

**ANALISIS KEAMANAN SISTEM WEBSITE RSUD PROVINSI
NTB DENGAN METODE PTES (PENETRATION
TESTING EXECUTION STANDARD)**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



Disusun oleh:

LALU YOGI PRATAMA SAPUTRA

19.83.0394

Kepada:

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2023**

**ANALISIS KEAMANAN SISTEM WEBSITE RSUD PROVINSI
NTB DENGAN METODE PTES (PENETRATION
TESTING EXECUTION STANDARD)**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

LALU YOGI PRATAMA SAPUTRA

19.83.0394

Kepada:

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

HALAMAN PERSETUJUAN

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS KEAMANAN SISTEM WEBSITE RSUD PROVINSI
NTB DENGAN METODE PTES (PENETRATION
TESTING EXECUTION STANDARD)**

yang disusun dan diajukan oleh

Lalu Yogi Pratama Saputra

19.83.0394

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 25 September 2023

Dosen Pembimbing,



Muhammad Kopravi S.Kom., M.Eng

NIK. 190302454

HALAMAN PENGESAHAN

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS KEAMANAN SISTEM WEBSITE RSUD PROVINSI NTB DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD)

yang disusun dan diajukan oleh

Lalu Yogi Pratama Saputra
19.83.0394

Telah dipertahankan di depan Dewan Penguji
pada tanggal 25 September 2023

Susunan Dewan Penguji

Nama Penguji

Melwin Syafrizal, S.Kom., M.Eng
NIK. 190302105

Wahid Miftahul Ashari, S.Kom., M.T
NIK. 190302452

Muhammad Kopravi, S.Kom., M.Eng
NIK. 190302454

Tanda Tangan

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 25 September 2023

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini,

Nama mahasiswa : **Lalu Yogi Pratama Saputra**
NIM : **19.83.0394**

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS KEAMANAN SISTEM WEBSITE RSUD PROVINSI NTB DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD)

Dosen Pembimbing: **Muhammad Kopravi S.Kom., M.Eng.**

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 25 September 2023

Yang Menyatakan,



The image shows a handwritten signature in black ink over a purple and yellow 10000 Rupiah stamp. The stamp includes the Garuda Pancasila emblem and the text 'REPUBLIK INDONESIA', '10000', and 'METERAL TEMPEL'.

Lalu Yogi Pratama Saputra

HALAMAN PERSEMBAHAN

Puji syukur kehadiran Allah SWT atas segala limpahan rahmat dan ridho-nya yang telah memberikan kesehatan, kelancaran, dan memberikan anugerah ilmu sehingga penulis dapat menyelesaikan skripsi ini. Skripsi ini saya persembahkan untuk:

1. Kedua orang tua tercinta serta adik saya yang selalu memberikan semangat serta dorongan untuk menyelesaikan skripsi, dan membiayai serta mendukung segala keputusan.
2. Aminatuzzohriah yang selalu memberikan support dan selalu menyemangati untuk menyelesaikan skripsi dan memberikan saya nasehat.
3. Dosen pembimbing Bapak Muhammad Kopravi, S.Kom., M.Eng yang telah membimbing saya dengan sabar serta memberikan nasihat dan meluangkan waktu untuk selalu memberikan saya bimbingan.
4. Dosen Penguji yang sudah memberikan arahan dan saran kepada penulis sehingga skripsi ini lebih baik lagi.
5. Pihak instansi Rumah Sakit Umum Daerah Provinsi Nusa Tenggara Barat yang telah memberikan saya izin penelitian sebagai tempat objek penelitian.
6. Teman – teman seperjuangan 19 – SITK – 01 yang selalu kompak selama empat tahun yang terasa begitu cepat, terima kasih kepada teman-teman yang datang saat ujian pendadaran.
7. Serta teman-teman kosan yang memberikan saya saran dalam pembuatan skripsi terutama Muhammad Gunawan Ismail Sholeh S.H., M.H. Terima kasih banyak mas gunawan

KATA PENGANTAR

Puji syukur kepada Allah SWT yang telah memberikan kita atas rahmat dan hidayahnya. Tak lupa shalawat serta salam kita haturkan kepada nabi baginda besar nabi Muhammad SAW yang telah memberikan petunjuk dari Allah SWT untuk kita semua dan tak lupa pula atas nikmat yang diberikan hingga saat ini, sehingga saya diberikan kesempatan yang sangat luar biasa untuk menyelesaikan penyusunan skripsi dengan judul "ANALISIS KEAMANAN SISTEM WEBSITE RSUD PROVINSI NTB DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD)" dapat diselesaikan dengan lancar.

Penulis juga menyadari dalam penyusunan skripsi ini tidak akan selesai tanpa bantuan dari berbagai pihak. Karena itu pada kesempatan ini ucapan terimakasih setulus-tulusnya kepada:

1. Allah SWT atas segala limpahan rahmat dan hidayah-nya sehingga penulis dapat menyelesaikan tugas akhir ini dengan baik.
2. Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas Amikom Yogyakarta.
3. Bapak Dony Ariyus, M.Kom selaku Kepala Program Studi Teknik Komputer Universitas Amikom Yogyakarta.
4. Bapak Muhammad Kopravi S.Kom., M.Eng. selaku pembimbing saya yang telah meluangkan waktunya dalam memberikan bimbingan, arahan, dan motivasi kepada penulis dalam menyelesaikan skripsi ini.
5. Bapak Banu Santoso, S.T., M.Eng. selaku dosen wali saya yang memberikan penulis motivasi dan arahan.
6. Segenap dosen dan staf Universitas Amikom Yogyakarta yang telah memberikan banyak ilmu dan pengetahuan.
7. Kedua orang tua, dan adik yang telah memberikan do'a dan memberikan dukungan.
8. Teman – teman 19 – SITK – 01 yang memberikan dukungan dan berbagi pengalaman.

9. Temen-teman yang sudah datang waktu sidang, terima kasih banyak.
10. Serta Temen-temen yang membantu baik secara langsung maupun tidak langsung. Semoga Allah SWT menjadikan amal baik yang senantiasa mendapatkan balasan dan kebaikan berlipat ganda, Aamiin ya rabbal alamin.

Yogyakarta, 25 September 2023



Lalu Yogi Pratama Saputra

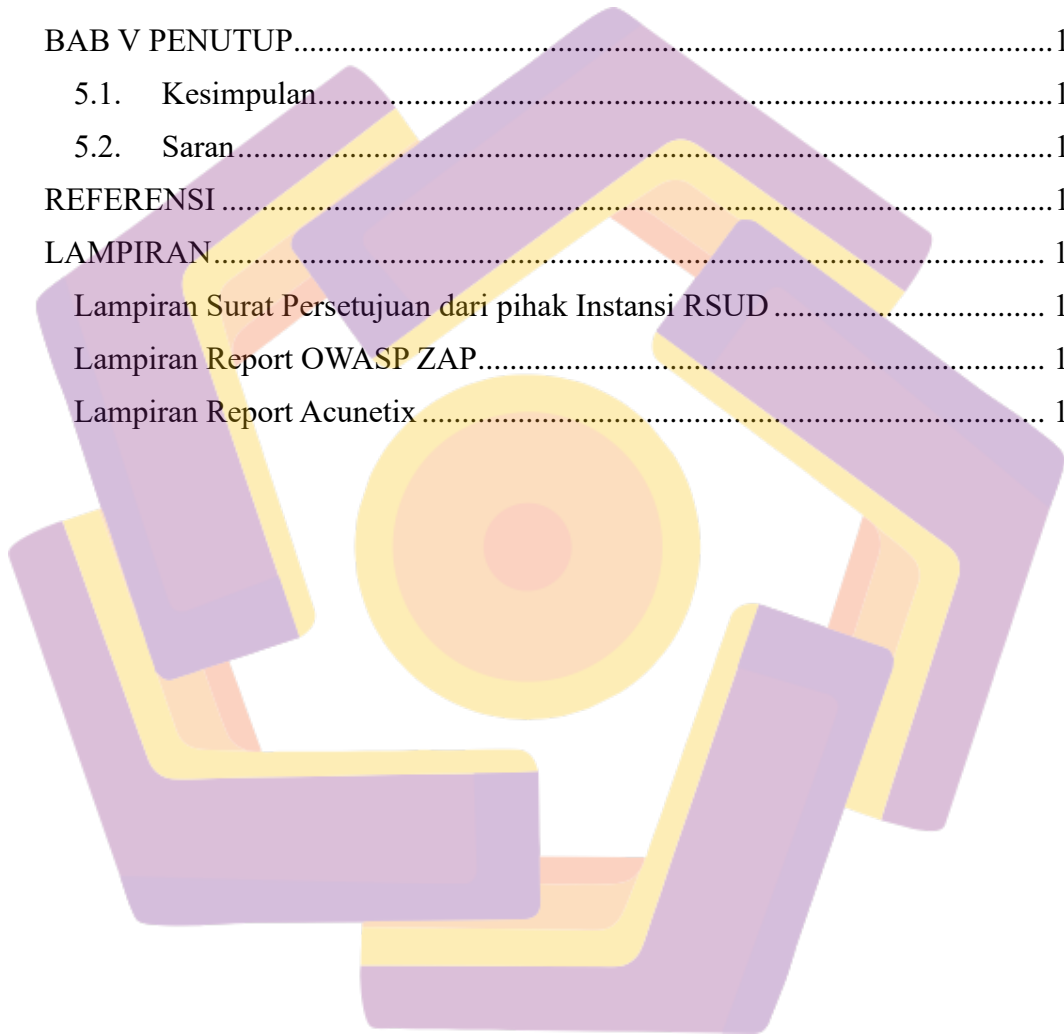
DAFTAR ISI

HALAMAN JUDUL	I
HALAMAN PERSETUJUAN.....	II
HALAMAN PENGESAHAN	III
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	IV
HALAMAN PERSEMBAHAN	V
KATA PENGANTAR.....	VI
DAFTAR ISI.....	VIII
DAFTAR TABEL	XII
DAFTAR GAMBAR	XIII
DAFTAR SYMBOL	XVII
INTISARI	XVIII
ABSTRACT.....	XIX
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	2
1.3. Batasan Masalah.....	2
1.4. Tujuan Penelitian.....	3
1.5. Manfaat Penelitian.....	3
1.6. Sistematika Penulisan.....	4
BAB II TINJAUAN PUSTAKA.....	6
2.1. Studi Literatur	6
2.2. Dasar Teori	14
2.2.1. Sistem Informasi	14
2.2.2. Website.....	14
2.2.3. Keamanan Informasi	15
2.2.4. Macam-Macam Serangan Pada Sistem Website	17
2.2.5. Macam – macam serangan pada System.....	19
2.2.6. <i>Web Analysis Scanning</i>	20
2.2.7. <i>Ethical Hacking</i>	20

2.2.8.	<i>Penetration Testing</i>	21
2.2.9.	<i>Reconnaissance</i> (pengintaian)	22
2.2.10.	<i>Scanning</i>	23
2.2.11.	<i>Gaining access</i>	23
2.2.12.	<i>Maintaining access</i>	23
2.2.13.	<i>Converging tracks</i>	24
2.2.14.	Macam-Macam metode <i>Penetration Testing</i>	24
2.2.15.	Pengertian PTES (<i>Penetration Testing Execution Standard</i>).....	25
2.2.16.	<i>Google Dork/Dorking</i>	28
2.2.17.	<i>Open Web Application Security Project (OWASP)</i>	28
2.2.18.	<i>Acunetix Vulnerability Scanner</i>	29
2.2.19.	<i>OWASP Top 10 web Application security risk 2021</i>	29
2.2.20.	<i>Metasploit Framework</i>	32
2.2.21.	<i>Sensitive data exposure</i>	33
2.2.22.	Analisis Kerentanan (<i>Vulnerability assessment</i>).....	33
BAB III METODE PENELITIAN		34
3.1.	Objek Penelitian	34
3.2.	Alur Penelitian.....	34
3.2.1.	Tahap Dalam Melakukan Pengujian pentes menggunakan metode <i>Penetration Testing Execution Standard (PTES)</i>	35
3.3.	Alat dan Bahan	38
3.2.2.	Perangkat Keras (<i>Hardware</i>).....	38
3.2.3.	Perangkat Lunak (<i>Software</i>).....	39
3.2.4.	Tools Pendukung Penelitian.....	39
BAB IV HASIL DAN PEMBAHASAN		40
4.1	<i>Pre-Engagement</i>	40
4.2	<i>Intelligence Gathering</i>	40
4.2.1	Ping rsud.ntbprov.go.id	41
4.2.2	<i>Port Scanning</i>	42
4.2.3	<i>Whois</i>	43
4.2.4	<i>Hosting History</i> Menggunakan Netcraft.....	45
4.2.5	Wappalyzer analisis.....	47

4.2.6	<i>WhatWeb Scanning</i>	47
4.2.7	<i>Whatwaf scanning</i>	48
4.2.8	<i>theHarvester scanning</i>	49
4.2.9	<i>Scanning SSL (Secure Socket Layer)</i>	49
4.3	<i>Threat Modelling</i>	51
4.4	<i>Vulnerability Analysis</i>	53
4.4.1	<i>Google Directive</i>	54
4.4.2	<i>Virus scanner</i>	76
4.4.3	<i>Scanning website Menggunakan Vulnerability Scanner</i>	77
4.4.4	<i>hasil gabungan pemindaian pada rsud.ntbprov.go.id</i>	88
4.5	<i>Exploitation</i>	90
4.5.1	<i>Absence of anti-CSRF token</i>	90
4.5.2	<i>Content security Policy (CSP) header not set</i>	91
4.5.3	<i>Cross-Domain Misconfiguration</i>	92
4.5.4	<i>Missing anti-clicjacking</i>	92
4.5.5	<i>Secure page includes mixed content (including scripts)</i>	93
4.5.6	<i>Testing Seassion ID in URL Rewrite</i>	94
4.5.7	<i>Testing Cookie with SameSite Attribute none</i>	94
4.5.8	<i>Testing Cookie without SameSite Attribute</i>	95
4.5.9	<i>Testing Cross-domain JavaScript Source File Inclusion</i>	95
4.5.10	<i>Testing Secure Pages Includes Mixed Content</i>	96
4.5.11	<i>Testing Server Leaks Information via “X-Powere-By” HTTP Response header field</i>	97
4.5.12	<i>Testing Server Leaks version information via “server” HTTP Response header field</i>	98
4.5.13	<i>Testing Strict-Transport-security header not yet</i>	98
4.5.14	<i>Testing Timestamp Disclosure-unix</i>	99
4.5.15	<i>X-Content-type-options header Missing</i>	100
4.5.16	<i>Testing Information Disclosure-sensitif Information in URL</i>	101
4.5.17	<i>Testing Lossely Scoped Cookie</i>	102
4.5.18	<i>HTML form Without CSRF Protection</i>	102
4.5.19	<i>Modern Web Application</i>	104
4.5.20	<i>Clicjacking: X-Frame-Options header Missing</i>	104

4.5.21	<i>Re-examine Cache-control Directive</i>	105
4.5.22	<i>Retrieved From Cache</i>	106
4.5.23	<i>User Controllabel HTML Element Attribute (Potential XSS)</i>	107
4.1.	<i>Post-Exploitation</i>	107
4.2.	Hasil Pengujian	109
4.3.	Rekomendasi	110
BAB V PENUTUP.....		114
5.1.	Kesimpulan.....	114
5.2.	Saran.....	115
REFERENSI		116
LAMPIRAN.....		120
	Lampiran Surat Persetujuan dari pihak Instansi RSUD	120
	Lampiran Report OWASP ZAP.....	121
	Lampiran Report Acunetix.....	146



DAFTAR TABEL

Tabel 2. 1 Keaslian Penelitian.....	9
Tabel 3. 1 Perangkat Keras (<i>Hardware</i>).....	38
Tabel 3. 2 Perangkat Lunak (<i>Software</i>).....	39
Tabel 3. 3 Tools Pendukung.....	39
Tabel 4. 1 Hasil <i>Pre-Engagement</i>	40
Tabel 4. 2 Daftar Ancaman Pendekatan OWASP ZAP Top 10 2017.....	52
Tabel 4. 3 <i>Scanning</i> Menggunakan OWASP ZAP.....	78
Tabel 4. 4 hasil pemindaian menggunakan Acunetix.....	87
Tabel 4. 5 hasil Pemindaian Uniscan.....	88
Tabel 4. 6 hasil gabungan pemindaian pada rsud.ntbprov.go.id.....	88
Tabel 4. 7 <i>Post</i> -Eksplorasi.....	108
Tabel 4. 8 Hasil Pengujian.....	109
Tabel 4. 9 Hasil Rekomendasi.....	111

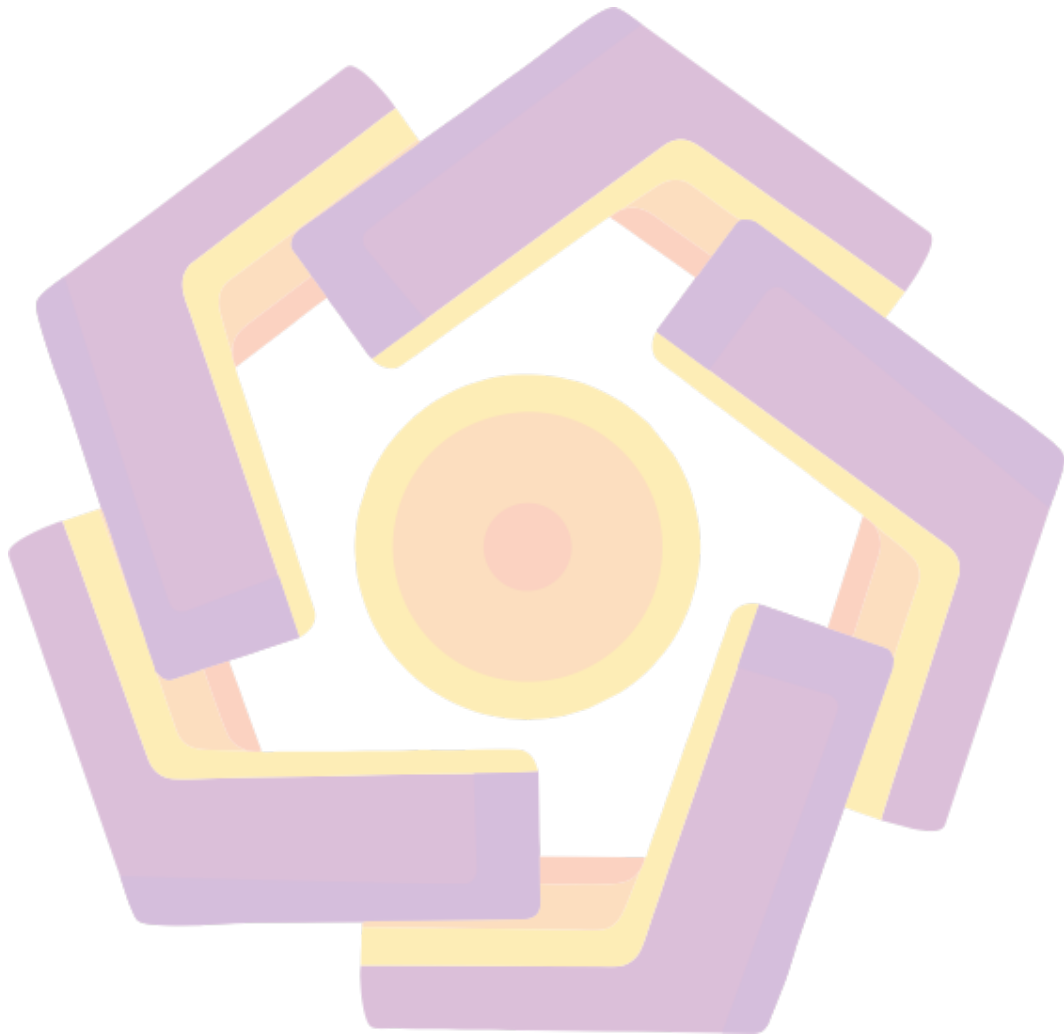
DAFTAR GAMBAR

Gambar 2. 1 fase pada <i>penetration testing</i> [25].....	22
Gambar 2. 2 PTES Metodologi[32]	26
Gambar 2. 3 <i>Risk</i> Keamanan aplikasi website 2021[39].	29
Gambar 3. 1 Alur Penelitian.....	35
Gambar 4. 1 Ping pada kali Linux	41
Gambar 4. 2 Ping pada Windows.....	41
Gambar 4. 3 Port Scanning Top 10 Teratas.....	42
Gambar 4. 4 Port Scanning p1-10000.....	43
Gambar 4. 5 Hasil analisis menggunakan Whois	44
Gambar 4. 6 Scanning menggunakan Netcraft	45
Gambar 4. 7 Netcraft Scanning lanjut.....	46
Gambar 4. 8 Netcraft Scanning hosting History	46
Gambar 4. 9 analisis menggunakan tools Wappalyzer.....	47
Gambar 4. 10 scanning menggunakan WhatWeb	47
Gambar 4. 11 Whatwaf scanning	48
Gambar 4. 12 Tools theHarvester.....	49
Gambar 4. 13 Scanning SSL.....	50
Gambar 4. 14 Scanning SSL Lanjut.....	51
Gambar 4. 15 Dorking pada Google Hacking Database.....	54
Gambar 4. 16 Daftar Dorking pada Google Hacking Database.....	54
Gambar 4. 17 Dorking WP Robot.txt.....	55
Gambar 4. 18 Dorking MC4WP-debug.log.....	55
Gambar 4. 19 Dorking wp-filebase.....	56
Gambar 4. 20 Dorking wp dump.sql.....	56
Gambar 4. 21 Dorking wp-smtp-easy	57
Gambar 4. 22 Dorking wp-Uploads.....	58
Gambar 4. 23 Dorking wp-content-backup	58
Gambar 4. 24 Dorking wp-security audit.log	59
Gambar 4. 25 Dorking Ailwm-backups	59
Gambar 4. 26 Dorking wp-config.bak	60


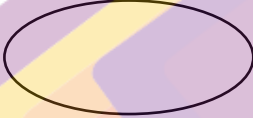


Gambar 4. 27 Dorking wp-json	61
Gambar 4. 28 Dorking wpbd-csv-exports.....	61
Gambar 4. 29 Dorking wp-includes/uploads	62
Gambar 4. 30 hasil analisis wp-includes/uploads	62
Gambar 4. 31 Dorking wp-admin	63
Gambar 4. 32 Dorking wp-links-opml.php.....	64
Gambar 4. 33 Dorking wp-content backup-db	64
Gambar 4. 34 Dorking wp-content/uploads/private.....	65
Gambar 4. 35 Dorking wp-backup-plus.....	65
Gambar 4. 36 Dorking wp-config.....	66
Gambar 4. 37 Dorking wp-includes.....	66
Gambar 4. 38 Dorking wp DB_PASSWORD.....	67
Gambar 4. 39 Dorking wp-content/uploads filetype:xls.....	68
Gambar 4. 40 Dorking wp content/uploads/ext/txt.....	68
Gambar 4. 41 Dorking wp-config.php.save.....	69
Gambar 4. 42 Dorking wp-content/backup.....	69
Gambar 4. 43 Dorking wp-config.php	70
Gambar 4. 44 Dorking wp-admin-post.php	71
Gambar 4. 45 Dorking wp content-error.....	71
Gambar 4. 46 Dorking wp-page-builders	72
Gambar 4. 47 Dorking wp-plugin/Google-site-kit.....	72
Gambar 4. 48 Dorking wp-plugin fgallery	73
Gambar 4. 49 Dorking wp-plugin-wpforms-lite.....	73
Gambar 4. 50 Dorking wp admin-Secure htaccess	74
Gambar 4. 51 Dorking wp plugin/wpmudev-updates.....	74
Gambar 4. 52 Dorking wp php_error log.....	75
Gambar 4. 53 Dorking wp repair.php	75
Gambar 4. 54 Dorking wp-Commentarss	76
Gambar 4. 55 Hasil Virus Scanner	77
Gambar 4. 56 Scanning menggunakan tools Acunetix	86
Gambar 4. 57 Hasil eksploitasi Absence of anti-CSRF Token	90

Gambar 4. 58 Hasil eksploitasi Absence of anti-CSRF Token Lanjut.....	91
Gambar 4. 59 Content Security Policy (CSP) header not set	91
Gambar 4. 60 Cross-Domain Misconfiguration.....	92
Gambar 4. 61 Missing anti-Clickjacking	92
Gambar 4. 62 Missing anti clickjacking lanjut	93
Gambar 4. 63 Security Page Includes Mixed Content(Including Scripts).....	93
Gambar 4. 64 Session ID in Url Rewrite	94
Gambar 4. 65 Cookie with SameSite Attribute None	94
Gambar 4. 66 Cookie without SameSite Attribute.....	95
Gambar 4. 67 Cross Domain JavaScript Source File Inclusion.....	95
Gambar 4. 68 Cross Domain JavaScript Source File Inclusion Lanjut	96
Gambar 4. 69 Secure page includes mixed content	96
Gambar 4. 70 Secure Page Includes Mixed Content lanjut	96
Gambar 4. 71 Server Leaks Information via (X-Powered-By) https Response header field.....	97
Gambar 4. 72 Server Leaks Information via “Server” https Response header field	98
Gambar 4. 73 Strict-Transport-security header not yet.....	98
Gambar 4. 74 Strict-Transport-security header not yet Lanjut	99
Gambar 4. 75 Timestamp Disclosure-unix	99
Gambar 4. 76 Test X-content-type-options header Missing	100
Gambar 4. 77 Hasil Test X-content-type-options header Missing.....	100
Gambar 4. 78 Information Disclosure-sensitif Information in URL	101
Gambar 4. 79 Information Disclosure-sensitif Information in URL Lanjut	101
Gambar 4. 80 Lossely Scoped Cookie	102
Gambar 4. 81 HTML form Without CSRF Protection.....	102
Gambar 4. 82 Testing scripts HTML form Without CSRF Protection.....	103
Gambar 4. 83 Hasil Testing script HTML form Without CSRF Protection.....	103
Gambar 4. 84 Modern Web Application	104
Gambar 4. 85 Clicjacking: X-Frame-Options header Missing	104
Gambar 4. 86 Testing For Clicjacking	105

Gambar 4. 87 Re-examine Cache-control Directive..... 105
Gambar 4. 88 Retrieved From Cache 106
Gambar 4. 89 hash/code yang tidak di kenal 107
Gambar 4. 90 User Controllabel HTML Element Attribute (Potential XSS) 107



DAFTAR SYMBOL

Simbol	Nama	Keterangan
	Simbol Arus (<i>Flow Direction symbol</i>)	Sebagai penghubung Antara symbol satu dengan symbol yang lain.
	Simbol Terminal (<i>Terminal Symbol</i>)	Fungsi sebagai permulaan (start) dan sebagai tanda akhir (stop) dari suatu kegiatan.
	Simbol Proses (<i>Terminal Symbol</i>)	Menunjukkan proses yang dilakukan oleh komputer
	Simbol Dokumen (<i>Dokument Symbol</i>)	Fungsi untuk memilih proses berdasarkan kondisi yang ada.

INTISARI

Rumah Sakit Umum Daerah Provinsi NTB adalah lembaga pelayanan kesehatan pada masyarakat umum. Sistem website Rumah Sakit Umum Daerah Provinsi NTB ini berfokus pada menyebarluaskan informasi kepada masyarakat umum. Saat ini Rumah Sakit Umum Daerah Provinsi NTB terus berkembang hingga saat ini dan telah mengimplementasikan sistem informasi berbasis *website* di dalam pelayanannya. Dalam hal ini data-data yang di *upload* pada sistem informasi website yang mereka miliki perlu di Analisa keamanannya. Pentingnya keamanan pada suatu informasi yang di *upload* pada *website* agar terhindar dari ancaman atau serangan dari orang yang tidak bertanggung jawab (*hacker*) yang dapat menimbulkan kerugian pada pihak organisasi dan pihak instansi. Maka oleh sebab itu perlu dilakukan pengujian *penetration testing* pada sistem website Rumah Sakit Umum Daerah Provinsi NTB untuk menemukan kelemahan yang ada pada sistem website tersebut.

Dalam pengujian *penetration testing* penulis menggunakan metode yang dijadikan acuan untuk melakukan *penetration testing* yaitu metode PTES (Penetration Testing Execution Standard) yang diantaranya memiliki 7 tahapan yaitu di antaranya *pre-engagement, intelligence gathering, threat modelling, vulnerability analysis, exploitation, post-exploitation*, dan terakhir yaitu *reporting*. Tujuan dari penelitian ini yaitu untuk meminimalisir resiko serangan yang berbahaya dari pihak yang tidak bertanggung jawab.

Berdasarkan dari hasil pengujian terhadap sistem website Rumah Sakit Umum Daerah Provinsi NTB dapat diketahui bahwa sistem website Rumah Sakit Umum Daerah Provinsi NTB memiliki 23 kerentanan, yang termasuk dalam kategori medium yaitu 9 dan sedangkan dengan kerentanan yang termasuk dalam kategori low yaitu 14. Tingkat keamanan ini di dapatkan dengan menggunakan OWASP Risk Rating.

Kata Kunci: *system informasi, System website, PTES, OWASP ZAP, RSUD Provinsi NTB*

ABSTRACT

The NTB Provincial General Hospital is a health service institution for the general public. The website system of the NTB Provincial General Hospital focuses on disseminating information to the general public. Currently, the NTB Provincial General Hospital continues to grow until now and has implemented a website-based information system in its services. In this case the data uploaded on the website information system that they have needs to be analyzed for security. The importance of security on information uploaded on the website in order to avoid threats or attacks from irresponsible people (hackers) that can cause losses to the organization and the agency. Therefore, it is necessary to conduct penetration testing on the NTB Province Regional General Hospital website system to find the weaknesses that exist in the website system.

In penetration testing, the author uses a method that is used as a reference for penetration testing, namely the PTES (Penetration Testing Execution Standard) method, which includes 7 stages, including pre-engagement, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, and finally reporting. The purpose of this research is to minimize the risk of malicious attacks from irresponsible parties.

Based on the test results of the NTB Provincial General Hospital website system, it can be seen that the NTB Provincial General Hospital website system has 23 vulnerabilities, which are included in the medium category namely 9 and while with vulnerabilities included in the low category namely 14. This security level is obtained using the OWASP Risk Rating.

Keywords: *information, website system, PTES, OWASP ZAP, NTB Provincial Hospital*