Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, Vol. 9, No. 1, Februari 2023, Hal. 01-07
e-ISSN 2502-8995 p-ISSN 2460-8181

ANALISIS CELAH KEAMANAN *WEBSITE SITASI* MENGGUNAKAN *VULNERABILITY ASSESSMENT*

Mona Fronita
Sistem Informasi, Sains dan Teknologi, UIN Suska Riau, Pekanbaru, Indonesia
Jl. H.R. Soebrantas No.155 KM.15 Tuah Madani – Pekanbaru 28129 PO Box 1004
monafronita@uin-suska.ac.id

ABSTRAK

Perkembangan teknologi website sudah sangat pesat dan menjadikan website sebagai salah satu fasilitas pendukung terlaksananya proses pendidikan lebih mudah, termasuk UIN Suska Riau khususnya Program Studi Sistem Informasi Fakultas Sains dan Teknologi yang dikenal dengan website Sistem Informasi Tugas Akhir (SITASI). Perkembangan teknologi website sebanding dengan resiko yang juga meningkat, oleh karena itu website harus dilakukan pengujian untuk memastikan bahwa tidak ada resiko atau masalah keamanan pada website. Kemudahan dalam website juga harus menjaga keamanan terhadap data dan informasi yang ada. Penelitian ini bertujuan untuk melakukan pengujian terhadap website SITASI untuk melihat kerentanan keamanan. Terdapat 3 tahapan dalam proses ini yaitu, *Information Gatering, Network Mapper* dan *Vulnerability Assessment.* Pengujian ini dilakukan dengan menggunakan utilities dan tools seperti whois, Nmap, Zenmap, OS Kali Linux dan Acunetix Vulnerability Scanner. Dari hasil acunetix scanner diperoleh ancaman pada level 2 yaitu 2 ancaman level medium severity vulnerabilities dan 6 ancaman level low severity vulnerabilities, yang dapat disimpulkan *website* SITASI ini sudah tergolong aman dari celah keamanan.
Kata kunci: *Acunetix, Assessment,* Keamanan, Vulnerability, Web.

Abstract

The development of website technology has been very rapid and has made the website one of the supporting facilities for making the educational process easier, including UIN Suska Riau, especially the Information Systems Study Program, Faculty of Science and Technology, which is known as the Final Project Information Systems website (SITASI). The development of website technology is proportional to the risk which also increases, therefore the website must be tested to ensure that there are no risks or security problems on the website. Ease of use on the website must also maintain the security of existing data and information. This study aims to test the SITASI website to see security vulnerabilities. There are 3 stages in this process, namely Information Gatering, Network Mapper and Vulnerability Assessment. This test was carried out using utilities and tools such as whois, Nmap, Zenmap, Kali Linux OS and Acunetix Vulnerability Scanner. From the results of the Acunetix scanner, threats at level 2 were obtained, namely 2 threats at medium severity level and 6 threats at low severity level, which can be concluded that the CITAS website is safe from security holes.
Keywords: Acunetix, Assessment, Security, Vulnerability, Web.

A. PENDAHULUAN

Keamanan dunia maya menjadi suatu permasalahan yang sangat penting di seluruh dunia pada saat ini. Serangan dunia maya dilakukan dengan baik oleh peretas setiap harinya untuk menargetkan lebih banyak perangkat lunak organisasi [1]. Berdasarkan data tahun 2018 Id-SIRTII (*Indonesian Security Incident Response Team on internet Infrastructure*) mencatat 10 serangan di internet seperti upaya mendapatkan hak *administrator*, pelanggaran kebijakan, percobaan pengintaian, percobaan pengintaian yang berhasil, aktivitas *Trojan*, percobaan *dos*, serangan yang tidak diketahui, percobaan *user* dan denial of service (IdSIRTII/CC 2018).

Serangan yang dilakukan dapat berupa *Cross Site Scripting* (XSS), *Cross Site Request Forgeri* (CSRF),

SQL *injection* dan lain sebagainya [2]. Salah satu serangan yang terjadi pada saat ini terhadap situs website, website sudah menjadi sumber utama dan diterapkan pada berbagai bidang kegiatan, salah satunya bidang kegiatan yang ada pada perguruan tinggi UIN Suska Riau terutama pada Program Studi Sistem Informasi Fakultas Sains dan Teknologi, Penerapan Website Sistem Sistem Informasi Tugas Akhir (SITASI). SITASI merupakan website mengelola proses Tugas Akhir (TA) mulai dari upload judul TA, TA diterima atau ditolak, penunjukkan pembimbing TA, penunjukkan penguji seminar dan sidang TA serta pemrosesan nilai.

Serangan yang dilakukan pada situs website untuk mencuri data, mengubah data dan untuk membuat pelayanan tidak berjalan sebagai mana mestinya [3]. Risiko keamanan yang memungkinan terjadinya serangan terhadap suatu website dikelompokkan sebagai vulnerability [4].

Vulnerability dilakukan secara berkala untuk dapat menjaga keamanan website dan untuk dapat meningkatkan dan menjaga keamanan perlu dilakukan vulnerability assesment baik secara manual atau otomatis. Hasil dari vulnerability assessment dapat membantu suatu organisasi untuk mendapatkan informasi keamanan dan kondisi infrastrukturnya serta dapat pula mengidentifikasi kemungkinan terjadinya ancaman keamanan berupa penyerangan terhadap infrastruktur dan aset dari perusahaan dimanfaatkan oleh pihak lain [5].

Vulnerability assessment (VA) merupakan proses yang dilakukan pada sebuat situs web untuk mendefinisikan, mengidentifikasi dan mengklasifikasi kemungkinan terjadinya celah keamanan pada jaringan komputer ataupun infrastruktur komunikasi. Kematangan suatu situs web dapat dinilai dari vulnerability assessment sehingga dapat memperkirakan sejauh mana efektifitas tindakan pencegahan dan evaluasi pada situs web yang telah diimplementasikan [6].

Untuk menguji Vulnerability assessment keamanan, merekam dan mengumpulkan tanggapan dari tes kerentanan keamanan situs web pada prodi sistem informasi. Untuk menguji Vulnerability assessment keamanan, merekam dan mengumpulkan tanggapan dari tes kerentanan keamanan situs web pada fakultas Sains dan Teknologi. Salah satu cara untuk melakukan uji Vulnerability assessment adalah menilai keamanan suatu situs web menggunakan perangkat lunak yang dirancang khusus untuk menemukan kerentanan sistem, yaitu Acunetix Vulnerability Scanner [7].

B. LANDASAN TEORI

1. *Information Gatering*

a. Whois

Ada prosedur untuk mendapatkan informasi domain, data mengenai kepemilikan domain, keberadaan domain, serta terdapat registar dari domain tersebut [8].

b. Nslook up

Nslook up adalah alat yang berguna untuk mengetahui alamat IP suatu domain. Selain itu, ini juga berguna untuk mendiagnosis masalah jaringan DNS [8]

2. Network Mapper

Network Mapper dikenal sebagai nmap. Nmap dioptimalkan untuk berjalan di sistem operasi Linux, bukan Windows. Nmap adalah alat yang biasa digunakan dalam pengujian keamanan jaringan dan penelitian jaringan. Nmap adalah alat sumber terbuka. Program standar Nmap seperti Zenmap, Ndiff, Nping, Ncrak, Ncat, NSE [8]

3. *Vulnerability assessment*

Vulnerability Assesment merupakan proses mengidentifikasi potensi kerentanan pada suatu organisasi. Kerentanan pada sistem adalah celah kelemahan dalam sistem atau jika di eksploitasi maka akan memudahkan hacker untuk menyerang system [9]

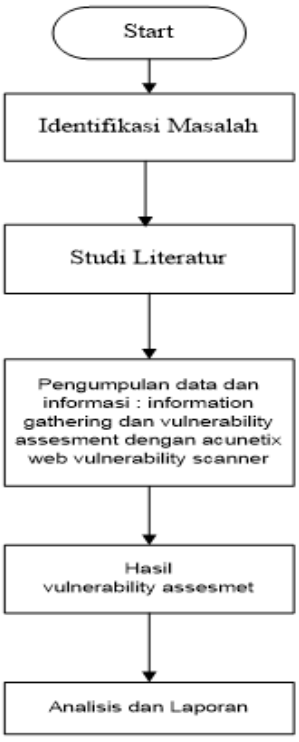
Penilaian kerentanan adalah pemeriksaan potensi poin yang dapat digunakan dalam serangan pada sistem atau jaringan oleh mengidentifikasi versi perangkat lunak yang kedaluwarsa, mengidentifikasi yang terbuka port dalam sistem operasi, dan aplikasi yang dijalankan jaringan, itu digunakan untuk mendeteksi kelemahan sistem dalam jaringan, aplikasi dan perangkat komunikasi dan mengukur kinerja sistem keamanan siber yang diterapkan, Namun, pemindai kerentanan juga menggunakan database besar yang telah ditentukan sebelumnya kerentanan, untuk mendeteksi kekurangan dan potensi pengurangan atas kekurangan tersebut.

Pemindaian kerentanan juga digunakan oleh penyerang yang mencari lubang sistem untuk masuk jaringan [10].

Acunetic merupakan program yang paling banyak digunakan untuk mendeteksi kerentanan terhadap injeksi SQL dan XSS, selain itu interface acunetix lebih mudah digunakan karena sangat sederhana dan user friendly. Kelengkapan bagian report menawarkan nilai tambah yang besar dibandingkan kompetitornya. Dalam pengaturan pra-deteksi, ia menawarkan beberapa opsi.

C. METODE PENELITIAN

Metodelogi penelitian ini dilakukan secara sistematis untuk dapat menjadi pedoman dalam melaksanakan penelitian agar mencapai tujuan yang diinginkan. Alat ukur metodelogi penelitian menggunakan bagan alur metodologi seperti pada bagan 3.1



Gambar 3.1 Tahapan Metodelogi Penelitian

I. Identifikasi Masalah

Pada tahapan ini, dilakukan pengecekkan alur bisnis proses website dengan domain uin-suska.ac.id untuk serta server yang digunakan

1.salah satu domainya sitasi.uin-suska.ac.id merupakan website sistem informasi yang dimanfaatkan untuk memudahkan mahasiswa dalam melakukan proses Tugas Akhir (TA) berupa pengajuan pembimbing, pengajuan proposal, penjadwalan seminar dan sidang dan nilai TA.

2. Server adalah terminal terakhir yang mengoordinasikan semua aktivitas berlangsung dalam infrastruktur jaringan yang berperan menangani penyimpanan, pemrosesan, dan distribusi data dalam pusat aplikasi terpusat dan terdistribusi (shared) dan dari gateway ke gateway (Internet).

II. Studi Literatur

Studi Literatur digunakan untuk membandingkan dan menyusun dasar teori kerangka penelitian sebelumnya yang bersumber buku, jurnal, dan referensi internet

1. Pengumpulan data dan informasi

Pada tahapan ini dilakukan pengumpulan data dan informasi yang dibutuhkan untuk penelitian agar mencapai tujuan yang diharapkan, tahapan ini dilakukan dengan beberapa langkah yaitu information gathering dengan whois, zenmap, kali linux dan vulnerability dengan tools acunetix web vulnerability scanner.

2. Hasil

Berdasarkan data dan informasi yang dihasilkan dari vulnerability diatas akan di telaah celah keamanan yang ditemukan berdasarkan jenis – jenis celah keamanan agar memepermudah dalam menganalisis. Data yang dihasilkan dari proses scanning menggunakan Acunetix web vulnerability scanner akan dikelompokkan dan dideskripsikan agar mempermudah pengelola dalam melakukan perbaikan jika ada celah keamanan yang bocor ataupun bermasalah.

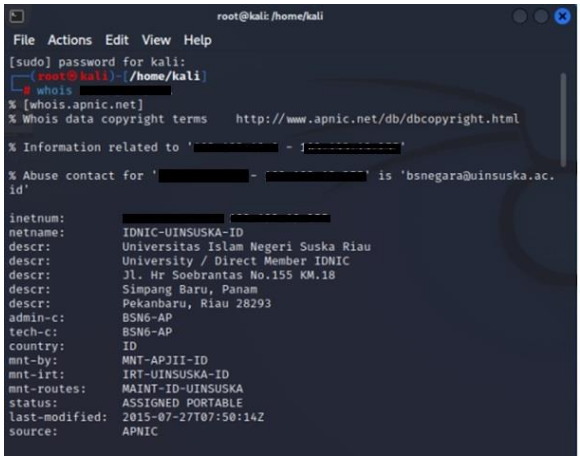
D. HASIL DAN PEMBAHASAN

Pada tahap ini akan dilakukan pengujian dan analisa terhadap untuk melihat celah ataupun kelemahan dari sistem dengan beberapa tahap yang dilakukan antara lain *information gatering*, *Network Mapping* dan *vulnerability scanning*.

1. *Information Gatering*

a. Whois

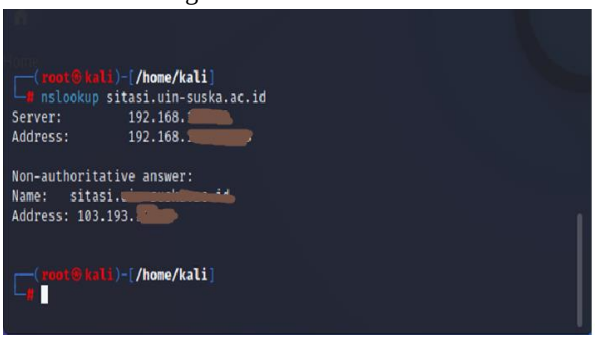
Pada tahapan ini dilakukan pengujian pada website sitasi.uin-suska.ac.id untuk mendapatkan informasi, pengujian ini menggunakan sistem operasi linux. Hasil dari pengujian ini dapat dilihat pada gambar 4.1



Gambar 4.1 Hasil Whois

b. Nslookup

Nslookup bertujuan untuk mengetahui IP dari sebuah *domain.* Disamping itu juga dapat berguna untuk mendiagnosa permasalahan jaringan yang berkaitan dengan *DNS.*



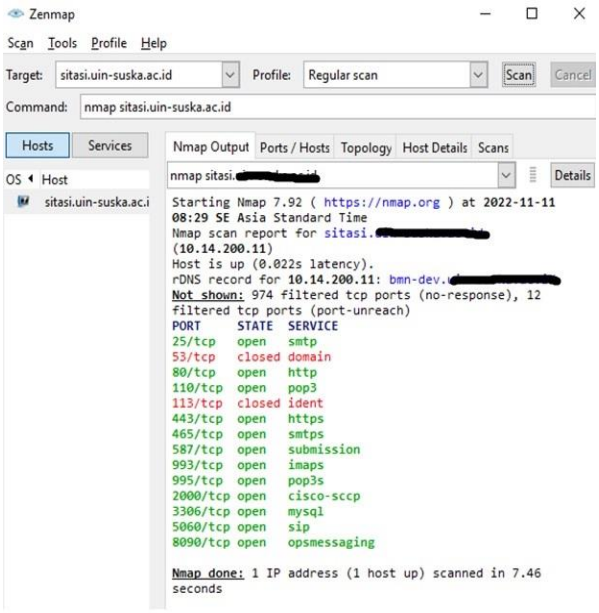
Gambar 4.2 Hasil Nslookup

Berdasarkan gambar 4.2 merupakan hasil dari nslookup didapat informasi IP Address dari SITASI 103.193.19.11

2. *Network Mapping*

Nmap dilakukan dengan menggunakan zenmap *tool* untuk melihat server atau port yang terbuka. Hasil dari pengujian Nmap dangan *port scanning* pada website sitasi.uin-suska.ac.id sebagai berikut

Zenmap

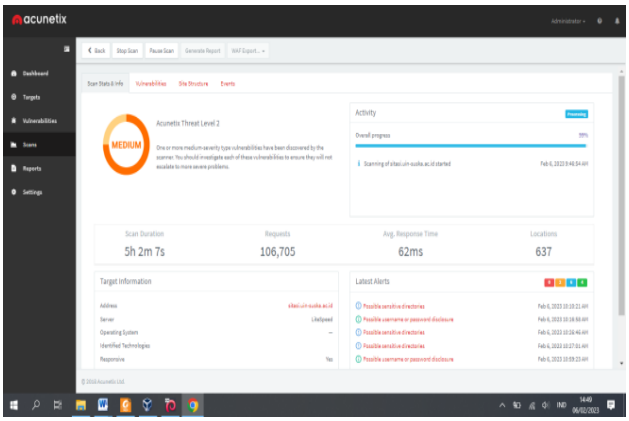


Gambar 4.3 Hasil Zenmap

Dari hasil zenmap terdapat port 53/tcp dan port 113/tcp dengan status closed sehingga port tertutup dapat diakses oleh nmap sebaiknya status pada npam adalah filtered sehinga tidak akan mudah di serang oleh hacket Sedang port yang statusnya open cukup banyak sehingga apat menerima koneksi paket TCP/UDP pada port ini

3. *Vulnerability Scanning*

Pada tahap ini dilakukan scanning terhadap website sitasi.uin-suska.ac.id dengan menggunakan aplikasi *Acunetix Web Vulnerability Scanner* versi 12.0.180911134 Hasil dari *vulnerability scanning* selama 3 jam 24 menit yaitu 2 *medium saverity vulnerabilities* dan 6 low saverity vulnerabilities yaitu seperti gambar 4.1



Gambar 4.4 *Output Acunetix Web Vulnerability Scanner*

Hasil dari pengujian acunetix vulnerability scanning yaitu Acunetix Threat Level 2 dengan deskripsi berikut ini:

1. *Alert Distribution*
   Tabel 4.1 data *Acunetix Web Vulnerability Scanner*

Total alerts found	12
High	0
Medium	2
Low	6
Informational	4

2. *Alert Distribution Application error message*
   Tabel 4.2 *Application error message*

Application error message	
Affected item	/logindosen
Affected parameter	nim
Risk Level	Medium
Request	

```
POST /logindosen HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://sitasi.[redacted]
Connection: keep-alive
Cookie:ci_session=l3nqu98caldt3rba6pkn31c1dr3
qvklbAuthorization: Basic
YW5vbnltb3VzOmFub255bW91cw==
Accept: */*
Accept Encoding: gzip,deflateContent-
Length: 85
Host: sitasi.[redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1;
WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
submit=Masuk&nim=12345'"\'\");|]*%00{%0d%0a<%0
0>%bf%27' &password=g00dPa%24%24w0rD
```

Pada permasalahan terdapat query yang error pada saat login dosen. Akan ada penampilkan pesan peringatan karena ada input yang tidak dapat diproses.

3. *Alert Distribution HTML form without CSFR Protection*
   Tabel 4.3 *HTML form without CSFR Protection*

HTML form without CSRF protection	
Affected item	Web Server
Affected parameter	
Risk Level	Medium
Request	

```
GET / HTTP/1.1
Cookie:ci_session=l3nqu98caldt3rba6
pkn31c1dr3qvklb
Accept: */*
Accept-Encoding: gzip,deflate
Host: sitasi.[redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1;
WOW64) AppleWebKit/537.21 (KHTML, like
Gecko)Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Metode form yang digunakan adalah method GET, menyebabkan form tidak bisa dilindungi dengan menggunakan CSRF, oleh karena itu form diganti dengan method POST dan selanjutnya mengaktifkan CSRF.

4. *Alert Distribution Clickjacking: X-Frame-Options header missing*

Tabel 4.4 *Clickjacking: X-Frame-Options header missing*

Clickjacking: X-Frame-Options header missing	
Affected item	Web Server
Affected parameter	
Risk Level	Low
Request	

```
GET / HTTP/1.1
Connection: keep-alive
Cookie:ci_session=l3nqu98caldt3rba6pk
n31c1dr3qvklb
Accept: */*
Accept Encoding:gzip,deflate
Host: sitasi.[redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1;
WOW64) AppleWebKit/537.21 (KHTML, like
Gecko)Chrome/41.0.2228.0 Safari/537.21
```

Clickjacking dimana hacker dapat mengubah menu/button pada website dan juga disebabkan tidak adanya XFrame-Options yang berguna untuk mengizinkan browser melakukan render halaman didalam frame.

5. *Alert Distribution Possible sensitive directories*
   Pada permasalahan *Possible sensitive directories* terdeteksi 5 Affected item yaitu
   a) /assets/adminLTE/bower_components/ckeditor
   b) /assets/adminLTE/bower_components/ckeditor/samples/old
   c) /assets/adminLTE/bower_components/ckeditor/plugins/save
   d) /assets/adminLTE/bower_components/ckeditor/samples/old
   e) /assets/adminLTE/bower_components/Ionicons/src
   f) /assets/adminLTE/bower_components/jquery/src

Tabel 4.5 *Possible sensitive directories*

Possible sensitive directories	
Affected item	/assets/adminLTE/bower_components/ckeditor
Affected parameter	
Risk Level	Low
Request	
GET/assets/adminLTE/bower_components/ckeditor HTTP/1.1 Accept: acunetix/wvs Range: bytes=0-99999 Connection: keep-alive Cookie:ci_session=cqov6v6ung84nchtq5qhl13i85r69e8bAuthorization: Basic YW5vbnltb3VzOmFub255bW91cw== Accept-Encoding: gzip,deflate Host: sitasi.u[redacted] User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)Chrome/41.0.2228.0 Safari/537.21	

6. *Alert Distribution Email address found*

Tabel 4. 6 *Email address found*

Email address found	
Affected item	Web Server
Affected parameter	
Request	
GET / HTTP/1.1 Cookie:ci_session=l3nqu98caldt3rba6pkn31c1dr3qvklb Accept: */* Accept-Encoding: gzip,deflate Host: sitasi.[redacted] User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)Chrome/41.0.2228.0 Safari/537.21 Connection: Keep-alive	

Kondisi ini mendeteksi terdapat halaman web yang menampilkan satu atau lebih email. Hal ini menimbulkan kekhawatiran pemilik email yang akan dimanfaatkan oleh spam-bots.

7. *Alert Distribution Password type input with auto-complete enabled*

Tabel 4.7 *Password type input with auto-complete enabled*

Password type input with auto-complete enabled	
Affected item	Web Server
Affected parameter	
Request	
GET /login HTTP/1.1 Cookie:ci_session=l3nqu98caldt3rba6pkn31c1dr3qvklb Accept: */* Accept-Encoding: gzip,deflate Host: [redacted] User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)Chrome/41.0.2228.0 Safari/537.21 Connection: Keep-alive	

Celah ini mendeteksi adanya fitur autocomleted pada browser yang dipakai oleh user. hal ini menyebabkan password masih tersimpan pada cache sehingga berpeluang untuk hacker yang menggunakan akses secara local.

8. *Alert Distribution Possible username or password disclosure*

Tabel 4.8 *Possible username or password disclosure*

Possible username or password disclosure	
Affected item	/assets/adminLTE/bower_components/Ionicons/css/ionicons.min.css
Affected parameter	
Request	

```
GET/assets/adminLTE/bower_compo
nents/Ionicons/css/ionicons.min
.css HTTP/1.1
Cookie:ci_session=l3nqu98caldt3
rba6pkn31c1dr3qvklb
Authorization: Basic
YW5vbnltb3VzOmFub255bW91cw==
Accept: */*
Accept-Encoding: gzip,deflate
Host: sitasi.[redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1;
WOW64) AppleWebKit/537.21 (KHTML, like
Gecko)Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Satu atau beberapa pasangan kredensial (nama username dan password) ditemukan. Informasi ini mungkin sensitif.

Satu atau lebih kerentanan tipe tingkat keparahan sedang telah ditemukan oleh acunetix vulnerability scanning. Harus dilakukan investigasi setiap kerentanan ini untuk memastikan mereka tidak akan meningkat menjadi masalah yang lebih parah.

E. KESIMPULAN

Berdasarkan proses penelitian yang dilakukan pada website SITASI dapat disimpulkan :

1. Pengujian Vulnerability Assessment pada Threat Level 2 sehinggan website SITASI tergolong cukup aman dari kerentanan hacker.
2. Implementasikan CSRF dalam HTML website untuk mencegah keamanan bisa dengan mudah ditemukan oleh hacker.
3. Vulnerability Aassessment merupakan alat bantu untuk meningkatkan keamanan informasi. Metode Vulnerability Aassessment secanggih apapun tidak akan berarti apabila tidak diikuti dengan kesadaran dan kesediaan dari internal akan pentingnya keamanan informasi

REFERENSI

[1] Y. Gan *et al.*, "Unveiling the Hardware and Software Implications of Microservices in Cloud and Edge Systems," *IEEE Micro*, vol. 40, no. 3, pp. 10–19, 2020, doi: 10.1109/MM.2020.2985960.

[2] I. Riadi, "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment," *JTIIK*, vol. vol 7 No 4, 2020.

[3] M. Aziz, "Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning Pada Universitas Xyz," *Jecsit*, vol. 1, no. 1, pp. 101–109, 2021.

[4] L. Collins, *Assessments and Audits*. Elsevier Inc., 2013. doi: 10.1016/B978-0-12-394397-2.00062-3.

[5] Krohn-Hansen and Hakon, "UNIVERSITY OF OSLO Department of Informatics," no. April, 2012.

[6] A. Kakareka, *What Is Vulnerability Assessment?*, no. February 2004. Elsevier Inc., 2017. doi: 10.1016/B978-0-12-803843-7.00031-4.

[7] R. Mayasari, A. A. Ridha, D. Juardi, and K. A. Baihaqi, "Analisis Vulnerability pada Website Universitas Singaperbangsa Karawang menggunakan Acunetix Vulnerability," 2020. [Online]. Available: http://drupal.org

[8] T. Wilhelm, "Information Gathering," in *Professional Penetration Testing*, Elsevier, 2013, pp. 151–183. doi: 10.1016/B978-1-59749-993-4.00006-9.

[9] V. Santhi, M. Tech, K. R. Kumar, B. L. V Vinay, and K. Research Scholar, "Penetration Testing using Linux Tools: Attacks and Defense Strategies." [Online]. Available: www.ijert.org

[10] C. K. Veitch, S. Wade, and J. T. Michalski, "Cyber Security Assessment Tools and Methodologies for the Evaluation of Secure Network Design at Nuclear Power Plants - A Letter Report to the U.S. NRC.," 2012.