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,

Subektiningsih, 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	Tanda Tangan
Nuri Cahyono, M.Kom	
NIK. 190302278	
Jeki Kuswanto, M.Kom	
NIK. 190302456	
Subektiningsih, M.Kom	
NIK. 190302413	

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 kehadirat 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* INSTITUSI 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 Dhuhita, 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 meyelesaikan 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 19S1IF07, 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

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

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.