

**IMPLEMENTASI *OPEN WEB APPLICATION SECURITY PROJECT*  
UNTUK *PENETRATION TESTING* PADA *WEBSITE* INSTITUSI  
PENDIDIKAN**

**SKRIPSI**

Diajukan untuk memenuhi salah satu persyaratan mencapai derajat Sarjana  
Program Studi Informatika



diajukan oleh  
**NANI SULISNAWATI**  
**19.11.3034**

Kepada

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

**IMPLEMENTASI *OPEN WEB APPLICATION SECURITY PROJECT*  
UNTUK *PENETRATION TESTING* PADA *WEBSITE* INSTITUSI  
PENDIDIKAN**

**SKRIPSI**

untuk memenuhi salah satu persyaratan memperoleh gelar Sarjana  
Program Studi Informatika



diajukan oleh  
**NANI SULISNAWATI**  
**19.11.3034**

Kepada

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

HALAMAN PERSETUJUAN

SKRIPSI

**IMPLEMENTASI *OPEN WEB APPLICATION SECURITY PROJECT*  
UNTUK *PENETRATION TESTING* PADA *WEBSITE* INSTITUSI  
PENDIDIKAN**

yang disusun dan diajukan oleh

**Nani Sulisnawati**

19.11.3034

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 22 Mei 2023

**Dosen Pembimbing.**

**Subektriningsih, M.Kom**

**NIK. 190302413**

**HALAMAN PENGESAHAN**

**SKRIPSI**

**IMPLEMENTASI *OPEN WEB APPLICATION SECURITY PROJECT*  
UNTUK *PENETRATION TESTING* PADA *WEBSITE* INSTITUSI  
PENDIDIKAN**

yang disusun dan diajukan oleh

**Nani Sulisnawati**

**19.11.3034**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 22 Mei 2023

**Susunan Dewan Penguji**

**Nama Penguji**

**Nuri Cahyono, M.Kom**

**NIK. 190302278**

**Jeki Kuswanto, M.Kom**

**NIK. 190302456**

**Subektiningsih, M.Kom**

**NIK. 190302413**

**Tanda Tangan**



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 22 Mei 2023

**DEKAN FAKULTAS ILMU KOMPUTER**



**Hanif Al Fatta, S.Kom., M.Kom**

**NIK. 190302096**

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Nani Sulisnawati  
NIM : 19.11.3034

Menyatakan bahwa Skripsi dengan judul berikut:

**IMPLEMENTASI OPEN WEB APPLICATION SECURITY PROJECT UNTUK  
PENETRATION TESTING PADA WEBSITE INSTITUSI PENDIDIKAN**

Dosen Pembimbing : Subektiningsih, M.Kom

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, 22 Mei 2023

Yang Menyatakan,



Nani Sulisnawati

## HALAMAN PERSEMBAHAN

Saya persembahkan Skripsi ini untuk saya.

*"I am the best partner for me"*



## KATA PENGANTAR

Puji dan syukur kehadiran Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan Skripsi ini dengan judul **“IMPLEMENTASI OPEN WEB APPLICATION SECURITY PROJECT UNTUK PENETRATION TESTING PADA WEBSITE INSTITTUSI PENDIDIKAN”**, sebagai salah satu syarat untuk menyelesaikan Program Sarjana Jurusan Informatika Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.

Penulis menyadari bahwa Skripsi ini tidak mungkin terselesaikan tanpa adanya bimbingan, bantuan, serta dukungan dari berbagai pihak dalam proses penyusunan. Secara khusus dengan ketulusan hati penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. M. Suyanto, M.M., selaku Rektor Universitas AMIKOM Yogyakarta.
2. Bapak Hanif Al Fatta, S.Kom., M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Ibu Windha Mega Pradnya Duhita, M.Kom., selaku Ketua Program Studi Informatika Universitas AMIKOM Yogyakarta.
4. Ibu Subektiningsih, S.Kom., M.Kom., selaku Dosen Pembimbing Skripsi yang telah membimbing penulis dengan disiplin dan kooperatif baik secara teknis maupun non teknis dalam proses penyusunan Skripsi ini.
5. Bapak Haryoko, S.Kom., M.Cs., selaku Dosen Wali yang telah memberikan bantuan serta bimbingan kepada penulis selama mengikuti dan menyelesaikan pendidikan di Program Studi Informatika Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
6. Seluruh staff pengajar yang telah memberikan ilmu pengetahuan yang sangat berharga selama penulis melaksanakan perkuliahan di Program Studi Informatika Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
7. Kedua orang tua dan kedua kakak tersayang, yang selalu memberikan dukungan doa, nasihat, serta kasih sayang yang tidak terbatas untuk penulis.
8. Seluruh teman-teman seperjuangan 19S11F07, Magang MBKM Batch 3, Kost Putri Bharata, serta sahabat terdekat yang telah memberikan bantuan, dukungan, semangat kepada penulis dalam proses penyusunan Skripsi ini.

Dalam penyusunan Skripsi ini penulis menyadari bahwa masih banyak kekurangan, untuk itu penulis sangat mengharapkan kritik dan saran yang bersifat membangun dan semoga Skripsi ini dapat bermanfaat sehingga dapat membantu penelitian selanjutnya di masa depan.

Yogyakarta, 22 Mei 2023

Penulis





## 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
DAFTAR LAMPIRAN .....	xiii
INTISARI .....	xiv
<i>ABSTRACT</i> .....	xv
BAB I.....	1
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 Penelitian.....	3
BAB II.....	5
TINJAUAN PUSTAKA.....	5
2.1 Studi Literatur.....	5
2.2 Dasar Teori.....	11
2.2.1 Sistem Keamanan Informasi.....	11
2.2.2 <i>Website</i> .....	11
2.2.3 <i>Penetration Testing</i> .....	11
2.2.4 <i>Open Web Application Security Project (OWASP)</i> .....	12
2.2.5 Alat Pengumpulan Informasi ( <i>Information Gathering Tools</i> ).....	14
2.2.6 Alat Pemindaian ( <i>Scanning and Vulnerability Assessment Tools</i> ).....	15
2.2.7 Alat Eksploitasi ( <i>Exploitation Tools</i> ).....	16

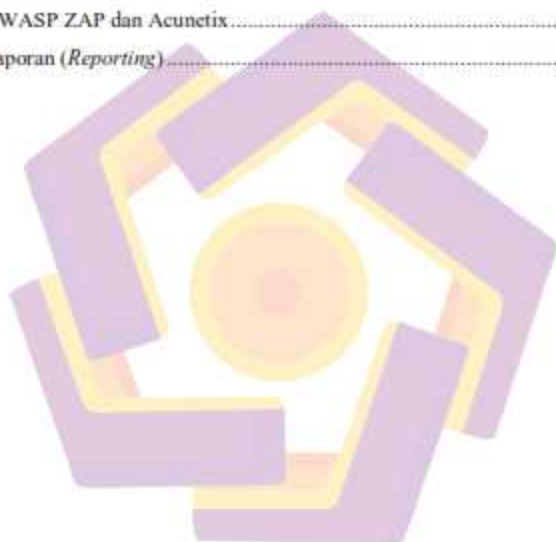
BAB III.....	17
METODE PENELITIAN .....	17
3.1 Objek Penelitian .....	17
3.1.1 Profil Institusi .....	17
3.1.2 Sejarah.....	17
3.1.3 Visi dan Misi.....	18
3.1.4 Struktur Organisasi .....	18
3.2 Alur Penelitian.....	19
3.2.1 Identifikasi Masalah.....	20
3.2.2 Studi Literatur.....	20
3.2.3 <i>Penetration Testing</i> menggunakan OWASP Top 10 2021 .....	20
3.2.4 Laporan ( <i>Reporting</i> ).....	21
3.3 Skenario Pengujian.....	21
3.4 Alat dan Bahan.....	21
3.3.1 Perangkat Keras ( <i>Hardware</i> ).....	21
3.3.2 Perangkat Lunak ( <i>Software</i> ).....	22
BAB IV.....	23
HASIL DAN PEMBAHASAN.....	23
4.1 Pengumpulan Informasi ( <i>Information Gathering</i> ).....	23
4.1.1 Whois .....	23
4.1.2 Harvester.....	24
4.1.3 Whatweb.....	24
4.1.4 Google <i>Directives</i> .....	25
4.1.5 Nmap.....	32
4.2 Pemindaian ( <i>Scanning and Vulnerability Assessment</i> ).....	34
4.2.1 OWASP ZAP.....	34
4.2.2 Acunetix .....	41
4.3 Eksploitasi ( <i>Exploitation</i> ).....	55
4.3.1 OWASP ZAP.....	55
4.3.2 Acunetix .....	55
4.3.3 OWASP ZAP dan Acunetix .....	57
4.4 Laporan ( <i>Reporting</i> ) .....	64
BAB V.....	71

PENUTUP .....	71
5.1 Kesimpulan.....	71
5.2 Saran .....	71
DAFTAR PUSTAKA.....	73
LAMPIRAN.....	76



## DAFTAR TABEL

Tabel 3. 1 Spesifikasi Perangkat Keras.....	21
Tabel 3. 2 Spesifikasi Perangkat Keras.....	21
Tabel 3. 3 Spesifikasi Perangkat Lunak.....	22
Tabel 4. 1 <i>Port dan Service</i> .....	33
Tabel 4. 2 OWASP ZAP.....	34
Tabel 4. 3 Acunetix.....	41
Tabel 4. 4 OWASP ZAP.....	55
Tabel 4. 5 Acunetix.....	55
Tabel 4. 6 OWASP ZAP dan Acunetix.....	57
Tabel 4. 7 Laporan ( <i>Reporting</i> ).....	64



## DAFTAR GAMBAR

Gambar 3. 1 Struktur Organisasi .....	19
Gambar 3. 2 Alur Penelitian .....	19
Gambar 4. 1 Whois .....	23
Gambar 4. 2 theHarvester .....	24
Gambar 4. 3 Whatweb .....	24
Gambar 4. 4 Google Hacking Database .....	25
Gambar 4. 5 Google Hacking Database .....	25
Gambar 4. 6 Google Hacking Database .....	25
Gambar 4. 7 Dorking filetype:ini "Bootstrap.php" (pass/passwd/password/pwd) .....	26
Gambar 4. 8 Dorking intitle:"index of" "cookies" "php" .....	26
Gambar 4. 9 Dorking allintext:"Index Of" "cookies.txt" .....	27
Gambar 4. 10 Dorking inurl:"Windows/Cookies/" ext:txt-telecom -forbidden -git .....	28
Gambar 4. 11 Dorking inurl:"Windows/Cookies/" ext:txt -git .....	28
Gambar 4. 12 Dorking intitle:"Index Of" cookies.txt "size" .....	29
Gambar 4. 13 Dorking intitle:"index of" "WindowsCookies" .....	30
Gambar 4. 14 Dorking "lv_poweredBy" .....	30
Gambar 4. 15 Dorking intitle:"b2evo > Login form" "Login form. You must log in! You will have to accept cookies in order to log in" -demo -site.b2evolution.net .....	31
Gambar 4. 16 Dorking intitle:"Member Login" "NOTE: Your browser must have cookies enabled in order to log into the site." ext:php OR ext:cgi .....	32
Gambar 4. 17 Absence of Anti-CSRF Tokens .....	59
Gambar 4. 18 Directory listings .....	60
Gambar 4. 19 Clickjacking: X-Frame-Options header .....	60
Gambar 4. 20 Cookie sithout SameSite Attribute .....	60
Gambar 4. 21 Cookie with missing, inconsistent or contradictory properties .....	61
Gambar 4. 22 Session cookie scoped to parent domain .....	61
Gambar 4. 23 Content Security Policy (CSP) not implemented .....	62
Gambar 4. 24 Cookie without Secure flag set .....	62
Gambar 4. 25 HTTP Strict Transport Security HSTS not implemented .....	63
Gambar 4. 26 TSL/SSL certificate about to expire .....	63
Gambar 4. 27 Cross-Domain JavaScript Source File Inclusion .....	63
Gambar 4. 28 Loosely Scoped Cookie .....	64

## DAFTAR LAMPIRAN

Lampiran 1. <i>Scanning and Vulnerability OWASP ZAP Tool</i> .....	76
Lampiran 2. <i>Scanning and Vulnerability Acunetix Tool</i> .....	76
Lampiran 3. Surat Permohonan Penelitian .....	77
Lampiran 4. Surat Pemberian Ijin Penelitian.....	78
Lampiran 5. Permohonan Dosen Pembimbing Skripsi/Tugas Akhir Lembar 1 .....	79
Lampiran 6. Permohonan Dosen Pembimbing Skripsi/Tugas Akhir Lembar 2 .....	80
Lampiran 7. Bukti Penyerahan Tugas Akhir/Skripsi kepada IC AMIKOM Yogyakarta.....	81



## INTISARI

Perkembangan teknologi informasi yang semakin canggih tidak lepas dari perkembangan internet dan aplikasi *website* serta ancaman dari keamanan siber. Universitas AMIKOM Yogyakarta menggunakan aplikasi *website* sebagai sarana sistem informasi dalam perkuliahan. Salah satu upaya penanganan dalam mengidentifikasi celah keamanan pada aplikasi *website* adalah dengan melakukan kegiatan *penetration testing*. Adapun target yang akan diuji yaitu *domain* *mhs.amikom.ac.id* dikarenakan *domain* tersebut memiliki data sensitif yang perlu pengamanan *realtime*. Pada penelitian ini, metode yang digunakan adalah *Open Web Application Security Project (OWASP) Top 10 2021*. Hasil yang diperoleh setelah melakukan pengujian kerentanan dan analisis, *domain* target memiliki 11 kerentanan yang dapat dieksploitasi. Dari 11 kerentanan tersebut ada 1 kerentanan masuk kategori tingkat risiko sedang (*medium*), 7 kerentanan masuk kategori tingkat risiko rendah (*low*), dan 3 kerentanan masuk kategori tingkat risiko informasi (*informational*). Berdasarkan hasil yang telah diperoleh, dapat disimpulkan bahwa kerentanan-kerentanan yang berhasil diidentifikasi perlu untuk segera diperbaiki oleh tim pengembang. Oleh karena itu, hasil akhir dari penelitian ini berupa laporan dokumentasi pertanggung jawaban yang berisi daftar celah keamanan dan rekomendasi perbaikan pada sistem aplikasi *website*.

### **Kata kunci:**

Pengujian Penetrasi, Keamanan Sistem Informasi, OWASP, Aplikasi *Website*.

## **ABSTRACT**

*The development of increasingly sophisticated information technology cannot be separated from the development of the internet and website applications as well as threats from cybersecurity. AMIKOM Yogyakarta University uses a website application as a means of information systems in lectures. One of the handling efforts in identifying security holes in website applications is to carry out penetration testing activities. The target to be tested is the mhs.amikom.ac.id domain because this domain has sensitive data that needs realtime security. In this study, the method used is the Open Web Application Security Project (OWASP) Top 10 2021. The results obtained after conducting vulnerability testing and analysis, the target domain has 11 vulnerabilities that can be exploited. Of the 11 vulnerabilities, there is 1 vulnerability in the medium risk category, 7 vulnerabilities in the low risk category, and 3 vulnerabilities in the informational risk category. Based on the results that have been obtained, it can be concluded that the identified vulnerabilities need to be fixed by the development team immediately. Therefore, the final result of this research is in the form of an accountability documentation report that contains a list of security holes and recommendations for improvements to the website application system.*

### **Keywords:**

*Penetration Testing, Information System Security, OWASP, and Web-Based Applications.*