JURNAL TEKNOLOGI TECHNOSCIENTIA ISSN: 1979-8415
Vol. 15 No. 2 Maret 2023 E-ISSN: 2714-8025

ANALISIS KEAMANAN SEBUAH DOMAIN MENGGUNAKAN *OPEN WEB APPLICATION SECURITY PROJECT* (OWASP) Zap

Verry Budiyanto[1], Nuniek Herawatie[1], Uminingsih[1].
[1] Jurusan Rekayasa Sistem Komputer, Fakultas Sains dan Terapan, IST AKPRIND
Email: [1]nuniekh@akprind.ac.id

Masuk: 8 Agustus 2022, Revisi masuk: 31 Maret 2022, Diterima: 31 Maret 2022

ABSTRACT

Along with the development of information technology in the wider community, information systems make it easier for people to access and search for information in the form of websites. The problem of security risk is one of the important aspects of an information system. But security risks are somehow less priority to be considered. In the present work, a security analysis of a domain was conducted using the Open Web Application Security Project (OWASP) Zap. The research method used is literature review and observation. The literature review is used to collect relevant previous research literature as well as relevant theories and concepts in terms of Vulnerability Analysis. The literatures is obtained from journals, books, scientific papers, and digital media such as the internet. While observation is used to determine, sort, collect, and review the data needed in the test. The results show that several vulnerabilities on the akprind.ac.id site have a detrimental impact on the campus. The security system on several akprind subdomains still does not meet the CIA TRIAD security principle, namely confidentiality. The OWASP Zap tools are still good as a basis for conducting penetration testing on several sites with the akprind.ac.id domain. Because there are still some security issues that match the owasp list. It is hoped that for the IST AKPRIND web, further research needs to be carried out using the ISSAF (Information System Security Assessment Framework) method so that it can be known more deeply if there are vulnerabilities from the web server.

Keywords: security analysis, Owasp, *vulnerability analysis*

INTISARI

Seiring berkembangnya teknologi informasi dikalangan masyarakat luas, maka sistem informasi dapat memudahkan masyarakat untuk mengakses dan mencari informasi dalam bentuk *website*. Permasalahan resiko keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Namun seringkali resiko keamanan berada di urutan terakhir dalam hal-hal yang dianggap penting. Dalam penelitian ini dilakukan analisis keamanan sebuah domain menggunakan *Open Web Application Security Project* (OWASP) Zap. Metode penelitian yang digunakan adalah studi kajian pustaka dan observasi. Kajian pustaka digunakan untuk mengumpulkan data pustaka penelitian sebelumnya yang relevan serta teori-teori dan konsep-konsep yang relevan dalam hal *Vulnerability Analysis*. Pustaka diperoleh dari jurnal, buku, paper ilmiah, dan media digital seperti internet. Sedangkan observasi digunakan untuk menentukan, memilah, mengumpulkan, dan mengkaji ulang data data yang dibutuhkan dalam pengujian. Hasil penelitian ini adalah didapatkan beberapa kerentanan pada situs akprind.ac.id yang dapat berdampak merugikan pihak kampus, Keamanan sistem pada beberapa *subdomain* akprind masih belum memenuhi prinsip keamanan CIA TRIAD yaitu *confidentiality*. Tools OWASP Zap masih bagus dijadikan sebagai dasar dalam melakukan uji *penetration testing* pada beberapa *situs* yang berdomain akprind.ac.id. Karena masih ditemukan beberapa celah keamanan yang sesuai dengan daftar owasp. Diharapkan untuk web IST AKPRIND perlu dilakukan penelitian lebih lanjut dengan metode ISSAF (*Information System Security Assessment Framework*) agar dapat diketahui lebih mendalam jika terdapat kerentanan dari sisi *web server.*

Kata-kata kunci: analisis keamanan, owasp, analisis *vulnerability.*

https://doi.org/10.34151/technoscientia.v15i2.4013

PENDAHULUAN

Seiring berkembangnya teknologi informasi dikalangan masyarakat luas, sistem informasi dapat memudahkan masyarakat untuk mengakses dan mencari informasi dalam bentuk website. Teknologi informasi atau *Information Technology* (IT) memiliki peran penting untuk mendukung kinerja dan aktivitas sebuah perusahaan, organisasi, dan perguruan tinggi untuk dapat bertahan dan meraih keunggulan kompetitif. Namun dalam pengelolaannya, IT membutuhkan penanganan yang profesional karena IT selalu memiliki resiko keamanan.

Menurut APJI (Asosiasi Penyelenggara Jasa Internet Indonesia, 2019) penetrasi pengguna internet di Indonesia meningkat dari tahun ke tahun. Sejak 10 tahun yang lalu pengguna selalu naik minimal + 10.000.000 pengguna setiap tahunnya. Pada tahun 2018 mengalami peningkatan + 27.900.000 pengguna dibandingkan tahun 2017. Resiko keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Namun seringkali resiko keamanan berada di urutan terakhir dalam hal-hal yang dianggap penting. Apabila mengganggu performa system seringkali keamanan dikurangi. Hal itu berbanding terbalik dengan semakin banyaknya celah keamanan khususnya keamanan website.

Kejahatan di dunia cyber dalam bidang penetrasi di Indonesia sering terjadi karena salah satu faktor kurangnya kelengkapan penulisan kode program yang dapat menimbulkan celah celah keamanan pada website. Celah keamanan pada website inilah yang dimanfaatkan oleh seseorang untuk menyerang sebuah website. Oleh karena itu pada penelitian ini mengangkat tema skripsi dengan judul "Analisis Keamanan sebuah domain menggunakan *Open Web Application Security Project* (Owasp) Zap". Sehingga jika terdapat kerentanan pada website bisa segera dilakukan perbaikan agar dapat terhindar dari dampak buruk orang yang kurang bertanggung jawab.

Penelitian lain yang dilakukan oleh (Guntoro, Costaner and Musfawati, 2020) yang berjudul "Analisis Keamanan Web Server Open Journal System (OJS) Menggunakan Metode Issaf Dan Owasp (Studi Kasus OJS Universitas Lancang Kuning)" dalam Jurnal Ilmiah Vol.5, No.1, Juni 2020, E-ISSN: 2540-8984 Universitas Lancang Kuning Riau yang membahas tentang pengujian keamanan pada sebuah situs web perusahaan menggunakan metode OWASP versi 4 dengan modul *Testing for Information Gathering*. Tujuan penelitian ini adalah bagaimana menganalisis keamanan sistem Open Journal System (OJS) menggunakan metode ISSAF dan OWASP pada Universitas Lancang Kuning. Hasil pengujian penelitian ini adalah untuk mencari vulnerability pada web server Open Journal System (OJS).

Penelitian lain yang dilakukan oleh (Rochman et al., 2021) yang berjudul "Analisis Keamanan Website Dengan Information System Security Assessment Framework (Issaf) Dan Open Web Application Security Project (Owasp) Di Rumah Sakit Xyz" dalam Jurnal Indonesia Sosial Teknologi Vol.2, No.4, April 2021, E-ISSN ; 2745-5254, STMIK LIKMI. Yang membahas tentang pengujian celah keamanan (*penetration testing*) pada *website* sistem HRD. Penelitian ini bertujuan untuk mengetahui apakah terdapat celah celah keamanan pada website sistem HRD. Hasil dari penelitian ini ditemukan beberapa kelemahan yang terdapat pada website target, kelemahan tersebut dapat dieksploitasi hingga database target dapat diakses oleh pihak yang tidak berwenang atau tidak memiliki akses.

Penelitian lain yang dilakukan oleh (Yunus, 2019) dengan judul "Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework OWASP Versi 4". Pada Jurnal Ilmiah Ilmu Komputer dan Teknologi Informasi Jawa Barat, Vol.24 No.1, April 2019 Universitas Gunadarma Depok, Jawa Barat yang membahas tentang variabel variabel keamanan sistem. Penelitian ini bertujuan untuk menganalisa keamanan aplikasi berbasis web dengan

https://doi.org/10.34151/technoscientia.v15i2.4013

framework OWASP versi 4 dengan kolaborasi beberapa tools security project untuk mengetahui keamanan suatu aplikasi, sehingga dapat dijadikan sebagai standar penilaian keamanan untuk aplikasi berbasis web. Hasil dari penelitian ini diketahui bahwa analisis kerentanan aplikasi berbasis web dengan teknik OWASP versi 4 mampu mengetahui keamanan suatu aplikasi. Definisi penting yang berhubungan dengan penelitian ini adalah sebagai berikut:

Open Web Application Security Project

Owasp merupakan sebuah organisasi nirlaba yang berfokus pada keamanan *web app*. OWASP banyak menawarkan sumber daya supaya kita bisa mempelajari lebih lanjut mengenai keamanan *web app*.

Domain

Menurut (Tedyyana and Kurniati, 2016), DNS (*Domain name system*) Adalah sebuah aplikasi *service* di internet yang menerjemahkan *domain* name ke IP *address* dan salah satu jenis *system* yang melayani permintaan pemetaan IP *address* ke FQPN (*Fany Qualified Domain Name*) dan dari FQDN ke IP *address*.

Dns Server

DNS server adalah server yang menghubungkan URL (*uniform resource locator*) dengan IP *Address* (*internet protocol address*). Sebelum domain dan DNS server hadir di internet, kita perlu memasukkan IP *address* sebuah *website* saat ingin mengaksesnya. DNS server adalah sebuah *database* server yang berfungsi untuk menyimpan alamat alamat IP yang digunakan oleh *host name*

Owasp Zap

Owasp Zap adalah aplikasi untuk melakukan penetrasi testing (pentest) dalam menemukan celah dalam suatu website, aplikasi ini juga menyediakan scanner secara otomatis

Keamanan Informasi

Menurut (ISO/IEC, 2018) Keamanan informasi merupakan perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, dan meningkatkan *return of investment* (ROI) serta peluang bisnis. Dalam menerapkan keamanan informasi, perusahaan organisasi harus memperhatikan 3 aspek yaitu *Confidentiality*, *Integrity*, dan *Availability* (CIA)

1). Confidentiality

Confidentiality dideskripsikan sebagai suatu properti bahwa informasi tidak akan tersedia atau diungkapkan kepada individu, entitas, atau proses yang tidak sah. Tidak hanya itu kerahasiaan juga harus dijaga dari kebocoran informasi yang disebabkan oleh suatu individu atau entitas dari dalam maupun dari luar perusahaan organisasi.

2). Integrity

Integrity berhubungan dengan akurasi dan kelengkapan data dan informasi. Data dan informasi yang berada di dalam perusahaan atau organisasi harus dijaga dalam keadaan yang benar dan tidak seorang pun boleh memodifikasinya dengan tidak semestinya, baik secara tidak sengaja atau ingin melakukan kejahatan.

3). Availability

Availability (Ketersediaan) adalah kemudahan akses dan penggunaan yang sesuai dengan permintaan oleh entitas yang berwenang. Maksud dari definisi tersebut adalah pengguna yang memiliki kewenangan dapat mengakses data dan informasi dimanapun dan kapanpun mereka perlu untuk melakukannya.

Vulnerability Assessment

Menurut (Priandoyo, 2006) Vulnerability Assessment adalah proses untuk mengidentifikasi, mengevaluasi, dan mengklasifikasikan tingkat kerentanan keamanan yang terdapat pada sebuah jaringan komputer, sistem, aplikasi, atau bagian lain yang ada di ekosistem IT berdasarkan risiko yang dapat ditimbulkan di sebuah instansi. Metode Vulnerability assessment yang akan digunakan dalam penelitian ini meliputi.

1. Network based scan
   Network based scans atau pemindaian berbasis jaringan merupakan penilaian keamanan untuk mengidentifikasi kemungkinan serangan pada keamanan jaringan. Pemindaian ini juga dapat

https://doi.org/10.34151/technoscientia.v15i2.4013

mendeteksi sistem yang rentan pada jaringan berkabel atau nirkabel

2. Host based scan
   Host based scans atau pemindaian berbasis host dilakukan untuk menemukan dan mengidentifikasi kerentanan yang ada di server, workstations, atau host jaringan lainnya. Ketika pemindaian ini dilakukan, yang dilakukan adalah memeriksa services dan ports yang mungkin juga terlihat pada network based scan.
3. Application based scan
   Application scan atau pemindaian aplikasi digunakan untuk mengidentifikasi kerentanan keamanan dan konfigurasi yang salah dalam web application serta source code yang digunakan. Biasanya pemindaian dilakukan menggunakan scanning tools otomatis pada bagian analisis source code front-end atau statis / dinamis

Penetration Testing

Meucci dan Matteo pada (OWASP, 2014) menjelaskan bahwa Penetration testing adalah teknik umum yang digunakan untuk menguji keamanan jaringan. Tujuan utama dari Penetration Testing adalah untuk mengidentifikasi celah-celah yang terdapat dalam sistem keamanan organisasi khususnya sistem komputer. Berikut ini adalah beberapa strategi yang digunakan oleh seorang pentesting.

Targeted testing, yaitu menggunakan skenario penguji keamanan beserta staf nya melakukan uji celah keamanan secara bersama-sama. External testing, yaitu mentargetkan server atau perangkat teknologi yang digunakan yang terlihat secara eksternal. Target dari penguji adalah server, nama domain, server, server web, atau firewall.

Internal testing,yaitu melakukan percobaan serangan menggunakan pola pikir orang dalam. Atau pihak yang memang mempunyai akses ke perangkat seperti server dan sistem yang lain. Double testing, hampir sama dengan blind testing, hanya saja ditambah dengan staf yang ada di organisasi atau perusahaan sudah mengetahui jika ada serangan di dalam sistemnya.

Black box testing, yaitu mempunyai kesamaan dengan blind testing, penguji hanya diberikan sedikit informasi misal nama perusahaan, kemudian penguji melakukan berbagai cara untuk mengumpulkan informasi.
White box testing, tidak seperti black box testing, pengujian strategi ini Penetration tester mendapat informasi lebih lengkap tentang jaringan target sebelum memulai pekerjaan mereka. Informasi ini dapat mencakup rincian seperti alamat IP, skema infrastruktur jaringan, dan protokol yang digunakan ditambah source code dari aplikasi yang digunakan.

Berdasarkan latar belakang di atas, dalam penelitian ini dilakukan pengujian menggunakan OWASP Zap sebagai *tools vulnerability scanner*. Perbedaan penelitian saat ini dengan penelitian sebelumnya adalah objek yang digunakan serta penggunaan tools pendukung untuk melakukan pemindaian kerentanan pada sebuah domain. Penulis menggunakan tools utama diantaranya, OWASP Zap, Nmap, Wpscan, Nikto. Dalam penelitian juga disertakan pengujian load balancing yang berfungsi untuk mendistribusikan beban pekerjaan pada dua atau bahkan lebih suatu koneksi jaringan secara seimbang agar pekerjaan dapat berjalan optimal dan tidak overload (kelebihan) beban pada salah satu jalur koneksi. Berikut ini adalah metodologi yang digunakan pada penelitian penetration testing terhadap objek domain yang sudah ditentukan.

Information Gathering

Tahapan ini dilakukan untuk mendapatkan informasi sebanyak banyaknya yang terkait dengan situs akprind.ac.id, seperti Ip address subdomain, dan beberapa informasi lain nya. Adapun tools pendukung dalam tahapan ini adalah

1. Whois

https://doi.org/10.34151/technoscientia.v15i2.4013

Whois adalah suatu prosedur untuk mendapatkan informasi mengenai sebuah domain. Informasi yang bisa di dapat meliputi siapa pemilik Domain, dimana alamatnya, no telepon, alamat email, kapan domain ini didaftarkan dan kapan domain ini akan expired.

2. Google Chrome
   Google Chrome adalah peramban web lintas platform yang dikembangkan oleh Google
3. Virus total
   Website ini digunakan untuk mencari subdomain dari akprind.ac.id yang akan dilakukan pengujian.
4. Whatweb
   Whatweb adalah salah satu dari sekian banyak tools scanning yang dapat digunakan untuk mengumpulkan informasi tentang lokasi server, Os server dan sebagainya.

Vulnerable Scanning

Pada tahap ini, hasil dari tahapan Information Gathering akan dilakukan vulnerability scanning pada target menggunakan Nikto dan Nmap yang berfungsi untuk mencari informasi yang lebih detail terhadap beberapa subdomain yang akan dilakukan pengujian kerentanan nya, dibawah ini adalah penjelasan dari scanning nmap dan nikto.

1. Nikto
   Tools ini berperan penting dalam tahapan ini, karena pada tahap ini informasi yang didapatkan berupa gambaran umum kerentanan yang terdapat pada website target dengan menggunakan perintah Nikto -h [localhost] -p [seri port]
2. Nmap
   Nmap (Network Mapper) adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan *port scanning*. Dengan menggunakan tool ini, kita dapat melihat host yang aktif, port yang terbuka, Sistem Operasi yang digunakan, dan feature-feature scanning lainnya

Vulnerability Analysis

Pada tahap ini peneliti akan menganalisis kerentanan yang ditemukan setelah dilakukan scanning terhadap target dengan beberapa tool web vulnerability analysis serta akan memberikan rekomendasi bagaimana memperbaiki kerentanan yang telah ditemukan.

Pada langkah ini tools yang digunakan adalah:

1) Wpscan
   WPScan merupakan *tools* yang berfungsi untuk menganalisa kerentanan CMS *WordPress* yang ditulis dengan menggunakan bahasa pemrograman ruby, WPScan mampu mendeteksi kerentanan umum serta daftar semua *plugin* dan *themes* yang terdapat pada sebuah *website* yang menggunakan CMS *WordPress*
2) Owasp Zap
   Hasil dari tahapan ini akan didapatkan kesimpulan, apakah website yang tersebut mempunyai masalah yang cukup serius ataupun tidak. Tools ini cara menjalankan bisa menggunakan secara otomatis ataupun dengan cara manual, dan hasil dari aktivitas menggunakan tools ini cukup lengkap untuk dijadikan *penetration* testing sebuah website sebelum dilakukan publikasi atau website yang masih dalam pengembangan

Pentesting

Pada tahap ini jika pada tahap vulnerability scanning dan vulnerability analysis terdapat kerentanan ataupun tidak terdapat kerentanan penguji akan melakukan pengujian pada beberapa aspek keamanan terhadap domain yang akan dilakukan pengujian.

HASIL DAN PEMBAHASAN

Pada tahap ini, dilakukan pengelompokan hasil dari *vulnerability assessment* menurut fungsi dari tools tersebut.

Information Gathering

https://doi.org/10.34151/technoscientia.v15i2.4013

ISSN: 1979-8415
E-ISSN: 2714-8025

Adapun tahapan awal sebelum melakukan pentest adalah pengumpulan informasi sebanyak mungkin tentang situs target, berikut ini adalah hasil dalam information gathering beserta tools yang digunakan.

1. Search engine
   Langkah awal tahapan ini adalah mencari website utama yang dimiliki oleh IST AKPRIND menggunakan google chrome dan didapatkan situs utama dari akprind adalah https://akprind.ac.id dengan ip 103.155.125.231.
   Dengan menggunakan tools whois, penulis mendapatkan gambaran umum tentang situs target berupa block Ip dari 103.155.125.0 sampai dengan 103.155.125.255, e-mail pengurus admin, nomor personal chat dan lain lain.

   Tahapan selanjutnya mencari subdomain dari situs target yang akan dilakukan pengujian menggunakan situs virus total yang terdapat pada browser chrome, hasil dari tahapan ini penulis menggunakan subdomain berikut yang akan dilakukan pengujian kemungkinan celah keamanan (siskom.akprind.ac.id, fst.akprind.ac.id, sister.akprind.ac.id, dan kemahasiswaan.akprind.ac.id)

2. Whatweb
   Whatweb adalah salah satu dari sekian banyak tools scanning yang tersedia, Whatweb dapat mengumpulkan informasi tentang lokasi server, Os server yang digunakan dan lain sebagainya, untuk hasil dari Whatsweb terhadap domain yang akan dilakukan analisis adalah sebagai berikut
   a) Siskom.akprind.ac.id
      Hasil dari scanning situs siskom.akprind.ac.id menunjukan bahwa situs ini menggunakan layanan nginx, bahasa pemrograman yang digunakan adalah Javascript, library yang digunakan JQuery versi 3.6.0, Wordpress yang digunakan versi 5.8.2.
   b) Fst.akprind.ac.id
      Hasil dari scanning situs fst.akprind.ac.id menunjukan bahwa menggunakan server nginx, Bahasa pemrograman Javascript situs tersebut menggunakan CMS Wordpress versi 5.8.2, library yang digunakan adalah JQuery versi 3.6.0 dan header yang terpasang adalah HSTS
   c) Kemahasiswaana.ac.id
      hasil dari scanning situs kemahasiswaan.akprind.ac.id menunjukan bahwa menggunakan server apache, Bahasa pemrograman Javascript, situs tersebut menggunakan CMS Wordpress versi 5.8.2, library yang digunakan adalah JQuery versi 3.6.0 dan versi Html yang digunakan versi 5.
   d) Sister.akprind.ac.id
      Hasil dari scanning situs sister.akprind.ac.id menunjukan bahwa menggunakan Os Ubuntu dan web server menggunakan apache versi 2.4.18, Bahasa pemrograman Javascript, situs tersebut menggunakan PHP laravel framework, library yang digunakan adalah JQuery versi 2.1.1, situs tersebut juga dideteksi menggunakan bootstrap untuk framework Html

Vulnerability Scanning

Langkah ini merupakan lanjutan dari proses Information Gathering, tujuan melakukan proses ini untuk mengidentifikasi kelemahan yang kemungkinan dapat dimanfaatkan untuk proses eksploitasi. Berikut ini adalah hasil dari tahapan vulnerability scanning dari beberapa tools yang digunakan.

https://doi.org/10.34151/technoscientia.v15i2.4013

ISSN: 1979-8415
E-ISSN: 2714-8025

Tools pertama yang digunakan pada tahap *vulnerability scanning* adalah nikto, *tools* ini dapat digunakan untuk mengetahui secara umum kerentanan apa saja yang terdapat pada situs target, berikut adalah hasil dari pengujian nikto

a) Siskom.akprind.ac.id
   Hasil dari vulnerability *scanning* terhadap situs siskom adalah tidak terdapat beberapa *header security*, diantaranya adalah (x-frame-option, x-xss-protection, strict-transport-security, expect-ct, dan x-content-type-option.
b) Fst.akprind.ac.id
   Hasil dari *vulnerability scanning* terhadap situs fst adalah tidak terdapat beberapa *header security,* diantaranya adalah x-frame-option, x-xss-protection, dan x-content-type-option, serta situs ini ditemukan halaman root/ redirect halaman dari https://fst.akprind.ac.id
c) Kemahasiswaan.akprind..ac.id
   Hasil dari vulnerability scanning terhadap situs kemahasiswaan adalah tidak terdapat beberapa *header security,* diantaranya adalah x-frame-option, x-xss-protection, expect-ct, dan x-content-type-option
d) Sister.akprind.ac.id
   Hasil dari *vulnerability scanning* terhadap situs sister adalah tidak terdapat beberapa *header security,* diantaranya adalah x-frame-option, x-xss-protection, dan x-content-type-option. Header yang digunakan situs ini adalah Access-control-allow-origin: *. Situs ini juga ditemukan redirect pages dari https://sister.akprind.ac.id/auth/login

Pada tahap ini informasi Ip yang diperoleh dari situs target akan dilakukan port scanning mengenai status port dan service apa saja yang berjalan pada port tersebut, hasil dari tahap ini sebagai berikut.

a) Siskom.akprind.ac.id dan Fst.akprind.ac.id
   Ip yang berstatus Open dan beserta service yang berjalan pada port tersebut adalah: 53 (Domain), 80 service (http), 443 service(http), 888 service(http), 3371 service(http).
b) Kemahasiswaana.ac.id
   Ip yang berstatus Open, status dan beserta service yang berjalan pada port tersebut adalah: 20(open) service(Tcpwrapped), 21(open) service(Tcpwrapped), 22(open) service(Ssh), 23(open) service(telnet), 25(open) service(Smtp), 53(open) service(Domain), 80(open) service(http).
c) Sister.akprind.ac.id
   Ip yang berstatus Open, status dan service yang berjalan pada port tersebut adalah: 21(filtered) service (ftp), 22(filtered) service (ftp), 23(ssh) service (telnet), 80(open) service (http), 139(filtered) service (Netbios-ssn), 445(filtered) service (Microsoft-ds), 646(filtered) service (ldp), 3389(filtered) service (Ms-wbt-server), 4444(filtered) service (Krb524), 8291(filtered) service (Unknown), 9999(filtered) service (Abyss).

Vulnerability Analysis

Pada tahap analisis ini, kerentanan yang didapat dari pengujian diatas dianalisis dan solusi dari kerentanan tersebut, berikut adalah hasil dari tahapan ini terhadap beberapa domain yang dilakukan pengujian

Wpscan dikhususkan untuk website yang menggunakan Wordpress, selain itu tools ini tidak berjalan seperti semestinya, hasil pengujian menggunakan tools Wpscan ini adalah sebagai berikut

a) Siskom.akprind.ac.id
   Ditemukan beberapa user login pada situs ini, diantaranya adalah J*k* Triy*n*, z*inj*ck, dll. Selain ditemukan kemungkinan user login situs ini juga ditemukan mengaktifkan XML-RPC, Website terdeteksi menggunakan plugin, Website ini mengaktifkan WP-Cron.
b) Fst.akprind.ac.id
   Ditemukan beberapa user login pada situs ini, diantaranya adalah

https://doi.org/10.34151/technoscientia.v15i2.4013

ISSN: 1979-8415
E-ISSN: 2714-8025

kem*hasisw**n. Selain ditemukan kemungkinan user login situs ini juga ditemukan robot.txt, Website ini mengaktifkan XML-RPC, Website ini mengaktifkan WP-Cron, Wordpress yang digunakan versi 5.8.2.

c) Kemahasiswaana.ac.id
Ditemukan beberapa user login pada situs ini, diantaranya adalah k*m-fst. Selain ditemukan kemungkinan user login situs ini juga ditemukan robot.txt dan Website ini mengaktifkan XML-RPC

Owasp Zap adalah alat pengujian penetrasi terintegrasi yang mudah digunakan untuk menemukan kerentanan dalam aplikasi web. Tabel 1 ini adalah hasil pengujian kerentanan pada domain target beserta solusi mengatasi kerentanan tersebut.

Tabel 1. Jenis kerentanan server dan solusi keamanan

Situs	Jenis kerentanan	Server	Solusi
Siskom Fst Kemahasiswaan	X-frame-option Header Not Set	Nginx	Menambahkan Script berikut pada file /etc/nginx/sites-enabled/example.conf add_header X-Frame-Options "SAMEORIGIN";
Sister		Apache	menambahkan header X-frame-option pada website, tambahkan script berikut di /etc/Apache2/sites-enabled/example.conf Header always set X-Frame-Options "SAMEORIGIN"
Siskom Fst Kemahasiswaan	Absence Of Anti CSRF Tokens	Nginx	Menerapkan generate token pada php dengan perintah seperti berikut $_SESSION['token'] = bin2hex(random_bytes(24));
Siskom Fst	Cookie No Http Only Flag	Nginx	Menyetel flag cookie sebagai Httponly dan secure di header response Http Set-Cookie, tambahkan perintah berikut pada file konfigurasi nginx.conf add_header Set-Cookie "Path=/; HttpOnly; Secure"; Opsi alternatif lain adalah menambahkan sintaks di bawah ini pada ssl.conf atau default.conf proxy_cookie_path / "/; HTTPOnly; Secure";
Sister		Apache	pastikan sudah mengaktifkan mod_header.so pada server apache. Kemudian tambahkan perintah berikut pada file apache.conf yang terletak pada /etc/apache2/apache2.conf Header edit Set-Cookie ^(.*)$ $1;HttpOnly
Siskom Fst	Cookie Without Same Site Attribute	Nginx	pastikan atribut SameSite diatur ke 'lax' atau idealnya 'strict' untuk semua cookie. Contoh perintah yang digunakan adalah Set-Cookie: flavor=choco; SameSite=Lax
Sister		Apache	pastikan atribut SameSite diatur ke 'lax' atau idealnya 'strict' untuk semua cookie. Contoh dari perintah yang digunakan adalah Set-Cookie: flavor=choco; SameSite=Lax
Siskom Fst Kemahasiswaan	Incomplete Or No Cache Control Header Set	Nginx	Pastikan header HTTP 'Cache-control' disetel dengan 'no-cache, no-store, must-revalidate' dan header 'Pragma' diatur ke 'no-cache' pada respons HTTP jika memungkinkan. Cache-Control: no-cache, no-store, must-revalidate Pragma: no-cache
Siskom Kemahasiswaan	Secure Pages Include Mixed Content	Nginx	Kita perlu merubah file konfigurasi yang terletak pada /etc/nginx/conf menjadi seperti dibawah ini Server { Listen 80 default_server Server_name_; Return 301

https://doi.org/10.34151/technoscientia.v15i2.4013

			https://$host$request_uri; }
Siskom Fst Kemahasiswaan	Time Stamp Disclosure Unix	Nginx	Solusi dari Timestamp Disclosure-Unix ialah dengan mengkonfirmasi secara manual bahwa data stempel waktu tidak sensitif dan data tidak dapat dikumpulkan untuk mengungkap pola yang dapat dieksploitasi.
Sister		Apache	
Siskom Fst Kemahasiswaan	X-Content Type Option Header Missing	Nginx	Menambahkan header X-Content-type-option pada Nginx yang berlokasi di /etc/nginx/sites-enabled/webdock dengan perintah dibawah ini. add_header X-Content-Type-Options nosniff;
Sister		Apache	menambahkan header X-Content-type-option pada file konfigurasi Apache yang berlokasi /etc/apache2/apache2.conf/example.conf untuk scriptnya seperti berikut <IfModule mod_headers.c> Header always set X-Content-Type-Options nosniff </IfModule>
Sister	Cross Domain Miss configuration	Apache	pastikan header Access-Control-Allow-Origin tidak terlalu permisif (tidak memiliki wildcard * sebagai nilainya). Tambahkan perintah berikut pada httpd.conf atau apache.conf Header set Access-Control-Allow-Origin "domain"
Sister	Vulnerable Java script Library	Apache	solusi dari permasalahan ini adalah perlu dilakukan update versi agar performa tetap terjaga kestabilan performa dari framework tersebut.

Reporting

Pada tahap ini dilakukan pengujian terhadap kemungkinan celah keamanan yang telah ditemukan pada tahap sebelumnya.

1) Denial Of Service
   Pengujian kemungkinan celah keamanan DoS perlu dilakukan, Disini penguji menggunakan tools hping3 dalam melakukan serangan DoS terhadap web target serangan ini bertipe three way handshake dimana penyerang membanjiri web server dengan request berupa paket SYN. namun dari serangan DoS terhadap website tersebut tidak berpengaruh terhadap serangan besar kemungkinan web siskom.akprind .ac.id sudah menggunakan load balancing.
2) Cross Site Scripting
   XSS adalah salah satu jenis serangan injeksi kode (code injection attack). XSS dilakukan oleh penyerang dengan cara memasukkan kode HTML atau client script kode lainnya ke suatu situs. Disini penguji melakukan serangan XSS secara manual dengan browser dan memasukan kode injeksi ke dalam web target. Akan tetapi serangan yang dilakukan penguji terdeteksi oleh firewall sehingga langsung dicegah oleh firewall tersebut.
3) Load balancing
   Load balancing adalah proses pembagian beban traffic sebuah aplikasi atau server. Dengan load balancer, beban traffic tidak akan dibebankan kepada beberapa jalur koneksi. Cara kerja load balancing adalah Saat server atau aplikasi kita menerima traffic dari luar, load balancer tool akan membagikan traffic tersebut ke beberapa servers yang tersedia secara rata dan optimal. Berikut ini adalah scanning load balancing pada situs akprind.ac.id. pada pengujian load balancing, penulis mendapatkan informasi bahwa situs target tidak ditemukan load balancing.

KESIMPULAN

Dari analisis uji penetration testing menggunakan tools OWASP 20 tahun 2022

https://doi.org/10.34151/technoscientia.v15i2.4013

ISSN: 1979-8415
E-ISSN: 2714-8025

yang bertujuan untuk menguji tingkat keamanan pada website yang berdomain akprind.ac.id yang dimiliki oleh Institut Sains dan Teknologi Akprind Yogyakarta maka dapat disimpulkan: *tools* OWASP Zap masih bagus dijadikan sebagai dasar dalam melakukan uji *penetration testing* pada beberapa *situs* yang berdomain akprind.ac.id. Karena masih ditemukan beberapa celah keamanan yang sesuai dengan daftar OWASP 20 tahun 2022.

1) Keamanan sistem pada beberapa *web* target masih belum memenuhi prinsip keamanan CIA TRIAD yaitu *confidentiality*. Hal tersebut dapat dilihat dari beberapa keberhasilan eksploitasi celah keamanan yang ada sehingga didapatkan informasi penting yang seharusnya memiliki hak akses khusus.
2) Domain Akprind.ac.id memiliki *firewall* yang cukup bisa diandalkan karena dalam beberapa kasus pentest seperti *Injection*, dapat terblok oleh *firewall* tersebut. Hal tersebut berguna dalam menanggulangi serangan seseorang yang tidak bertanggung jawab
3) Berdasarkan hasil penelitian yang sudah dilakukan, beberapa langkah yang dapat dilakukan untuk perbaikan keamanan website yang berdomain akprind.ac.id perlu dilakukan penelitian lebih lanjut dengan metode ISSAF (Information System Security Assessment Framework) agar dapat diketahui lebih mendalam jika terdapat kerentanan dari sisi web server. Selain itu juga diperlukan pemasangan server Load balancer agar dapat membantu server server tersebut mentransfer data secara efisien, dan mengoptimalkan penggunaan aplikasi pengiriman sumber daya sehingga terhindar dari server yang overload.

DAFTAR PUSTAKA

Guntoro, G., Costaner, L. and Musfawati, M. (2020) 'Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)', *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 5(1), p. 45.

ISO/IEC (2018) 'International Standard ISO / IEC Information technology — Security Techniques — Information Security Management Systems — Overview and', *ACM Workshop on Formal Methods in Security Engineering.Washington, DC, USA*, 34(19), pp. 45–55.

OWASP (2014) '4.0 Testing Guide', *OWASP foundation*, (Cc), p. 224.

Priandoyo, A. (2006) 'Vulnerability Assessment untuk Meningkatkan Kesadaran Pentingnya Keamanan Informasi', *Ernst & Young*, 1(2), pp. 73–83.

Rochman, A. *et al.* (2021) 'Di Rumah Sakit Xyz', *Analisis Keamanan Website Dengan Information System Security Assessment Framework (Issaf) Dan Open Web Application Security Project*, 2(4).

Tedyyana, A. and Kurniati, R. (2016) 'Membuat Web Server Menggunakan Dinamic Domain', *Jurnal Teknologi Informasi & Komunikasi Digital Zone*, 7(1), pp. 1–10.

Yudiana, Y., Elanda, A. and Buana, R.L. (2021) 'Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10', *CESS (Journal of Computer Engineering, System and Science)*, 6(2), p. 185.

Yunus, M. (2019) 'Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4', *Jurnal Ilmiah Informatika Komputer*, 24(1), pp. 37–48.

Zen, B.P., Gultom, R.A.G. and Reksoprodjo, A.H.S. (2020) '*Analisis Security Assessment* Menggunakan Metode *Penetration Testing* dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara', *Jurnal Teknologi Penginderaan*, 2(1), pp.

https://doi.org/10.34151/technoscientia.v15i2.4013

ISSN: 1979-8415
E-ISSN: 2714-8025

105–122.

https://doi.org/10.34151/technoscientia.v15i2.4013