

**ANALISIS CELAH KEAMANAN WEBSITE MENGGUNAKAN
METODE VULNERABILITY ASSESSMENT**

SKRIPSI



Disusun oleh:
AGUS SETIAWAN
17.83.0093

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2022

**ANALISIS CELAH KEAMANAN WEBSITE MENGGUNAKAN
METODE VULNERABILITY ASSESMENT**

SKRIPSI

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



diajukan oleh
AGUS SETIAWAN
17.83.0093

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022**

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS CELAH KEAMANAN WEBSITE MENGGUNAKAN METODE
VULNERABILITY ASSESSMENT**

yang disusun dan diajukan oleh

Agus Setlawan

17.83.0093

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 6 juli 2022

Dosen Pembimbing,

ii

**Banu Santoso, S.T., M.Eng.
NIK. 190302327**

HALAMAN PENGESAHAN

SKRIPSI

**ANALISIS CELAH KEAMANAN WEBSITE MENGGUNAKAN
METODE VULNERABILITY ASSESMENT**

yang disusun dan diajukan oleh

Agus Setiawan

17.83.0093

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Juli 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Banu Santoso, S.T., M.Eng.
NIK. 190302327

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

Dony Arlyus, M.Kom.
NIK. 190302128

Skrripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 5 September 2022

DEKAN FAKULTAS ILMU KOMPUTER

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

BALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang beresdandan di bawah ini,

Nama mahasiswa : Agus Setiawan
NIM : 17.03.0093

Menatakan bahwa Skripsi dengan judul berikut

Analisis celah keamanan website menggunakan metode *Vulnerability Assessment*

Dosen Pembimbing : Bani Samudra, S.T., S.H.Eng

1. Karya tulis ini adalah benar-benar ASLI dan BUKAN PERBAH dipaparkan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Penerapan lainnya.
2. Karya tulis ini merupakan gagasan, tujuan 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 diungkapkan sebagai acuan dalam tulisan 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 pembatukan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 23 Juli 2022

Yang Menandatangani,



Agus Setiawan

HALAMAN PERSEMBAHAN

Alhamdulillah, segala puji Allah SWT dengan kemurahan dan ridho-Nya, skripsi ini dapat ditulis dengan baik dan lancar hingga selesai. Dengan ini akan saya persembahkan skripsi ini kepada:

Nabi Muhammad SAW sebagai panutan umat muslim yang penuh dengan kemuliaan dan ketaatan kepada Allah SWT memberiku motivasi tentang kehidupan dan mengajarkan hidup melalui sunnah-sunnahnya.

Keluarga saya Suwar (Ayah), Karni (Ibu), Supriyadi (kakak), dan Ika (calon Istri) yang selalu memberikan saya ketenangan, kenyamanan, motivasi, doa terbaik dan menyisihkan finansial nya, sehingga saya bisa menyelesaikan studi ini. Kalian sangat berarti bagiku.

Bapak Banu Santoso, S.T., M.Eng. yang telah sabar membimbing saya untuk menyelesaikan tugas akhir ini.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadiran Allah SWT, karena rahmat dan karunianya penulis dapat menyelesaikan skripsi yang berjudul “analisis celah keamanan website menggunakan metode *Vulnerability Assessment*”. Dalam skripsi ini dibahas mengenai temuan kerentana pada website. Adapun maksud dan tujuan dari penulisan skripsi ini adalah untuk memenuhi salah satu syarat untuk mengikuti sidang skripsi, jurusan Teknik Komputer Universitas Amikom Yogyakarta.

Selama penulisan dan penelitian skripsi ini banyak sekali hambatan yang penulis alami, namun berkat bantuan, dorongan serta bimbingan dari berbagai pihak, akhirnya skripsi ini dapat terselesaikan dengan baik.

Penulis beranggapan bahwa skripsi ini merupakan karya terbaik yang dapat penulis persembahkan. Tetapi penulis menyadari bahwa tidak tertutup kemungkinan didalamnya terdapat kekurangan-kekurangan. Oleh karena itu kritik dan saran yang membangun sangat penulis harapkan. Akhir kata, semoga skripsi ini dapat bermanfaat bagi penulis dan pembaca.

Boyolali, 16 juli 2022

Penulis

Agus Setiawan

DAFTAR ISI

| | |
|-------------------------------------|------|
| HALAMAN PERSETUJUAN..... | ii |
| SKRIPSI..... | ii |
| HALAMAN PENGESAHAN..... | iii |
| HALAMAN PERSEMBAHAN..... | v |
| KATA PENGANTAR..... | vi |
| DAFTAR ISI..... | vii |
| DAFTAR TABEL..... | viii |
| DAFTAR GAMBAR..... | ix |
| DAFTAR LAMPIRAN..... | x |
| INTISARI..... | xi |
| Abstract..... | xii |
| BAB I PENDAHULUAN..... | 1 |
| 1.1 Latar Belakang Masalah..... | 1 |
| 1.2 Rumusan Masalah..... | 2 |
| 1.3 Batasan Masalah..... | 2 |
| 1.4 Tujuan Penelitian..... | 2 |
| 1.5 Manfaat Penelitian..... | 2 |
| 1.6 Sistematika Penulisan..... | 2 |
| BAB II LANDASAN TEORI..... | 4 |
| 2.1 Tinjauan Pustaka..... | 4 |
| 2.2 Dasar Teori..... | 6 |
| BAB III METODOLOGI PENELITIAN..... | 10 |
| BAB IV PEMBAHASAN..... | 13 |
| 4.1 Implementasi sistem..... | 13 |
| 4.2 Hasil Pengujian Kerentanan..... | 17 |
| BAB V PENUTUP..... | 34 |
| 5.1 Kesimpulan..... | 34 |
| 5.2 Saran..... | 34 |
| DAFTAR PUSTAKA..... | 35 |

DAFTAR TABEL

| | |
|--|----|
| Tabel 2. 1 Tinjauan Pustaka | 5 |
| Tabel 4. 1 Report Vulnerability Acunetix | 18 |
| Tabel 4. 2 Hasil Scanning Acunetix | 20 |
| Tabel 4. 3 Report Vulnerability Owasp ZAP | 21 |
| Tabel 4. 4 Hasil Pengujian Owasp ZAP | 23 |
| Tabel 4. 5 Report Vulnerability Nessus | 24 |
| Tabel 4. 6 Hasil Pengujian Nessus | 25 |
| Tabel 4. 7 Rekomendasi dari Acunetix | 27 |
| Tabel 4. 8 Rekomendasi Nessus | 29 |
| Tabel 4. 9 Rekomendasi Owasp Zap | 30 |

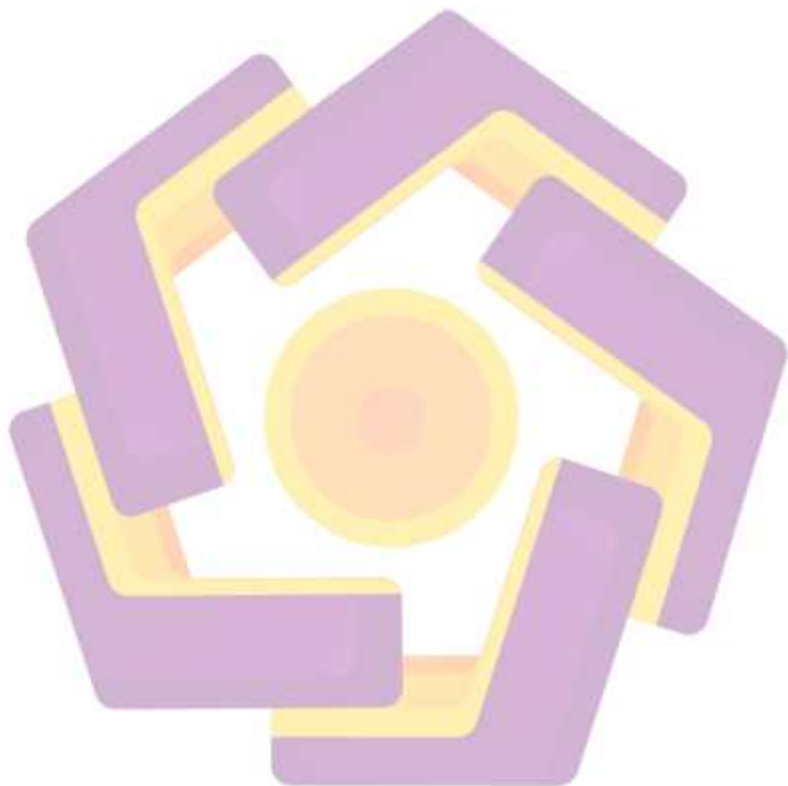


DAFTAR GAMBAR

| | |
|--|----|
| Gambar 3. 1 Alur peneltltan | 11 |
| Gambar 4. 1 Halaman Registrasi Acunetix | 13 |
| Gambar 4. 2 Halaman LogIn Acunetix | 13 |
| Gambar 4. 3 Halaman Scan Target Acunetix | 14 |
| Gambar 4. 4 Halaman Download Owasp ZAP | 14 |
| Gambar 4. 5 Halaman Instalasi Owasp ZAP | 15 |
| Gambar 4. 6 Halaman Owasp ZAP | 15 |
| Gambar 4. 7 Halaman Scan Target Owasp ZAP | 16 |
| Gambar 4. 8 Halaman Registrasi Nessus | 16 |
| Gambar 4. 9 Halaman LogIn Nessus | 17 |
| Gambar 4. 10 Halaman Scan Target Nessus | 17 |
| Gambar 4. 11 Hasil Scanning Acunetix | 18 |
| Gambar 4. 12 Report Acunetix high dan medium | 19 |
| Gambar 4. 13 Report Acunetix Low | 20 |
| Gambar 4. 14 Scanning Acunetix | 21 |
| Gambar 4. 15 Report Owasp ZAP low | 22 |
| Gambar 4. 16 Report Owasp ZAP medium | 23 |
| Gambar 4. 17 Hasil Scanning Owasp ZAP | 24 |
| Gambar 4. 18 Hasil Scan Nessus | 24 |
| Gambar 4. 19 Report Nessus Medium | 25 |
| Gambar 4. 20 Hasil Pengujian Nessus | 26 |
| Gambar 4. 21 Waktu Scanning | 27 |
| Gambar 4. 22 Perbandingan Hasil | 32 |

DAFTAR LAMPIRAN

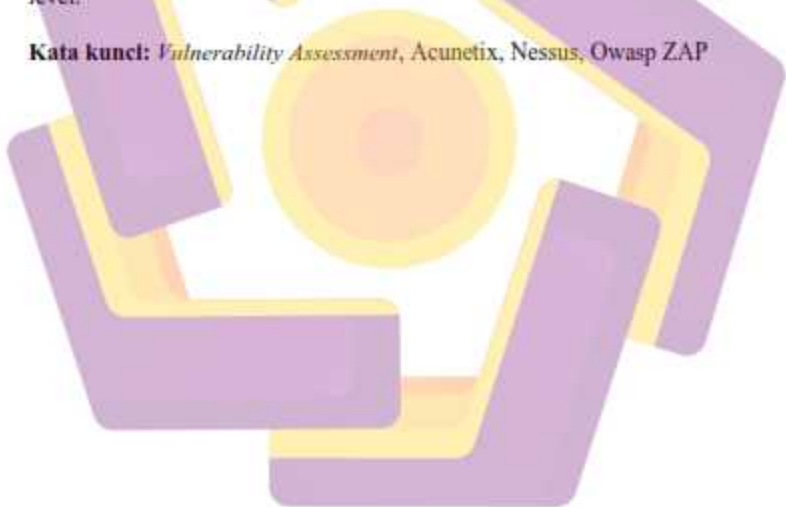
| | |
|------------|----|
| Lampiran 1 | 37 |
| Lampiran 2 | 40 |
| Lampiran 3 | 43 |



INTISARI

Keamanan website merupakan hal yang perlu untuk diperhatikan. Karena untuk melindungi informasi dari pihak yang tidak terkait, meski website dapat diakses oleh publik akan tetapi dalam sebuah website juga menyimpan informasi penting yang harus dijaga. Maka faktor keamanan pada *website* perlu diperhatikan, salah satunya menggunakan metode *Vulnerability Assessment*. metode *Vulnerability Assessment* merupakan metode yang melakukan pengujian kelemahan atau kerentanan pada web atau aplikasi. secara garis besar penelitian ini dilaksanakan menggunakan 3 tahap dari proses *Vulnerability Assessment* yaitu *Implementasi sistem, vulnerability scanning dan reporting*. *Vulnerability Assessment* dilakukan menggunakan *software* Acunetix, Nessus dan Owasp ZAP. Proses *Vulnerability Assessment* pada *website* menghasilkan temuan kerentanan atau kelemahan. Acunetix menemukan celah keamanan sejumlah 1 high, 14 medium dan 10 Low level. Nessus menemukan celah keamanan sejumlah 6 medium level dan Owasp ZAP menemukan celah berjumlah 5 medium dan 7 low level.

Kata kunci: *Vulnerability Assessment*, Acunetix, Nessus, Owasp ZAP



ABSTRACT

Website security is something that needs to be considered. Because to protect information from unrelated parties, although the website can be accessed by the public, a website also stores important information that must be protected. So the security factors on the website need to be considered, one of which is using the Vulnerability Assessment method. The Vulnerability Assessment method is a method that tests weaknesses or vulnerabilities in a web or application. This research was carried out using 3 stages of the Vulnerability Assessment process, namely system implementation, vulnerability scanning, and reporting. A Vulnerability Assessment was carried out using Acunetix, Nessus, and Owasp ZAP software. The Vulnerability Assessment process on the website results in finding vulnerabilities or weaknesses. Acunetix found a security gap of 1 high, 14 medium, and 10 low levels. Nessus found a security gap of 6 medium, and Owasp ZAP found a gap of 5 medium and 7 low levels.

Keyword: *Vulnerability Assessment, Acunetix, Nessus, Owasp ZAP*