

**ANALISIS KEAMANAN WEBSITE E-LEARNING FAKULTAS
KESEHATAN UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA MENGGUNAKAN METODE
VULNERABILITY ASSESSMENT**

TUGAS AKHIR

Diajukan sebagai salah satu syarat memperoleh gelar Sarjana
Program Studi S-1 Teknologi Informasi



Disusun oleh:

MAFA MAGETA
202104004

**PROGRAM STUDI S-1 TEKNOLOGI INFORMASI
FAKULTAS TEKNIK & TEKNOLOGI INFORMASI
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA
2024**

HALAMAN PENGESAHAN

TUGAS AKHIR

ANALISIS KEAMANAN *WEBSITE E-LEARNING* FAKULTAS KESEHATAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA MENGGUNAKAN METODE *VULNERABILITY ASSESSMENT*

Diajukan oleh:

MAFA MAGETA
202104004

Telah dipertahankan di depan dewan penguji dan dinyatakan sah
sebagai salah satu syarat untuk memperoleh gelar Sarjana
di Fakultas Teknik & Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta

Tanggal: 11 Juli 2024

Mengesahkan:

Pembimbing I

Alfina Rizqi Lahitani, S.Kom., M.Eng.
NIDN: 0506019202

Pembimbing II

Adkhan Sholeh, S.Si., M.Cs.
NIDN: 0510127501

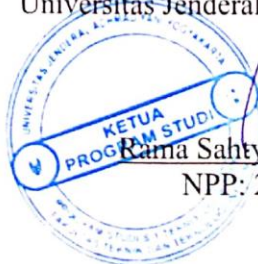
Penguji I

Arief Ikhwan Wicaksono, S.Kom., M.Cs.
NIDN: 0512128401

Penguji II

Rama Sahtyawan, S.T., M.Cs.
NIDN: 0518108001

Ketua Program Studi S-1 Teknologi Informasi
Fakultas Teknik & Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta



Rama Sahtyawan, S.T., M.Cs.
NPP: 2019.13.0150

PERNYATAAN

Saya yang bertanda tangan di bawah ini, adalah mahasiswa Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta,

Nama : Mafa Mageta
NPM : 202104004
Program Studi : S-1 Teknologi Informasi
Judul Tugas Akhir : Analisis Keamanan *Website E-Learning* Fakultas Kesehatan
Universitas Jenderal Achmad Yani Yogyakarta
Menggunakan Metode *Vulnerability Assessment*

Menyatakan bahwa hasil penelitian dengan judul tersebut di atas adalah asli karya saya sendiri dan bukan hasil plagiarisme. Semua referensi dan sumber terkait yang dikutip dalam karya ilmiah ini telah ditulis sesuai kaidah penulisan ilmiah yang berlaku. Dengan ini, saya menyatakan untuk menyerahkan hak cipta penelitian kepada Universitas Jenderal Achmad Yani Yogyakarta guna kepentingan ilmiah.

Demikian surat pernyataan ini dibuat dengan sebenar-benarnya tanpa ada paksaan dari pihak mana pun. Apabila terdapat kekeliruan atau ditemukan adanya pelanggaran akademik di kemudian hari, maka saya bersedia menerima konsekuensi yang berlaku sesuai ketentuan akademik.

Yogyakarta, 11 Juli 2024


Mafa Mageta

KATA PENGANTAR

Dengan penuh rasa syukur kepada Tuhan Yang Maha Esa, penulis berhasil menyelesaikan skripsi berjudul “Analisis Keamanan *Website E-Learning* Fakultas Kesehatan Universitas Jenderal Achmad Yani Yogyakarta Menggunakan Metode *Vulnerability Assessment*”. Skripsi ini merupakan salah satu syarat untuk memperoleh gelar Sarjana Komputer di Fakultas Teknik dan Teknologi Informasi, Universitas Jenderal Achmad Yani Yogyakarta. Dalam proses penulisan skripsi ini, tentunya penulis tidak dapat berjalan sendiri. Oleh karena itu, pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan bantuan dan dukungan.

1. Bapak Rama Sahtyawan, S.T., M.Cs. selaku Ketua Program Studi Teknologi Informasi Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
2. Ibu Alfirna Rizqi Lahitani, S.Kom., M.Eng. selaku Dosen Pembimbing Tugas Akhir karena atas bimbingan, dukungan, dan kesabarannya selama proses penulisan tugas akhir ini. Tanpa bimbingan dan masukan berharga dari beliau mungkin saya tidak akan dapat menyelesaikan tugas akhir ini dengan baik;
3. Bapak Adkhan Sholeh, S.Si., M.Cs. selaku Dosen Pembimbing Akademik saya selama perkuliahan;
4. Seluruh dosen yang telah memberikan saya wawasan, ilmu serta pengalaman selama menjadi mahasiswa di Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
5. Ibu, Ayah dan Keluarga besar saya yang telah memberikan saya dukungan dan restu, sehingga saya dapat menyelesaikan masa studi ini;
6. Teman-Teman saya Susi Dwi Nur Putri, Melainaya Agusaputri, Firmansyah, Isnaini Syarifatun Nisa, Rindiani Aprilianti, Anggita Naura Zahruf, Ahmad Nurhidayat, Khoirul Anam serta seluruh angkatan 20 Prodi Teknologi Informasi yang tidak bisa saya sebutkan satu-persatu;

7. Diri saya sendiri Mafa Mageta, yang telah bekerja keras, mengorbankan waktu serta tenaga dalam proses penulisan laporan akhir ini.

Penulis menyadari bahwa laporan akhir ini belum mencapai kesempurnaan. Oleh karena itu, dengan rendah hati, penulis sangat menghargai kritik dan saran yang membangun dari semua pihak yang telah meluangkan waktu untuk membaca laporan tugas akhir ini.

Yogyakarta, 11 Juli 2024

Mafa Mageta

DAFTAR ISI

JUDUL	i
HALAMAN PENGESAHAN	ii
PERNYATAAN.....	iii
KATA PENGANTAR.....	iv
DAFTAR TABEL	viii
DAFTAR GAMBAR.....	ix
DAFTAR LAMPIRAN	x
DAFTAR SINGKATAN	xi
INTISARI	xii
ABSTRACT	xiii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	4
1.3 Batasan Masalah.....	4
1.4 Pertanyaan Penelitian.....	4
1.5 Tujuan Penelitian	5
1.6 Manfaat Hasil Penelitian	5
BAB 2 TINJAUAN PUSTAKA DAN LANDASAN TEORI	6
2.1 Tinjauan Pustaka	6
2.2 Landasan Teori.....	11
2.2.1 Website	11
2.2.2 E-learning.....	14
2.2.3 Keamanan Informasi	14
2.2.4 Vulnerability Assessment.....	15
2.2.5 Vulnerability (Kerentanan).....	16
2.2.6 NsLookup.....	22
2.2.7 Nmap	23
2.2.8 Nessus.....	23

2.2.9 CVSS (<i>The Common Vulnerability Scoring System</i>)	24
2.2.10 Downgrade Attacks	27
2.2.11 SSL Stripping Man in The Middle Attacks.....	27
2.2.12 Cookie Hijacking	27
2.2.13 Cross Site Scripting (XSS).....	28
2.2.14 Clickjacking.....	28
2.2.15 SYN Scan	31
BAB 3 METODE PENELITIAN	32
3.1 Bahan dan Alat Penelitian.....	33
3.2 Jalan Penelitian.....	34
BAB 4 HASIL PENELITIAN	36
4.1 Ringkasan Hasil Penelitian	36
4.2 Testing.....	36
4.2.1 Identifikasi alamat IP menggunakan Nslookup	36
4.2.2 Pemindaian alamat IP menggunakan Nmap.....	37
4.2.3 Pemindaian alamat IP menggunakan Nessus	40
4.3 Analisa.....	44
4.3.1 Analisis hasil pemindaian menggunakan Nmap	44
4.3.2 Analisis hasil pemindaian menggunakan Nessus.....	45
4.4 Pembahasan.....	49
4.4.1 Rekomendasi	49
BAB 5 KESIMPULAN DAN SARAN	56
5.1 Kesimpulan	56
5.2 Saran.....	56
DAFTAR PUSTAKA	58
LAMPIRAN.....	63

DAFTAR TABEL

Tabel 2.1 Daftar Penelitian Sebelumnya	9
Tabel 2.2 Perbedaan <i>Penetration</i> dan <i>Vulnerability Assessment</i>	16
Tabel 2.3 Daftar Nama Kerentanan	16
Tabel 2.4 Tingkat Keparahan CVSS pada Nessus	24
Tabel 4.1 Keterangan Kategori Kerentanan Pada Nessus	40
Tabel 4.2 Daftar port yang terbuka pada Nmap	45
Tabel 4.3 Daftar hasil kerentanan pada Nessus	45
Tabel 4.4 Daftar HTTP (<i>Web Servers</i>) dan HTTP (<i>CGI abuses</i>)	47
Tabel 4.5 HSTS <i>Missing from HTTPS</i> Server	49
Tabel 4.6 <i>Missing or Permissive Content-Security-Policy frame-ancestors</i> HTTP <i>Response Header</i>	51
Tabel 4.7 <i>Missing or Permissive X-Frame-Options</i> HTTP <i>Response Header</i>	53
Tabel 4.8 Nessus SYN scanner	54

DAFTAR GAMBAR

Gambar 2.1 Cara Kerja Website	13
Gambar 2.2 Kalkulator CVSS	25
Gambar 3.1 Tahapan Penelitian.....	32
Gambar 4.1 Hasil Pemindaian Alamat Web.....	37
Gambar 4.2 Topologi Nmap	38
Gambar 4.3 Hasil pemindaian IP menggunakan Nmap	39
Gambar 4.4 Topologi Nessus	40
Gambar 4.5 Tahapan Pertama	41
Gambar 4.6 Tahapan Kedua	41
Gambar 4.7 Tahapan Ketiga.....	42
Gambar 4.8 Tahapan Keempat	42
Gambar 4.9 Tahapan Kelima.....	43
Gambar 4.10 Tahapan Keenam	43
Gambar 4. 11 Hasil Pemindaian IP Menggunakan Nessus	44
Gambar 4.12 <i>Output HSTS Missing from HTTPS Server</i>	50
Gambar 4.13 <i>Output Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header</i>	51
Gambar 4.14 <i>Output Missing or Permissive X-Frame-Options HTTP Response Header</i>	53
Gambar 4.15 <i>Output Nessus SYN scanner</i>	54

DAFTAR LAMPIRAN

Lampiran 1 Surat Ijin Penelitian	63
Lampiran 2 Jadwal Penelitian	64
Lampiran 3 Kartu Bimbingan Skripsi	65
Lampiran 4 Hasil Cek Plagiarisme	66

PERPUSTAKAAN
UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA

DAFTAR SINGKATAN

CGI	<i>Common Gateway Interface</i>
CSS	<i>Cascading Style Sheet</i>
CSP	<i>Content Security-Policy</i>
CVSS	<i>Common Vulnerability Scoring System</i>
DNS	<i>Domain Name System</i>
FKES	Fakultas Kesehatan
FTP	<i>File Transfer Protocol</i>
GOV-CSIRT	<i>Government Computer Security Incident Response Team</i>
HTML	<i>HyperText Markup Language</i>
HTTP	<i>Hypertext Transfer Protocol</i>
HTTPS	<i>Hypertext Transfer Protocol Secure</i>
HSTS HTTP	<i>Strict Transport Security</i>
IP	<i>Internet Protocol</i>
MITM	<i>Man in the middle</i>
Nmap	<i>Network Mapper</i>
Nslookup	<i>Name Server Lookup</i>
OJS	<i>Open Journal System</i>
PCIDSS	<i>Payment Card Industry Data Security Standard</i>
SSH	<i>Secure Shell</i>
SSL	<i>Secure Sockets Layer</i>
TCP	<i>Transmission Control Protocol</i>
TLS	<i>Transport Layer Security</i>
UNJAYA	Universitas Jenderal Achmad Yani Yogyakarta
URL	<i>Uniform Resource Locator</i>
W3C	<i>World Wide Web Consortium</i>
XSS	<i>Cross-site Scripting</i>