ANALISIS KERENTANAN KEAMANAN PADA WEBSITE MENGGUNAKAN REDHAWK

SKRIPSI

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

diajukan oleh

Kukuh Putra Handayanta
18.83.0159

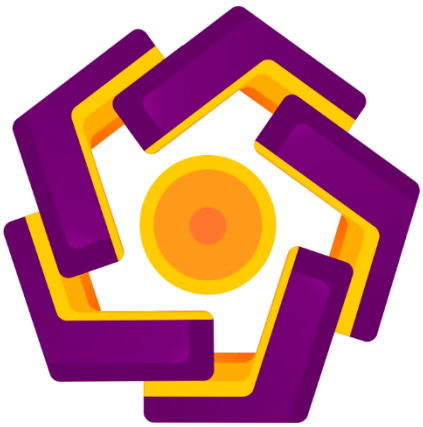
Kepada

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022

ANALISIS KERENTANAN KEAMANAN PADA WEBSITE MENGGUNAKAN REDHAWK

SKRIPSI

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



diajukan oleh

Kukuh Putra Handayanta

18.83.0159

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS KERENTANAN KEAMANAN PADA WEBSITE MENGGUNAKAN REDHAWK

yang disusun dan diajukan oleh

Kukuh Putra Handayanta

18.83.0159

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 2 Oktober 2021

Dosen Pembimbing,

Joko Dwi Santoso. M.Kom
NIK. 190302181

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS KERENTANAN KEAMANAN PADA WEBSITE MENGGUNAKAN REDHAWK

yang disusun dan diajukan oleh

Kukuh Putra Handayanta

18.83.0159

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Juli 2022

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
JokoDwiSantoso,M.Kom **NIK. 190302181**	
Melwin Syafrizal, S.Kom., M.Eng. **NIK. 190302105**	
Ria Andriani, M.Kom **NIK. 190302458**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Juli 2022

DEKAN FAKULTAS ILMU KOMPUTER

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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Kukuh Putra Handayanta
NIM : 18.83.0159

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS KERENTANAN KEAMANAN PADA WEBSITE MENGGUNAKAN REDHAWK
Dosen Pembimbing : Joko Dwi Santoso. 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, 21 Juli 2022

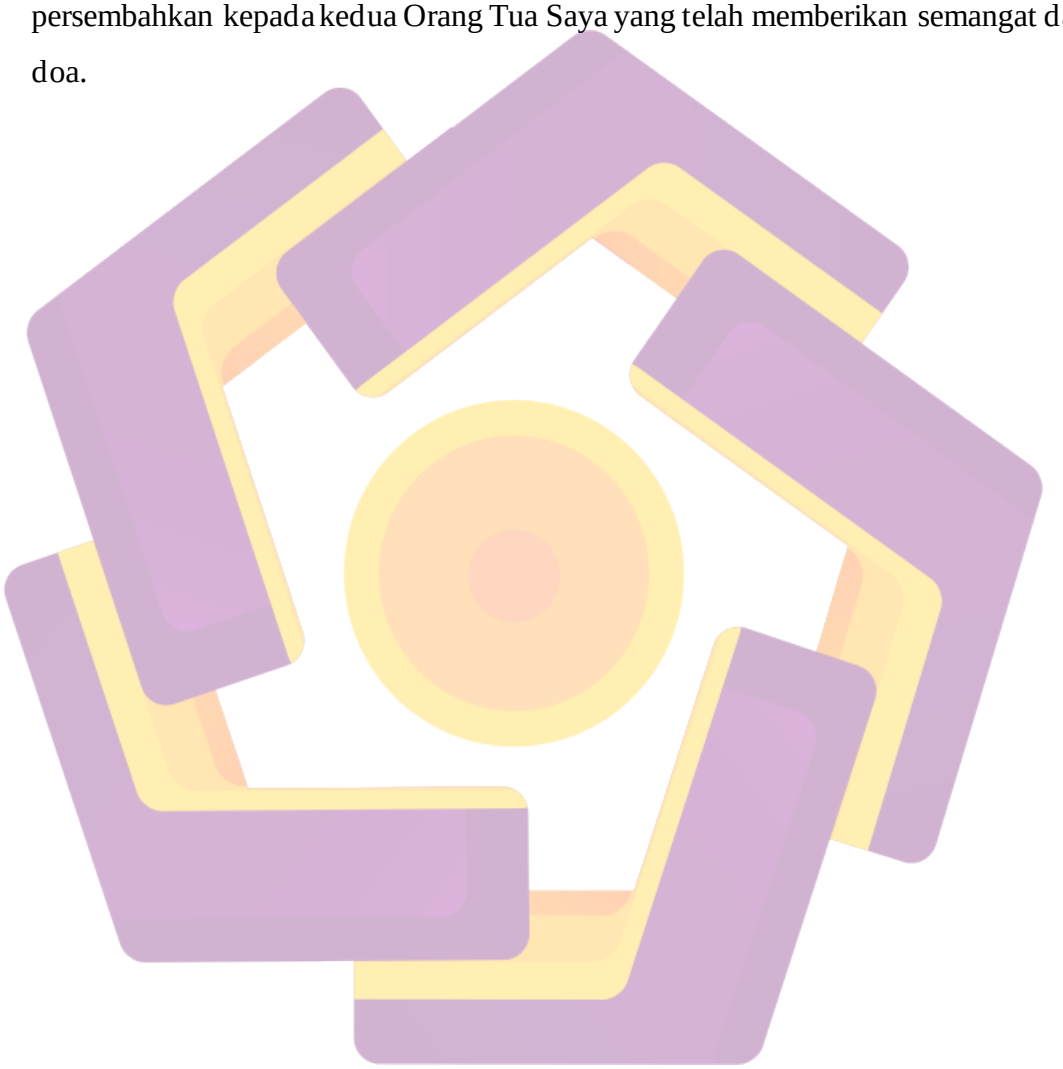
Yang Menyatakan,

Kukuh Putra Handayanta

v

HALAMAN PERSEMBAHAN

Pertama-tama saya ucapakan puji syukur kepada Allah SWT yang telah membantu dengan memberikan kemudahan kepada saya. Sehingga skripsi ini berjalan dengan lancar dan mendapatkan hasil terbaik. Maka skripsi saya persembahkan kepada kedua Orang Tua Saya yang telah memberikan semangat dan doa.



KATA PENGANTAR

Segala Puji Syukur saya ucapkan kepda Allah SWT atas segala rahmat dan kemudahan serta limpahan rezeki-Nya yang telah di berikan. Sehingga Skripsi yang sedang saya tempuh saat ini dengan judul"Analisis Kerentanan Keamanan Pada Website Menggunakan RedHawk" dapat saya selesaikan dengan baik dan lancer.

Pada kesempatan kali ini ingin mengucapkan terima kasih kepada beberapa pihak yang berkait dalam membantu serta membimbing saya sampai menyelesaikan skripsi ini dengan baik dan lancar . ucapan terima kasih ini saya persembahkan kepada yang terhormat:

1. Prof. Dr. M. Suyanto, M.M. selaku sebagai Rektor di perguruan tinggi swasta Universitas Amikom Yogyakarta
2. Joko Dwi Santoso, M.Kom. selaku sebagai Dosen Pembimbing yang mau meluangkan waktunya dalam membimbing saya dalam meraih gelar S1 sarjana
3. Kedua orang tua, yang telah sabar dan selalu memotivasi saya dalam menyelesaikan Skripsi
4. Dony Ariyus, M.Kom. selaku ketua prodi S1 Teknik Komputer di perguruan tinggi swasta Universitas Amikom Yogyakarta

Pada Penelitian ini penulis sangat menyadari bahwasannya masih bisa di bilang belom mendekati kata sempurna hasil yang di berikan. Karena masih jauh dari kata sempurna sehingga penulis tetap berharap hasil dari karya ilmiah yang telah disusun sedemikian rupa dapat membantu dan memberikan manfa'at bagi semua pihak yang membacanya.

Yogyakarta, 6 Maret 2022

Penulis

DAFTAR ISI

HALAMAN PERSETUJUAN.....iii
HALAMAN PENGESAHAN.....iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI**Error! Bookmark not defined.**
HALAMAN PERSEMBAHAN.....vi
KATA PENGANTAR.....vii
DAFTAR ISI.....viii
DAFTAR TABEL.....xi
DAFTAR GAMBAR.....xii
INTISARI.....xiii
Abstract.....xiv
BAB I PENDAHULUAN.....1
1.1 Latar Belakang.....1
1.2 Perumusan masalah.....2
1.3 Tujuan Penelitian.....3
1.4 Batasan Masalah.....3
1.5 Manfaat Penelitian.....3
BAB II TINJAUAN PUSTAKA.....4
2.1 Literature Review.....4
2.2 Landasan Teori.....12
2.2.1 Kualitatif.....12
2.2.2 Pengertian *Word, Wide, Web*.....12
2.2.3 Pengertian *Website*.....12
2.2.4 Unsur *Website*.....13
2.2.4.1 *Domain*.....13
2.2.4.2 *Web Hosting*.....13
2.2.4.3 Konten.....13
2.5 Pengertian *Virtual Machine*.....13
2.6 Mengenal *Vulnerability Assesment*.....13

2.6.1 Pengertian *Vulnerability Assesment* 13
2.6.2 Jenis-Jenis Vulnerability Assesment 14
2.6.2.1 Network-bases Scans 14
2.6.2.2 Host-based Scans 14
2.6.2.3 Wireless network Scans 14
2.6.2.4 Application Scans 14
2.6.2.5 Database Scans 14
2.7 Macam Macam *Vulnerability Website* top 10:2021 14
2.7.1 *Broken Access Control* 14
2.7.2 *Cryptographic Failures* 15
2.7.3 *Injection* 15
2.7.4 *Insecure Design* 15
2.7.5 *Security Misconfiguration* 15
2.7.6 *Vulnerable and Outdated Components* 15
2.7.7 *Identification and Authentication Failures* 16
2.7.8 *Software* and data *intergrity Failures* 16
2.7.9 *Security Logging and Monitoring Failures* 16
2.7.10 *Server-Side Request Forgery* (SSRF)* 16
2.8 Mengenal *Openlitespeed* 16
2.8.1 Pengertian *OpenLiteSpeed* 16
2.8.2 Features OpenLiteSpeed 17
2.8.2.1 *Event-Driven Architecture* 17
2.8.2.2 Understands APACHE Rewrite Rules 17
2.8.2.3 Friendly Admin Interfaces 17
2.8.2.4 Built for Speed and Security 17
2.8.2.5 Intelligent Cache Acceleration 17
2.8.2.6 *PHP LiteSpeed SAPI* 17
2.9 Mengenal *WordPress* 17
2.9.1 Pengertian *WordPress* 17
2.9.2 Sejarah *WordPress* 18
2.10 Mengenal *RedHawk* 18
2.10.1 Pengertian *RedHawk* 18

2.11 Perangkat yang digunakan.....19
2.11.1 *Windows 10* 19
2.11.2 *Virtual Box*.....19
2.11.3 *Kali Linux* 19
2.11.4 *Ubuntu* 20
BAB III METODOLOGI PENELITIAN.....21
3.1 Analisis Permasalahan 21
3.2 Langkah Penelitian: 23
3.2.1 Pengumpulan Informasi.....24
3.2.2 Investigasi.....24
3.2.3 Pengujian 24
3.2.5 Laporan.....25
3.3 Alat dan Bahan Penelitian 25
BAB IV HASIL DAN PEMBAHASAN 26
4.1 Implementasi 26
4.1.1 *Website Offline* 26
4.1.2 Website Online.....30
4.2 Pengujian 34
4.2.1 website Offline.....34
4.2.2 Website Online.....35
BAB V KESIMPULAN DAN SARAN.....37
5.1 Kesimpulan.....37
5.2 Saran 37
DAFTAR PUSTAKA 38

DAFTAR TABEL

Tabel 2. 1 Tabel Perbandingan Pustaka 6
Table 3. 1 informasi celah keamanan periode 2018 ID-SIRTII.....21
Table 3. 2 Alat dan Bahan.....25

DAFTAR GAMBAR

Gambar 3. 1 Laporan Data yang mengalami kebocoran ditahun 2018 22
Gambar 3. 2 Tren Serangan siber Malware 23
Gambar 3. 3 Flowchart Penelitian 24
Gambar 4. 1 Halaman Awal RedHawk 26
Gambar 4. 2 Website Target 27
Gambar 4. 3 Information Gathering Scan Basic 28
Gambar 4. 4 Information Gathering dengan Banner Grabbing 28
Gambar 4. 5 CMS Wordpress 29
Gambar 4. 6 Webserver yang digunakan target 30
Gambar 4. 7 Scan Basic 31
Gambar 4. 8 Information Gathering dengan Whois 32
Gambar 4. 9 Information Gathering dengan Whois 33
Gambar 4. 10 Information Gathering dengan Nmap 34
Gambar 4.2 1 Hasil Vulnerability Scans mendapatkan halaman login 34
Gambar 4.2 2 Halaman login CMS Wordpress 35
Gambar 4.2 3 Vulnerability Scanner 36

INTISARI

Pada era saat ini yang mengalami perkembangan teknologi informasi yang sangat cepat yang membuat keamanan informasi menjadi sangat krusial. Menurut *Open Web Application Security Project* (OWASP) tepat pada tahun 2017 muncul beberapa kerentanan yang ditemukan pada situs web seperti kelemahan terhadap Injeksi, otentikasi rusak, data sensitif yang terekspos, kontrol akses yang rusak, kesalahan dalam konfigurasi, serta kelemahan Cross-Site-Scripting (XSS) yang membuat pelaku penyerang dapat melakukan eksploitasi sistem dari kerentanan-kerentanan tersebut.

Metode penelitian yang digunakan dalam penelitian adalah menggunakan metode Kualitatif dengan menggunakan Redhawk, dan melakukan beberapa tahapan seperti mengumpulkan informasi, investigasi, pengujian dan pelaporan.

Hasil dari penelitian fokus pada pengguna'an Tool RedHawk dalam mencoba menemukan kerentanan pada website yang dijadikan target dan hasilnya menemukan beberapa kerentanan dan dari sisi informasi terhadap website target yaitu wp-login.php, ip address 192.168.159.3, judul websitenya, nama webserver yang digunakan dan versi wordpress yang digunakan yaitu 5.8.2 yang dibangun sendiri dengan Wordpress atau CMS (*Content Management System*). dan yang terkait kerentanan lainnya seperti CVE (*Common Vulnerabilities and Exposures*), sehingga hal tersebut bisa dimanfaatkan oleh penyusup untuk mengakses dan mengumpulkan informasi sensitif, dengan hal tersebut penyusup akan dengan mudah melakukan eksploitasi kelemahan yang ada.

Kata kunci: *OWASP*, *RedHawk*, CMS, CVE, Keamanan sistem.

Abstract

In the current era, which is experiencing a very rapid development of information technology which makes information security very crucial. According to the Open Web Application Security Project (OWASP) in 2017, several vulnerabilities were found on websites such as weaknesses in Injection, corrupted authentication, exposed sensitive data, corrupted access control, errors in configuration, as well as Cross-Site-Scripting (XSS) weaknesses that allowed attackers to exploit the system from these vulnerabilities.

The research method used in the research is to use the Qualitative method using Redhawk, and carry out several stages such as collecting information, investigation, testing and reporting.

The results of the research focused on using the RedHawk Tool in trying to find vulnerabilities in the targeted website and the results found several vulnerabilities and in terms of information on the target website, namely wp-login.php, ip address 192.168.159.3, the title of the website, the name of the webserver used and the wordpress version used, namely 5.8.2 which was built by wordpress or CMS (Content Management System). and those related to other vulnerabilities such as CVE (Common Vulnerabilities and Exposures), so that it can be exploited by intruders to access and collect sensitive information, with which intruders will easily exploit existing weaknesses.

Keyword: *OWASP, RedHawk, CMS, CVE, system security*