# *Vulnerability Assessment* Pada Situs Web KPPM FRI Dengan Burp Suite dan Intruder

1st Rizal Indera
*Fakultas Rekayasa Industri*
*Universitas Telkom*
Bandung, Indonesia
rizalindera@student.telkomuniversity.ac.id

2nd Avon Budiono
*Fakultas Rekayasa Industri*
*Universitas Telkom*
Bandung, Indonesia
avonbudi@telkomuniversity.ac.id

3rd Umar Yunan Kurnia Septo Hediyanto
*Fakultas Rekayasa Industri*
*Universitas Telkom*
Bandung, Indonesia
umaryunan@telkomuniversity.ac.id

**Abstrak--- Perkembangan aplikasi berbasis web dari tahun ke tahun mengalami perkembangan yang pesat, dan memberikan banyak manfaat di berbagai aspek, termasuk aspek pendidikan, termasuk pada Fakultas Rekayasa Industri (FRI) yang menggunakan situs web untuk mengelola kegiatan Kerja Praktik dan Pengabdian Masyarakat (KPPM). Situs web yang digunakan ini belum pernah dilakukan *vulnerability scanning*, sementara resiko kerentanan pada situs web ini tergolong besar karena situs web ini harus diakses oleh pihak eksternal yaitu pembimbing lapangan tempat dimana mahasiswa melakukan kerja praktik. Metode yang digunakan dalam *vulnerability scanning* ini adalah *automated testing* dan tipe *web application scanning*, dengan bantuan *software* Burp Suite dan Intruder. Hasil dari penelitian ini ditemukan bahwa situs web KPPM FRI memiliki total 12 kerentanan, yaitu 9 kerentanan ditemukan oleh Burp Suite dengan 3 kerentanan berada pada kategori *Low* dan 4 kerenatanan berada pada kategori *Information*, dan 7 kerentanan ditemukan oleh Intruder, dengan 2 kerentanan berada pada kategori *High*, 3 kerentanan berada pada kategori *Medium* dan 2 kerentanan berada pada kategori *Low*.**

***Kata kunci— Vulnerability, Scanning, Confidential, Automated, Burp Suite, Intruder.***

## I. PENDAHULUAN

Seiring perkembangan teknologi yang semakin pesat, maka perkembangan sistem informasi pun semakin berkembang. Berbagai entitas sudah melakukan digitalisasi, termasuk berbagai entitas yang menyimpan berbagai data-data pribadi dari pelanggan atau pengguna. Namun, banyak entitas yang masih kurang memperhatikan keamanan sistem informasi ini. Karena kurangnya perhatian dari entitas ini, banyak sekali potensi *vulnerability* yang dapat dengan mudah dimasuki oleh *attacker*. Dengan mudahnya *attacker* masuk ke dalam sistem, maka berbagai data yang terdapat di dalam sistem akan dengan mudah dicuri untuk keuntungan pribadi *attacker*.

Dengan adanya sistem perkuliahan daring yang dijalani saat ini, maka kebutuhan akan aplikasi yang mendukung perkuliahan semakin meningkat. Segala aktivitas perkuliahan yang tadinya dilakukan secara tatap muka, dengan adanya sistem perkuliahan daring ini, dilakukan secara daring dengan dukungan berbagai aplikasi. Aplikasi yang dibuat oleh Fakultas Rekayasa Industri (FRI) Universitas Telkom ini berbasis situs web, untuk memudahkan mahasiswa mengakses aplikasi dari berbagai perangkat, seperti telepon genggam, PC (*Personal Computer*) tablet, laptop, ataupun komputer desktop.

Kerja Praktek merupakan sebuah kegiatan yang dilakukan oleh mahasiswa untuk mendapatkan pengetahuan dan pengalaman praktis di dunia kerja berdasarkan dasar keilmuan yang telah dicapai. Dalam pelaksanaannya, kerja praktek dilakukan di industri selama minimal 30 (tiga puluh) hari kerja, dan dilakukan pada saat libur antar semester sehingga tidak mengganggu jadwal perkuliahan. Setelah melakukan kerja praktek, mahasiswa diwajibkan untuk menyusun laporan hasil kerja praktek dan dipresentasikan di hadapan dosen pembimbing dalam sidang kerja praktek. Mahasiswa disarankan untuk mengambil kerja praktek sesuai dengan program studi dan kelompok keahlian yang dipilih, supaya memudahkan mahasiswa untuk lebih mendalami kelompok keahlian yang dipilih sebelum mengerjakan Tugas Akhir.

Untuk memudahkan pelaksanaan Kerja Praktek, maka Fakultas Rekayasa Industri (FRI) membuat sebuah aplikasi dalam bentuk situs web. Aplikasi ini bernama KPPM (Kerja Praktek dan Pengabdian Masyarakat) Virtual FRI, dalam domain kppm.virtualfri.id. Aplikasi ini disusun menggunakan *framework* Sails.js yang berbasis pada bahasa pemrograman JavaScript dan berjalan di dalam *Virtual Private Server* (VPS) milik FRI. Aplikasi ini dapat digunakan oleh mahasiswa untuk memilih topik KPPM, mengunggah laporan, *logbook*, dan file presentasi yang diperlukan untuk presentasi sidang laporan akhir KPPM, dan memantau progress penilaian laporan akhir KPPM.

Situs web KPPM ini perlu diuji keamanannya karena dalam situs KPPM ini banyak menyimpan data yang *confidental,* seperti data Nomor Induk Mahasiswa (NIM), data Nomor Induk Pegawai (NIP) dari dosen pembimbing dan pembimbing lapangan mahasiswa tersebut yang dapat digunakan untuk mengambil berbagai data yang tersambung dengan mahasiswa dan dosen tersebut oleh pihak yang tidak bertanggung jawab, dan digunakan secara tidak bertanggung jawab untuk kepentingan pribadi *attacker* tersebut.

Kasus pencurian data *confidental* sudah banyak terjadi di Indonesia. Pada bulan Mei 2021, terjadi kebocoran data dari situs BPJS (Badan Penyelenggara Jaminan Sosial) sebanyak 279 juta data yang mengandung berbagai informasi pribadi dari pengguna BPJS, dan 20 juta data diantaranya mengandung foto personal. Dan pada bulan Mei 2020, terjadi pembobolan data oleh peretas yang telah mendapatkan data sebanyak 2,3 juta warga Indonesia yang mengandung

berbagai informasi pribadi, seperti NIK (Nomor Induk Kependudukan), nama lengkap, alamat, dan tanggal lahir.

Berbagai langkah dan mitigasi yang telah dilakukan sebelumnya hanya dapat meningkatkan keamanan dan mengurangi resiko, tidak menjadikan situs web KPPM ini sepenuhnya terbebas dari ancaman kebocoran data. Untuk memastikan bahwa sistem sepenuhnya aman, maka diperlukan kegiatan VA (*Vulnerability Assessment*) untuk menganalisa keamanan sistem dan mencoba keamanan sistem, apakah terdapat *exploit* di dalam sistem ataupun kemungkinan *exploit* yang memungkinkan *attacker* untuk masuk ke dalam sistem.

## II. KAJIAN TEORI

### A. Keamanan Informasi

Keamanan informasi menurut G. J. Simons adalah bagaimana usaha untuk dapat mencegah penipuan (*cheating*) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. Dapat disimpulkan, keamanan informasi merupakan sebuah usaha untuk mengamankan sebuah informasi yang dinilai berbahaya dan beresiko. Tindakan yang dapat dilakukan berupa tindakan pencegahan kebocoran informasi ataupun pendeteksian keamanan informasi.

Terdapat 3 (tiga) aspek yang harus diperhatikan dalam keamanan informasi, yaitu *Confidentality, Integrity, dan Availability*, yang biasa disebut CIA Triad (Andress, 2019).

*Confidentality* merupakan aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang, dan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan.

*Integrity* merupakan aspek yang menjamin bahwa data tidak dapat diubah tanpa ada ijin pihak yang berwenang (authorized) untuk menjaga keakuratan dan keutuhan informasi.

*Availibility* merupakan aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan pengguna yang berhak dapat menggunakan informasi bila diperlukan.

### *B. Vulnerability*

Secara terjemahan bahasa Indonesia, *vulnerability* berarti kerentanan. Pada bidang keamanan siber, *vulnerability* adalah kelemahan yang terdapat pada sebuah sistem yang dapat menjadi pintu masuk oleh peretas untuk mengambil keuntungan secara ilegal dari sebuah sisetm. Kelemahan pada sistem dapat berada di bagian *software* yang digunakan untuk menjalankan sistem, *hardware* yang digunakan, ataupun *brainware* atau manusia yang menjalankan sistem tersebut.

### *C. Vulnerability Assessment*

*Vulnerability Assessment* (VA) merupakan proses untuk melakukan pemindaian pada sistem, perangkat lunak, infrastruktur, atau jaringan untuk menemukan kelemahan dan celah di dalamnya. Celah-celah tersebut dapat memberikan akses *backdoor* yang semula dibuat untuk memudahkan tim pengembang dalam melakukan identifikasi kerusakan yang terdapat pada sistem kepada *attacker.*

### D. Burp Suite

Burp Suite merupakan sebuah perangkat lunak berbasis Java yang berguna untuk melakukan pengujian keamanan pada aplikasi berbasis web. Burp Suite dikembangkan oleh sebuah perusahaan yang bernama Portswigger, yang didirikan oleh Dafydd Stuttard. Burp Suite dibuat dengan tujuan menjadi sebuah perangkat lunak yang lengkap dan dapat diandalkan oleh penguji keamanan infrastruktur, tanpa menggunakan banyak perangkat lunak lainnya.

Dalam implementasinya, Burp Suite ditempatkan di antara server dan *client*, dimana seluruh *request* dan *response* yang muncul di antara server dan *client* dapat diarahkan dan ditangkap oleh Burp Suite. Dengan metode implementasi seperti ini, Burp Suite memiliki kemampuan untuk mencatat, menunda, memodifikasi, dan menampilkan semua *traffic* yang terjadi pada *protocol* HTTP (*Hypertext Transfer Protocol*) dan HTTPS (*Hypertext Transfer Protocol Secure*). Burp Suite dapat berjalan secara *spidering,* yaitu memindai aplikasi web secara aktif, atau *crawling,* yaitu memindai aplikasi web secara pasif.

Burp Suite tersedia dalam 3 versi, yaitu *Enterprise, Professional,* dan *Community.* Versi *Enterprise* dan *Professional* merupakan versi berbayar, sedangkan versi *Community* merupakan versi gratis dan dapat digunakan oleh siapa saja.

### E. Intruder

Intruder merupakan sebuah perangkat lunak yang dapat digunakan untuk melakukan pengujian keamanan pada aplikasi berbasis *web, cloud,* dan dapat melakukan pengujian pada *network infrastructure*. Intruder juga dapat berjalan secara otomatis sesuai jadwal yang telah ditentukan.

Dalam implementasinya, Intruder digunakan oleh *end-user,* dimana *end-user* mengakses Intruder menggunakan *Graphical User Interface* (GUI) yang dijalankan langsung pada *web browser* milik *end-user.* Setelah itu, proses *scanning* dan *reporting* akan dilakukan secara otomatis oleh Intruder. Ini menjadi keunggulan Intruder dimana *vulnerability assessment* dapat dilakukan oleh *end-user*, dan *reporting* dapat dilakukan secaara otomatis.

Hasil *reporting* juga dapat diunggah secara otomatis dan terintegrasi dengan Zapier, Jira, Slack, dan ServiceNow, sehingga pengguna tidak perlu melakukan *reporting* secara manual.

Intruder juga dapat terintegrasi dengan *cloud infrastructure,* seperti Google Cloud, Microsoft Azure, dan Amazon Web Service (AWS), sehingga pengguna tidak perlu melakukan instalasi secara manual.

Intruder tersedia dalam 3 versi, yaitu *Essential, Pro*, dan *Vanguard*. Versi *Essential* merupakan versi terendah yang ditawarkan oleh Intruder, dengan harga USD101, atau 101 (seratus satu) dolar per bulannya. Dalam versi ini, jumlah pengguna dibatasi sebanyak 2 pengguna, *scanning* menggunakan metode *open-source,* dan *automated scanning* sebanyak 1 kali dalam 1 bulan.

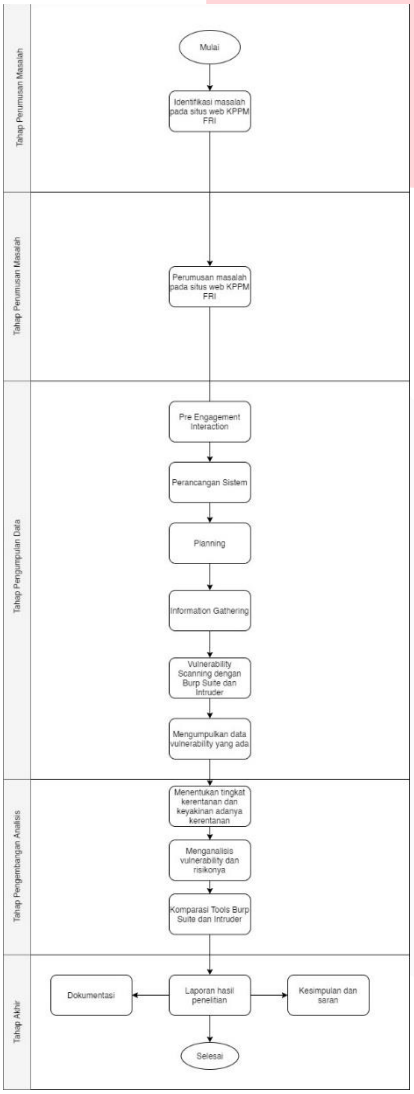
Versi *Pro* merupakan versi yang lebih lengkap. Dengan harga USD129, atau 129 (seratus dua puluh sembilan) dolar per bulannya. Dalam versi ini, jumlah pengguna tidak dibatasi, *scanning* menggunakan metode *professional-curated,* dan sinkronisasi dengan Google Cloud dan AWS.
Versi teratas merupakan versi *Vanguard.* Dalam versi ini, pengguna mendapatkan seluruh fitur dari versi Pro ditambah *testing* oleh *certified penetration testers,* sehingga pengguna tidak perlu melakukan *scanning* dan *testing* secara mandiri. Tidak ada harga khusus untuk versi ini, pengguna harus

melakukan kontak secara khusus dengan pihak Intruder sebelum melakukan pembelian versi *Vanguard* ini.

## III. METODE

### A. Skema Pemecahan Masalah

Skema pemecahan masalah dalam penelitian ini disajikan dalam bentuk bagan yang berisi tahapan yang dilakukan yang dijabarkan secara sistematis, terstruktur, dan deskriptif. Skema ini terbagi menjadi beberapa tahapan yaitu identifikasi masalah, rumusan masalah, pengumpulan data, pengembangan analisis, dan tahap akhir. Ilustrasi terkait sistematika penelitian ini dijabarkan dalam bagan seperti pada Gambar 1 berikut:




GAMBAR 1
SKEMA PEMECAHAN MASALAH

1. Identifikasi Masalah

   Peneliti memulai dengan identifikasi masalah yang ada pada situs web KPPM FRI, yaitu situs web KPPM FRI berada pada status rentan karena menyimpan berbagai data *confidental* dan dapat diakses oleh pihak eksternal.

2. Rumusan Masalah

   Peneliti melanjutkan perumusan masalah setelah mengidentifikasi masalah pada situs web KPPM FRI, yaitu mengetahui struktur dan spesifikasi dari situs web KPPM FRI, potensi kerentanan yang ada pada situs web KPPM FRI, dan perbandingan dari tools yang digunakan untuk kegiatan *Vulnerability Assessment,* yaitu Burp Suite dan Intruder, yang akan digunakan juga sebagai batasan dalam penelitian ini.

3. Pengumpulan Data

   Data yang diperlukan pada penelitian ini adalah data terkait struktur situs web KPPM FRI, VPS FRI, dan kerentanan yang ditemukan pada situs web KPPM FRI.

   Data struktur situs web FRI diambil menggunakan software *information gathering* yang dapat menampilkan struktur situs web KPPM FRI secara detail.

   Data kerentanan yang ditemukan pada situs web KPPM FRI diambil menggunakan *software* Burp Suite dan Intruder. Data dari kedua *software* tersebut kemudian dikumpulkan dan dilakukan analisis untuk memvalidasi kerentanan tersebut dan mencari solusi dari kerentanan tersebut.

4. Pengembangan Analisis

   Penelitian dilanjutkan dengan proses pengembangan analisis. Proses ini dimulai setelah mendapatkan data hasil *vulnerability assessment* dari *software* Burp Suite dan Intruder. Data keamanan dari situs web KPPM FRI dianalisis berdasarkan hasil *vulnerability assessment,* klasifikasi kerentanan, dan komponen yang mengalami kerentanan.

5. Tahap Akhir

   Setelah mendapatkan hasil analisis mengenai tingkat keamanan pada situs web KPPM FRI, peneliti menyusun laporan hasil penelitian, yang dilengkapi dengan dokumentasi, kesimpulan dan saran.

## IV. HASIL DAN PEMBAHASAN

### A. *Pre-Engagement Interaction*

Dalam melakukan *vulnerability assessment* ini perlu menentukan *tools* dan teknik pengujian yang akan digunakan serta perancangan pengujian untuk mendapatkan data mengenai kerentanan target. Penelitian ini menggunakan *tools* Burp Suite dan Intruder

### B. Perancangan Sistem

Dalam proses pengujian *vulnerability assessment* ini diperlukan perangkat pendukung seperti *hardware* dan *software* untuk melakukannya. Oleh karena itu, sebelum melakukan pengujian maka diperlukan proses identifikasi terhadap *hardware* dan *software* yang akan digunakan. Spesifikasi *hardware* dan *software* yang akan digunakan pada pengujian ini dapat dilihat pada Tabel 1 dan Tabel 2.

TABEL 1
SPESIFIKASI *HARDWARE* YANG DIGUNAKAN

| Perangkat | Informasi |
|---|---|

| | | |
|---|---|---|
| Lenovo Ideapad Slim 3i (*Main* OS) | *Processor* | Intel® Core™ i5-1035G1 @ 1.00 GHz, 3.60 GHz with Turbo Boost (4 CPUs, 8 thread) |
| | *Memory* | 12GB RAM |
| | *Hard Disk* | 512GB SSD |
| | *Operating System* | Windows 11 Pro 64-bit |
| *Virtual Computer* | *Processor* | Intel® Core™ i5-1035G1 @ 1.00 GHz, 3.60 GHz with Turbo Boost (1 CPUs, 2 thread) |
| | *Memory* | 4GB RAM |
| | *Hard Disk* | 40GB *Virtual Disk* |
| | *Operating System* | Kali Linux 2020.3 |

TABEL 2
SPESIFIKASI *SOFTWARE* YANG DIGUNAKAN

| Perangkat Lunak | Fungsi |
|---|---|
| Windows 11 | Sebagai sistem operasi utama untuk menjalankan virtualisasi pengujian *vulnerability assessment.* |
| Kali Linux 2020.3 | Sebagai sistem operasi yang berjalan secara virtual untuk menjalankan operasi pada pengujian *vulnerability assessment.* |
| VMware Workstation | Sebagai perangkat lunak yang digunakan untuk menampung *operating system* Kali Linux. |
| Burp Suite | Sebagai alat yang dijalankan di dalam Kali Linux untuk menguji tingkat keamanan pada server. |
| Microsoft Edge | Sebagai peramban yang digunakan untuk menjalankan pemindaian menggunakan Intruder. |
| Chromium | Sebagai peramban yang digunakan untuk menjalankan target situs web KPPM FRI pada pemindaian menggunakan Burp Suite. |

C. Tahap *Planning*

Pada tahap ini, penguji melakukan perencanaan untuk menentukan target, metode, dan tujuan dilakukannya pengujian. Target pengujian adalah situs web KPPM FRI yang terdapat dalam tabel 1.

TABEL 3
*WEBSITE* TARGET DALAM PENELITIAN

| No | Nama Domain | Sub Domain |
|---|---|---|
| 1 | virtualfri.id | kppm.virtualfri.id |

D. Hasil *Information Gathering*

*Information Gathering* ini bertujuan untuk mengetahui struktur situs web KPPM FRI dan struktur VPS FRI. Pada tahap ini, yang perlu diketahui dari situs web KPPM FRI adalah nama domain, alamat IP, *framework, database*, *port*, dan *software* pendukung yang digunakan. Berikut merupakan hasil *Information Gathering* dari situs web KPPM FRI yang disajikan dalam tabel 4:

TABEL 4
HASIL *INFORMATION GATHERING* PADA SITUS WEB KPPM FRI

| Spesifikasi | Keterangan |
|---|---|
| Nama Domain | kppm.virtualfri.id |
| Alamat IP | 103.41.206.192 |
| Framework | Sails 1.4.3 berbasis pada Node.JS |
| Port yang Digunakan | 81, 82, 83, 84, 8080, 8081, 8084, 3307, 3308, 3309, 3310, 3311, 443 |

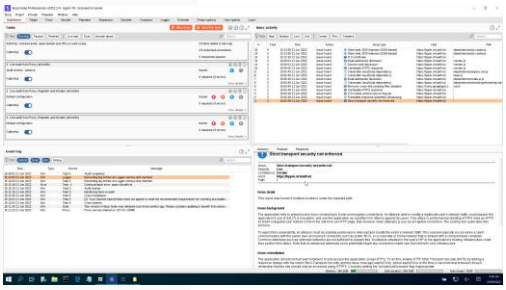
E. *Vulnerability Scanning*

1. *Vulnerability Scanning* dengan Burp Suite

Langkah pertama pada skenario *vulnerability scanning* dengan Burp Suite yaitu menentukan situs web yang akan dijadikan target. Situs web yang akan dijadikan target merupakan situs web KPPM FRI. Kemudian proses dilanjutkan dengan melakukan *scanning* dengan tools yang tersedia pada *software* Burp Suite.

Setelah berhasil melakukan *scanning*, maka dilanjutkan dengan *generate* hasil scan dari Burp Suite. Hasil *scanning* berupa jenis kerentanan, *severity* atau tingkat resiko kerentanan, *confidence* atau tingkat keyakinan adanya kerentanan, dan klasifikasi mengenai kerentanan yang disusun oleh CVE, CAPEC, dan OWASP.

Untuk mengakses Burp Suite, penguji menggunakan jaringan internet wireless, kemudian menggunakan Virtual Computer dalam aplikasi VMWare Workstation yang menjalankan Kali Linux dalam mode *Undercover,* sehingga *user interface* Kali Linux yang digunakan oleh penguji identik dengan Windows 10. Kemudian, penguji menjalankan *tools* Burp Suite dari dalam Virtual Computer yang dijalankan tersebut, seperti pada gambar 2 berikut:



GAMBAR 2
PROSES *VULNERABILITY SCANNING* DENGAN BURP SUITE

Hasil kerentanan yang terdeteksi oleh Burp Suite dapat dilihat pada tabel 5 berikut:

TABEL 5
KERENTANAN YANG TERDETEKSI OLEH BURP SUITE

| Jenis Kerentanan | *Severity, Confidence* | Klasifikasi Kerentanan |
|---|---|---|
| *Strict transport security not enforced* | *Low, Certain* | CWE-523<br>CAPEC-94<br>CAPEC-157 |
| *Frameable response (potential Clickjacking)* | *Information, Firm* | CWE-693<br>CAPEC-103 |
| *TLS cookie without secure flag set* | *Information, Certain* | CWE-614 |

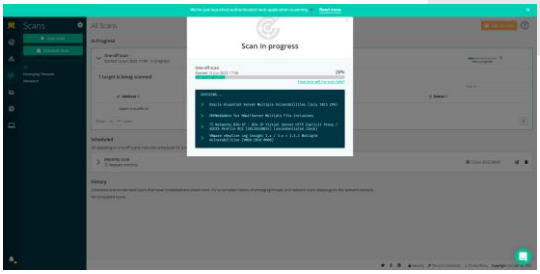
| | | |
|---|---|---|
| *Cacheable HTTPS response* | *Information, Certain* | CWE-524<br>CWE-525<br>CAPEC-37 |
| *Vulnerable JavaScript dependency* | *Low, Tentative* | CWE-1104<br>A9 |
| *Email addresses disclosed* | *Information, Certain* | CWE-200<br>CAPEC-37 |
| *Source code disclosure* | *Low, Tentative* | CWE-18 (sudah diperbarui ke CWE-699)<br>CWE-200<br>CWE-388<br>CWE-540<br>CWE-541<br>CWE-615<br>CAPEC-37 |
| *TLS certificate* | *Low, Certain* | CWE-295<br>CWE-326<br>CWE-327 |
| *Client-side JSON injection (DOM-based)* | *Low, Firm* | CWE-79<br>CWE-116<br>CWE-159<br>CAPEC-153 |

2. *Vulnerability Scanning* dengan Intruder

Langkah pertama pada skenario *vulnerability scanning* dengan Intruder yaitu menentukan situs web yang akan dijadikan target. Situs web yang akan dijadikan target merupakan situs web KPPM FRI. Kemudian proses dilanjutkan dengan melakukan set-up pada software Intruder yang dilakukan di peramban lokal. Set-up ini dilakukan dengan tujuan melakukan vulnerability scan secara otomatis.

Setelah set-up berhasil, dilanjutkan dengan *scanning* situs web KPPM FRI secara *automated scanning*. Setelah proses *scanning* selesai, maka laporan hasil *scanning* dapat langsung *di-generate*. Laporan yang muncul setelah scanning dengan aplikasi Intruder dapat langsung digunakan untuk proses selanjutnya yaitu analisis hasil.

Untuk mengakses Intruder, penguji menggunakan jaringan internet wireless, kemudian menggunakan Windows 11 sebagai sistem operasi untuk menjalankan peramban Microsoft Edge. Kemudian, penguji menjalankan *tools* Intruder dengan menggunakan peramban tersebut, seperti pada gambar 3 berikut:




GAMBAR 3
PROSES *VULNERABILITY SCANNING* DENGAN INTRUDER

Setiap *vulnerability scanning* yang dilakukan menggunakan *tools* Intruder ini melakukan 11.260 pengujian yang mengikuti standar dari CVE (*Common Vulnerability and Exposures*) sesuai pengujian yang dilakukan dan *software* yang digunakan untuk menjalankan situs web tersebut.

Hasil kerentanan yang terdeteksi oleh Intruder dapat dilihat pada tabel 6 berikut:

TABEL 6
KERENTANAN YANG TERDETEKSI OLEH INTRUDER

| Jenis Kerentanan | Tingkat Isu Kerentanan | Letak Kerentanan (Port) |
|---|---|---|
| *Vulnerable Apache Version* | *Critical* | Apache (81) |
| *Unsupported PHP Version* | *High* | PHP (82, 83, 84) |
| *Vulnerable jQuery Version* | *Medium* | jQuery (81, 8080, 8081, 8084) |
| *Vulnerable PHP Version* | *Medium* | PHP (82, 83, 84) |
| *Error Page Information Disclosure* | *Low* | Situs Web (81) |
| *Strict Transport Security HTTP Header Not Set* | *Low* | HTTP Header (443) |

F. Analisis Hasil *Vulnerability Scanning*

1. Analisis Hasil *Vulnerability Scanning* dengan Burp Suite

Hasil analisis dikategorikan berdasarkan hasil pengujian yang telah dilakukan dengan tools Burp Suite. Berikut merupakan hasil analisis dari hasil *vulnerability scanning* menggunakan Burp Suite yang disajikan dalam tabel 7:

TABEL 7
ANALISIS HASIL KERENTANAN DARI BURP SUITE

| Jenis Kerentanan | Hasil Analisis |
|---|---|
| *Strict transport security not enforced* | Situs web KPPM FRI sudah menggunakan *default* SSL, tetapi kerentanan ini tetap ada karena *default* SSL dinilai kurang efektif dalam melindungi dan mengenkripsi data. Masalah ini dapat diselesaikan dengan memperbaiki mekanisme *login* dengan mengimplementasikan sistem SSL tambahan, dan bisa dibantu juga dengan mengimplementasikan enkripsi tambahan dengan menyusun sistem *secure login* pada *source code* situs web KPPM FRI. |
| *Frameable response (potential Clickjacking)* | Kerentanan ini memungkinkan adanya aksi *clickjacking*, karena mekanisme perlindungan terhadap *source code* masih dinilai rendah. Masalah ini dapat diselesaikan dengan memperbaiki mekanisme perlindungan *source code*, |

| | |
|---|---|
| | sehingga mengurangi resiko peniruan *source-code front-end* situs web KPPM FRI dan mengurangi resiko aksi *clickjacking* dengan menyerupai situs web KPPM FRI. |
| *TLS cookie without secure flag set* | *HTTP Strict Transport Security* (HSTS) pada situs web KPPM FRI tidak diatur. Fungsi HSTS adalah memastikan setiap pengguna yang masuk ke situs web menggunakan protokol koneksi HTTPS. Efek jika HSTS tidak diatur adalah tidak adanya enkripsi data, integritas data, dan autentikasi saat mengakses situs web tersebut. Masalah ini dapat diselesaikan dengan mengatur HSTS dengan baik, sehingga pengguna secara otomatis masuk ke situs web KPPM FRI dengan menggunakan protokol koneksi HTTPS. |
| *Cacheable HTTPS response* | *Cache* pada situs web KPPM FRI menampung data yang bersifat *confidental*, yang seharusnya tidak disimpan dalam *cache*. Masalah ini dapat diselesaikan dengan memperbaiki sistem *caching* pada situs web KPPM FRI sehingga tidak menyimpan data yang *confidental*. |
| *Vulnerable JavaScript dependency* | Situs web KPPM FRI menggunakan *dependency* JavaScript yang rentan. Hasil scanning yang dilakukan tidak menyebutkan *dependency* apa yang rentan, namun masalah ini dapat diselesaikan dengan memperbarui seluruh versi *dependency* JavaScript yang digunakan untuk mendapatkan *patch* terbaru dari kerentanan tersebut. |
| *Email addresses disclosed* | Situs web KPPM FRI menampilkan informasi mengenai alamat *e-mail* dari pengguna atau pengembang, namun kerentanan ini dapat diabaikan jika informasi alamat *e-mail* tersebut diperlukan untuk informasi |
| *Source code disclosure* | Adanya informasi *confidental* pada *source code* situs web KPPM FRI dan *database* situs web KPPM FRI. Informasi *confidental* ini dapat digunakan oleh *attacker* untuk menyerang dan mengambil informasi lainnya dari situs web KPPM FRI, yang menyebabkan situs web tidak dapat digunakan lagi. |
| | Masalah ini dapat diselesaikan dengan memeriksa kembali folder instalasi situs web dan *database* KPPM FRI untuk memastikan tidak ada informasi *confidental* yang terbuka begitu saja. |
| *TLS certificate* | *HTTP Strict Transport Security* (HSTS) pada situs web KPPM FRI tidak diatur. Fungsi HSTS adalah memastikan setiap pengguna yang masuk ke situs web menggunakan protokol koneksi HTTPS. Efek jika HSTS tidak diatur adalah tidak adanya enkripsi data, integritas data, dan autentikasi saat mengakses situs web tersebut. Masalah ini dapat diselesaikan dengan mengatur HSTS dengan baik, sehingga pengguna secara otomatis masuk ke situs web KPPM FRI dengan menggunakan protokol koneksi HTTPS. |
| *Client-side JSON injection (DOM-based)* | Tidak adanya proteksi pada situs web KPPM FRI terhadap pengguna untuk melakukan input saat menggunakan situs web KPPM FRI, sehingga pengguna bisa memasukkan *script* yang akhirnya dapat digunakan dalam serangan XSS. Masalah ini dapat diselesaikan dengan mengatur tipe *input* dari pengguna. Pengguna hanya diizinkan memasukkan *input* sesuai data yang diperlukan, sebagai contoh, di *field* NIM pengguna hanya dapat memasukkan angka, dan di *field* dokumen pengguna hanya dapat mengunggah *file* dengan format .pdf, sehingga dapat mengurangi resiko injeksi *script* yang dapat digunakan untuk serangan XSS. |

2. Analisis Hasil *Vulnerability Scanning* dengan Intruder

Hasil analisis dikategorikan berdasarkan hasil pengujian yang telah dilakukan dengan tools Intruder. Berikut merupakan hasil analisis dari hasil *vulnerability scanning* menggunakan Intruder:

TABEL 8
ANALISIS HASIL KERENTANAN DARI INTRUDER

| Jenis Kerentanan | Hasil Analisis |
|---|---|
| *Vulnerable Apache Version* | Situs web KPPM FRI berjalan menggunakan web server Nginx, sedangkan Intruder mendeteksi adanya kerentanan pada Apache, menandakan bahwa kerentanan ini tidak berlaku |

| | |
|---|---|
| | karena situs web KPPM FRI dan VPS FRI tidak menggunakan Apache. |
| *Unsupported PHP Version* | Situs web KPPM FRI berjalan menggunakan *framework* Sails.js yang berbasis pada JavaScript, menandakan bahwa kerentanan ini tidak berlaku karena situs web KPPM FRI tidak menggunakan PHP. |
| *Vulnerable jQuery Version* | jQuery berfungsi sebagai *library* untuk menjalankan situs web KPPM FRI yang berjalan pada Sails.js. Pada hasil *scanning* tidak disebutkan versi jQuery yang digunakan, namun masalah ini dapat diselesaikan dengan memperbarui versi jQuery yang digunakan menjadi versi terakhir. |
| *Vulnerable PHP Version* | Situs web KPPM FRI berjalan menggunakan *framework* Express yang berbasis pada JavaScript, menandakan bahwa kerentanan ini tidak berlaku karena situs web KPPM FRI tidak menggunakan PHP. |
| *Error Page Information Disclosure* | Informasi yang ditampilkan pada halaman *error* situs web KPPM FRI langsung menyebutkan letak *error* pada saat menampilkan halaman *error,* karena tidak dikonfigurasi dan disimpan dengan benar. Informasi yang dapat diambil dengan mudah ini dapat digunakan untuk mengetahui struktur situs web KPPM FRI dan VPS FRI, sehingga memudahkan *attacker* untuk menyusun strategi dalam menyerang situs web KPPM FRI dan VPS FRI. Masalah ini dapat diselesaikan dengan menyembunyikan seluruh *file* yang berisi informasi tentang *backend server,* seperti versi PHP, versi Nginx, nama database, dan informasi lainnya. |
| *Strict Transport Security HTTP Header Not Set* | *HTTP Strict Transport Security* (HSTS) pada situs web KPPM FRI tidak diatur. Fungsi HSTS adalah memastikan setiap pengguna yang masuk ke situs web menggunakan protokol koneksi HTTPS. Efek jika HSTS tidak diatur adalah tidak adanya enkripsi data, integritas data, dan autentikasi saat mengakses situs web tersebut. Masalah ini dapat diselesaikan dengan mengatur HSTS dengan baik, sehingga pengguna secara otomatis masuk ke situs web KPPM FRI dengan menggunakan protokol koneksi HTTPS. |

## V. KESIMPULAN

Berdasarkan hasil pengujian dan analisis yang telah dilakukan pada situs web KPPM FRI dengan menggunakan software Burp Suite dan Intruder, dapat disimpulkan bahwa kerentanan yang ditemukan oleh *software* Burp Suite sebanyak 9 kerentanan yang seluruhnya valid, sehingga tingkat akurasi *scanning* pada *software* Burp Suite sebesar 100%, dengan 5 kerentanan pada kategori *Low* dan 4 kerentanan pada kategori *Information*, dengan tingkat keyakinan *Firm* sebanyak 2 kerentanan, *Certain* sebanyak 5 kerentanan, dan *Tentative* sebanyak 2 kerentanan, sementara Kerentanan yang ditemukan oleh *software* Intruder sebanyak 6 kerentanan, sedangkan kerentanan yang valid hanya sebanyak 3 kerentanan, sehingga tingkat akurasi *scanning* pada *software* Intruder sebesar 50%, dengan 1 kerentanan pada kategori *Medium* dan 2 kerentanan pada kategori *Low*, dan Intruder tidak memberikan informasi mengenai tingkat keyakinan kerentanan. Kerentanan yang ada pada situs web KPPM FRI bersifat *Medium, Low dan Information*, yang berarti kerentanan ini tidak akan terlalu berdampak fatal pada situs web KPPM FRI namun perlu dilakukan perbaikan untuk menghindari resiko dari kerentanan tersebut.

## REFERENSI

Rui, Liu, Yan Danfeng, Lin Fan, and Yang Fangchun. 2009. "Optimization of Hierarchical Vulnerability Assessment Method." *Proceedings of 2009 2nd IEEE International Conference on Broadband Network and Multimedia Technology, IEEE IC-BNMT2009* (1):458–62. doi: 10.1109/ICBNMT.2009.5348535.

Riadi, Imam, Anton Yudhana, and Yunanri W. 2020. "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment." *Jurnal Teknologi Informasi Dan Ilmu Komputer* 7(4):853. doi: 10.25126/jtiik.2020701928.

Rahalkar, Sagar. 2021. *Guide to Burp Suite*. Pune: Apress.

Qu, Guangzhi, J. Rudraraju, and R. Modukuri. 2002. "A Framework for Network Vulnerability Analysis." *Communications, ...* 2(4):1–6.

Chazar, Chalifa. 2017. "Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2005." *Jurnal Informasi* VII(2):48–57.

Li, Huan Chung, Po Huei Liang, Jiann Min Yang, and Shiang Jiun Chen. 2010. "Analysis on Cloud-Based Security Vulnerability Assessment." *Proceedings - IEEE International Conference on E-Business Engineering, ICEBE 2010* 490–94. doi: 10.1109/ICEBE.2010.77.
Backdoors, About, Trojan Horses, and Embedding Backdoors. 2001. "Backdoors and Trojan Horses."

*Information Security Technical Report* 6(4):31–57. doi: 10.1016/s1363-4127(01)00405-8.

Goel, Jai Narayan, and B. M. Mehtre. 2015. "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology." *Procedia Computer Science* 57:710–15. doi: 10.1016/j.procs.2015.07.458.

Ermawelis, Ermawelis. 2018. "Teknologi Informasi Untuk Perpustakaan, Pusat Dokumentasi Dan Informasi." *AL MUNIR : Jurnal Komunikasi Dan Penyiaran Islam* (1):11–18. doi: 10.15548/amj-kpi.v0i1.5.