Tersedia di http://jtsiskom.undip.ac.id (21 Agustus 2016)
DOI: 10.14710/jtsiskom.4.3.2016.479-484
Jurnal Teknologi dan Sistem Komputer, 4(3), 2016, 479-484

Analisis Keamanan pada Aplikasi Her-registrasi Online Mahasiswa Universitas Diponegoro

Hilal Afrih Juhad*), R. Rizal Isnanto, Eko Didik Widianto
Jurusan Sistem Komputer, Fakultas Teknik, Universitas Diponegoro
Jl. Prof. Sudharto, Tembalang, Semarang, Indonesia

Abstract – ***The security aspect is often forgotten in the application of Information Technology. The attacks were caused by the negligence of the developer causes damage to the system used. SQL Injection attacks, Cross Site Scripting attacks, and no use of encrypted channels lead to the exposure of sensitive data users. Objectives of this research is to perform an audit and analysis of the security aspects against the Her-registration Colege Students Online Application of Diponegoro University. Audit and security analysis is prevention step so that the vulnerabilities found not to be a entrances to the system hackers. The results of this research are a security audit report that contains the vulnerability Her-registration College Students Online Application of Diponegoro University. The audit report will be used as a reference for application developers Her-registration Colege Students Online Application of Diponegoro University to improve the system.***

Keywords : SQL Injection, Cross Site Scripting

I PENDAHULUAN

Keamanan data elektronik menjadi hal yang sangat penting di perusahaan penyedia jasa Teknologi Informasi (TI) maupun industri lainnya, seperti perusahaan export-import, tranportasi, lembaga pendidikan, pemberitaan, hingga perbankan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur kritikal (penting).[2]

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.[5]

Menurut kutipan dari Rahardjo[5] dan Syafrizal[2] aspek keamanan data ini menjadi aspek yang sangat penting walaupun pada praktiknya seringkali dilupakan, hanya karena mengejar kinerja. Pengamanan ini diperlukan untuk memenuhi aspek Kerahasiaan *(Confidentially)*, Integritas *(Integrity)* dan Ketersediaan *(Availability)* dari sebuah sistem informasi.Registrasi *Online* merupakan suatu aplikasi *web* untuk melakukan registrasi mahasiswa baru Universitas Diponegoro Semarang, yang terdiri dari jalur masuk : PSSB D3, SNMPTN, SBMPTN, UJIAN MANDIRI, dan UM D3. Adapun registrasi yang dilakukan dengan cara mengisikan data, meliputi data pribadi, data sekolah, data orang tua/wali, dan data prestasi.[7]

Menurut penjelasan dari situs resmi Registrasi *Online* Mahasiswa Universitas Diponegoro[7], secara tidak langsung menyebutkan bahwa aplikasi tersebut menyimpan data-data penting mulai dari kategori jalur masuk mahasiswa, sampai data diri dari mahasiswa. Dari data-data tersebut bisa diolah menjadi informasi mengenai kriteria pembayaran SPP mahasiswa. Jika data-data tersebut dimanipulasi oleh pengguna yang tidak sah, maka dapat menyebabkan integritas data tersebut menjadi tidak valid. Oleh karena itu evaluasi secara berkala terhadap aspek keamanan pada Aplikasi Registrasi *Online* Mahasiswa Universitas Diponegoro perlu diterapkan. Tindakan evaluasi ini dilakukan dengan menggunakan uji penetrasi baku *(standard penetration testing)* yang kemudian hasilnya dianalisis untuk menentukan langkah-langkah yang perlu dilakukan untuk memperbaiki indikasi celah keamanan pada aplikasi *web* tersebut.

Penetration testing (uji penetrasi) adalah sebuah upaya proaktif, disetujui dan diberi wewenang untuk mengevaluasi keamanan infrastruktur Teknologi Informasi dengan aman, kemudian penguji penetrasi *(penetration tester)* mencoba untuk mengeksploitasi kerentanan sistem. Tindakan eksploitasi tersebut termasuk mengeksploitasi sistem operasi, identifikasi layanan *(service)* yang sedang berjalan, identifikasi kelemahan aplikasi, dan mengidentifikasi konfigurasi sistem yang kurang tepat.
[8]

Langkah-langkah yang biasanya dilakukan dalam melakukan uji penetrasi secara garis besar dibagi menjadi 5, di antaranya adalah sebagai berikut.

a. *Target discovery and enumeration* (Deteksi target dan enumerasi)
b. *Vulnerability identification* (Deteksi kerentanan)
c. *Exploitation* (Eksploitasi)
d. *Level of control after exploitation* (Level kendali setelah eksploitasi)
e. *Reporting*[4]

*) Penulis Korespondensi
Email : afrihjuhadasyifa@gmail.com

Dikirim:22 Juli 2016; Direvisi:19 Agustus 2016; Diterima:21 Agustus 2016

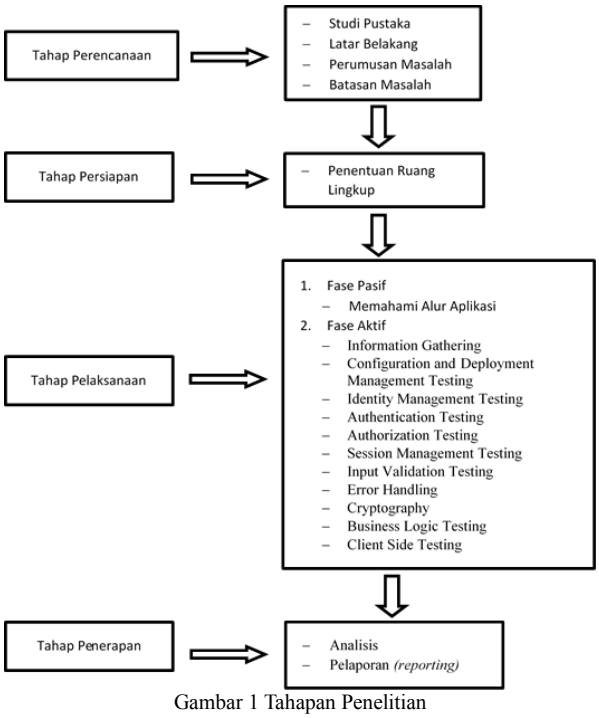
II METODOLOGI PENELITIAN

A. Metodologi Penelitian

Penelitian ini bertujuan untuk melakukan audit keamanan pada Aplikasi Her-registrasi Online Mahasiswa Universitas Diponegoro. Audit keamanan aplikasi Aplikasi Her-registrasi Online Mahasiswa Universitas Diponegoro dilakukan menggunakan aplikasi audit keamanan automatis Acunetix.

Hasil audit keamanan tersebut disajikan dalam bentuk kerentanan yang dialami berdasarkan kebutuhan minimum keamanan aplikasi berdasarkan standar ISO 27001:2005.

Pada Gambar 1 menunjukan diagram alir proses audit keamanan Aplikasi Her-registrasi Online Mahasiswa Universitas Diponegoro.



Gambar 1 Tahapan Penelitian

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

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) [6]

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. Contoh dari tabel tersebut disajikan dalam bentuk sebagai berikut.

Tabel 1 Contoh Penyajian Hasil audit keamanan

	PARAMETER	**NILAI**
CVSS	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	None
Base Score **……** **(…….)**	Scope	Unchanged
	Confidentiality Impact	Low
	Integrity Impact	None
	Availability Impact	None
CWE	**CWE-…….**	
STANDAR ISO 27001:2005 YANG TERPENGARUH		
Poin-poin yang terpengaruh		

Pada penilaian *Base Score*, jika nilai *Base Score* semakin besar maka kerentanan tersebut perlu segera ditangani untuk mencegah eksploitasi lebih dalam oleh peretas.

Proses audit keamanan Aplikasi Her-registrasi Online Mahasiswa Universitas Diponegoro dibantu menggunakan aplikasi Acunetix Web Vulnerability Scanner. Acunetix Web Vulnerability Scanner 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.[1]

Penilaian kerentanan ini akan direpresentasikan ke dalam bentuk angka. Angka ini nantinya akan dijadikan acuan seberapa parah kerentanan yang dialami. *Common Vulnerability Scoring System* (CVSS) merupakan sebuah kerangka *(framework)* terbuka yang digunakan untuk mengkomunikasikan karakteristik dan dampak yang ditimbulkan oleh sebuah kerentanan aplikasi. CVSS terdiri dari tiga kelompok pengukuran yaitu *Base, Temporal,* dan

Environmental. Kelompok *Base* mewakili kualitas intrinsik sebuah kerentanan, kelompok *Temporal* mencerminkan karakteristik dari sebuah kerentanan yang berubah sewaktu-waktu, sedangkan kelompok *Environmental* mewakili karakteristik sebuah kerentanan yang unik untuk lingkungan pengguna.[3]

Common Weakness Enumeration (CWE) merupakan proyek perangkat lunak komunitas yang berisi katalog kelemahan dan kerentanan dari sebuah perangkat lunak. Tujuan dari proyek ini adalah untuk lebih memahami kelemahan sebuah perangkat lunak dan untuk menciptakan alat otomatis yang dapat digunakan untuk mengidentifikasi, memperbaiki, dan mencegah kerentanan-kerentanan tersebut. Proyek ini disponsori oleh Mitre.[9]

Common Vulnerability and Exposures (CVE) adalah sebuah kamus yang dipublikasikan secara umum dan berisi identitas (identitas CVE) kerentanan keamanan informasi. Pengidentifikasi CVE mempermudah untuk saling berbagi data di dalam database mengenai keamanan informasi pada jaringan yang berbeda serta menyediakan dasar untuk mengevaluasi alat kemanan milik sebuah organisasi. Jika laporan dari alat pengevaluasi keamanan dilengkapi dengan identitas CVE, maka akan lebih cepat dan mudah dicari penangananya.[10]

III ANALISIS DAN PEMBAHASAN

Dari penelitian yang telah dilakukan didapatkan hasil kerentanan sebagai berikut.

A. Daftar direktori

Tabel 2 Daftar direktori

	PARAMETER	NILAI
CVSS	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	None
***Base Score* 5.3 (MEDIUM)**	Scope	Unchanged
	Confidentiality Impact	Low
	Integrity Impact	None
	Availability Impact	None
CWE	**CWE-538**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**10.7.3, 10.10.3, 12.4.1, 12.5.4**	
Poin-poin yang terpengaruh		
1. /herregs1d3/system/application/javascript/colorbox 2. /herregs1d3/system/application/javascript/colorbox/css 3. /herregs1d3/system/application/javascript/colorbox/images 4. /herregs1d3/system/application/javascript/colorbox/images/internet_explorer 5. /herregs1d3/system/application/javascript/colorbox/js 6. /info/css 7. /info/fonts 8. /info/images 9. /info/js 10. /info/js/google-code-prettify 11. /info/js/sharrre 12. /system/application/css/images		

B. Berkas dokumentasi

Tabel 3 Berkas dokumentasi

	PARAMETER	NILAI
CVSS	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	None
***Base Score* 5.1 (MEDIUM)**	Scope	Unchanged
	Confidentiality Impact	Low
	Integrity Impact	None
	Availability Impact	None
CWE	**CWE-200**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**10.7.3, 10.10.3, 12.5.4.1**	
Poin-poin yang terpengaruh		
1. /herpasca/license.txt 2. /license.txt 3. /pasca/license.txt		

C. Kemungkinan direktori sensitif

Tabel 4 Kemungkinan direktori sensitif

	PARAMETER	NILAI
CVSS	Attack Vector	Adjacent
	Attack Complexity	High
	Privilege Required	None
	User Interaction	None
***Base Score* 3.1 (MEDIUM)**	Scope	Unchanged
	Confidentiality Impact	Low
	Integrity Impact	None
	Availability Impact	None
CWE	**CWE-538**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**10.7.3, 10.10.3, 12.5.4.1**	
Poin-poin yang terpengaruh		
1. /herpasca/system 2. /herpasca/system/application/config 3. /herpasca/system/application/errors 4. /herpasca/system/database 5. /herpasca/system/logs 6. /herpasca/uploads 7. /herregs1d3/system 8. /herregs1d3/system/application/config 9. /herregs1d3/system/application/errors 10. /herregs1d3/system/database 11. /herregs1d3/system/logs 12. /herregs1d3/uploads 13. /pasca/system 14. /pasca/system/application/config 15. /pasca/system/application/errors 16. /pasca/system/database 17. /pasca/system/logs 18. /pasca/uploads 19. /system 20. /system/application/config 21. /system/application/errors 22. /system/database 23. /system/logs 24. /uploads		

D. Alamat email ditemukan

Tabel 5 Alamat email ditemukan

	PARAMETER	NILAI
CVSS	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	None
***Base Score* 0.0 (None)**	Scope	Unchanged
	Confidentiality Impact	None
	Integrity Impact	None
	Availability Impact	None
CWE	**CWE-538**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**10.7.3, 10.10.3, 12.5.4**	
Poin-poin yang terpengaruh		
/info		

E. Penulisan *password* dengan fitur *auto-complete* diaktifkan

Tabel 6 Penulisan *password* dengan fitur *auto-complete* diaktifkan

	PARAMETER	NILAI
CVSS	Attack Vector	Network
	Attack Complexity	High
	Privilege Required	Low
	User Interaction	Required
***Base Score* 4.4 (MEDIUM)**	Scope	Changed
	Confidentiality Impact	Low
	Integrity Impact	Low
	Availability Impact	None
CWE	**CWE-200**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**10.7.3, 10.10.3, 12.5.4**	
Poin-poin yang terpengaruh		
1. /herpasca 2. /herregs1d3 3. /index.php 4. /pasca		

F. Kemungkinan pengungkapan *username* atau *password*

Tabel 7 Kemungkinan pengungkapan *username* atau *password*

	PARAMETER	NILAI
CVSS	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	None
***Base Score* 0.0 (None)**	Scope	Unchanged
	Confidentiality Impact	None
	Integrity Impact	None
	Availability Impact	None
CWE	**CWE-200**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**10.7.3, 10.10.3, 12.5.4**	
Poin-poin yang terpengaruh		
/info/css/modern.css		

G. Data penting pengguna dikirimkan dalam bentuk teks utuh

Tabel 8 Pengiriman data tanpa melalui jalur enkripsi

	PARAMETER	NILAI
CVSS	Attack Vector	Adjacent
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	None
***Base Score* 6.1 (MEDIUM)**	Scope	Changed
	Confidentiality Impact	Low
	Integrity Impact	Low
	Availability Impact	None
CWE	**CWE-310**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**10.8.1, 10.9.2**	
Poin-poin yang terpengaruh		
1. /herpasca 2. /index.php 3. /herpasca/ 4. /herregs1d3/		

H. *SQL Injection*

Tabel 9 *SQL Injection*

	PARAMETER	NILAI
CVSS	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	None
***Base Score* 8.2 (MEDIUM)**	Scope	Unchanged
	Confidentiality Impact	High
	Integrity Impact	Low
	Availability Impact	None
CWE	**CWE-89**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**10.9.1, 10.9.3, 12.2.1, 12.2.2**	
Poin-poin yang terpengaruh		
Poin-poin yang terpengaruh	**/herpasca/index.php/home**	
Parameter yang terpengaruh	nomor_peserta	
Poin-poin yang terpengaruh	**/herpasca/index.php/home**	
Parameter yang terpengaruh	*Password*	
Poin-poin yang terpengaruh	**/herregs1d3/index.php/home**	
Parameter yang terpengaruh	nomor_peserta	
Poin-poin yang terpengaruh	**/herregs1d3/index.php/home**	
Parameter yang terpengaruh	*Password*	
Poin-poin yang terpengaruh	**index.php/home**	
Parameter yang terpengaruh	nomor_peserta	
Poin-poin yang terpengaruh	**index.php/home**	
Parameter yang terpengaruh	*Password*	
Poin-poin yang terpengaruh	**/pasca/index.php/home**	
Parameter yang terpengaruh	*Password*	

I. Cross Site Scripting

Tabel 10 *Cross Site Scripting*

	PARAMETER	NILAI
CVSS	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None

	User Interaction	None
Base Score **5.3** **(MEDIUM)**	Scope	Unchanged
	Confidentiality Impact	Low
	Integrity Impact	None
	Availability Impact	None
CWE	**CWE-79**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**10.9.3, 12.2.1, 12.2.2, 12.2.4**	
Poin-poin yang terpengaruh		
Poin-poin yang terpengaruh	**/index.php/home**	
Parameter yang terpengaruh	nomor_peserta	

J. jQuery versi lama

Tabel 11 jQuery versi lama

CVSS	**PARAMETER**	**NILAI**
	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	Required
Base Score **5.4** **(MEDIUM)**	Scope	Unchanged
	Confidentiality Impact	Low
	Integrity Impact	Low
	Availability Impact	None
CWE	**CWE-538**	
CVS	**CVE-2011-46969**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**10.9.3, 12.2.1, 12.2.4, 12.4.1**	
Poin-poin yang terpengaruh		
1. /herpasca/system/application/javascript/j*query*.min.js 2. /pasca/system/application/javascript/j*query*.min.js 3. /system/application/javascript/j*query*.min.js		

K. Form HTML tanpa perlindungan *Cross Site Request Forgery* (CSRF)

Tabel 12 From HTML tanpa perlindungan CSRF

CVSS	**PARAMETER**	**NILAI**
	Attack Vector	Network
	Attack Complexity	High
	Privilege Required	None
	User Interaction	Required
Base Score **3.1** **(Low)**	Scope	Unchanged
	Confidentiality Impact	Low
	Integrity Impact	None
	Availability Impact	None
CWE	**CWE-352**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**11.2.2**	
Poin-poin yang terpengaruh		
1. /herpasca 2. /index.php 3. /herregs1d3 4. /pasca		

L. Serangan tebak *password* pada form login

Tabel 13 Serangan tebak *password*

CVSS	**PARAMETER**	**NILAI**
	Attack Vector	Network
	Attack Complexity	High
	Privilege Required	None
	User Interaction	None
Base Score **6.5** **(MEDIUM)**	Scope	Changed
	Confidentiality Impact	Low
	Integrity Impact	Low
	Availability Impact	Low
CWE	**CWE-307**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**12.2.2, 11.2.2, 12.2.1, 12.2.2, 12.4.1**	
Poin-poin yang terpengaruh		
1. /herregs1d3/index.php/home 2. /herpasca/ 3. /index.php 4. /herpasca/		

M. Method OPTIONS diaktifkan

Tabel 14 Method OPTIONS diaktifkan

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 Impact	None
	Availability Impact	None
CWE	**CWE-200**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**12.4.1**	
Poin-poin yang terpengaruh		
Web Server		

N. *Session cookie* tanpa pengaturan *HttpOnly Flag*

Tabel 15 *Session Cookie* tanpa pegaturan *HttpOnly Flag*

CVSS	**PARAMETER**	**NILAI**
	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	Required
Base Score **0.0** **(None)**	Scope	Unchanged
	Confidentiality Impact	None
	Integrity Impact	None
	Availability Impact	None
CWE	**CWE-16**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**12.4.1**	
Poin-poin yang terpengaruh		
/		

O. *Session Cookie* tanpa mengatur *Secure Flag*

Tabel 16 *Session Cookie* tanpa mengatur *Secure Flag*

CVSS	**PARAMETER**	**NILAI**
	Attack Vector	Network
	Attack Complexity	Low
	Privilege Required	None
	User Interaction	Required
***Base Score* 0.0 (None)**	Scope	Unchanged
	Confidentiality Impact	None
	Integrity Impact	None
	Availability Impact	None
CWE	**CWE-16**	
STANDAR ISO 27001:2005 YANG TERPENGARUH	**12.4.1**	
Poin-poin yang terpengaruh		
/		

IV KESIMPULAN

Dari hasil pengujian keamanan pada Aplikasi Her-registrasi Online Mahasiswa Universitas Diponegoro, diperoleh kerentanan-kerentanan yang bersifat kredensial seperti serangan *SQL Injection* pada form login, *serangan Cross Site Scripting* (XSS) pada form login. Kemudian terdapat pula kerentanan yang bersifat informasional bagi peretas untuk mengeksploitasi sistem lebih jauh seperti kemungkinan serangan tebak password, terlihatnya daftar direktori sensitif, tidak adanya pengaturan mengenai *httpOnly Flag* dan *Secure Flag*, serta tidak adanya kanal terenkripsi (HTTPS) dalam pengiriman data dari pengguna menuju server yang dapat mengakibatkan terendusnya informasi sensitif pengguna oleh peretas.

Dari penelitian yang telah dilakukan, perlu dilakukan penelitian mendalam mengenai kerentanan Aplikasi Her-registrasi Online Mahasiswa Universitas Diponegoro 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.

UCAPAN TERIMAKASIH

Terimakasih disampaikan kepada seluruh civitas akademik Prodi Sistem Komputer Undip yang telah memberikan berbagai masukan terhadap penelitian yang telah dilaksanakan, serta memberikan berbagai fasilitas laboratorium sebagai penunjang dan pengujian kegiatan akademik.

DAFTAR PUSTKA

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

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

[3] FIRST, *Common Vulnerability Scoring System v3.0: User Guide*, 2014.

[4] A. Singh, *Metasploit Penetration Testing Cookbook*, Birmingham: Packt Publishinf, 2012.

[5] B. Rahardjo, "Keamanan Sistem Informasi Berbasis Internet," *PT Insan Komunikasi Indonesia, Bandung*, 2002.

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

[7] ---, *Registrasi Online Mahasiswa*, http://reg-online.undip.ac.id/index.php, 19 Oktober 2015.

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

[9] ---, Mitre. *About CWE*, http://cwe.mitre.org/about/index.html, 2 Februari 2016.

[10] ---, Mitre. *Common Vulnerability and Exposures*, https://cve.mitre.org/about/index.html, 8 Februari 2016.

