

**ANALISIS TINGKAT KEAMANAN *WEBSITE* PPDB SMK MUHAMMADIYAH
GAMPING TERHADAP KERENTANAN OWASP TOP 10 2021
MENGUNAKAN METODE *PENETRATION TESTING EXECUTION
STANDARD (PTES)***

SKRIPSI

**Disusun untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana**



Disusun Oleh:

Dicky Rizky Pangestu
2015018296

**PROGRAM STUDI S1 INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS AHMAD DAHLAN**

2024

**SECURITY LEVEL ANALYSIS OF THE PPDB SMK MUHAMMADIYAH
GAMPING WEBSITE AGAINST OWASP TOP 10 2021 VULNERABILITIES
USING THE PENETRATION TESTING EXECUTION STANDARD (PTES)
METHOD.**

S1 THESIS

**Submitted as a Partial Fulfillment of
Requirements to Obtain a Bachelor Degree**



Written By:

Dicky Rizky Pangestu

2015018296

**INFORMATICS STUDY PROGRAM
FACULTY OF INDUSTRIAL TECHNOLOGY
UNIVERSITAS AHMAD DAHLAN**

2024

LEMBAR PERSETUJUAN PEMBIMBING

SKRIPSI

**ANALISIS TINGKAT KEAMANAN *WEBSITE* PPDB SMK MUHAMMADIYAH
GAMPING TERHADAP KERENTANAN OWASP TOP 10 2021
MENGUNAKAN METODE *PENETRATION TESTING EXECUTION
STANDARD (PTES)***

Dipersiapkan dan disusun oleh:

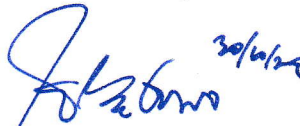
Dicky Rizky Pangestu

2015018296

**Program Studi S1 Informatika
Fakultas Teknologi Industri
Universitas Ahmad Dahlan**

Telah disetujui oleh:

Pembimbing



Eko Aribowo S.T.,M.Kom.

NIPM. 197002062005011001.

LEMBAR PENGESAHAN

SKRIPSI

ANALISIS TINGKAT KEAMANAN *WEBSITE* PPDB SMK MUHAMMADIYAH
GAMPING TERHADAP KERENTANAN OWASP TOP 10 2021
MENGUNAKAN METODE *PENETRATION TESTING EXECUTION
STANDARD (PTES)*

Dipersiapkan dan disusun oleh:

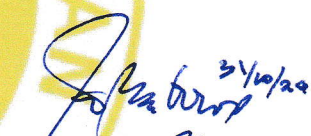
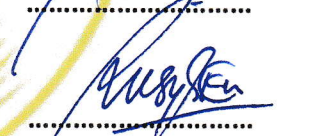
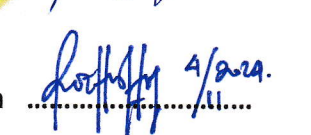
Dicky Rizky Pangestu
2015018296

Telah dipertahankan di depan Dewan Penguji
pada tanggal 4 Oktober 2024
dan dinyatakan telah memenuhi syarat
Susunan Dewan Penguji

Ketua : Eko Aribowo S.T., M.Kom.

Penguji 1 : Rusydi Umar, S.T., M.T., Ph.D.

Penguji 2 : Ir. Nur Rochmah Dyah Pujiastuti, S.T., M.Kom


.....

.....

.....

Yogyakarta, 15 November 2024

Dekan Fakultas Teknologi Industri

Universitas Ahmad Dahlan



Prof. Dr. Ir. Siti Jamilatun, M.T.

NIPM. 19660812 199601 011 0784324.

LEMBAR PERNYATAAN KEASLIAN

SURAT PERNYATAAN

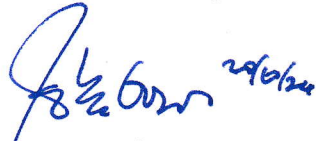
Yang bertanda tangan di bawah ini:

Nama : Dicky Rizky Pangestu
NIM : 2015018296
Prodi : Informatika
Judul TA/Skripsi : Analisis Tingkat Keamanan *Website* PPDB Smk Muhammadiyah
Gamping Terhadap Kerentanan Owasp Top 10 2021 Menggunakan
Metode *Penetration Testing Execution Standard* (PTES)

Dengan ini saya menyatakan bahwa Laporan Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar Ahli Madya/Kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 4 Oktober 2024

Mengetahui,
Dosen Pembimbing



Eko Aribowo, S.T., M.Kom.
NIPM. 197002062005011001.

Yang menyatakan,



Dicky Rizky Pangestu
2015018296

PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan dibawah ini:

Nama : Dicky Rizky Pangestu

NIM : 2015018296

Email : dicky2015018296@webmail.uad.ac.id

Program Studi : Informatika

Fakultas : Teknologi Industri

Judul Tesis : Analisis Tingkat Keamanan Website PPDB Smk Muhammadiyah Gamping Terhadap Kerentanan Owasp Top 10 2021 Menggunakan Metode Penetration Testing Execution Standard (PTES)

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah mendapatkan gelar keserjanaan baik di Universitas Ahmad Dahlan maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasilpelaksanaan penelitian dan implementasi saya sendiri, tanpa bantuan pihak lain kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan di setujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan oranglain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan danketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Ahmad Dahlan.

Yogyakarta, 4 Oktober 2024

Yang Menyatakan



Dicky Rizky Pangestu

2015018296

PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : Dicky Rizky Pangestu
NIM : 2015018296
Email : dicky2015018296@webmail.uad.ac.id
Program Studi : Informatika
Fakultas : Teknologi Industri
Judul tugas akhir : Analisis Tingkat Keamanan Website PPDB Smk Muhammadiyah Gamping Terhadap Kerentanan Owasp Top 10 2021 Menggunakan Metode Penetration Testing Execution Standard (PTES)

Dengan ini saya menyerahkan hak *sepenuhnya* kepada Perpustakaan Universitas Ahmad Dahlan untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut

Saya (~~mengijinkan~~/~~tidak mengijinkan~~)* karya tersebut diunggah ke dalam Repository Perpustakaan Universitas Ahmad Dahlan.

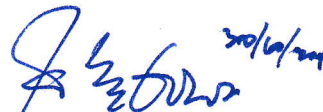
Demikian pernyataan ini saya buat dengan sebenarnya.

Yogyakarta, 4 Oktober 2024



Dicky Rizky Pangestu
2015018296

Mengetahui, Pembimbing



Eko Aribowo, S.T., M.Kom.
NIPM. 197002062005011001

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan penelitian ini yang berjudul "ANALISIS TINGKAT KEAMANAN WEBSITE PPDB SMK MUHAMMADIYAH GAMPING TERHADAP KERENTANAN OWASP TOP 10 2021 MENGGUNAKAN METODE *PENETRATION TESTING EXECUTION STANDARD (PTES)*". Skripsi ini disusun sebagai . Penulis menyadari bahwa penelitian ini tidak akan dapat terselesaikan tanpa dukungan, bimbingan, serta doa dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Prof. Dr. Muchlas, M.T., selaku Rektor Universitas Ahmad Dahlan, yang telah memberikan fasilitas dan dukungan dalam pelaksanaan penelitian ini.
2. Prof. Dr. Ir. Siti Jamilatun, M.T., selaku Dekan Fakultas Teknologi Industri Universitas Ahmad Dahlan, yang telah memberikan bimbingan dan arahan selama masa studi.
3. Dr. Murinto, S.Si, M.Kom., selaku ketua program studi prodi Informatika Universitas Ahmad Dahlan.
4. Eko Aribowo S.T.,M.Kom., selaku dosen pembimbing skripsi, yang dengan sabar telah memberikan bimbingan, arahan, dan motivasi kepada penulis dalam menyelesaikan penelitian ini.
5. Miftahurrahma Rosyda S.Kom., M.Eng., selaku dosen pembimbing akademik yang telah memberikan arahan dan bimbingan selama masa studi.
6. Orang tua saya, Ibunda Aminah yang tiada henti selalu memberikan dukungan moral serta doa yang tulus di setiap langkah kehidupan penulis. Tanpa pengorbanan, doa, dan restu dari orang tua, penyelesaian tugas akhir ini tidak mungkin tercapai.
7. Teman-teman, yang tidak bisa saya sebutkan satu persatu yang selalu memberikan semangat dan bantuan selama proses penyusunan penelitian ini.

Akhir kata, penulis berharap penelitian ini dapat memberikan manfaat yang sebesar-besarnya, terutama dalam bidang keamanan informasi. Penulis menyadari bahwa penelitian ini masih jauh dari sempurna, oleh karena itu kritik dan saran yang membangun sangat diharapkan.

Yogyakarta, 11 September 2024
Penulis



Dicky Rizky Pangestu
2015018296

DAFTAR ISI

LEMBAR PERSETUJUAN PEMBIMBING	iv
LEMBAR PENGESAHAN.....	v
LEMBAR PERNYATAAN KEASLIAN	vi
PERNYATAAN TIDAK PLAGIAT	vii
PERNYATAAN PERSETUJUAN AKSES.....	viii
KATA PENGANTAR.....	ix
DAFTAR ISI.....	x
DAFTAR GAMBAR.....	xii
DAFTAR TABEL.....	xiv
DAFTAR KODE PROGRAM.....	xv
DAFTAR LAMPIRAN	xvi
ABSTRAK.....	xvii
BAB I. Pendahuluan	1
1.1. Latar Belakang Masalah	1
1.2. Batasan Masalah Penelitian	3
1.3. Rumusan Masalah	3
1.4. Tujuan Penelitian.....	4
1.5. Manfaat Penelitian.....	4
BAB II. Tinjauan Pustaka	5
2.1. Kajian Penelitian Terdahulu	5
2.2. Landasan Teori	8
2.2.1. Website	8
2.2.2. Keamanan Website	9
2.2.3. Vulnerability Assessment	9
2.2.4. Vulnerability Scanning.....	10
2.2.5. Penetration testing.....	11
2.2.6. Penetration Testing Execution Standar (PTES)	13
2.2.7. Open Worldwide Application Security Project.....	15
2.2.8. OWASP Zed Attack Proxy	20
2.2.9. Burp Suite.....	21
2.2.10. Wapiti Vulnerability Scanner	22
BAB III. METODOLOGI PENELITIAN	23
3.1. Pengumpulan Data.....	23
3.2. Software dan Hardware	23
3.3. Tahapan Penelitian.....	24
3.4. Skenario penelitian.....	27
BAB IV. HASIL DAN PEMBAHASAN	29
4.1. Pre-Engagment.....	29
4.2. Information Gathering	31
4.2.1. Wawancara	31
4.2.2. Whois	33
4.2.3. The Harvester	34
4.3. Threat Modeling	35
4.3.1. OWASP ZAP	36

4.3.2.	Wapiti.....	38
4.4.	<i>Vulnerability Assessment</i>	41
4.4.1.	OWASP ZAP	41
4.4.2.	Wapiti.....	42
4.5.	<i>Exploitation</i>	43
4.5.1.	OWASP ZAP	44
4.5.2.	Wapiti.....	60
4.6.	<i>Post-Exploitation</i>	73
4.6.1.	<i>Post-Exploitation</i> Kerentanan yang ditemukan OWASP-ZAP	74
4.6.2.	<i>Post-Exploitation</i> Kerentanan yang ditemukan Wapiti	75
4.7.	<i>Reporting</i>	77
4.7.1.	Pelaporan Hasil Eksploitasi.....	77
4.7.2.	Rekomendasi Perbaikan Kerentanan	79
4.7.3.	Pengujian Rekomendasi Perbaikan	82
BAB V.	KESIMPULAN DAN SARAN	89
5.1.	Kesimpulan.....	89
5.2.	Saran.....	91
DAFTAR PUSTAKA.....		92
LAMPIRAN		96
Lampiran 1.	Surat Permohonan Izin Penelitian Riset Fakultas Teknologi Industri	96
Lampiran 2.	Bukti Perizinan Dalam Melakukan Pengujian Terhadap <i>Website</i>	97
Lampiran 3.	Bukti Pengumpulan Data Dengan Wawancara	98

DAFTAR GAMBAR

Gambar 2.1 Tahap <i>Penetration testing Execution Standar</i>	13
Gambar 2.2 Daftar Kerentanan OWASP TOP 10 2021	16
Gambar 2.3 Logo Aplikasi OWASP-ZAP	21
Gambar 2.4 Logo Aplikasi Burp Suite	21
Gambar 2.5 Logo Aplikasi Wapiti	22
Gambar 3.1 Tahapan Penelitian	25
Gambar 4.1 Hasil Pengumpuln Informasi menggunakan Whois	34
Gambar 4.2 Hasil Pengumpuln Informasi menggunakan theHarvester	35
Gambar 4.3 Proses <i>Vulnerability Scanning</i> OWASP ZAP	36
Gambar 4.4 Hasil <i>Vulnerability Scanning</i> OWASP ZAP	37
Gambar 4.5 Proses <i>Vulnerability Scanning</i> Wapiti.....	39
Gambar 4.6 Hasil <i>Vulnerability Scanning</i> Aplikasi Wapiti	40
Gambar 4.7 Proses Generate Report Kerentanan CSRF.....	44
Gambar 4.8 Hasil Pengujian Serangan CSRF	46
Gambar 4.9 Hasil Pengujian SSL Checker	47
Gambar 4.10 Hasil Percobaan Serangan XSS	48
Gambar 4.11 Penyuntikan Script Pada Elemen Form	49
Gambar 4.12 Hasil Pengujian terhadap Kerentanan CSP: style-src unsafe-inline.....	50
Gambar 4.13 Tampilan Program Serangan Clickjacking	53
Gambar 4. 14 Hasil Identifikasi Kerentanan <i>Library</i> JavaScript.....	54
Gambar 4. 15 Hasil Penyerangan <i>Prototype Pollution</i>	55
Gambar 4. 16 Data Cookie yang Disimpan pada URL Login	56
Gambar 4. 17 Data Cookie yang disimpan Melalui Script CSRF	56
Gambar 4. 18 Data yang Ditampilkan <i>Header X-Powered By</i>	57
Gambar 4. 19 Hasil Pengujian Kerentanan Strict-Transport-Security Header Not Set	58
Gambar 4.20 Skrip Serangan MIME-Sniffing.....	59
Gambar 4. 21 Proses Upload Script Melalui Form Upload File	60
Gambar 4.22 Hasil Temuan File Tersembunyi Menggunakan Aplikasi Wapiti.....	61
Gambar 4. 23 Proses Pengunduhan File Tersembunyi.....	61
Gambar 4.24 Capture Lalu Lintas Data Aplikasi Burp Suite.....	63
Gambar 4.25 Proses Pembuatan Script XSS dengan Aplikasi BurpSuite	63
Gambar 4. 26 Hasil Penyerangan XSS menggunakan Aplikasi BurpSuite	64
Gambar 4. 27 Hasil <i>Scanning</i> Kerentanan CSRF dari Aplikasi Wapiti.....	65
Gambar 4.28 Hasil Capture Lalu Lintas Data Request Ganti Password.....	65
Gambar 4. 29 Pembuatan Script CSRF pada Aplikasi BurpSuite	66
Gambar 4. 30 Hasil Penyerangan CSRF Menggunakan Burp Suite.....	66
Gambar 4. 31 Hasil <i>Scanning</i> kerentanan HTTP Secure Headers oleh Aplikasi Wapiti.....	67
Gambar 4. 32 Proses Penyerangan Clickjacking Menggunakan burp Suite	68
Gambar 4. 33 Hasil Penyerangan Clickjacking Menggunakan Aplikasi Burp Suite	69
Gambar 4. 34 Proses Serangan XSS Menggunakan Aplikasi burp Suite.....	70
Gambar 4. 35 Hasil <i>Capture</i> Lalu Lintas Data dengan Aplikasi Burp Suite	71
Gambar 4. 36 Hasil Percobaan Serangan MIME-Sniffing	71
Gambar 4. 37 Proses Mengakses <i>Website</i> Menggunakan Protokol HTTP	72
Gambar 4. 38 Hasil Capture dari Aplikasi Burp Suite pada request HTTP.....	73
Gambar 4. 39 Hasil <i>Vulnerability Scanning</i> dari <i>Website</i>	82
Gambar 4. 40 Penambahan header HTTP X-Frame-Options.....	83

Gambar 4. 41 Hasil Pengujian Rekomendasi Perbaikan <i>Missing Anti-clickjacking Header</i>	83
Gambar 4.42 Penambahan <i>Script</i> untuk memperbaharui <i>JS Library</i>	84
Gambar 4.43 Hasil pengujian perbaikan kerentanan <i>Vulnerable JS Library</i>	85
Gambar 4. 44 Penambahan perintah <code>header_remove("X-Powered-By")</code>	86
Gambar 4. 45 Hasil pengujian rekomendasi perbaikan server leak by <i>X-Powered-By</i>	86
Gambar 4.46 Penambahan perintah untuk mengamankan file backup	87
Gambar 4. 47 Hasil pengujian rekomendasi perbaikan backupfile.....	88

DAFTAR TABEL

Tabel 2. 1 Perbandingan beberapa penelitian terdahulu	7
Tabel 3.1 Spesifikasi Hardware	24
Tabel 3.2 Software yang Digunakan.....	24
Tabel 4.1 Hasil Tahap <i>Pre-Engagment</i>	30
Tabel 4. 2 Hasil Pengumpulan Data Melalui Wawancara	31
Tabel 4.3 Hasil <i>Vulnerability Scanning</i> menggunakan OWASP ZAP	37
Tabel 4.4 Hasil <i>Vulnerability Scanning</i> Aplikasi Wapiti	40
Tabel 4.5 Hasil Identifikasi <i>vulnerability scanning</i> aplikasi OWASP ZAP	41
Tabel 4.6 Hasil Identifikasi <i>Vulnerability Scanning</i> Aplikasi Wapiti.....	43
Tabel 4.7 Tabel Post-Exploitation dari Hasil <i>Scanning</i> Aplikasi OWASP-ZAP	74
Tabel 4. 8 Tabel Post-Exploitation dari Hasil <i>Scanning</i> Aplikasi Wapiti	76
Tabel 4.9 Tabel Pelaporan Hasil Eksploitasi Kerentanan yang Ditemukan OWASP-ZAP.....	77
Tabel 4.10 Tabel Pelaporan Hasil Eksploitasi Kerentanan Yang Ditemukan Wapiti	78

DAFTAR KODE PROGRAM

Kode Program 4.1 Kode Program Serangan CSRF	45
Kode Program 4.2 Program Serangan Clickjacking	52

DAFTAR LAMPIRAN

Lampiran 1 Surat Izin Riset Penelitian.....	96
Lampiran 2 Bukti Perizinan Pengujian.....	97
Lampiran 3 Bukti Pengumpulan Data dengan Wawancara.....	98

ABSTRAK

Dalam pembuatan sebuah *website*, keamanan dari *website* merupakan satu dari sekian hal terpenting yang harus diperhatikan. Semakin berkembangnya zaman, *website* dimanfaatkan guna menyampaikan informasi yang lebih cepat dan efisien. Selain sebagai media penyampaian informasi *website* juga dapat digunakan sebagai sebuah sistem manajemen, hal ini juga berlaku bagi SMK Muhammadiyah Gamping yang mempunyai salah satu *website* untuk manajemen pendaftaran siswa baru secara daring yang bernama *website* PPDB SMK Muhammadiyah Gamping. Oleh karena hal tersebut perlu dilaksanakannya pengujian keamanan pada *website* tersebut dengan tujuan untuk menguji tingkat keamanan dan menemukan kerentanan dari keamanan yang terdapat pada *website* PPDB SMK Muhammadiyah Gamping, serta memberikan rekomendasi perbaikan pada celah yang ditemukan.

Pada penelitian kali ini metode yang digunakan adalah *penetration testing execution standard* (PTES) yang dilakukan guna menemukan kerentanan sistem pada 10 daftar kerentanan *Open Web Application Security Project* (OWASP TOP 10), untuk mencari kerentanan tersebut perlu dilakukan pengujian *penetration testing* terhadap *website* PPDB SMK Muhammadiyah Gamping. Tahapan penelitian ini terdiri dari 7 tahap yang diawali dari tahap Interaksi Pra-Keterlibatan (*Pre-engagement*), Pengumpulan data (*information Gathering*), Pemodelan Ancaman (*Threat Modeling*), Analisis Kerentanan (*Vulnerability Asesment*), Eksploitasi (*Exploitation*), Pasca Eksploitasi (*Post-Exploitation*), dan Pelaporan (*Reporting*). Penelitian ini menggunakan beberapa aplikasi pendukung yaitu, OWASP Zed Attack Proxy (OWASP-ZAP) dan Wapiti yang digunakan untuk melakukan *vulnerability scanning* dan aplikasi Burp Suite yang digunakan untuk melakukan *penetration testing* pada celah yang ditemukan oleh aplikasi OWASP-ZAP dan Wapiti.

Hasil dari pengujian keamanan dari *website* PPDB SMK Muhammadiyah Gamping terdapat 10 jenis kerentanan dengan 6 tingkat kerentanan kategori *medium* dan 4 tingkat kerentanan kategori *low* pada hasil *scanning* menggunakan OWASP-ZAP, sedangkan pada aplikasi Wapiti ditemukan 4 jenis kerentanan pada *website* PPDB SMK Muhammadiyah Gamping. Setelah dilakukan pengujian eksploitasi pada kerentanan yang ditemukan menggunakan aplikasi OWASP-ZAP ditemukan 4 kerentanan yang berhasil dieksploitasi, sedangkan pada hasil kerentanan yang ditemukan menggunakan aplikasi Wapiti ditemukan 2 kerentanan yang dapat dieksploitasi. Hasil dari kerentanan yang ditemukan diberikan rekomendasi perbaikan dengan tujuan agar kerentanan tersebut dapat ditutup dan dapat meningkatkan keamanan dari *website* PPDB SMK Muhammadiyah Gamping.

Kata Kunci : *Keamanan Website, Penetration testing, PTES, OWASP TOP 10 2021, Website*