Jurnal Borneo Informatika & Teknik Komputer **p-ISSN:** 2808-8190
Vol. 4, No. 1, 2024. Hlm 26—35 **e-ISSN:** 2808-6600

ANALISIS KEAMANAN *WEBSITE* SIAKAD UNTIRTA MENGGUNAKAN TEKNIK *FOOT PRINTING* DAN *VULNERABILITY SCANNING*

Alim Hardiansyah[1], Holilah[2], A'idah Eka Septiana[3], Manisa Rahmalia Eka Putri[4]
[1,2,3]Universitas Sultan Ageng Tirtayasa, Serang, Banten, 78124, Indonesia

e-mail: [*1]alim.hardiansyah@untirta.ac.id

Diterima	Direvisi	Disetujui
29-07-2024	12-08-2024	28-08-2024

Abstract: *Sultan Ageng Tirtayasa University (Untirta) is one of Indonesia's state universities, located specifically in Banten Province. Untirta utilizes its website and internet to support both academic and non-academic activities. One of the websites used is the Academic Information System (SIAKAD). SIAKAD can only be accessed by users with official accounts provided by the university, including faculty, students, and academic administration, to manage academic administration such as course registration, grade transcripts, schedules, classroom assignments, and others. SIAKAD sometimes experiences disruptions, such as accessibility issues which may occur due to server downtime and other factors. SIAKAD can face security issues such as brute force attacks, SQL Injection, and others. Security and confidentiality of data in SIAKAD must be carefully maintained to ensure that data cannot be accessed by unauthorized parties through mechanisms like usernames and passwords. Furthermore, ensuring that the information remains intact without any changes, and providing undeniable proof, is crucial. To ensure these aspects are met, techniques such as Foot Printing can be employed to analyze and enhance the security of the SIAKAD website. This research adopts an Ethical Hacking approach, focusing on Foot Printing to gather information about the SIAKAD website and identify vulnerabilities with varying degrees of risk, from low to high.*

Keywords*: Foot Printing, Vulnerability Scanning, Security, SIAKAD Untirta*

Abstrak: Universitas Sultan Ageng Tirtayasa (Untirta) merupakan salah satu perguruan tinggi negeri di Indonesia tepatnya berada di Provinsi Banten. Untirta memanfaatkan website dan internet untuk menunjang kegiatan akademik maupun non-akademik. Salah satu website yang digunakan adalah Sistem Informasi Akademik (SIAKAD). SIAKAD hanya dapat digunakan oleh pengguna yang memiliki akun resmi yang diberikan pihak universitas yang melibatkan dosen, mahasiswa, dan administrasi akademik untuk mengelola administrasi akademik seperti Pendaftaran KRS, Transkrip Nilai, Jadwal, Ruangan Perkuliahan, dan lainnya. SIAKAD terkadang mengalami gangguan seperti tidak dapat diakses hal ini dapat terjadi karena mengalami server down, dan beberapa faktor lainnya. SIAKAD dapat mengalami masalah keamanan seperti brute force, SQL Injection, dan lainnya, masalah keamanan dan kerahasiaan data dalam SIAKAD harus lebih diperhatikan untuk memastikan data tidak dapat diakses oleh pihak yang tidak berwenang melalui mekanisme seperti username dan password selain itu agar informasi yang didapatkan tetap utuh tanpa perubahan, serta pembuktian yang tidak dapat disangkal. Untuk memastikan aspek tersebut terpenuhi dapat dilakukan melalui teknik *Foot Printing* agar dapat dilakukan analisis untuk memastikan keamanan terhadap Website SIAKAD. Penelitian ini dilakukan dengan pendekatan *Ethical Hacking*, yang berfokuskan terhadap *Foot Printing* yang akan memberikan informasi mengenai Website SIAKAD dan beberapa kerentanan dengan berbagai tingkat resiko dari rendah hingga tinggi.

Kata kunci: Foot Printing, Vulnerability Scanning, Keamanan, SIAKAD Untirta

I. PENDAHULUAN

Dengan pesatnya perkembangan teknologi informasi di masyarakat, sistem yang memungkinkan orang mengakses dan mencari informasi melalui internet terus berkembang. Teknologi informasi sangat penting untuk mendukung aktivitas dan kinerja bisnis dan organisasi. Namun, pengelolaan keamanan IT sering diabaikan dan dianggap kurang penting.

Di era digital yang terus berkembang, keamanan informasi menjadi semakin penting. Memahami teknik *Foot Printing* dan reconnaissance sangat penting untuk melindungi sistem informasi. Sebagai tahap awal dalam penelusuran informasi, *Foot Printing* memungkinkan profesional keamanan untuk memahami infrastruktur dan kerentanan yang mungkin dimanfaatkan oleh pihak yang tidak berwenang. Pengumpulan data menyeluruh, baik internal maupun eksternal, memberikan pemahaman lebih lanjut.

Untuk memberikan informasi yang cepat, mudah, dan akuntabel, seluruh masyarakat, termasuk pemerintah, membutuhkan teknologi informasi. Namun, jika keamanan website diabaikan, hacker dapat mencuri informasi penting atau merusak tampilan nya. Hal ini menunjukkan betapa pentingnya menjaga data pribadi, akurat, dan autentikasi di sebuah situs web.

Website adalah kumpulan halaman informasi yang dapat diakses secara global selama terhubung dengan internet. Keamanan informasi pada website, termasuk yang dikelola oleh institusi pendidikan tinggi di Indonesia, harus dijaga dengan baik. Jika informasi pada website diakses oleh pihak yang tidak bertanggung jawab, keakuratan informasi tersebut bisa dipertanyakan dan bahkan bisa menjadi menyesatkan. Ethical hacking adalah metode yang menggunakan aplikasi hacking, trik, dan teknik untuk mengidentifikasi kerentanan sistem guna memastikan keamanannya.

Vulnerability adalah kelemahan yang mengancam integritas, kerahasiaan, dan ketersediaan suatu aset. Ethical hacking adalah metode yang melibatkan penggunaan aplikasi hacking, trik, dan teknik untuk mengidentifikasi kerentanan sistem guna memastikan keamanannya. Berdasarkan masalah tersebut, peneliti akan melakukan pengujian terhadap website Sistem Informasi Akademik (SIAKAD) Universitas Sultan Ageng Tirtayasa (Untirta) untuk menilai seberapa rentan celah keamanan yang dapat dieksploitasi oleh peretas (hacker). Pengujian penetrasi pada jaringan adalah salah satu metode yang bisa digunakan untuk mengidentifikasi kerentanan keamanan pada website. Kerentanan pada keamanan website harus diperhatikan oleh setiap institusi agar terhindar dari tindakan kejahatan di dunia maya (*CyberCrime*).

Berdasarkan latar belakang di atas, tujuan dari penelitian ini adalah untuk melakukan analisis keamanan website SIAKAD Untirta dengan menggunakan metode *Foot Printing* dan Scanning Vulnerability. Diharapkan penelitian ini akan menemukan masalah keamanan yang ada dan menawarkan saran untuk meningkatkan keamanan situs web.

II. METODE PENELITIAN

Metode Penelitian yang digunakan pada kali ini dengan pendekatan pada *Ethical Hacking* yang berfokus pada teknik *Foot Printing*. Objek yang digunakan pada penelitian ini adalah *Website Academic System Information* (SIAKAD) Universitas Sultan Ageng Tirtayasa.

1. Studi Literatur

Keamanan Website

Salah satu aspek penting yang harus diperhatikan oleh setiap organisasi, termasuk lembaga pendidikan tinggi, adalah keamanan website, yang merupakan upaya untuk melindungi website dari serangan hacker yang terhubung melalui jaringan. Website yang aman dapat mencegah akses yang tidak sah dan melindungi integritas, kerahasiaan, dan ketersediaan informasi yang disajikan kepada masyarakat, mahasiswa, dan alumni.

Vulnerability dan Ethical Hacking

Vulnerability, juga dikenal sebagai kerentanan, adalah kelemahan yang dapat mengancam integritas, kerahasiaan, dan ketersediaan suatu aset. Ethical Hacking melibatkan penggunaan

aplikasi hacking, trik, dan teknik untuk mengidentifikasi kerentanan dalam sistem untuk memastikan keamanannya. Ethical Hacking sering digunakan untuk menguji dan mengevaluasi keamanan sistem informasi melalui teknik Foot Printing dan vulnerability scanning.

Teknik Foot Printing

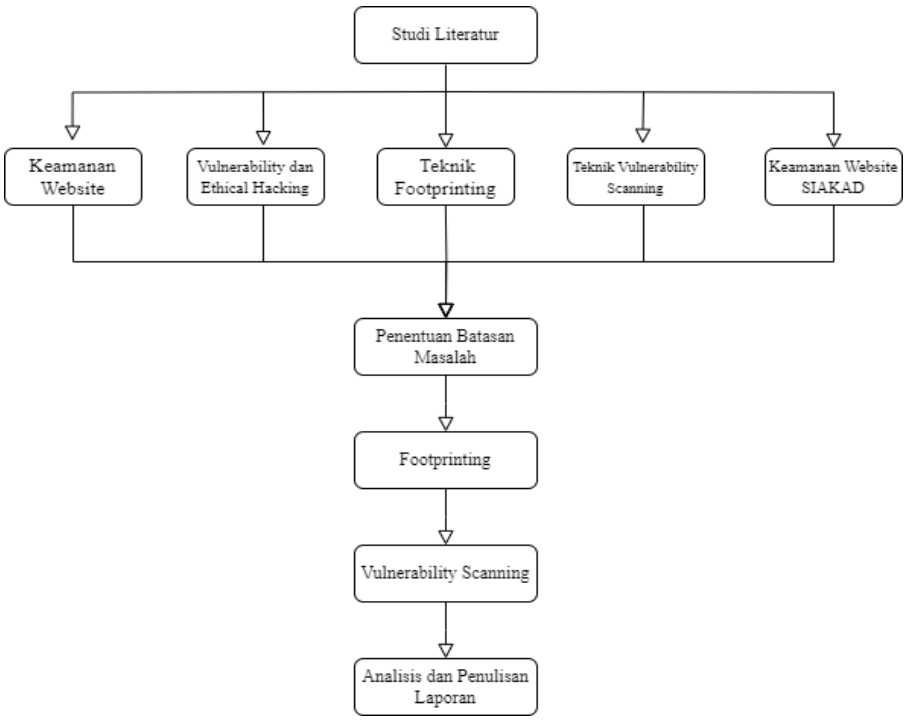
Proses mengumpulkan informasi sebanyak mungkin tentang target dikenal sebagai Foot Printing. Informasi ini dapat mencakup merek, tipe, perangkat yang digunakan, versi sistem operasi, topologi jaringan, perangkat keamanan, alamat jaringan, dan subnetting. Berbagai alat, seperti Foot Printing adalah proses pengumpulan informasi sebanyak mungkin mengenai target. Informasi yang dikumpulkan dapat mencakup perangkat yang digunakan, merek, tipe, versi sistem operasi, topologi jaringan, perangkat keamanan, alamat jaringan, dan subnetting. Foot Printing dapat dilakukan dengan berbagai alat seperti command prompt (CMD), Zenmap, dan Whois domain, dapat digunakan untuk melakukan Foot Printing.

Teknik Vulnerability Scanning

Vulnerability scanning adalah proses mengumpulkan informasi tentang kerentanan jaringan dengan menggunakan berbagai alat scanning kerentanan dan scanner kerentanan jaringan. Tujuan scanning kerentanan adalah untuk menemukan port yang terbuka, bug pada aplikasi server, dan kerentanan lainnya yang dapat dimanfaatkan oleh pencuri. Acunetix, OWASP ZAP, dan Pentest-tools.com adalah beberapa alat yang sering digunakan untuk memeriksa kelemahan.

Keamanan Website SIAKAD

Sistem Informasi Akademik (SIAKAD) adalah platform yang digunakan oleh banyak perguruan tinggi untuk mengelola data akademik mahasiswa. Mengingat pentingnya data yang dikelola oleh SIAKAD, keamanan website SIAKAD menjadi sangat krusial(Panggabean et al. 2023). Penelitian ini akan menggunakan teknik Foot Printing dan vulnerability scanning untuk mengidentifikasi dan menganalisis kerentanan pada website SIAKAD Universitas Sultan Ageng Tirtayasa (Untirta). Dengan melakukan pengujian ini, diharapkan dapat memberikan rekomendasi untuk meningkatkan keamanan website SIAKAD Untirta dan melindungi data akademik dari ancaman serangan hacker.



Gambar 1. Tahapan Penelitian

Beberapa penelitian sebelumnya telah mengkaji keamanan website menggunakan teknik *Foot Printing* dan vulnerability scanning. Misalnya, penelitian yang dilakukan oleh (Alwi and Ilmawan 2021) menekankan pentingnya keamanan jaringan dan metode yang dapat digunakan untuk melindungi sistem informasi. Selain itu, penelitian oleh (Natalia et al. 2024) dan (Kestina, Yuhandri, and Nurcahyo 2023) juga memberikan panduan mengenai teknik ethical hacking dan aplikasi praktisnya dalam mengidentifikasi kerentanan keamanan. Studi literatur ini menunjukkan bahwa keamanan website adalah aspek yang sangat penting, terutama untuk institusi pendidikan tinggi yang mengelola data sensitif. Teknik *Foot Printing* dan vulnerability scanning adalah metode yang efektif untuk mengidentifikasi dan menganalisis kerentanan pada website(Harahap and Zufria 2024). Dengan melakukan analisis keamanan website SIAKAD Untirta, penelitian ini diharapkan dapat memberikan rekomendasi yang berguna untuk meningkatkan keamanan dan melindungi data akademik dari potensi serangan *cyber*.

2. Penentuan Batasan Masalah

Batasan masalah pada penelitian ini dilakukan pada Website objek yang diuji adalah terbatas dengan menggunakan teknik Foot Printing dan Vulnerability Scanning tanpa melakukan eksploitasi sistem seperti mengubah tampilan, melakukan SQL Injection, brute force, dan lain sebagainya.

a. Foot Printing

Pada tahap Foot Printing dilakukan dengan tujuan mendapatkan sebanyak mungkin data atau informasi dari objek yang diuji, termasuk merek, tipe, nomor versi Sistem Operasi, dan alamat jaringan perangkat. Dalam penelitian ini alat yang digunakan untuk Foot Printing adalah Command Prompt (CMD). CMD adalah aplikasi berbasis Command Line Interpreter pada sistem operasi Windows. Pada tahap ini, perintah ping siakad.untirta.ac.id digunakan untuk menemukan alamat IP dari target. Kemudian Zenmap merupakan antarmuka grafis (GUI) untuk Nmap, alat pemindaian jaringan terkemuka yang digunakan untuk menilai keamanan jaringan. Selain itu, Whois Domain digunakan untuk mengumpulkan informasi tentang domain yang dimaksud, seperti alamat, kontak, pemilik, dan nama server.

b. Vulnerability Scanning

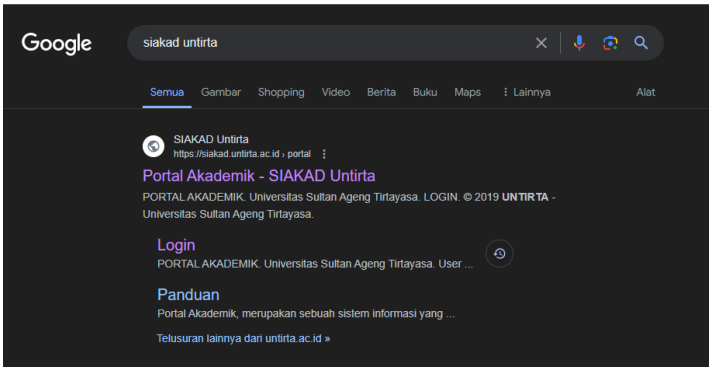
Tahap penting dalam pengujian keamanan adalah vulnerability scanning. Tahap ini mengumpulkan informasi tentang kerentanan jaringan dari target, seperti port yang terbuka, bug aplikasi, dan lainnya(Tinambunan, Junaidi, and Mustika Rizki 2024). Tujuan pencarian ini adalah untuk mengumpulkan informasi tentang kerentanan yang ada. Salah satu alat yang dapat digunakan adalah pentest-tools.com. Dengan mengunjungi situs web dan memasukkan alamat IP target, Anda dapat melakukan aktivitas pemindaian seperti identifikasi port yang terbuka, versi perangkat lunak yang digunakan, dan pencarian kerentanan yang mungkin ada. Tahap ini hanya mengumpulkan informasi tanpa penyerangan aktif, sehingga disebut sebagai serangan pasif. Namun, penting untuk memastikan bahwa tindakan ini dilakukan dengan izin dan dalam lingkungan yang terkontrol untuk menghindari konsekuensi yang tidak diinginkan.

3. Analisis dan Penulisan Laporan

Tahap terakhir pada penelitian ini adalah melakukan analisis serta dokumentasi kerentanan terhadap Website SIAKAD yang ditemukan setelah dilakukannya analisis.

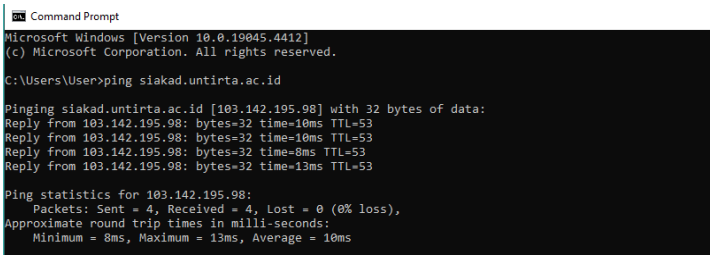
III. HASIL DAN PEMBAHASAN

Foot Printing yaitu kegiatan mengumpulkan informasi sebanyak-banyaknya terhadap objek target yang akan diteliti, langkah awal yang dilakukan pada penelitian ini yaitu melakukan riset terhadap web SIAKAD Untirta dengan menggunakan *search engine* Google, yang menghasilkan informasi yang dapat dilihat pada Gambar 2. Berdasarkan hasil pencarian didapatkan informasi yang berfokus pada informasi akademik Universitas Sultan Ageng Tirtayasa.



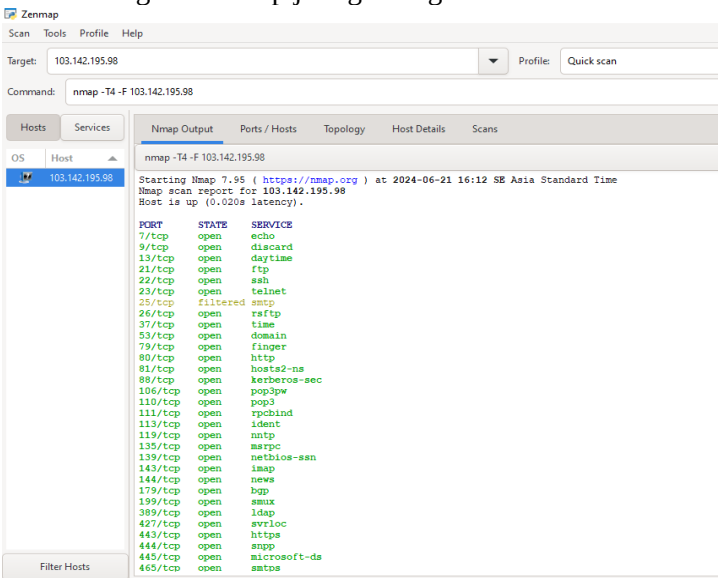
Gambar 2. Hasil Search Engine menggunakan Google

Setelah itu, menggunakan *Command Prompt* (CMD) untuk melakukan ping ke web siakad.untirta.ac.id. Ini dilakukan untuk menguji koneksi antara komputer dan web SIAKAD yang dimaksud, yang memungkinkan untuk mengetahui alamat IP web tersebut, seperti yang ditunjukkan pada Gambar 3.

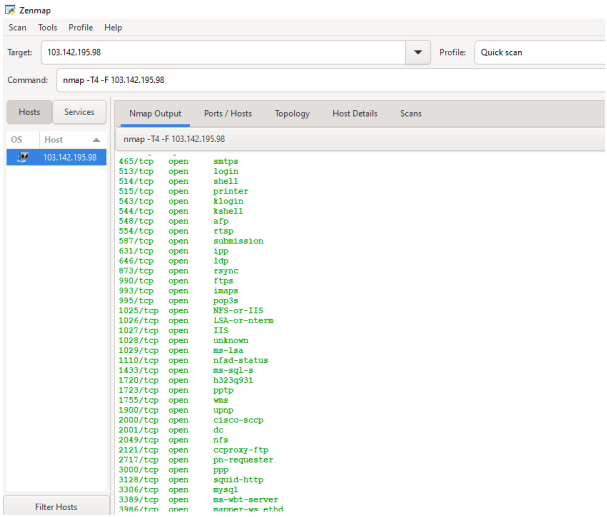


Gambar 3. Hasil ping menggunakan CMD

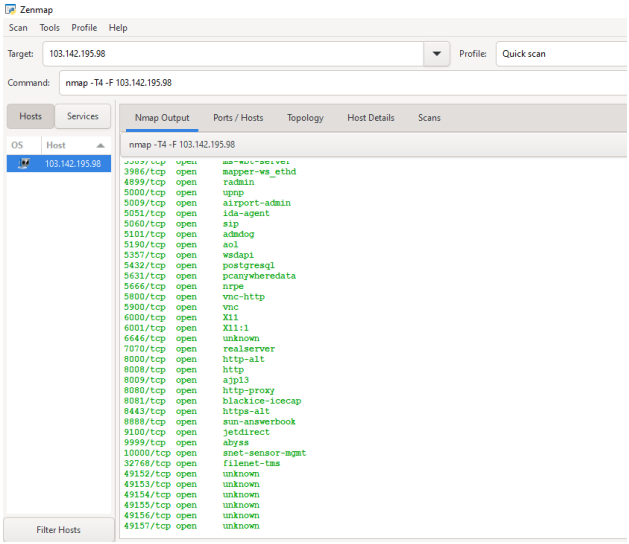
Kemudian, melakukan scan port untuk mengetahui port mana yang terbuka dan aktif. Dalam proses ini, tools yang digunakan adalah *Zenmmap*, dan hasilnya ditunjukkan pada Gambar 4 sampai dengan Gambar 7. *Zenmap* menemukan beberapa informasi port yang terbuka, *Traceroute*, Versi operasi sistem (OS), topologi jaringan target, dan versi layanan server yang dapat digunakan oleh hacker untuk melakukan serangan terhadap jaringan target.



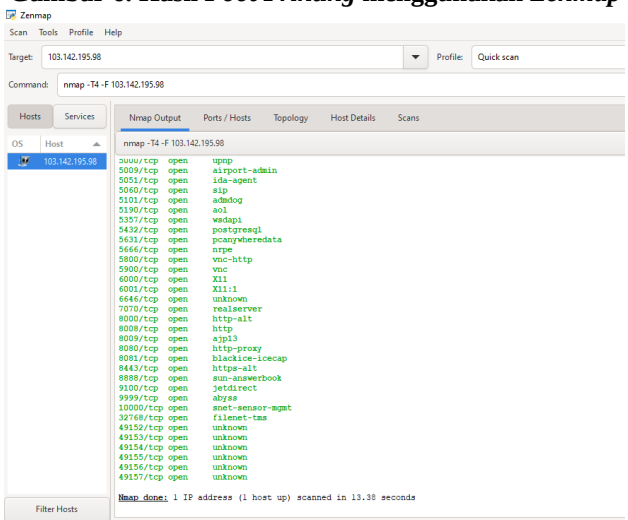
Gambar 4. Hasil *Foot Printing* menggunakan *Zenmap*



Gambar 5. Hasil *Foot Printing* menggunakan *Zenmap*



Gambar 6. Hasil *Foot Printing* menggunakan *Zenmap*



Gambar 7. Hasil *Foot Printing* menggunakan *Zenmap*

Proses selanjutnya adalah melakukan pengecekan menggunakan alat *whois*, seperti yang ditunjukkan pada Gambar 8 dan 9 didapatkan informasi domain dan juga informasi *whois*.

Domain:	untirta.ac.id
Registrar:	PT Digital Registra Indonesia
Registered On:	2009-11-04 13:27:03
Expires On:	2025-11-10 23:59:59
Updated On:	2024-04-17 04:51:56
Status:	clientTransferProhibited serverTransferProhibited
Name Servers:	jo.ns.cloudflare.com vern.ns.cloudflare.com

Gambar 8. Informasi Domain

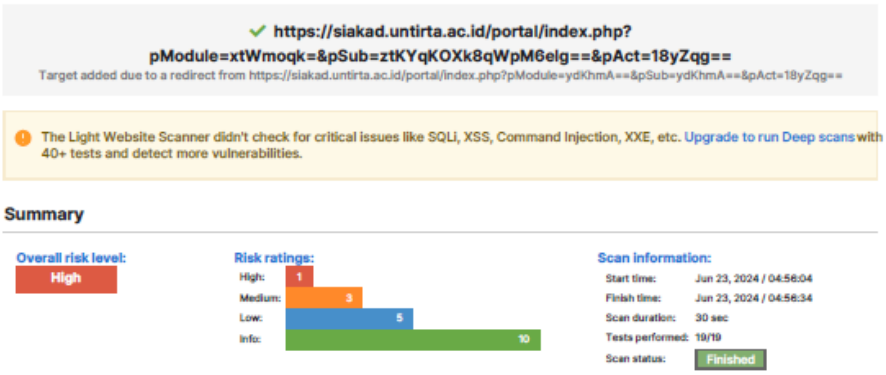
```
Domain Name: untirta.ac.id
Created On: 2009-11-04 13:27:03
Last Updated On: 2024-04-17 04:51:56
Expiration Date: 2025-11-10 23:59:59
Status: clientTransferProhibited
Status: serverTransferProhibited

================================================
Sponsoring Registrar Organization: PT Digital Registra Indonesia
Sponsoring Registrar URL: www.digitalregistra.co.id
Sponsoring Registrar Street: Jl. lempongsari no. 39C  Jongkang RT/RW 12/35 Sariharjo
Sponsoring Registrar City: Sleman
Sponsoring Registrar State/Province: Yogyakarta
Sponsoring Registrar Postal Code: 55281
Sponsoring Registrar Country: ID
Sponsoring Registrar Phone: 0274882257
Sponsoring Registrar Email: info@digitalregistra.co.id
Name Server: jo.ns.cloudflare.com
Name Server: vern.ns.cloudflare.com
DNSSEC: Unsigned
```

Gambar 9. Informasi Whois

Hasil pengujian *Foot Printing* yang dilakukan pada website siakad.untirta.ac.id menggunakan tools *Command Prompt, Whois, dan Zenmap* menunjukkan bahwa informasi terkait seperti IP server, *Operating System*, *version server*, nama domain, email, lokasi server, kontak pengelola server, dan port-port yang terbuka ditemukan. Pengelola situs web disarankan untuk melindungi data pribadi mereka. Ini memastikan bahwa pencuri atau pihak yang tidak berkepentingan tidak dapat mengakses atau mengeksploitasi data tersebut.

Tahap berikutnya adalah melakukan pemeriksaan kelemahan dengan menggunakan alat pentest-tools.com. Hasil pemindaian mencakup kerentanan yang ditemukan dan rekomendasi untuk mengatasinya. Pada Gambar 10 adalah hasil yang didapatkan setelah melakukan *vulnerability scanning* terhadap *website* siakad.untirta.ac.id.



Gambar 10. Hasil vulnerability scanning menggunakan petest-tools.com

Dari dilakukannya *vulnerability scanning*, didapatkan 1 *high risk*, 3 *medium risk*, 5 *low risk*, serta 10 *informational*, berikut merupakan rincian kerentanan yang dihasilkan.

Tabel 1. Hasil *Vulnerability Scanning* menggunakan pentest-tools.com

No	Kerentanan	Rekomendasi	Tingkat Resiko
1.	*Vulnerabilities found for server-side software*	Tingkatkan perangkat lunak yang terpengaruh ke versi terbaru untuk menghilangkan risiko kerentanan ini.	*High*
2.	*Insecure cookie setting missing HttpOnly flag*	Pastikan tanda *HttpOnly* disetel untuk semua cookie.	*Medium*
3.	*Insecure cookie setting missing Secure flag*	Setiap kali cookie berisi informasi sensitif atau merupakan token sesi, maka cookie tersebut harus selalu diteruskan menggunakan saluran ter enkripsi. Pastikan tanda aman disetel untuk cookie yang berisi informasi sensitif tersebut.	*Medium*
4.	*Directory listing is enabled*	Konfigurasi ulang server web untuk menolak daftar direktori. Selain itu, Anda harus memverifikasi bahwa tidak ada yang sensitif file di URL yang disebutkan.	*Medium*
5.	*Missing security header: Referrer-Policy*	Header Referrer-Policy harus dikonfigurasi di sisi server untuk menghindari pelacakan pengguna dan kebocoran informasi yang tidak disengaja. Nilai no-referrer dari header ini memerintahkan browser untuk menghilangkan Header Referrer seluruhnya.	*Low*
6.	*Missing security header: Strict-Transport-Security*	Header HTTP Strict-Transport-Security harus dikirim bersama setiap respons HTTPS. Sintaks nya adalah sebagai berikut: Strict-Transport-Security: max-age=<seconds>[; includeSubDomains] Parameter max-age memberikan kerangka waktu untuk kebutuhan HTTPS dalam hitungan detik dan harus dipilih cukup tinggi, misalnya. beberapa bulan. Nilai di bawah 7776000 dianggap terlalu rendah oleh pemeriksaan pemindai ini. Bendera includeSubDomains mendefinisikan bahwa kebijakan tersebut juga berlaku untuk subdomain pengirim respons.	*Low*
7.	*Missing security header: Content-Security-Policy*	Konfigurasikan Content-Security-Header untuk dikirim bersama setiap respons HTTP untuk menerapkan kebijakan spesifik yang diperlukan oleh aplikasi.	*Low*
8.	*Missing security header: X-Content-Type-Options*	Kami merekomendasikan pengaturan header X-Content-Type-Options seperti: X-Content-Type-Options: nosniff .	*Low*
9.	*Server software and technology found*	Menghilangkan informasi yang memungkinkan identifikasi platform perangkat lunak, teknologi, server, dan pengoperasian sistem: header server HTTP, informasi meta HTML, dll.	*Low*

Dari hasil pengujian *vulnerability scanning* pada Tabel 1, dihasilkan celah kerentanan pada website target dengan menggunakan tools vulnerability scanning secara online (pentest-tools.com). Kerentanan tersebut dapat diatasi dengan rekomendasi yang diberikan pada Tabel 1. untuk meminimalisir celah keamanan pada website di eksploitasi oleh hacker.

IV. KESIMPULAN DAN SARAN

Penelitian ini telah berhasil melakukan analisis keamanan terhadap website Sistem Informasi Akademik (SIAKAD) Universitas Sultan Ageng Tirtayasa (Untirta) menggunakan teknik *Foot Printing* dan *vulnerability scanning.* Dari hasil *Foot Printing* didapatkan informasi mengenai port yang terbuka, Traceroute, Versi operasi sistem (OS), topologi jaringan target, versi layanan server, informasi domain dan *whois*. Dari hasil *vulnerability scanning* didapatkan 1 *high risk*, 3 *medium risk*, 5 *low risk,* seperti *Vulnerabilities found for server-side software, Insecure cookie setting: missing HttpOnly flag, Insecure cookie setting: missing Secure flag, Directory listing is enabled, Missing security header: Referrer-Policy, Missing security header: Strict-Transport-Security, Missing security header: Content-Security-Policy, Missing security header: X-Content-Type-Options, Server software and technology found.* Dari celah kerentanan tersebut, peneliti memberi saran untuk mengatasi solusi kerentanan tersebut dengan menggunakan rekomendasi yang terdapat pada Tabel 1. Dengan menerapkan saran-saran di atas, diharapkan keamanan website SIAKAD Untirta dapat ditingkatkan secara signifikan, sehingga melindungi data akademik dari ancaman serangan cyber dan memastikan integritas serta kerahasiaan informasi.

UCAPAN TERIMA KASIH

Segala puji bagi Allah SWT. Dengan kehendak dan ridha-Nya, peneliti dapat menyelesaikan penelitian ini. Ucapan terima kasih juga saya sampaikan kepada semua pihak yang telah memberikan dukungan dan kontribusi nya dalam penelitian ini. Terutama, penulis mengucapkan terima kasih kepada Universitas Sultan Ageng Tirtayasa (Untirta) atas kesempatan dan fasilitas yang diberikan untuk melakukan analisis keamanan pada *website* SIAKAD. Ucapan terima kasih juga disampaikan kepada bapak Alim Hardiansyah, S.T., M.Kom. yang telah memberikan saran dan masukan berharga selama proses penelitian ini. Tidak lupa, penulis berterima kasih kepada keluarga dan teman-teman yang selalu memberikan dukungan moral dan motivasi. Semoga hasil penelitian ini dapat memberikan manfaat bagi peningkatan keamanan sistem informasi akademik di Untirta dan institusi lainnya.

REFERENSI

Alwi, Erick Irawadi, and Lutfi Budi Ilmawan. 2021. "Analisis Keamanan Sistem Informasi Akademik (SIAKAD) Universitas XYZ Menggunakan Metode Vulnerability Assessment." INFORMAL: Informatics Journal 6(3):131. doi: 10.19184/isj.v6i3.27053.

Andress, Jason. 2019. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. 2nd ed. USA: Syngress

Harahap, Parlindungan, and Ilka Zufria. 2024. "Analisis Keamanan Pada Website UPM SAINTEK UIN-SU Medan Menggunakan Metode Vulnerability Assesment." Februari 2(1):10–20.

Herdianti, H., & Umar, F. (2020). Analisis keamanan website menggunakan teknik footprinting dan vulnerability scanning. *INFORMAL: Informatics Journal*, *5*(2), 43-48.

Kendek Allo, Alvin, and Indrastanti Ratna Widiasari. 2024. "Analisis Keamanan Website SIASAT Menggunakan Teknik Footprinting Dan Vulnerability Scanning." *Jurnal JTIK (Jurnal Teknologi Informasi Dan Komunikasi)* 8(2):316–23. doi: 10.35870/jtik.v8i2.1723.

Kestina, Lusi, Yuhandri, and Gunadi Widi Nurcahyo. 2023. "Penanganan Celah Keamanan Website Dengan Ethical Hacking Dan Issaf Menggunakan Acunetix Vulnerability (Studi Kasus Di Bkpsdmd Kabupaten Kerinci)." INNOVATIVE: Journal Of Social Science Research 3(4):9192–9203.

Mulyanto, Yudi, Mohammad Taufan Asri Zaen, Yuliadi Yuliadi, and Safwan Sihab. 2022. "Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration

Testing (Pentest)." *Journal of Information System Research (JOSH)* 4(1):202–9. doi: 10.47065/josh.v4i1.2335.

Natalia, D., S. Maulana, E. U. Gani, E. N. Fawwaz, and ... 2024. "Tinjauan Penggunaan Keamanan Perangkat Lunak Di Kalangan Mahasiswa UNNES." Jurnal … 1(1):48–68.

Panggabean, David Bekham, Raihana Lutfiyah Rosanti, Firnanda Al-Islama, Achyunda Putra, and Kata Kunci. 2023. "Pengaruh Kualitas Sistem Dan Kualitas Informasi Terhadap Layanan Pengguna SIAKAD Universitas Merdeka Malang." Seminar Nasional Sistem Informasi (September):4409–20.

Prabowo, W. A., Rifki Adhitama, Auliya Burhanuddin, Paradise, Khusnul Fauziah, and Aufa Salsabila Nahrowi. 2024. "Peningkatan Kesadaran Keamanan Informasi Siswa SMK Telkom Purwokerto Melalui Pelatihan Footprinting Dan Reconnaissance." *Indonesian Journal of Community Service and Innovation (IJCOSIN)* 4(1):29–35. doi: 10.20895/ijcosin.v4i1.1346.

Tinambunan, Fernanda, Achmad Junaidi, and Agung Mustika Rizki. 2024. "Pengujian Sistem Informasi Akademik Universitas X Melalui Pendekatan Penetration Testing Berdasarkan Owasp Top 10." JATI (Jurnal Mahasiswa Teknik Informatika) 8(1):1062–69. doi: 10.36040/jati.v8i1.8920.