ANALISIS KEAMANAN APLIKASI WEB PRODI TEKNIK INFORMATIKA UIKA MENGGUNAKAN ACUNETIX WEB VULNERABILITY

Febri Al Fajar
Universitas Ibn Khaldun; JL. K.H Sholeh Iskandar Km2 Bogor, telp 0251-7551570
Teknik Informatika, Fakultas Teknik UIKA, Bogor.
febrialfajar225@gamil.com

Abstrak

Aspek keamanan sering dilupakan dalam penerapan Teknologi Informasi. Kerentanan biasanya disebabkan oleh kelalaian pengembang yang menyebabkan kerusakan pada sistem yang digunakan. Serangan SQL Injection, Cross Site Scripting dan tidak ada penggunaan saluran terenkripsi menyebabkan pemaparan pengguna data sensitif. Tujuan dari penelitian ini adalah untuk melakukan audit dan analisis aspek keamanan terhadap Aplikasi Web Prodi Teknik Informatika UIKA. Audit dan analisis keamanan adalah langkah pencegahan sehingga kerentanan yang ditemukan tidak menjadi pintu masuk bagi peretas sistem. Hasil dari penelitian ini dalam bentuk laporan audit keamanan yang memuat tentang kerentanan Aplikasi Web Prodi Teknik Informatika UIKA. Laporan tersebut akan digunakan sebagai referensi bagi pengembang aplikasi online, Analisis Keamanan Aplikasi Web Prodi Teknik Informatika UIKA untuk meningkatkan system di keamanan pada Aplikasi Web .Metode yang dilakukan pada pengujian ini akan menggunakan tool berupa perangkat lunak dan cara-cara tertentu yang digunakan untuk menguji keamanan sebuah AplikasiWeb. Untuk melakukan analisis keamanan Aplikasi Web, software yang digunakan adalah Acunetix Web Vulnerability scanner.

Hasil dari pengujian dapat ditemukan berbagai level kerentanan dari level kerentanan Low pada domain ti.ft.uika-bogor.ac.id sampai level kerentanan High pada sub domain lainnya yang berupa sub domain fakultas. Dari hasil analisis yang diperoleh dan dapat dilihat berbagai web alerts yang terdapat pada sebuah Aplikasi web tersebut. Adapun berbagai web alerts yang berhasil ditemukan berupa SQL Injection, Cross Site Scripting dan berbagai web alerts lainnya.

Kata kunci : *Analisis Keamanan, Audit, Aplikasi Web, Acunetix Web Vulnerability.*

.

Abstract

Security aspects are often forgotten in the application of Information Technology. Vulnerability is usually caused by developer negligence which causes damage to the system used. SQL Injection attacks, Cross Site Scripting and no use of encrypted channels cause exposure to sensitive data users. The purpose of this study was to conduct an audit and analysis of security aspects of the UIKA Informatics Engineering Study Program Web Application. Security audits and analysis are preventative measures so that vulnerabilities found are not the entrance for system hackers. The results of this study are in the form of a security audit report that contains the vulnerability of the UIKA Informatics Engineering Study Program Web Application. The report will be used as a reference for online application developers, Web Application Security Analysis of UIKA Informatics Engineering Study Program to improve the system in security on Web Applications. The methods used in this test will use tools such as software and certain methods used to test security. a Web Application. To conduct web application security analysis, the software used is Acunetix Web Vulnerability scanner.

The results of the testing can be found various levels of vulnerability from the level of Low vulnerability in the domain ti.ft.uika-bogor.ac.id to the level of High vulnerability in the other sub domains in the form of the sub domain of the faculty. From the results of the analysis obtained and can be seen various web alerts contained in a web application. The various web alerts that were found were SQL Injection, Cross Site Scripting and various other web alerts.

Keywords: *Security Analysis, Audit,Application Web, Acunetix Web Vulnerability.*

1. PENDAHULUAN

Keamanan data elektronik menjadi hal yang sangat penting di perusahaan penyedia jasa Teknologi Informasi (TI) maupun industry lainnya, seperti perusahaan export-import, tranportasi, lembaga pendidikan, pemberitaan, hingga perbankan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur kritikal (penting) [1].

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila menggangu kinerja dari sistem, seringkali keamanan dikurangi atau ditiadakan.

Kebutuhan akan keamanan sistem aplikasi timbul dari kebutuhan untuk melindungi data. dan adanya yang tidak diinjinkan hendak mengakses atau mengubah data. Tanpa keamanan yang baik, maka aplikasi menyebabkan integritas data tersebut menjadi tidak valid dan belum dapat dikatakan aman. aspek keamanan data ini menjadi aspek yang sangat penting walaupun pada praktiknya seringkali dilupakan, hanya karena mengejar kinerja. Pengamanan ini diperlukan untuk memenuhi aspek-aspek keamanan Kerahasiaan (Confidentially), Integritas (Integrity) dan Ketersediaan (Availability) dari keamanan sistem aplikasi.

Salah satu sistem yang umumnya menjadi sasaran hacker dan cracker adalah aplikasi berbasis website. Hal tersebut dikarenakan pemanfaatan aplikasi mengalami pertumbuhan yang sangat pesat saat ini. Hacker adalah seseorang yang melakukan peretasan dengan mencari celah keamanan dari sebuah sistem, kemudian memberikan gagasan dan solusi kepada administrator sistem bila terdapat celah keamanan. Sedangkan cracker adalah seseorang yang

melakukan peretasan dengan mencari celah keamanan dari sebuah sistem, kemudian menggunakan celah tersebut untuk kepentingan individu seperti mencuri data,menghapus data, merusak data, dan

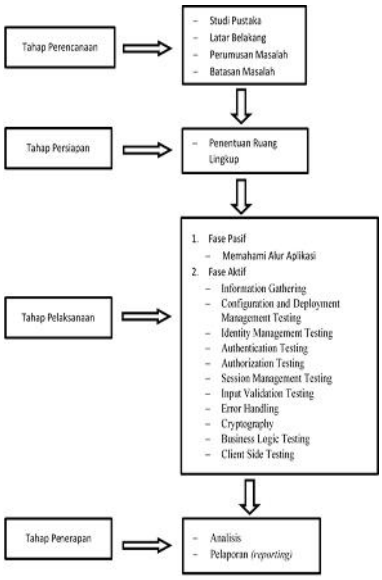
melakukan hal-hal lain yang merugikan pemilik system [8].

Berdasarkan hal tersebut, sangat dianjurkan untuk menerapkan analisis keamanan terhadap aplikasi yang bertujuan untuk meminimalisir terjadinya gangguan pada kinerja aplikasi berbasis web sehingga harus adanya evaluasi terhadap keamanan sistem aplikasi. Dengan adanya Analisis Keamanan Aplikasi Web Prodi Teknik Informatika UIKA dengan tujuan menemukan keretanan dan menguji pada aplikasi sehingga pemilik aplikasi web tersebut dapat memperbaiki dan meningkatkan keamanan dari sebuah aplikasi .

2. METODE PENELITIAN

Untuk melakukan Penenelitian ini bertujuan untuk melakukan audit keamanan Aplikasi. Audit Keamanan Aplikasi dilakukan menggunakan Tabel audit keamanan yang dihasilkan *Acunetix*. Hasil audit keamanan tersebut disajikan dalam bentuk kerentanan yang dialami berdasarkan kebutuhan minimum keamanan aplikasi berdasarkan standar *ISO 27001:2005*. Melalui pengujian analisis deskriptif, selain itu mengunakan studi literatur mengenai penelitian- penelitian yang sudah pernah dilakukan.

Pada Gambar 1 menujukan Diagram alur yang melalui tahapan proses audit keamanan aplikasi web.



Gambar 1 Tahapan Penelitian

Adapun kebutuhan yang harus dipenuhi dalam aspek Keaamanan teknologi pada sebuah aplikasi pelayanan publik menurut standar ISO 27001 adalah [5]:

1. Prosedur Penanganan Informasi (10.7.3)
2. Kebijakan dan Prosedur Pertukaran Data (10.8.1)
3. Pesan Elektronik (10.8.4)
4. Perdagangan Elektronik (10.9.1)
5. Transaksi Online (10.9.2)
6. Informasi Publik Yang Tersedia (10.9.3)
7. Perlindungan Log Informasi (10.10.3)
8. Manajemen Hak Akses (11.2.2)
9. Penggunaan Password (11.3.1)
10. Autentikasi Pengguna Untuk Melakukan Koneksi Dari Luar (11.4.2)
11. Pembatasan Akses Informasi (11.6.1)
12. Validasi Data Masukan (12.2.1)
13. Kontrol Pemrosesan Internal (12.2.2)
14. Validasi Data Keluaran (12.2.4)
15. Kontrol Operasional Perangkat Lunak (12.4.1)
16. Kontrol Akses Ke Baris Kode Aplikasi (12.4.3)
17. Kebocoran Informasi (12.5.4)

Pada poin-poin kebutuhan minimum keamanan aplikasi menurut standar *ISO 27001:2005* ditampilkan pula tabel yang berisi penilaian kerentanan dan bagian-bagian dari aplikasi yang memiliki kerentanan.

Acunetix web Vulnerability adalah sebuah alat layanan aplikasi web untuk pengujian keamanan otomatis yang mengaudit aplikasi tersebut dengan memeriksa kerentanan seperti *SQL Injection, Cross site scripting*, dan kerentanan aplikasi yang *dieksploitasi* lainnya. *Acunetix* merupakan alat otomatis yang dapat membantu perusahaan memindai aplikasi web mereka untuk mengidentifikasi dan mengetahui celah pada aplikasi [6].

Acunetix Web Vulnerability juga telah menjadi alat pilihan bagi banyak pelanggan di Pemerintahan, Militer, Pendidikan, Telekomunikasi, Perbankan, Keuangan, dan perusahaan *E-Commerce*, dan termasuk perusahaan-perusahaan besar lainnya dari berbagai negara.

Acunetix Web Vulnerability juga dapat mendeteksi dan melaporkan berbagai macam kerentanan dalam aplikasi yang dibangun pada arsitektur seperti *WordPress, PHP, ASP.NET, Java Frameworks, Ruby on Rails* dan masih banyak lainnya. *Acunetix Web Vulnerability* membawa fitur-set yang luas dari alat pengujian penetrasi otomatis,memungkinkan analis keamanan untuk melakukan penilaian kerentanan yang lengkap, dan memberikan laporan lengkap mengenai hasil dari scan secara jelas. Salah satu komponen kunci dari hasil scan adalah daftar semua kerentanan yang ditemukan dalam target pemindaian selama pemindaian. Tergantung pada jenis scan, ini dapat berupa *web alerts* atau *network alerts*, dan tanda dikategorikan menurut 4 tingkat keparahan: [10]

1. *High Risk Alert Level 3* : Kerentanan dikategorikan sebagai yang paling berbahaya, yang menempatkan target pada resiko maksimum untuk hacking dan pencurian data .
2. *Medium Risk Alert Level 2* : Kerentanan disebabkan oleh *server misconfiguration* dan *sitecoding* yang lemah, yang memfasilitasi gangguan *server* dan intruksi .
3. *Low Risk Alert Level 1* : Kerentanan berasal dari kurangnya enkripsi lalu lintas data atau jalur direktori pengungkapan .
4. *Information Alert* : ini adalah item yang telah ditemukan selama scan dan yang dianggap menarik, misalnya kemungkinan pengungkapan alamat *internal IP* atau alamat email, atau pencocokan *string* pencarian ditemukan di database Google Hacking, atau informasi tentang layanan yang telah ditemukan selama scanning .

Acunetix Web Vulnerability adalah salah satu aplikasi scanner web terkemuka yang sangat baik sebagai solusi untuk memecahkan masalah keamanan situs web Anda. Acunetix mampu menemukan kerentanan keamanan web lebih dari alat scanner lain yang bertebaran di internet.

Berikut adalah beberapa fitur utama yang ditawarkan oleh Acunetix Web Vulnerability Scanner [10]:

1. Teknologi *Acusensor*
2. Industri yang paling canggih dan mendalam dalam *SQL injection* dan pengujian *Cross site scripting*.
3. Mendukung *HTML5* penuh dengan *Acunetix DeepScan Teknologi*
4. Aplikasi scanning komprehensif baik untuk Halaman Single dan situs berbasis *JavaScript*
5. Mendukung *Mobile web site*
6. Dapat mendeteksi kerentanan *Blind XSS* dengan layanan *AcuMonitor*
7. Dapat mendeteksi otomatis kerentanan *XSS* berbasis *DOM*
8. Alat pengujian penetrasi Canggih, seperti *HTTP Editor* dan *HTTP Fuzzer*

9. Fasilitas pelaporan ekstensif termasuk laporan kepatuhan *PCI*
10. Multi-berulir dan petir scanner cepat merangkak ratusan ribu halaman dengan mudah.
11. *Acunetix* sudah digunakan oleh banyak perusahaan besar dan ternama diseluruh dunia seperti *Pentagon, American Express, AVG, HSBC* dan *Skype*.

Analisis keamanan pada sisi web server dalam penelitian ini dilakukan dengan menggunakan software Acunetix web vurnerability.

Pada penilaian *Base Score*, jika nilai *Base Score* semakin besar maka kerentanan tersebut perlu segera ditangani untuk mencegah *eksploitasi* lebih dalam oleh peretas [4]. Proses audit keamanan Aplikasi Web Prodi Teknik Informatika dibantu menggunakan aplikasi Acunetix Web Vulnerability. Acunetix Web Vulnerability merupakan aplikasi yang digunakan untuk mengaudit keamanan dari aplikasi berbasis web.

Aplikasi ini merupakan aplikasi yang dirancang untuk meniru cara seorang hacker dalam menemukan kerentanan seperti, *SQL Injection* dan *Cross Site Scripting Attack* sebelum peretas (*hacker*) melakukanya.Acunetix mendeteksi dan melaporkan beragam kerentanan yang dibangun dengan menggunakan arsitektur seperti *WordPress, PHP, ASP.NET, Java Frameworks, Ruby on Rails* dan lain-lain. Acunetix Web Vulnerability Scanner Hasil dari pemindaian keamanan aplikasi ini juga dapat digunakan sebagai laporan yang dapat diberikan kepada pengembang dan pihak manajemen yang bertanggung jawab.

3. HASIL DAN PEMBAHASAN

Analisis dilakukan untuk mengetahui permasalahan yang dialami saat ini dan memberikan solusi terhadap permasalahan tersebut. Analisis keamanan pada sisi web server dalam penelitian ini dilakukan dengan menggunakan *software Acunetix web vurnerability*. Aspek-aspek yang dianalisis meliputi:

1. *Blind injection*
2. *Cgi tester*
3. *Directory file*
4. *File checks*
5. *Google Hacking testing Database (GHDB)*
6. *Parameter manipulation*
7. *Sql injection*
8. *Text search*
9. *Version checks*
10. *Web application xfs*
11. *Entity encode heap overflow*

Dari analisis terhadap Aplikasi Web Prodi Teknik Informatika diUIKA menghasilkan keretanan dari sistem yang telah dilakukan didapatkan ,hasil kerentanan sebagai berikut.

1. Cross site scripting (XSS)

Tabel 1 Cross site scripting (XSS)

CVSS	Parameter	Nilai
	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	None
Base Score 6.4 (Medium)	Scope	Unchanged
	Confidentiality Impact	Partial
	Integrity Impact	Partial
	Availability Impact	None
CWE	CWE-79	
STANDAR ISO 27001:2005 YANG TERPENGARUH	12.4.1	
Discovered by		
/http://ti.fti.uika-bogor.ac.id/Scripts/PerScheme.XSS script		

2. SQL Injection

Tabel 2 SQL injection

CVSS	Parameter	Nilai
	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	None
Base Score 10.0 (Critical)	Scope	Unchanged
	Confidentiality Impact	High
	Integrity	High
	Availability	None
CWE	CWE-89	
STANDAR ISO 27001:2005 YANG TERPENGARUH	12.2.2,12.2.1,10.9.3	
Discovered by		
/Scripts/PerScheme/Sql_Injection.script		

3. Application error message

Tabel 3 Application Error Message

CVSS	Parameter	Nilai
	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	None
Base Score 5.3 (Medium)	Scope	Unchanged
	Confidentiality Impact	Low
	Integrity	None
	Availability	None
CWE	CWE-200	
STANDAR ISO 27001:2005 YANG TERPENGARUH	10.7.3,10.10.3,11,12.4.1	
Discovered by		
/Scripts/PerScheme/Error_Message.script		

4. Berkas Dokumentasi

Tabel 4 Berkas Dokumentasi

CVSS	Parameter	Nilai
	Attack Vector	Network
	Attack Complexity	Low
	Authentication	None
Base Score 5 (None)	Confidentiality Impact	Partial
	Integrity	None
	Availability	None
CWE	CWE-538	
STANDAR ISO 27001:2005 YANG TERPENGARUH	12.4.1	
Discovered by		
/Scripts/PerFolder/Backup_Folder.script		

5. Daftar Direktori

Tabel 5 Daftar Direktori

CVSS	Parameter	Nilai
	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	None
Base Score 7.5 (High)	Scope	Uchanged
	Confidentiality Impact	High
	Integrity	None
	Availability	None
CWE	CWE-538	
STANDAR ISO 27001:2005 YANG TERPENGARUH	10.7.3	
Discovered by		
/Scripts/PerFolder/Directory_Listing.script		

5. Daftar Direktori

Tabel 6 Daftar Direktori

CVSS	Parameter	Nilai
	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	None
Base Score 7.5 (High)	Scope	Uchanged
	Confidentiality Impact	High
	Integrity	None
	Availability	None
CWE	**CWE-538**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	10.7.3	
Discovered by		
/Scripts/PerFolder/Directory_Listing.script		

6. From HTML tanpa perlindungan Cross Site Request Forgery (CSFR)

Tabel 7 From HTML Tanpa Perlindungan (CSFR)

CVSS	Parameter	Nilai
	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	Required
Base Score 4.3 (Medium)	Scope	Unchanged
	Confidentiality Impact	None
	Integrity Impact	Low
	Availability Impact	None
CWE	**CWE-352**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	11.2.2	
Discovered by		
/Crawler/12-Crawler_Form_NO_CSRF.js		

7. Data penting pengguna dikirimkan dalam bentuk teks utuh

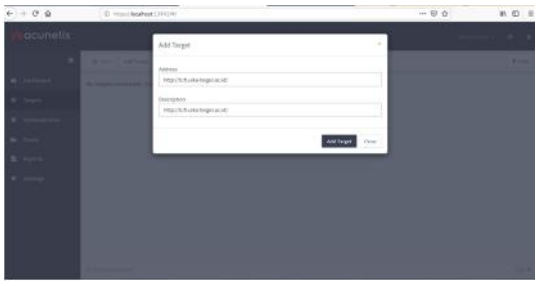
Tabel 8 Data penting pengguna

CVSS	Parameter	Nilai
	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	None
Base Score 9.1 (Critical)	Scope	Uchanged
	Confidentiality Impact	High
	Integrity	High
	Availability	None
CWE	**CWE-310**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	10.8.1	
Discovered by		
/Crawler/12-Crawler_User_Credentials_Plain_Text.js		

Pemindaian Acunetix Web Vulnerability

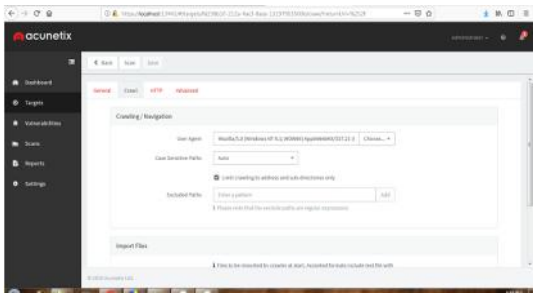
Pada tahapan ini melakukan uji coba pada objek, aplikasi Web Prodi Teknik Informatika dengan pemindaian menggunakan Acunetix untuk mengetahui kerentanan-kerentanan oleh aplikasi yang dilakukan dengan yang diharapkan. Target pengujian terdiri dari alamat website yang berada di indonesia dan alamat website yang berasal dari luar negeri. Target tersebut telah ditentukan oleh peneliti aplikasi. Metode yang digunakan dalam penelitian ini adalah metode kualitatif dengan menggunakan beberapa tools berupa perangkat lunak dan cara-cara tertentu yang lazim digunakan untuk menguji keamanan aplikasi.

Untuk melakukan analisis keamanan aplikasi , dilakukan menggunakan software, yaitu dengan Acunetix web vurnerability scanner. Langkah-langkah melakukan pemindaian yaitu :



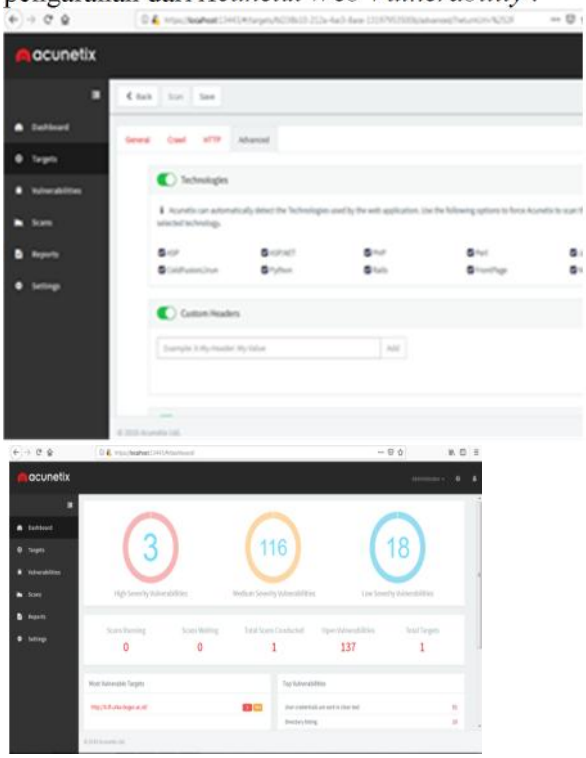
Gambar 2 Add Target

Add Target merupakan input dari *url* target *address* beserta *description* dengan *http//ti.ft.uika-bogor.ac.id/*



Gambar 3 *Crawl* atau *Navigation*

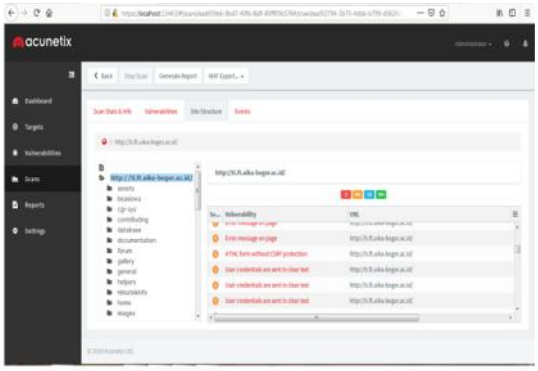
Carwl atau *navigation* menrupakan pengarahan dari *Acunetix Web Vulnerability* .



Gambar 4 Configurasi Advanced

Configurasi Advanced berfungsi mencari kerentanan dengan dukungan teknologi dan fungsi lainnya yang biasanya ada aplikasi web, sehingga objek tersebut dapat ditemukan keretanan

Gambar 5 Create Scanning
Gambar diatas menunjukan saya mencari kerentanan secara keseluruhan dengan mengambil type full scan.

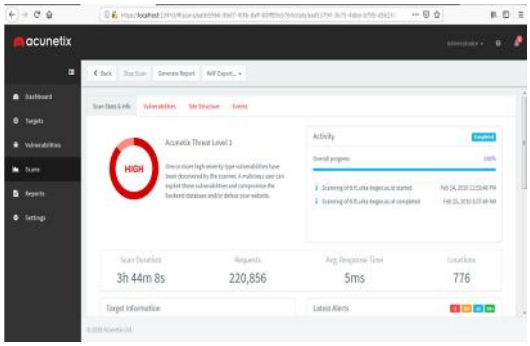


Gambar 6 Strktutur Data

Struktur data yang ditemukan merupakan hasil yang didapat dari dalam aplikasi web tersebut.Setiap data yang ditemukan keretanannya baik rendah maupun *high* .

3.2.2 Hasil Analisis

Hasil yang ditemukan merupakan kerentanan yang dapat diukur dari jumlah keretanan pada aplikasi web tersebut dan level yang ditemukan oleh *Acunetix Web Vulnerability*.



Gambar 7 Hasil dari Keretanan

Hasil yang ditampilkan dari

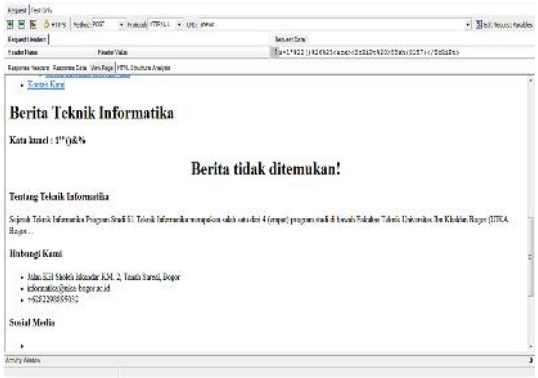
Acunetix Web Vulnerability mencapai level tiga yang merupakan harus adanya evaluasi terhadap celah atau keretanan yang di temukan untuk base score biasanya hanya ditampilkan di kerentanan atau celah.Sendangkan total kerentanan yang ditemukan terdapat gambar 7.

Gambar 8 Total Keseluruhan Keretanan

Gambar 8 menujukan keseluruhan keretanan yang didapat dari *Acunetix Web Vulnerability* terhadap Aplikasi Web Prodi Teknik Informatika diUIKA. Untuk yang kredensial jumlahnya 3, sendangkan yang mendium jumlah 116 dan low berjumlah 18.

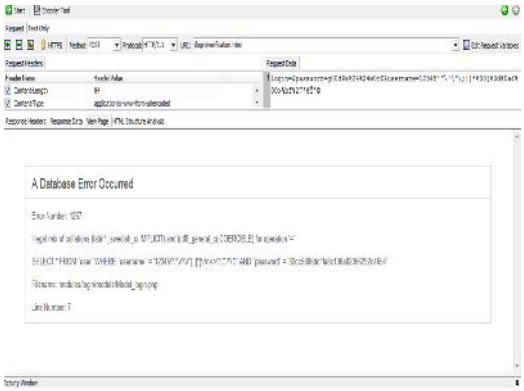
Pengujian Aplikasi Web

Pengujian yang didapat dari Acunetix Web Vulnerability dengan menggunakan *Launch Attack HTTP Editor* ,salah satu kerentanan yang didapat dengan menghasilkan page dari aplikasi web tersebut.



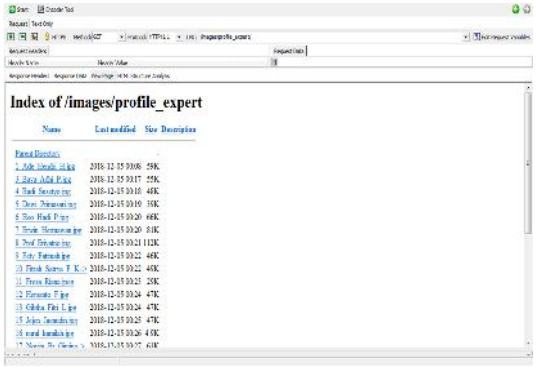
Gambar 9 Tampilan Kerentanan News

Hasil yang ditemukan berupa page dari *Cross site scripting (XSS)* dengan isi berita tidak ditemukan dan kata kunci : 1''''()&% .



Gambar 10 Aplikasi *Eror Message*

Hasil yang ditemukan *Database Eror Occurred* dari server ke pengguna sehingga menjadi rentan.



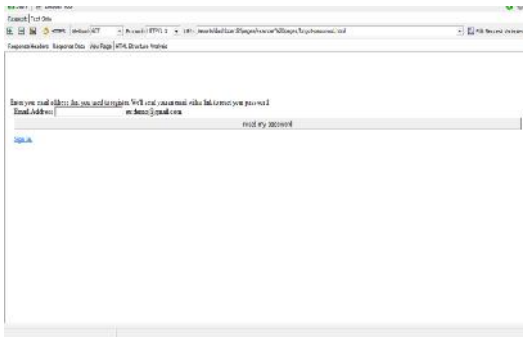
Gambar 11 Derektori Listing

Hasil dari Daftar *Direktori* berupa *Listing* yang ditemukan berasal dari *http://ti.ft.uika-bogor.ac.id/images/profile_expert/*.

Gambar 12 *From HTML* Tanpa Perlindungan *CSRF*

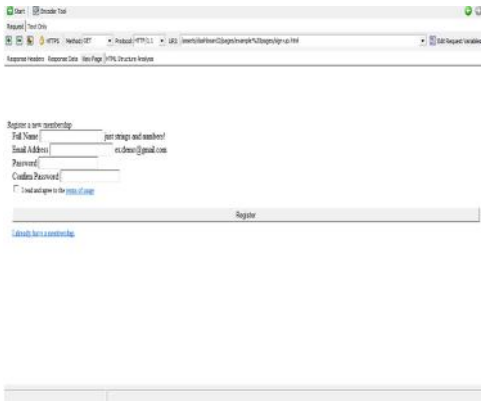
Gambar 12 hasil yang ditemukan pemalsuan permintaan lintas situs, juga dikenal sebagai serangan satu kali klik saat jaringan berjalan situs web di mana perintah

yang tidak sah dikirimkan dari pengguna yang dipercaya oleh situs web tersebut.



Gambar 13 Tampilan Dashboard Email

Gambar 14 Tampilan login



Gambar14 Tampilan Register

4. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan tentang aplikasi Profil Potensi Berdasarkan hasil yang diperoleh kerentanan-kerentanan yang bersifat kredensial seperti serangan *SQL Injection*, *Direktori* berupa *Listing*, *HTML* tanpa perlindungan *Cross Site Request Forgery (CSFR)*, dan serangan *Cross Site Scripting (XSS)*. hasil yang ditemukan Aplikasi web Prodi Teknik Informatika mencapai *level High Critical*, sehingga keamanan pada aplikasi web tersbut belum dikatakan aman dengan ditemukannya *web alert* yang berbahaya.

Dari penelitian yang telah dilakukan, perlu dilakukan penelitian mendalam mengenai kerentanan Aplikasi dari segi *Temporal* dan *Environmental* agar penilaian dari kerentanan-kerentanan yang dialami memiliki penilaian yang lebih akurat. Serta diperlukan penyajian hasil audit keamanan ini dalam bentuk kerangka audit yang lain seperti OWASP atau standar keamanan standar keamanan informasi lain agar hasilnya lebih optimal.

DAFTAR PUSTAKA

[1] M . Syafrizal, "ISO 17799: Standar Sistem Manajemen Keamanan Informasi."

[2] B. Rahardjo ,“Keamanan Sistem Informasi Berbasis Internet,” PT Insan Komunikasi Indonesia, Bandung, 2002.

[3] Remick. (2011). Aplikasi Web. Retrievedfrom http://technophoriajogja.com/2014/01/28/pengertian-tentang-aplikasi-berbasis-web/ FIRST, Common Vulnerability Scoring System v3.0: User Guide, 2014.

[4] ISO,"Information technology Security techniques ,Information security management systems -- Requirements," ISO Organization 2005

[5] Acunetix, "Acunetix Web Vulnerability Scanner," 2005.

[6] Satoto, Kodrat Iman, Sistem Analisis Keamanan Informasi Akademik Berbasis Web Di Fakultas Teknik Universitas Diponegoro 2009

[7] Detty Metasari, Fatah Yasin Irsyadi, S.T., M.T, Ir. Jatmiko, M.T, Analisis Keamanan Website , di UNIVERSITAS MUHAMMADIYAH SURAKARTA 2014

[8] Edhy Sutanta , Analisis Keamanan Sistem Aplikasi (STUDY KASUS

APLIKASI E-LEARNING DI IST AKPRIND YOGYAKARTA) 2008.

[9] Acunetix, https://www.centerklik.com/amankan-website-dengan-acunetix-web-vulnerability-scanner/ 2005.

[10] Penetration Testing Overview, http :// www. coresecurity.com/ penetration -testing - overview, 28 Oktober 2015.

[11] ISO, "Information technology -- Security techniques -- Information security management systems Requirements," ISO Organization,2005.

[12] Ritzkal R, Goeritno A, Hendrawan AHH. 2016. Implementasi ISO/IEC 27001:2013 Untuk Sistem Manajemen Keamanan Informasi (SMKI) Pada Fakultas Teknik Uika-Bogor. Seminar Nasional Sains dan Teknologi 2016.