *5*.

Romadhon, M. H., Yudhistira, Y., & Mukrodin, M. (2021). Sistem Informasi Rental Mobil Berbsasis Android Dan Website Menggunakan Framework Codeigniter 3 Studi Kasus : CV Kopja Mandiri. *Jurnal Sistem Informasi Dan Teknologi Peradaban (JSITP)*, *2*(1), 30–36.

Saputra Ahad, D., & Akbar, M. (2015). *Serangan Pada Website Pdam Tirta Musi*.

Wibowo, F., Harjono, H., & Wicaksono, A. P. (2019). Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS. *Jurnal Informatika*, *6*(2), 212–217. https://doi.org/10.31311/ji.v6i2.5925