ANALISIS KEAMANAN WEBSITE FEBI UIN SMH BANTEN MENGGUNAKAN PENETRATION TESTING

Chendri Irawan Satrio Nugroho [1], Ibnu Mas'ud [2], Muhammad Fikry [3], Dedi Miftah Nabhatul F [4], Nayla Rahmanidzfah [5], Ratu Salma Erliani [6], Alief Ibrahimauviq [7], Eka Agustiyan [8]
[1] Teknologi Informasi, Institut Teknologi Tangerang Selatan Komplek Komersial BSD, Jl.RayaSerpongNo.Kav.9, Lengkong Karya, Serpong Utara, South Tangerang City, Banten
[2-8] Informatika, Universitas Islam Negeri Sultan Maulana Hasanudin Banten
Jl. Raya Syeikh Nawawi Bantani No. 30 Curug Kota Serang, Banten
241730050.dedimiftahnabhatulf@uinbanten.ac.id

ABSTRAK

Keamanan website merupakan aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi, khususnya pada institusi pendidikan yang mengelola data publik dan akademik. Website Fakultas Ekonomi dan Bisnis Islam (FEBI) UIN Sultan Maulana Hasanuddin Banten berperan sebagai media informasi dan layanan digital bagi civitas akademika maupun masyarakat umum. Permasalahan dalam penelitian ini adalah belum diketahuinya tingkat keamanan website FEBI UIN SMH Banten serta potensi kerentanan yang terdapat pada sistem. Oleh karena itu, penelitian ini bertujuan untuk menganalisis keamanan website FEBI UIN SMH Banten melalui proses evaluasi dan pengujian keamanan sistem. Metode yang digunakan dalam penelitian ini adalah penetration testing yang dilakukan pada lingkungan pengujian untuk tujuan akademik. Pengujian difokuskan pada identifikasi potensi kerentanan, konfigurasi sistem, serta celah keamanan yang berisiko terhadap data dan layanan website. Hasil penelitian menunjukkan adanya beberapa potensi kerentanan dengan tingkat risiko yang bervariasi. Temuan tersebut diharapkan dapat menjadi bahan evaluasi dan rekomendasi perbaikan bagi pengelola sistem dalam upaya meningkatkan keamanan website terhadap ancaman keamanan siber.

Kata kunci : *keamanan website, penetration testing, keamanan informasi, kerentanan sistem, keamanan siber.*

1. PENDAHULUAN

Website merupakan komponen penting dalam sistem informasi institusi pendidikan yang berfungsi sebagai media penyedia informasi, layanan akademik, serta sarana komunikasi antara institusi dan masyarakat. Website Fakultas Ekonomi dan Bisnis Islam (FEBI) UIN Sultan Maulana Hasanuddin Banten digunakan sebagai media resmi untuk menyampaikan informasi akademik dan kelembagaan, sehingga aspek keamanan menjadi faktor krusial dalam menjaga kepercayaan pengguna serta keberlangsungan layanan digital. Keamanan sistem informasi bertujuan untuk memastikan kerahasiaan, integritas, dan ketersediaan data agar tidak mudah diakses, dimodifikasi, atau disalahgunakan oleh pihak yang tidak berwenang[1].

Seiring meningkatnya ancaman keamanan siber, website publik sering menjadi target pengujian maupun serangan karena dapat diakses secara luas. Beberapa penelitian menunjukkan bahwa website instansi pemerintah dan institusi pendidikan masih memiliki berbagai celah keamanan akibat konfigurasi sistem yang kurang optimal, penggunaan versi perangkat lunak yang rentan, serta belum diterapkannya mekanisme keamanan tambahan secara menyeluruh. Pengujian keamanan berbasis penetration testing pada aplikasi web instansi publik menemukan kerentanan umum seperti kesalahan konfigurasi keamanan, pengelolaan sesi yang tidak aman, serta penggunaan komponen sistem yang memiliki potensi celah keamanan[2].

Penelitian lain di bidang keamanan website pendidikan juga menunjukkan bahwa banyak aplikasi web akademik masih memiliki tingkat risiko keamanan yang signifikan, meskipun tidak ditemukan eksploitasi aktif. Kondisi ini disebabkan oleh lemahnya konfigurasi keamanan, kurangnya penerapan security header, serta terbukanya layanan jaringan yang tidak sepenuhnya dibatasi. Hal tersebut menunjukkan bahwa evaluasi keamanan secara berkala sangat diperlukan sebagai langkah pencegahan sebelum potensi kerentanan dimanfaatkan oleh pihak yang tidak bertanggung jawab[3].

Berdasarkan kondisi tersebut, permasalahan dalam penelitian ini adalah belum diketahuinya tingkat keamanan website FEBI UIN Sultan Maulana Hasanuddin Banten serta potensi kerentanan yang mungkin terdapat pada sistem. Oleh karena itu, penelitian ini bertujuan untuk mengevaluasi tingkat keamanan website FEBI UIN Sultan Maulana Hasanuddin Banten serta mengidentifikasi potensi kerentanan yang berisiko terhadap data dan layanan website.

Salah satu pendekatan yang umum digunakan untuk mengevaluasi keamanan sistem adalah penetration testing, yaitu metode pengujian keamanan dengan mensimulasikan teknik serangan secara terkendali untuk mengidentifikasi kerentanan tanpa melakukan eksploitasi yang merugikan. Dalam penelitian ini, penetration testing dilakukan menggunakan metode pemindaian ringan (light scan) dan analisis pasif terhadap website FEBI UIN Sultan Maulana Hasanuddin Banten. Pengujian meliputi vulnerability scanning aplikasi web, pemindaian subdomain, pemindaian port TCP dan UDP, serta

pengujian URL fuzzer. Acuan pengujian mengadaptasi standar OWASP Top 10 yang digunakan secara luas dalam identifikasi kerentanan aplikasi web kritis[4]. Hasil penelitian ini diharapkan dapat memberikan gambaran kondisi keamanan website serta menjadi dasar rekomendasi perbaikan dan penguatan sistem keamanan.

2. TINJAUAN PUSTAKA

Setelah peneliti melakukan telaah terhadap beberapa penelitian, terdapat beberapa penelitian yang memiliki keterkaitan dengan penelitian yang sedang peneliti lakukan. Penelitian yang pertama yang berhasil peneliti temukan adalah penelitian yang dilakukan oleh Hidayat dan Nugroho yang berjudul "Analisis Celah Keamanan Pada Website SMA Negeri 3 Berau Dengan Metode Penetration Testing". Tujuan dari penelitian tersebut adalah untuk mengetahui dan menganalisis celah keamanan yang terdapat pada website SMA Negeri 3 Berau yang berbasis WordPress dengan menggunakan metode penetration testing.

Pada penelitian tersebut, metode yang digunakan adalah penetration testing dengan memanfaatkan beberapa tools pengujian keamanan, yaitu OWASP ZAP, WPScan, dan Nikto. Pengujian dilakukan untuk mengidentifikasi berbagai kerentanan yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab. Website yang diuji merupakan website institusi pendidikan yang berfungsi sebagai media informasi, sehingga aspek keamanan menjadi hal yang penting untuk diperhatikan.

Hasil dari penelitian tersebut menunjukkan bahwa penggunaan OWASP ZAP berhasil menemukan beberapa celah keamanan yang berkaitan dengan konfigurasi aplikasi web, seperti tidak diterapkannya security header dan pengelolaan cookie yang belum aman. Selain itu, pengujian menggunakan WPScan menemukan beberapa kerentanan, antara lain masih aktifnya fitur XML-RPC, penggunaan versi WordPress yang belum diperbarui, serta terekspos nya file sensitif yang berpotensi meningkatkan risiko serangan brute force dan Distributed Denial of Service (DDoS).

Pengujian lebih lanjut menggunakan Nikto menunjukkan adanya sejumlah kerentanan yang berkaitan dengan konfigurasi server, termasuk potensi terjadinya BREACH Attack serta belum diterapkannya beberapa security header penting seperti Content-Security-Policy dan Referrer-Policy. Berdasarkan hasil penelitian tersebut, dapat disimpulkan bahwa metode penetration testing mampu mengidentifikasi berbagai celah keamanan pada website secara komprehensif dan dapat dijadikan sebagai dasar dalam upaya peningkatan keamanan sistem web.

2.1. Keamanan Informasi

Keamanan informasi merupakan aspek penting dalam pengelolaan sistem informasi yang bertujuan untuk melindungi data dari ancaman yang dapat menyebabkan kebocoran, perubahan, maupun gangguan layanan. Keamanan informasi tidak hanya berfokus pada perlindungan data, tetapi juga pada keberlangsungan sistem agar tetap dapat digunakan secara optimal oleh pengguna yang berwenang [4].

Dalam praktiknya, konsep keamanan informasi dikenal dengan CIA Triad yang terdiri dari kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Ketiga prinsip tersebut menjadi dasar dalam perancangan sistem informasi yang aman, khususnya pada sistem berbasis web yang bersifat terbuka dan dapat diakses secara publik [5].

2.2. Website sebagai Sistem Informasi

Website merupakan salah satu bentuk sistem informasi berbasis web yang digunakan untuk menyampaikan informasi dan layanan secara daring. Pada institusi pendidikan, website berfungsi sebagai media resmi penyedia informasi akademik, administrasi, serta sarana komunikasi antara institusi dan masyarakat umum [6].

Karena website institusi pendidikan dapat diakses secara luas melalui internet, website tersebut memiliki tingkat paparan risiko keamanan yang tinggi. Beberapa penelitian menunjukkan bahwa website publik sering menjadi target serangan akibat konfigurasi keamanan yang kurang optimal dan minimnya pengujian keamanan secara berkala [7].

2.3. Penetration Testing

Penetration testing merupakan metode pengujian keamanan sistem yang dilakukan dengan cara mensimulasikan teknik serangan secara terkendali untuk mengidentifikasi celah keamanan yang ada pada sistem. Metode ini bertujuan untuk membantu pengelola sistem memahami kelemahan keamanan sebelum dimanfaatkan oleh pihak yang tidak berwenang [8].

Dalam konteks evaluasi awal dan penelitian akademik, penetration testing umumnya dilakukan secara terbatas, seperti melalui pemindaian ringan (light scan) dan teknik deteksi pasif. Pendekatan ini digunakan untuk mengurangi risiko gangguan layanan sekaligus tetap memperoleh gambaran kondisi keamanan sistem secara umum [9].

2.4. Kerentanan Keamanan Website

Kerentanan keamanan (vulnerability) merupakan kelemahan pada sistem, aplikasi, atau konfigurasi yang dapat dimanfaatkan untuk melakukan serangan. Pada website, kerentanan sering muncul akibat penggunaan perangkat lunak yang belum diperbarui, pengelolaan sesi yang tidak aman, serta kurangnya penerapan mekanisme perlindungan tambahan seperti header keamanan [10].

Untuk membantu mengidentifikasi dan mengklasifikasikan jenis kerentanan yang sering ditemukan pada aplikasi web, OWASP mengembangkan standar OWASP Top 10. Standar ini digunakan secara luas karena mampu menggambarkan kerentanan aplikasi web paling kritis serta membantu penentuan tingkat risiko dan prioritas perbaikan keamanan sistem [11].

3. METODE PENELITIAN

3.1. Jenis Penelitian

Penelitian ini merupakan studi deskriptif teknis yang menggunakan pendekatan pengujian penetrasi. Pendekatan ini digunakan untuk mengidentifikasi dan menganalisis tingkat keamanan situs web FEBI UIN Sultan Maulana Hasanuddin Banten berdasarkan hasil pengujian keamanan sistematis. Penelitian ini berfokus pada proses identifikasi kerentanan tanpa secara aktif memanfaatkannya, yang dapat mengganggu operasi sistem.

3.2. Objek Penelitian

Objek penelitian adalah situs web resmi Fakultas Ekonomi dan Bisnis Islam (FEBI) UIN Sultan Maulana Hasanuddin Banten, yang dapat diakses di: https://febi.uinbanten.ac.id/

Situs web ini dipilih karena berfungsi sebagai media informasi publik dan akademik, sehingga memerlukan tingkat keamanan yang tinggi untuk melindungi data dan layanan yang disediakannya.

3.3. Metode Pengujian Keamanan

Metode pengujian keamanan yang digunakan adalah pengujian penetrasi dengan pemindaian ringan dan skema deteksi pasif. Metode ini mensimulasikan perspektif pengguna eksternal (pengguna yang tidak terautentikasi) dalam mengidentifikasi potensi kerentanan keamanan yang dapat dideteksi tanpa melakukan serangan agresif atau eksploitasi langsung terhadap sistem.

3.4. Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui proses pemindaian keamanan situs web menggunakan alat pengujian penetrasi berbasis web. Data yang dikumpulkan meliputi:

a. Hasil pemindaian kerentanan situs web, termasuk informasi tingkat risiko (Tinggi, Sedang, Rendah, dan Informasional).
b. Informasi tentang versi teknologi yang digunakan, seperti server web, kerangka kerja, dan bahasa pemrograman.
c. Konfigurasi keamanan aplikasi, termasuk cookie sesi dan header keamanan.
d. Informasi struktur domain dan subdomain.
e. Data port dan layanan jaringan aktif di server.
f. Titik akhir atau jalur sensitif yang terdeteksi melalui pengujian URL fuzzing.

3.5. Alat Parameter Pengujian

Pengujian dilakukan menggunakan platform pengujian penetrasi dengan konfigurasi sebagai berikut:

a. Jenis pemindaian: Pemindaian ringan
b. Mode pengujian: Tanpa otentikasi
c. Teknik deteksi: Deteksi pasif
d. Pengujian jaringan: Pemindaian port TCP (1000 port teratas) dan pemindaian port UDP (100 port teratas)
e. Fitur tambahan: Pencari Subdomain dan Penguji URL

Pemindaian dilakukan dalam rentang waktu tertentu dan tidak melibatkan serangan brute-force, injeksi eksploit, atau modifikasi data pada server target.

3.6. Tahapan Penelitian

Tahapan penelitian yang dilakukan dalam studi ini meliputi:

a. Identifikasi Target
   Menentukan situs web FEBI UIN SMH Banten sebagai target pengujian keamanan.
b. Pelaksanaan Pemindaian Keamanan
   Memindai situs web, subdomain, port jaringan, dan URL menggunakan alat pengujian penetrasi sesuai parameter yang telah ditentukan.
c. Pengumpulan Hasil Pengujian
   Mendokumentasikan semua temuan pemindaian, termasuk jenis kerentanan, tingkat risiko, dan informasi teknis pendukung.
d. Analisis Kerentanan
   Menganalisis setiap temuan berdasarkan dampaknya terhadap keamanan sistem, stabilitas layanan, dan kemungkinan penyalahgunaan.
e. Pengembangan Rekomendasi
   Mengembangkan rekomendasi peningkatan keamanan berdasarkan temuan kunci untuk meningkatkan tingkat perlindungan sistem.

3.7. Teknik Analisis Data

Analisis data dilakukan menggunakan analisis deskriptif kualitatif, dengan menjelaskan secara sistematis setiap temuan kerentanan berdasarkan kategori risiko dan dampaknya terhadap sistem. Analisis ini berfokus pada kerentanan konfigurasi, penggunaan versi perangkat lunak, serta pengaturan keamanan jaringan dan aplikasi web.

3.8. Aspek Etika Penelitian

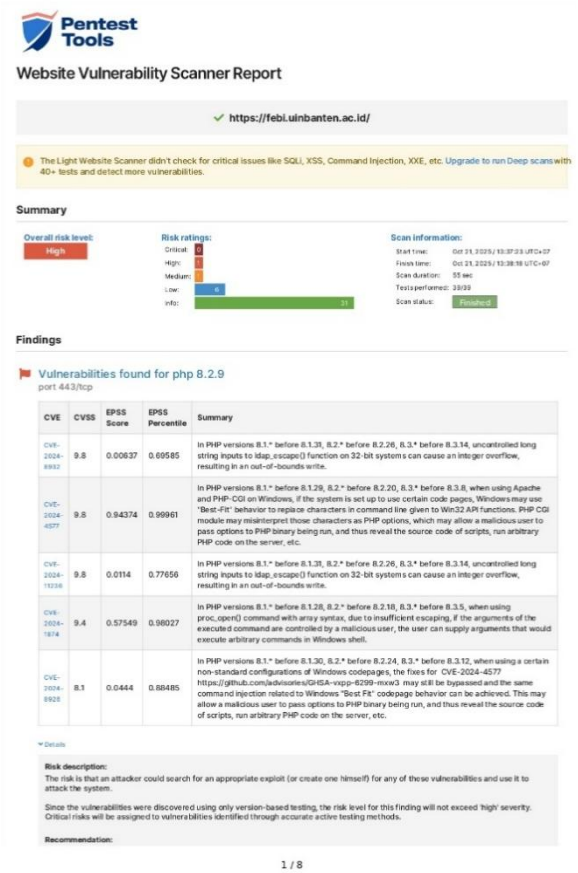
Penelitian ini dilakukan dengan memperhatikan etika pengujian keamanan sistem. Semua pengujian dilakukan secara pasif, tanpa eksploitasi aktif, tanpa upaya untuk mengambil alih sistem, dan tanpa mengubah konfigurasi atau data pada server target. Penelitian ini dilakukan semata-mata untuk tujuan akademik dan untuk meningkatkan keamanan sistem informasi.

4. HASIL DAN PEMBAHASAN

Pada bagian ini dibahas hasil pengujian keamanan website FEBI UIN SMH Banten yang dilakukan menggunakan metode penetration testing. Pengujian bertujuan untuk mengidentifikasi potensi kerentanan yang terdapat pada website, baik dari sisi konfigurasi sistem, layanan jaringan, maupun pengelolaan keamanan aplikasi web. Hasil pemindaian yang diperoleh digunakan sebagai dasar analisis tingkat risiko serta penyusunan rekomendasi perbaikan keamanan. Metode penetration testing digunakan untuk mengidentifikasi celah keamanan pada website dengan mengacu pada standar OWASP yang umum digunakan dalam pengujian aplikasi web.

4.1. Hasil Pemindaian Keamanan Website

Pengujian keamanan website dilakukan menggunakan fitur *Website Scanner* dengan metode *Light Website Scan* terhadap domain https://febi.uinbanten.ac.id/. Pemindaian ini bersifat ringan dan tidak melakukan eksploitasi aktif, sehingga aman digunakan untuk tahap awal analisis keamanan.



Gambar 1. Hasil website Security Scan

Berdasarkan hasil pemindaian yang ditunjukkan pada Gambar 1, tingkat risiko keseluruhan (overall risk level) website berada pada kategori High. Dari proses pemindaian tersebut ditemukan total 39 temuan, yang terdiri dari 1 temuan berisiko tinggi (*High*), 1 temuan berisiko sedang *(Medium*), 6 temuan berisiko rendah (*Low*), dan 31 temuan bersifat informasional (Informational). Hasil ini menunjukkan bahwa meskipun sebagian besar temuan bersifat informasional, keberadaan temuan dengan tingkat risiko tinggi tetap memerlukan perhatian khusus karena berpotensi memengaruhi keamanan website.

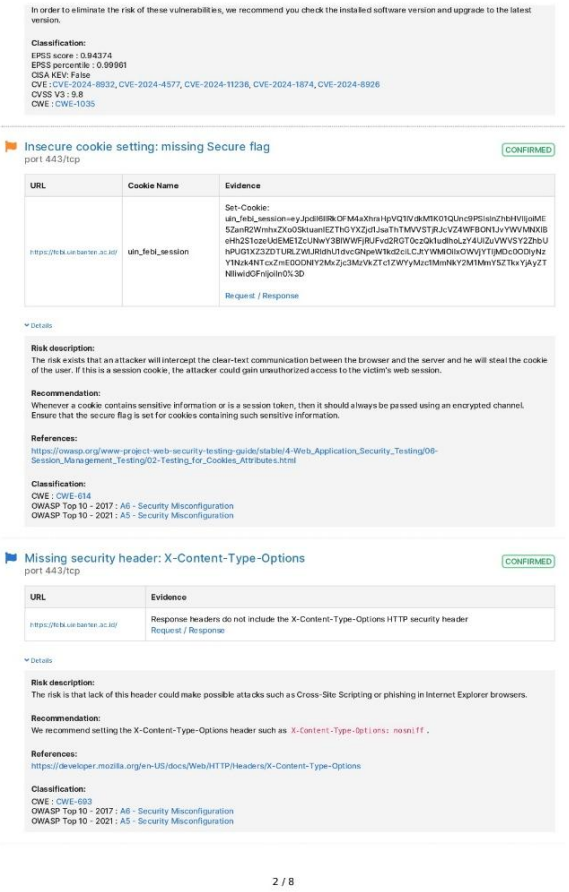
Tabel 1 menampilkan ringkasan hasil pemindaian keamanan website yang mencakup jumlah temuan pada setiap tingkat risiko, mulai dari High hingga Informational.

Berdasarkan Tabel 1, temuan dengan tingkat risiko tinggi menjadi prioritas utama untuk ditangani karena berpotensi memberikan dampak langsung terhadap keamanan sistem.

Tabel 1. Ringkasan Hasil Pemindaian website

No	Tingkat Risiko	Jumlah Temuan
1	High	1
2	Medium	1
3	Low	6
4	Informational	31

4.2. Analisis Kerentanan Sistem



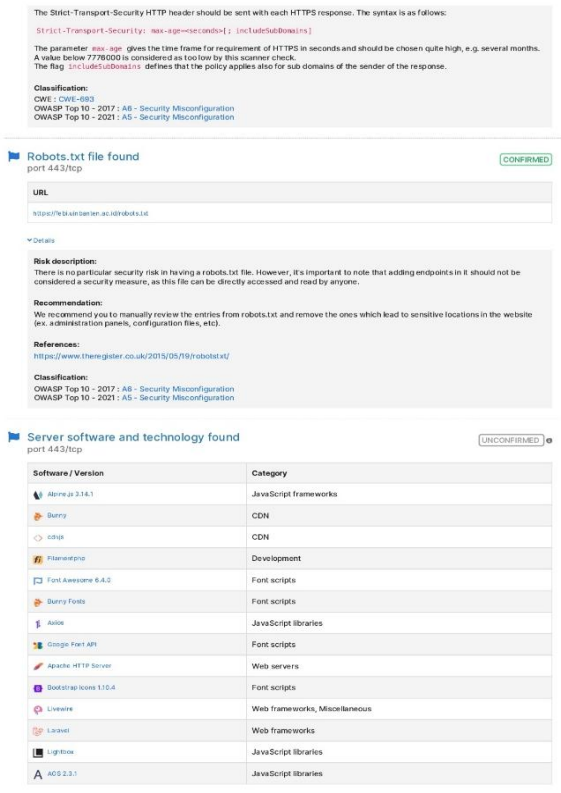
Gambar 2. Deteksi Kerentanan PHP dan Header Keamanan

Salah satu temuan penting dari hasil pemindaian adalah terdeteksinya pengguna PHP versi 8.2.9 pada server website. Versi PHP tersebut diketahui memiliki beberapa potensi celah keamanan berbasis CVE.

Meskipun deteksi ini bersifat version-based dan belum tentu dapat dieksploitasi secara langsung, kondisi tersebut tetap berisiko apabila tidak dilakukan pembaruan sistem secara berkala. Penggunaan versi perangkat lunak yang tidak diperbarui secara berkala berpotensi menimbulkan celah keamanan yang dapat dimanfaatkan oleh penyerang.

Berdasarkan Gambar 2,hasilpemindaian menunjukkan penggunaan versi PHP yang memiliki potensi kerentanan serta belum diterapkannya beberapa header keamanan penting, sehingga berisiko terhadap serangn keamanan aplikasi web.

Dampak yang dapat ditimbulkan apabila kerentanan ini tidak ditangani antara lain kemungkinan ekseku kode berbahaya, pengambilalihan sistem, gangguan layanan (*Denial of Service*), serta menurunnya stabilitas server. Oleh karena itu, pengelola sistem disarankan untuk melakukan pembaruan PHP ke versi yang lebih aman atau menambahkan lapisan keamanan tambahan seperti *Web Application Firewall* (WAF).



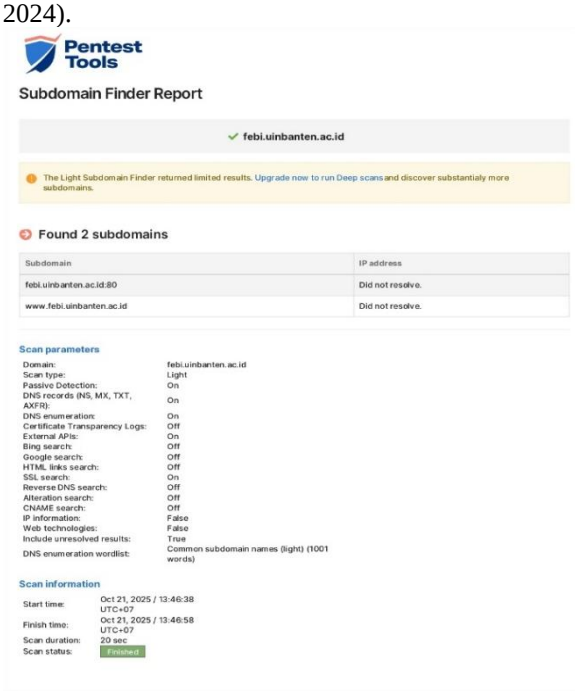
Gambar 3. Deteksi Konfigurasi Header Keamanan Website

Berdasarkangambar3,dapat di ketahui bahwa beberapa header keamanan penting belum dikonfigurasi dengan baik, antara lain Strict-Transport-Security (HSTS), Content-Security-Policy (CSP), Referrer-Policy, dan X-Content-Type-Options. Ketiadaan header tersebut berpotensi meningkatkan risiko serangan seperti man-in-the-middle, cross-site scripting (XSS), serta kebocoran informasi *referer*.

Selain itu, hasil pemindaian juga menunjukkan bahwa cookie sesi login belum dilengkapi dengan atribut keamanan *Secure* dan *HttpOnly*.Kondisi ini berpotensi dimanfaatkan untuk melakukan pencurian sesi pengguna(*session hijacking*).Penambahan atribut tersebut diperlukan agar cookie hanya dikirim melalui koneksi HTTPS dan tidak dapat diakses oleh skrip berbahaya pada browser.

4.3. Hasil Pemindaian Subdomain

Pemindaian subdomain dilakukan menggunakan fitur Subdomain *Finde*r terhadap domain febi.uinhbanten.ac.id. Tujuan pemindaian ini adalah untuk memastikan tidak terdapat subdomain aktif lain yang berpotensi menyimpan celah keamanan. Pemindaian subdomain merupakan bagian penting dalam tahapan penetration testing untuk mengidentifikasi potensi perluasan permukaan serangan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab apabila terdapat subdomain aktif yang tidak terkelola dengan baik (Nurrizki et al., 2024).



Gambar 4. Hasil Pemindaian Subdomain Website FEBI UIN SMH Banten

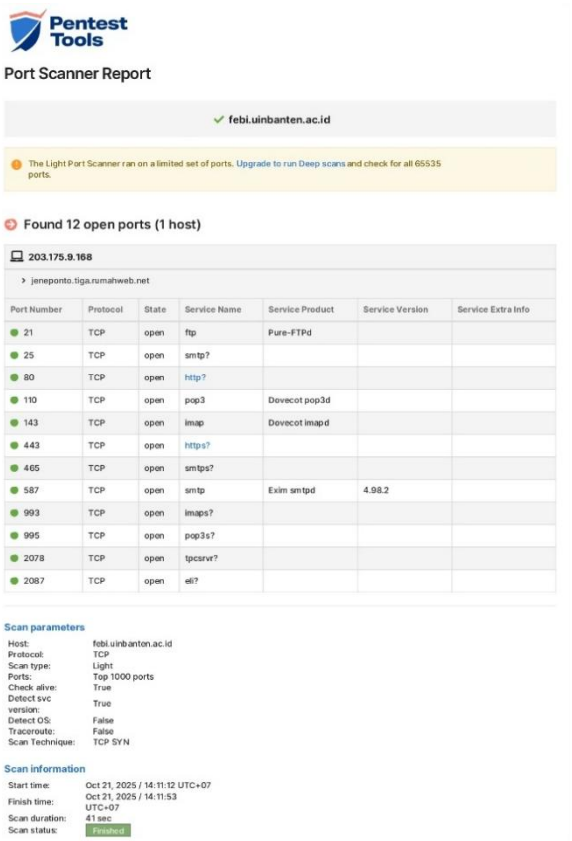
Berdasarkan Gambar 4, menunjukkan bahwa subdomain yang terdeteksi tidak memberikan respons(did not resolve), sehingga tidak ditemukan subdomain aktif lain yang dapat diakses atau diuji lebih lanjut. Hal ini mengindikasikan bahwa pengelolaan subdomain pada website FEBI UIN SMH Banten relatif sederhana dan tidak memperluas permukaan serangan.

Hasil pemindaian menunjukkan bahwa terdeteksi dua subdomain, yaitu febi.uinbanten.ac.id dan www.febi.uinbanten.ac.id, namun keduanya tidak memberikan respons (*did not resolve*). Hal ini menunjukkan bahwa tidak terdapat subdomain aktif

lain yang dapat diakses dan diuji lebih lanjut. Dengan demikian, struktur domain website FEBI UIN SMH Banten dapat dikategorikan sederhana dan relatif aman dari sisi pengelolaan subdomain.

4.4. Hasil Pemindaian Port Scanner

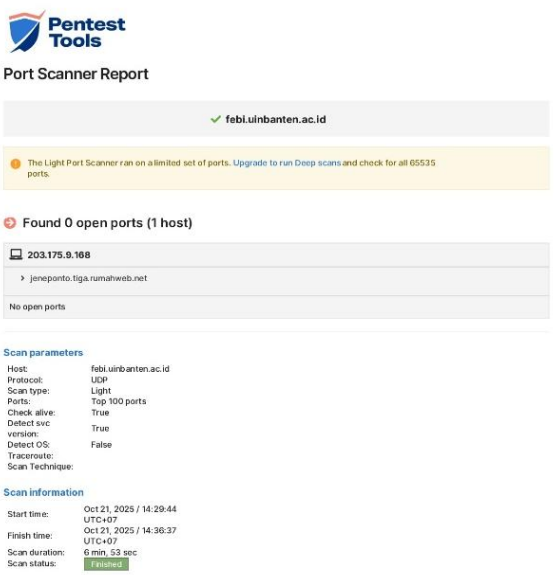
Pemindaian port dilakukan menggunakan metode *TCP SYN Scan* terhadap 1000 port teratas. Hasil pemindaian menunjukkan bahwa terdapat beberapa port terbuka yang menjalankan layanan web, email, dan FTP.



Gambar 5 Hasil Pemindaian Port Scanner pada Domain febi.uinbanten.ac.id

Berdasarkan gambar 5 hasil pemindaian port pada domain febi.uinbanten.ac.id menunjukkan adanya beberapa port terbuka.

Port 80 dan 443 digunakan untuk layanan web, sedangkan beberapa port lain digunakan untuk layanan email. Selain itu, terdeteksi port 21 (FTP) dan port administrasi server yang perlu mendapat perhatian khusus. Port-port tersebut berpotensi menjadi celah keamanan apabila tidak dikonfigurasi dengan pembatasan akses yang memadai. Selain itu ada juga pemindaian UDP dilakukan terhadap alamat 203.175.9.168 (febi.uinbanten.ac.id) menggunakan Light UDP Scan pada 100 port teratas.

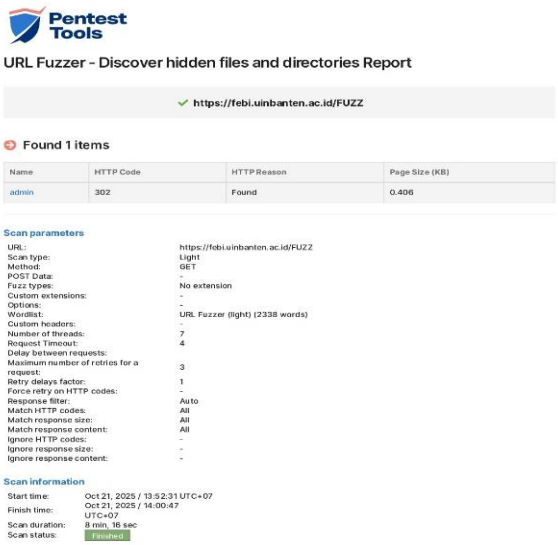


Gambar 6 Hasil Pemindaian Port Scanner (UDP)

Berdasarkan gambar 6 Hasil "0 open ports" berarti pemindaian tidak mendapatkan respons UDP yang mengindikasikan layanan aktif pada port-port yang diperiksa. Namun perlu dicatat bahwa UDP bersifat connectionless — banyak layanan UDP tidak memberikan balasan ketika dipanggil kecuali menerima query yang benar, dan banyak firewall/IDS juga memblokir paket UDP. Karena itu, hasil negatif pada UDP tidak selalu berarti tidak ada layanan UDP yang berjalan; bisa juga berarti respon diblokir atau paket probe tidak sesuai.

Untuk meningkatkan keamanan server, disarankan untuk menonaktifkan layanan yang tidak digunakan, menerapkan enkripsi SSL/TLS, serta membatasi akses port manajemen hanya untuk administrator.

4.5. Hasil Pemindaian URL Fuzzer



Gambar 7. Hasil Pemindaian URL Fuzzer pada Domain febi.uinbanten.ac.id

Pemindaian URL Fuzzer dilakukan untuk mengidentifikasi kemungkinan direktori tersembunyi pada website. Hasil pemindaian menemukan path /*admin* yang merespons dengan status HTTP 302 (*redirect*). Temuan ini mengindikasikan adanya mekanisme pengalihan menuju halaman login administrator.

Berdasarkan Gambar 7, Pemindaian URL Fuzzer pada https://febi.uinbanten.ac.id/FUZZ (light wordlist) menemukan 1 path: admin yang merespons dengan HTTP 302 Found (redirect). Artinya ada endpoint /admin yang mengarahkan ke lokasi lain (kemungkinan halaman login atau panel admin).

Meskipun tidak secara langsung menunjukkan kerentanan, keberadaan endpoint administratif perlu mendapat perhatian khusus. Pengelola website disarankan untuk membatasi akses ke halaman admin, menerapkan autentikasi ganda, serta membatasi percobaan login untuk mencegah serangan *brute force*.

5. KESIMPULAN DAN SARAN

Studi ini berhasil mengevaluasi tingkat keamanan website FEBI UIN SMH Banten menggunakan metode penetration testing pasif, dengan hasil menunjukkan 39 isu keamanan yang terdiri dari 1 risiko tinggi, 1 risiko sedang, 6 risiko rendah, dan 31 temuan informatif, menempatkan website pada kategori risiko tinggi secara keseluruhan. Permasalahan keamanan kritis yang ditemukan antara lain versi PHP 8.2.9 yang memiliki kerentanan CVE, tidak adanya pengaturan header keamanan krusial (HSTS, CSP, Referrer-Policy, X-Content-Type-Options), konfigurasi cookie sesi yang lemah tanpa proteksi Secure dan HttpOnly, layanan FTP pada port 21 yang dapat diakses, dan jalur administrator (/admin) yang rentan terhadap serangan paksa. Meskipun pengelolaan subdomain menunjukkan struktur yang baik, kerentanan tingkat tinggi yang ada membutuhkan penanganan segera untuk mencegah potensi serangan yang membahayakan sistem. Oleh karena itu, tim pengelola sistem direkomendasikan untuk melakukan upgrade PHP ke versi yang lebih aman, menerapkan seluruh header keamanan sesuai standar OWASP, mengaktifkan proteksi Secure dan HttpOnly pada cookie, membatasi akses FTP hanya untuk administrator terverifikasi, mengimplementasikan verifikasi dua faktor dan pembatasan percobaan login pada panel admin, serta mengintegrasikan Web Application Firewall untuk perlindungan tambahan. Untuk pengembangan riset selanjutnya, disarankan melakukan pengujian dengan akses terautentikasi untuk menemukan kerentanan tersembunyi, melaksanakan evaluasi keamanan rutin untuk memantau keberhasilan perbaikan, mengembangkan standar penilaian keamanan spesifik untuk portal akademik, dan melakukan kajian komparatif dengan website fakultas lain di seluruh UIN untuk mengadopsi praktik keamanan terbaik dalam rangka meningkatkan ketahanan keamanan siber institusi pendidikan secara menyeluruh.

DAFTAR PUSTAKA

[1] R. marta Dinata, M. Alzril, M. I. Yamin, H. Effendi, and M. Febriansyah, "Analisis Keamanan Situs Web Rumah Sakit Menggunakan Metode Penetration Testing OWASP," *SAINSTECH: JURNAL PENELITIAN DAN PENGKAJIAN SAINS DAN TEKNOLOGI*, vol. 35, no. 2, pp. 99–100, Jun. 2025, doi: 10.37277/stch.v35i2.2383.

[2] R. R. J and J. S. Patty, "PENETRATION TESTING OF A COMPUTERIZED PSYCHOLOGICAL ASSESSMENT WEBSITE USING SEVEN ATTACK VECTORS FOR CORPORATION WEBSITE SECURITY," *Jurnal Teknik Informatika (Jutif)*, vol. 5, no. 3, pp. 831–842, Jun. 2024, doi: 10.52436/1.jutif.2024.5.3.1731.

[3] T. Anugrah, "PENETRATION TESTING KEAMANAN WEBSITE STIE SAMARINDA MENGGUNAKAN TEKNIK SQL INJECTION DAN XSS," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 12, no. 1, Jan. 2024, doi: 10.23960/jitet.v12i1.3882.

[4] "FIKS+Article_Template_2023_JUTIN".

[5] M. Syarifudin, L. Widyawati, and O. Asroni, "Journal of Artificial Intelligence and Engineering Applications Web Security Vulnerability Analysis and Mitigation Based on OWASP TOP 10," 2025. [Online]. Available: https://ioinformatic.org/

[6] T. Rahmadi and R. Supardi, "Website Security Analysis Using Penetration Testing Method," *Print) GATOTKACA Journal (Teknik Sipil*, vol. 2, no. 2, pp. 147–152, 2021, doi: 10.37638/gatotkaca.2.1.147-152.

[7] I. Uji *et al.*, "Implementation of Penetration testing on Websites to Improve Security of Information Assets UPN 'Veteran' Yogyakarta," *Jurnal Informatika dan Teknologi Informasi*, vol. 20, no. 2, pp. 153–162, 2023, doi: 10.31515/telematika.v20i2.7757.

[8] N. Hidayat and M. A. Nugroho, "ANALISIS CELAH KEAMANAN PADA WEBSITE SMA NEGERI 3 BERAU DENGAN METODE PENETRATION TESTING," 2025.

[9] H. Jati Setyadi and M. Rivani Ibrahim, "Penetration Testing Website E-Journals Metode NIST SP 800-115 dan OWASP," vol. 9, p. 2025, doi: 10.47002/metik.v9i1.1030.

[10] A. Zainal Abidin, H. Saputra, and M. Taufiq Sumadi, "Penetration testing on mail server website using the OWASP method," 2023. [Online]. Available: www.ejournal.isha.or.id/index.php/Mandiri

[11] N. Daniasti Darno, E. Lesmana Tjiong, F. Ilmu Komputer dan Desain, and U. Kalbis Jalan Pulomas Selatan Kav, "Analisis Celah Keamanan Pada Website PDDIKTI Menggunakan Metode Penetration Testing Dan Framework ISSAF," *Jurnal Sains dan Teknologi*, vol. 12, no. 02, 2025