

**ANALISIS KEAMANAN WEBSITE PADA INSTANSI XYZ  
MELALUI PENETRATION TESTING MENGGUNAKAN  
FRAMEWORK ISSAF & OWASP**

**SKRIPSI**

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



disusun oleh  
**ABDULLAH**  
**19.83.0362**

Kepada:

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM  
YOGYAKARTA  
2023**

**ANALISIS KEAMANAN WEBSITE PADA INSTANSI XYZ  
MELALUI PENETRATION TESTING MENGGUNAKAN  
FRAMEWORK ISSAF & OWASP**

**SKRIPSI**

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



disusun oleh  
**ABDULLAH**  
19.83.0362

Kepada:

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM  
YOGYAKARTA  
2023**

**HALAMAN PERSETUJUAN**

**SKRIPSI**

**ANALISIS KEAMANAN WEBSITE PADA INSTANSI XYZ MELALUI  
PENETRATION TESTING MENGGUNAKAN FRAMEWORK ISSAF &  
OWASP**

yang disusun dan diajukan oleh

**ABDULLAH**

**19.83.0362**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 26 Juli 2023

Dosen Pembimbing,



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

**HALAMAN PENGESAHAN**  
**SKRIPSI**  
**ANALISIS KEAMANAN WEBSITE PADA INSTANSI XYZ MELALUI**  
**PENETRATION TESTING MENGGUNAKAN FRAMEWORK ISSAF &**  
**OWASP**

yang disusun dan diajukan oleh

**ABDULLAH**

**19.83.0362**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 26 Juli 2023

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

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

Joko Dwi Santoso, M.Kom  
NIK. 190302181

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

Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 26 Juli 2023

**DEKAN FAKULTAS ILMU KOMPUTER**



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

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan dibawah ini,

Nama mahasiswa : ABDULLAH  
NIM : 19.83.0362

Menyatakan bahwa Skripsi dengan judul berikut:  
ANALISIS KEAMANAN WEBSITE PADA INSTANSI XYZ MELALUI  
PENETRATION TESTING MENGGUNAKAN FRAMEWORK ISSAF &  
OWASP

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 dikemudian 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, 26 Juli 2023

Yang Menyatakan,



Abdullah

## HALAMAN PERSEMBAHAN

Alhamdulillah Robbil 'Alamin. Segala puji dan syukur atas kehadiran Allah Subhana Wa Ta'ala yang telah memberikan rahmat, ridho, dan karunia-Nya serta nikmat yang tiada tara kepada saya. Shalawat serta salam kepada Nabi Muhammad Shallallahu 'Alaihi Wasallam, sebagai pembawa risalah Allah terakhir dan penyempurna seluruh risalah-Nya yang telah membawa umatnya dari zaman yang gelap gulita ke zaman yang terang benderang. Tugas akhir ini kupersembahkan untuk semua orang yang aku cintai. Terutama teruntuk kepada Ibu tersayang yang tidak pernah lelah memberikan kasih sayang, bimbingan akhlak, dan doa dari kecil hingga sekarang. Kepada Ayah tercinta yang selalu memberikan kasih sayang, nasehat menghadapi kehidupan, pentingnya kerja keras dan doa. Kepada sahabat-sahabatku, terima kasih atas segala kebersamaan, bantuan, dukungan, pengalaman, nasehat, dan doa yang telah diberikan



## KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh Dengan mengucap Alhamdulillah, puji dan syukur atas kehadiran Allah Subhanahu Wa Ta'ala yang telah memberikan berkat rahmat dan hidayah-Nya, sehingga tugas akhir yang berjudul "ANALISIS KEAMANAN WEBSITE PADA INSTANSI XYZ MELALUI PENETRATION TESTING MENGGUNAKAN FRAMEWORK ISSAF & OWASP" dapat diselesaikan dengan baik. Shalawat serta salam tidak lupa senantiasa dilimpahkan kepada Nabi Muhammad Shallallahu 'Alaihi Wasallam, yang telah membawa kita dari zaman jahiliyah menuju ke zaman terang benderang. Laporan tugas akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata-1 (S1) di Jurusan Teknik Komputer, Universitas Amikom Yogyakarta. Selain itu, tugas akhir ini juga sebagai sarana untuk menerapkan ilmu dan teori yang telah didapatkan selama menjalani masa studi di jurusan Teknik Komputer, Universitas Amikom Yogyakarta. Akhirnya, dengan segala kerendahan hati izinkanlah penulis untuk menyampaikan rasa terimakasih dan penghargaan yang setinggi-tingginya atas motivasi, bantuan, bimbingan, dan doa. Penulis menyampaikan rasa dan penghargaan tersebut kepada:

1. Kedua orang tua dan keluarga besar yang selalu memberikan do'a, dukungan dan motivasi sehingga penulis dapat menyelesaikan laporan tugas akhir ini
2. Bapak Dony Ariyus, M. Kom., selaku Ketua Jurusan Teknik Komputer Fakultas Ilmu Komputer Universitas Amikom Yogyakarta
3. Bapak Muhammad Kopravi, S. Kom., M.Eng. Dosen pembimbing tugas akhir yang telah memberikan masukan, arahan, ide, bimbingan mengenai cara-cara melakukan penelitian ini, dan arahan dalam pembuatan laporan tugas akhir dan report hasil penelitian serta dorongan sehingga penelitian ini dapat terlaksana dan diselesaikan
4. Bapak Joko Dwi Santoso, M. Kom. selaku dosen wali saya yang selalu memberikan motivasi arahan dan semangat dalam menjalani perkuliahan dari tahapan awal perkuliahan hingga saat ini

5. Sahabat-sahabat terbaik saya yang tidak dapat saya sebutkan satu persatu terimakasih banyak.
6. Teman-teman Teknik Komputer angkatan 2019 terima kasih atas pengalaman kuliah yang tidak terlupakan.
7. Kepada PT Delta Food cabang Jogja yang telah menambah wawasan dan pengalaman saya dalam mengenali dunia kerja
8. Kepada PT OTSKYR SysBraykr yang telah menambah pengalaman, ilmu dan wawasan saya dibidang cyber security
9. Kepada semua pihak yang telah membantu baik secara langsung maupun tidak langsung, semoga Allah SWT menjadikannya amal baik yang senantiasa mendapatkan balasan dan kebaikan berlipat ganda.

Yogyakarta, 26 Juli 2023



Abdullah



## 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 .....	xi
DAFTAR GAMBAR .....	xii
INTISARI .....	xv
ABSTRACT .....	xvi
BAB I PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	3
1.3 Batasan Masalah .....	3
1.4 Tujuan Penelitian .....	3
1.5 Manfaat Penelitian .....	4
1.6 Sistematika Penulisan .....	5
BAB II TINJAUAN PUSTAKA .....	6
2.1 Studi Literatur .....	6
2.2 Dasar Teori .....	14
2.2.1 Internet .....	14
2.2.2 Keamanan Informasi .....	15
2.2.3 <i>Penetration Testing</i> .....	18
2.2.4 <i>Black Box Testing</i> .....	19
2.2.5 <i>White Box Testing</i> .....	19
2.2.6 <i>Grey Box Testing</i> .....	19
2.2.7 <i>Open Web Application Security Project (OWASP)</i> .....	20
2.2.8 <i>Information System Security Assessment Framework (ISSAF)</i> .....	20
2.2.9 Kerentanan Sistem .....	21
2.2.10 Macam Macam Serangan Terhadap Sistem .....	22
2.2.11 <i>Scanning Tools</i> .....	25
2.2.12 <i>Web Analysis Scanning</i> .....	25
2.2.13 <i>Information Gathering</i> .....	26
2.2.14 <i>Configuration and Deploy Management Testing</i> .....	27
2.2.15 <i>Identity Management Testing</i> .....	27
2.2.16 <i>Authentication Testing</i> .....	28

2.2.17	<i>Authorization Testing</i> .....	28
2.2.18	<i>Session Management Testing</i> .....	29
2.2.19	<i>Input Validation Testing</i> .....	30
2.2.20	<i>Testing For Error Handling</i> .....	30
2.2.21	<i>Testing For Weak Cryptography</i> .....	30
2.2.22	<i>Business Logic Testing</i> .....	31
2.2.23	<i>Client-Side Testing</i> .....	32
2.2.24	<i>Web Server</i> .....	32
2.2.25	<i>Website</i> .....	34
2.2.26	<i>IP Address</i> .....	36
2.2.27	<i>DNS (Domain Name System / Server)</i> .....	37
<b>BAB III METODE PENELITIAN</b> .....		39
3.1	<i>Objek Penelitian</i> .....	39
3.2	<i>Alur Penelitian</i> .....	39
3.2.1	<i>Tahananpan Dalam Melakukan Penetration Testing</i> .....	40
3.3	<i>Alur Penelitian</i> .....	42
3.4	<i>Alat Dan Bahan</i> .....	44
3.4.1	<i>Perangkat Keras (Hardware)</i> .....	44
3.4.2	<i>Perangkat Lunak (Software)</i> .....	45
3.4.3	<i>Tools Pendukung Penelitian</i> .....	45
<b>BAB IV HASIL DAN PEMBAHASAN</b> .....		46
4.1	<i>Penetration Testing</i> .....	46
4.1.1	<i>Gathering Publicly Available Information</i> .....	46
4.1.1.1	<i>Conduct Search Engine Discovery Reconnaissance for information leakage</i> .....	46
4.1.1.2	<i>whois information gathering</i> .....	50
4.1.1.3	<i>Virus scanner</i> .....	52
4.1.1.4	<i>Hostingan History</i> .....	53
4.1.1.5	<i>Review Web server Metafiles for Information Leakage</i> .....	54
4.1.1.6	<i>Review Webpage Content for Information Leakage</i> .....	55
4.1.1.7	<i>Fingerprint Web Application Framework</i> .....	57
4.1.1.8	<i>Detection Firewall</i> .....	59
4.1.2	<i>Network Scanning</i> .....	59
4.1.2.1	<i>Ping Network</i> .....	59
4.1.2.2	<i>Nmap Network Host Scanner</i> .....	61
4.1.3	<i>System Profiling</i> .....	62
4.1.3.1	<i>Nmap system profiling</i> .....	62
4.1.4	<i>Service profiling</i> .....	62
4.1.4.1	<i>nmap service profiling</i> .....	63
4.1.5	<i>Application Testing</i> .....	64
4.1.5.1	<i>Test File Extensions Handling for Sensitive Information</i> .....	64
4.1.5.2	<i>Enumerate Infrastructure and Application Admin Interfaces</i> .....	67
4.1.5.3	<i>Test HTTP method</i> .....	70
4.1.5.3.1	<i>Testing the PUT Method</i> .....	70
4.1.5.3.2	<i>Testing for Access Control Bypass</i> .....	70

4.1.5.3.3	<i>Testing for Cross-Site Tracing Potential</i>	72
4.1.5.3.4	<i>Testing for HTTP Method Overriding</i>	74
4.1.5.4	<i>Test File permission</i>	74
4.1.5.5	<i>Test Account Provisioning Process</i>	75
4.1.5.6	<i>Testing for Account Enumeration and Guessable User Account</i>	78
4.1.5.7	<i>Testing for Credentials Transported over an Encrypted Channel</i>	79
4.1.5.8	<i>Testing for Default Credentials</i>	81
4.1.5.9	<i>Testing for Weak Lock Out Mechanism</i>	83
4.1.5.10	<i>Testing for Browser Cache Weaknesses</i>	84
4.1.5.11	<i>Testing for Weak Password Change or Reset Functionalities</i>	86
4.1.5.12	<i>Testing Directory Traversal File Include</i>	87
4.1.5.13	<i>Testing for Session Management Schema</i>	90
4.1.5.14	<i>Testing for Cookies Attributes</i>	91
4.1.5.15	<i>Testing for Session Fixation</i>	93
4.1.5.16	<i>Testing Session Timeout</i>	94
4.1.5.17	<i>Testing for Reflected Cross Site Scripting</i>	95
4.1.5.18	<i>Testing for Stored Cross Site Scripting</i>	97
4.1.5.19	<i>Testing for SQL Injection</i>	97
4.1.5.20	<i>Testing for Weak Transport Layer Security</i>	99
4.1.6	<i>Vulnerability Identification / Assessment</i>	100
4.1.6.1	<i>OWASP Zap Scanning</i>	100
4.1.6.2	<i>BrupSuit Scanning</i>	103
4.1.6.3	<i>Perbandingan Antara Kedua Tools</i>	105
4.2	<i>Hasil pengujian</i>	106
4.3	<i>Rekomendasi</i>	108
<b>BAB V PENUTUP</b>		111
5.1	<i>Kesimpulan</i>	111
5.2	<i>Saran</i>	111
<b>REFERENSI</b>		112
<b>LAMPIRAN</b>		116
	<i>OWASP ZAP Scanning</i>	116
	<i>Burp Suite Scanning</i>	133

## DAFTAR TABEL

Table 2. 1 Keaslian Penelitian .....	8
Table 3. 1 keterangan temuan .....	43
Table 3. 2 spesifikasi perangkat keras .....	44
Table 3. 3 spesifikasi <i>virtual machine</i> .....	45
Table 3. 4 <i>tools</i> pendukung penelitian .....	45
Tabel 4. 1 <i>payload</i> google dorking .....	47
Tabel 4. 2 <i>hidden path</i> .....	54
Tabel 4. 3 <i>path default admin example</i> .....	68
Tabel 4. 4 <i>path example traversal directory</i> .....	87
Tabel 4. 5 perbandingan <i>tools</i> .....	105
Tabel 4. 6 hasil pengujian .....	106
Tabel 4. 7 rekomendasi .....	108

## DAFTAR GAMBAR

Gambar 1. 1 jumlah anomaly nasional serangan siber pada tahun 2021 .....	2
Gambar 2. 1 jumlah pengguna internet aktif dari tahun 2018 - 2022 .....	15
Gambar 2. 2 proses <i>penetration testing</i> secara umum .....	19
Gambar 3. 1 alur penelitian .....	41
Gambar 4. 1 <i>Publicly exposed documents payload</i> .....	47
Gambar 4. 2 <i>Directory listing vulnerabilities payload</i> .....	47
Gambar 4. 3 <i>Database files exposed payload</i> .....	47
Gambar 4. 4 <i>Backup and old files</i> .....	48
Gambar 4. 5 <i>Log files exposed payload</i> .....	48
Gambar 4. 6 <i>Signup pages payload</i> .....	48
Gambar 4. 7 <i>SQL Errors payload</i> .....	49
Gambar 4. 8 <i>Login pages payload</i> .....	49
Gambar 4. 9 <i>Show only IP addresses payload</i> .....	50
Gambar 4. 10 <i>whois tools</i> .....	51
Gambar 4. 11 <i>virustotal scanner</i> .....	52
Gambar 4. 12 <i>netcraft tools</i> .....	53
Gambar 4. 13 <i>netcraft tools</i> .....	53
Gambar 4. 14 <i>html webpage content menggunakan payload &lt;--</i> .....	56
Gambar 4. 15 <i>html webpage content menggunakan komentar user</i> .....	56
Gambar 4. 16 <i>html webpage content menggunakan komentar admin</i> .....	56
Gambar 4. 17 <i>javascript webpage content menggunakan komentar password</i> .....	56
Gambar 4. 18 <i>javascript webpage content menggunakan komentar password</i> .....	57
Gambar 4. 19 <i>Whatweb tools</i> .....	57
Gambar 4. 20 <i>Wappalyzer tools</i> .....	58
Gambar 4. 21 <i>Whatwaf tools</i> .....	59
Gambar 4. 22 <i>ping menggunakan kali linux</i> .....	60
Gambar 4. 23 <i>ping menggunakan windows</i> .....	60
Gambar 4. 24 <i>network host scanner</i> .....	61
Gambar 4. 25 <i>Identifikasi system</i> .....	62

Gambar 4. 26 Identifikasi layanan .....	63
Gambar 4. 27 robots.txt ext.....	64
Gambar 4. 28 <i>directory</i> ext.....	65
Gambar 4. 29 <i>Documents</i> ext.....	65
Gambar 4. 30 woff file ext.....	65
Gambar 4. 31 cgi ext.....	66
Gambar 4. 32 <i>vulnerability</i> ext.js.....	67
Gambar 4. 33 <i>scanning path default admin example</i> .....	68
Gambar 4. 34 <i>response 400 for path default admin example</i> .....	69
Gambar 4. 35 <i>response 404 for path default admin example</i> .....	69
Gambar 4. 36 <i>Put method</i> .....	70
Gambar 4. 37 halaman yang digunakan untuk pengujian <i>Access Control Bypass</i> 71	
Gambar 4. 38 <i>HEAD method for Access Control Bypass</i> .....	71
Gambar 4. 39 <i>POST method for Access Control Bypass</i> .....	71
Gambar 4. 40 <i>PUT method for Access Control Bypass</i> .....	72
Gambar 4. 41 <i>CATS method for Access Control Bypass</i> .....	72
Gambar 4. 42 <i>TRACE method menggunakan alternatif header Random:Header</i> 73	
Gambar 4. 43 <i>TRACE method menggunakan alternatif header berupa serangan XSS</i> .....	73
Gambar 4. 44 <i>DELETE method for HTTP Method Overriding</i> .....	74
Gambar 4. 45 <i>PHP file permission</i> .....	75
Gambar 4. 46 mengubah kredensial menggunakan admin .....	76
Gambar 4. 47 menghapus data menggunakan admin .....	76
Gambar 4. 48 mengubah informasi penting menggunakan admin .....	77
Gambar 4. 49 mengubah kredensial menggunakan <i>user</i> .....	77
Gambar 4. 50 export data menggunakan <i>user</i> .....	78
Gambar 4. 51 mekanisme <i>autentikasi</i> dengan <i>password</i> yang salah .....	79
Gambar 4. 52 saluran <i>HTTPS</i> .....	80
Gambar 4. 53 saluran <i>HTTP</i> .....	80
Gambar 4. 54 <i>vulnerable default kredensial</i> .....	81
Gambar 4. 55 akun yang rentan .....	82

Gambar 4. 56 <i>default kredensial for Lock Out Mechanism</i> .....	83
Gambar 4. 57 respon <i>default kredensial</i> .....	83
Gambar 4. 58 autentikasi menggunakan kredensial yang valid.....	84
Gambar 4. 59 halaman login .....	85
Gambar 4. 60 <i>cache control</i> yang ditangani .....	85
Gambar 4. 61 <i>update kredensial menggunakan user</i> .....	86
Gambar 4. 62 respon pembaharuan kredensial .....	86
Gambar 4. 63 <i>random path traversal directory</i> .....	89
Gambar 4. 64 <i>etc password path traversal directory</i> .....	89
Gambar 4. 65 <i>HTTPS session</i> .....	90
Gambar 4. 66 <i>HTTP session</i> .....	91
Gambar 4. 67 <i>attribute cookie</i> .....	92
Gambar 4. 68 <i>session</i> sebelum autentikasi.....	93
Gambar 4. 69 <i>session</i> sesudah autentikasi .....	93
Gambar 4. 70 <i>session timeout</i> .....	94
Gambar 4. 71 keterangan <i>session timeout</i> setelah <i>logout</i> .....	95
Gambar 4. 72 <i>payload XSS</i> .....	96
Gambar 4. 73 <i>payload XSS</i> yang tidak <i>redirect</i> .....	96
Gambar 4. 74 <i>XSS stored</i> .....	97
Gambar 4. 75 <i>sqlmap injection</i> .....	98
Gambar 4. 76 <i>payload sql injections</i> .....	98
Gambar 4. 77 <i>ssllscan tools</i> .....	99
Gambar 4. 78 <i>fingerprints</i> .....	99
Gambar 4. 79 <i>alert OWASP scanner</i> .....	101
Gambar 4. 80 <i>alert detail</i> .....	101
Gambar 4. 81 <i>alert detail</i> .....	102

## INTISARI

Seiring dengan perkembangan zaman dimana semuanya serba digital semua bisa kita lakukan dengan bantuan teknologi canggih dan akses internet yang bisa kita gunakan dimana saja dan kapan saja. Kemajuan peradaban manusia juga dapat dilihat melalui kemajuan teknologi, bahkan tidak jarang ada organisasi yang aktif memanfaatkan kemajuan teknologi seperti instansi, bahkan perusahaan besar. Di era digital ini, informasi menjadi salah satu hal yang paling berharga bagi instansi XYZ, instansi ini bergerak di bidang kesehatan dimana informasi dan database menjadi salah satu aset penting bagi instansi tersebut. Pentingnya keamanan pada suatu jaringan adalah hal utama dimana fungsi keamanan digunakan untuk mencegah serangan dari pihak luar yang tidak bertanggung jawab yang dapat menimbulkan kerugian. Untuk mengetahui seberapa rentan suatu jaringan website terhadap serangan dari luar, maka perlu dilakukan *penetration testing* dimana seseorang melakukan analisis keamanan dan mencoba mensimulasikan serangan pada jaringan organisasi atau perusahaan tertentu untuk menemukan kelemahan yang ada pada sistem jaringan.

Dalam melakukan *penetration testing* di sini penulis menggunakan *framework* ISSAF dan OWASP yang dijadikan sebagai acuan dalam melakukan pengujian dengan meliputi enam segmen diantaranya *Gathering Publicly Available Information, Network Scanning, System Profiling, Service Profiling, Application Testing, Vulnerability Identification / Assessment. Framework* ISSAF dan OWASP dipilih karena memiliki penjelasan yang mudah untuk di ikuti. Tujuan dilakukannya *penetration testing* adalah untuk meminimalisir serangan yang berbahaya dari pihak yang merugikan.

Berdasarkan pengujian yang telah dilakukan oleh penulis website instansi xyz memiliki 3 celah keamanan diantaranya *Identified Viruses, File Extensions Information dan Default Credentials*. Penulis memberikan 12 rekomendasi kepada pihak website untuk meningkatkan keamanan website instansi XYZ.

**Kata kunci:** Informasi, ISSAF dan OWASP, *Penetration Testing*, Website.



## ABSTRACT

*Along with the development of the era where everything is completely digital, we can do everything with the help of advanced technology and internet access that we can use anywhere and anytime. The progress of human civilization can also be seen through technological advances. It is not uncommon for organizations to actively take advantage of technological advances such as agencies, even large companies. In this digital era, information is one of the most valuable things for the XYZ agency, this agency is engaged in the health sector where information and databases are one of the important assets for the agency. The importance of security on a network is the main thing where the security function is used to prevent attacks from irresponsible outsiders that can cause losses. To find out how vulnerable a website network is to attacks from outside, it is necessary to do penetration testing where someone conducts a security analysis and tries to simulate attacks on certain organizational or company networks to find weaknesses in the network system.*

*In conducting penetration testing here the author uses the ISSAF and OWASP frameworks which are used as a reference in conducting the test covering six segments including Gathering Publicly Available Information, Network Scanning, System Profiling, Service Profiling, Application Testing, Vulnerability Identification/Assessment. The ISSAF and OWASP frameworks were chosen because they have explanations that are easy to follow. The purpose of doing penetration testing is to minimize malicious attacks from harmful parties.*

*Based on tests that have been carried out by the author of the xyz agency website, it has 3 security holes including Identified Viruses, File Extensions Information and Default Credentials. The author provides 12 recommendations to the website to improve the security of the XYZ agency website.*

**Keywords:** *Information, ISSAF and OWASP, Penetration Testing, Website.*