

**ANALISIS CELAH KEAMANAN WEBSITE
PEMERINTAH KABUPATEN BANYUMAS DENGAN
METODE *PORT SCANNING*, *BRUTE FORCE*,
*DAN SQL INJECTION***



SKRIPSI

HARDI DANU PRAKOSO

1503040046

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN SAINS
UNIVERSITAS MUHAMMADIYAH PURWOKERTO
JUNI, 2020**

**ANALISIS CELAH KEAMANAN WEBSITE
PEMERINTAH KABUPATEN BANYUMAS DENGAN
METODE *PORT SCANNING*, *BRUTE FORCE*,
DAN *SQL INJECTION***



SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar
Sarjana Komputer

HARDI DANU PRAKOSO

1503040046

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN SAINS
UNIVERSITAS MUHAMMADIYAH PURWOKERTO
JUNI, 2020**

HALAMAN PERSETUJUAN

UJIAN PENDAHULUAN TUGAS AKHIR

ANALISIS CELAH KEAMANAN WEBSITE PEMERINTAH KABUPATEN BANYUMAS DENGAN METODE PORT SCANNING, BRUTE FORCE, DAN SQL INJECTION

Disusun Oleh :

Hardi Danu Prakoso

1503040046

Telah disetujui untuk diajukan dalam ujian skripsi
Purwokerto.

PEMBIMBING

Ermadi Satriya Wijaya, S.T., M.Kom.

NIK. 2160767

HALAMAN PENGESAHAN

Skrripsi yang diajukan oleh:

Nama : Hardi Danu Prakoso

NIM : 1503040046

Program Studi : Teknik Informatika

Fakultas : Teknik dan Sains

Perguruan Tinggi : Universitas Muhammadiyah Purwokerto

Judul : Analisis Celah Keamanan Website

Pemerintah Kabupaten Banyumas dengan Metode
Port Scanning, Brute Force, Dan Sql Injection

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer (S.Kom) pada Program Studi Teknik Informatika, Fakultas Teknik dan Sains, Universitas Muhammadiyah Purwokerto.

DEWAN PENGUJI

Penguji 1 : Ermadi Satria Wijaya, S.T., M.Kom.

Penguji 2 : Hindayati Mustafidah, S.Si., M.Kom.

Penguji 3 : Mukhlis Prasetyo Aji, S.T., M.Kom.

Ditetapkan di : Purwokerto

Tanggal : Juni 2020

Mengetahui:

Dekan Fakultas Teknik dan Sains

P. Teguh Marheni, S.T., MT, ASEAN Eng. IPM

NIM 2160172

HALAMAN PERNYATAAN ORISINALITAS

Saya yang bertanda tangan di bawah ini:

Nama : Hardi Danu Prakoso
NIM : 1503040046
Program Studi : Teknik Informatika
Fakultas : Teknik dan Sains
Perguruan Tinggi : Universitas Muhammadiyah Purwokerto

Menyatakan dengan sebenar-benarnya bahwa skripsi ini adalah hasil karya saya dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar serta bukan hasil penjiplakan dari karya orang lain.

Demikian pernyataan ini saya buat dan apabila kelak di kemudian hari terbukti ada unsur penjiplakan, saya bersedia mempertanggungjawabkan sesuai dengan ketentuan yang berlaku.

Purwokerto, Juni 2020

Yang membuat pernyataan



Hardi Danu Prakoso

HALAMAN PERSEMBAHAN

Kupersembahkan Skripsi ini untuk orang tua tercinta, kakak-kakak yang hebat, teman-teman yang membantu, dan dosen pembimbing yang selalu mendukung dan membimbing. Terima kasih banyak.



HALAMAN MOTTO

“YOLO (You Only Live Once) And Be Human As Always”



KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah subhanahu wa ta'ala yang telah melimpahkan kasih dan sayang-Nya kepada kita, sehingga penulis bisa menyelesaikan skripsi dengan tepat waktu. Salam dan salawat selalu tercurah kepada junjungan kita baginda Rasulullah SAW, yang telah membawa manusia dari alam jahiliyah menuju alam yang berilmu seperti sekarang ini.

Penyusunan skripsi ini dimaksudkan untuk memenuhi sebagian syarat-syarat guna mencapai gelar Sarjana Informatika di Universitas Muhammadiyah Purwokerto. Laporan skripsi ini dapat hadir seperti sekarang ini tak lepas dari bantuan banyak pihak. Untuk itu sudah sepantasnya penulis mengucapkan rasa terimakasih yang sebesar-besar untuk mereka yang telah berjasa membantu selama proses pembuatan laporan skripsi ini dari awal hingga akhir.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna dikarenakan terbatasnya pengalaman dan pengetahuan yang dimiliki penulis. Oleh karena itu, penulis mengharapkan segala bentuk saran serta masukan bahkan kritik yang membangun dari berbagai pihak. Semoga skripsi ini dapat bermanfaat bagi para pembaca dan semua pihak khususnya dalam bidang teknologi dan sains.

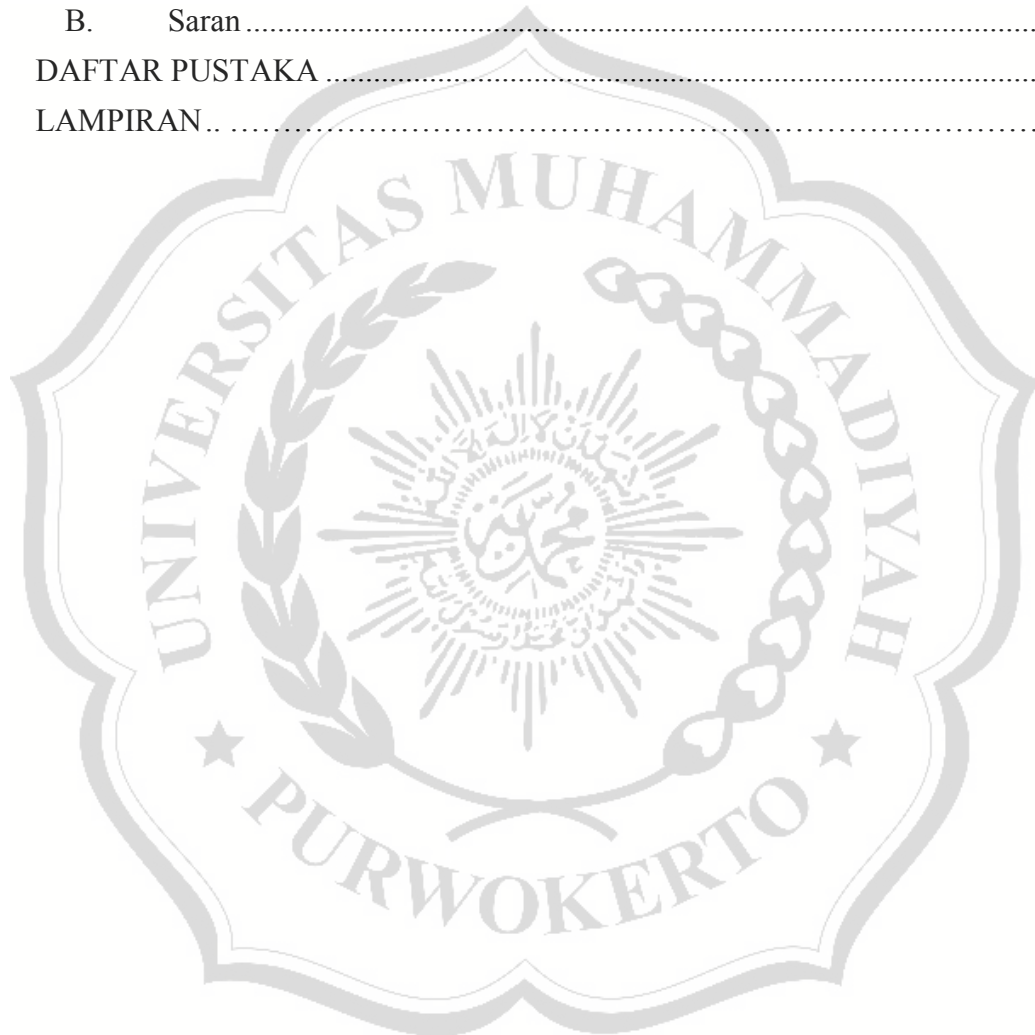
Purwokerto, Juni 2020

Hardi Danu Prakoso

DAFTAR ISI

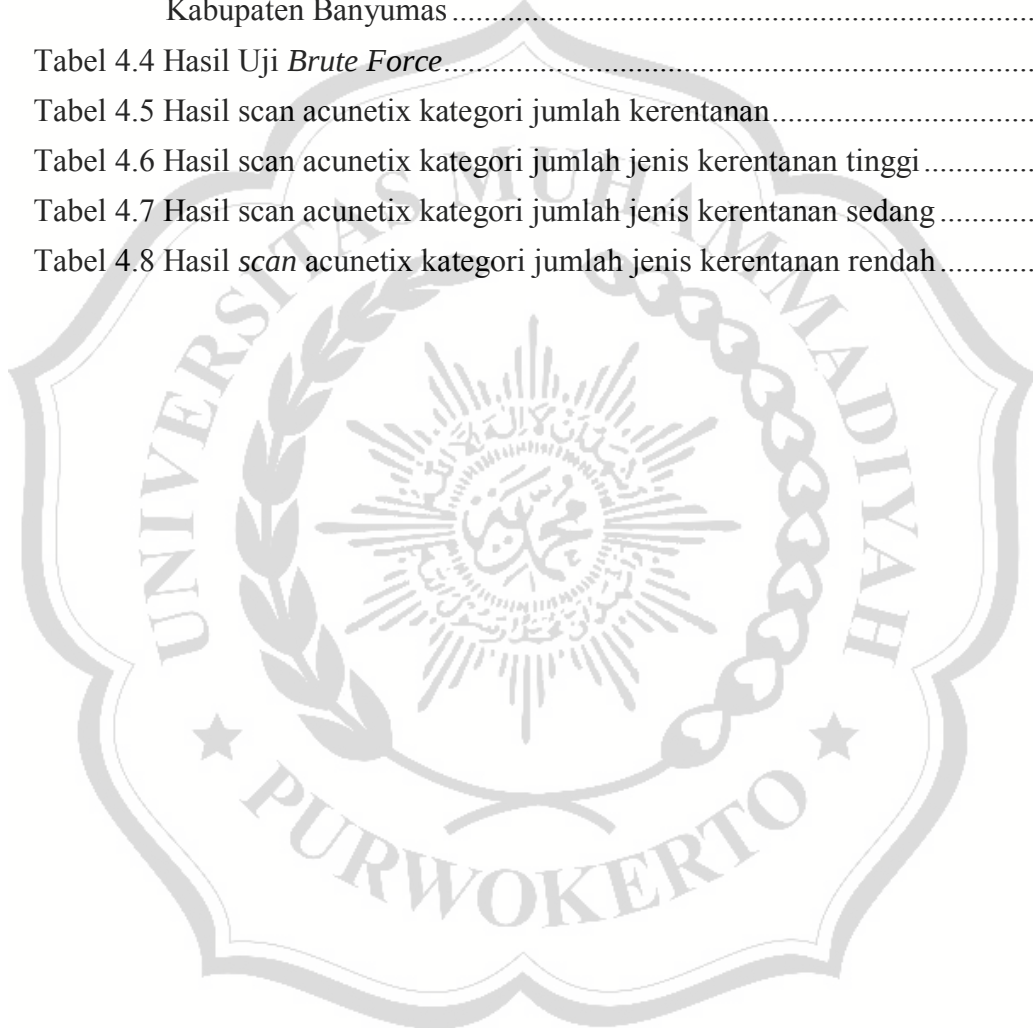
HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERNYATAAN ORISINALITAS	v
HALAMAN PERSEMBAHAN	vi
HALAMAN MOTTO	vii
KATA PENGANTAR	viii
DAFTAR ISI	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN	xiii
ABSTRAK	xiv
ABSTRACT	xv
BAB I PENDAHULUAN	1
A. Latar Belakang	1
B. Perumusan Masalah	3
C. Batasan Masalah	4
D. Tujuan Penelitian	5
E. Manfaat Penelitian	5
BAB II TINJAUAN PUSTAKA	13
A. Penelitian Terdahulu	13
B. Landasan Teori	18
BAB III METODE PENELITIAN	20
A. Jenis Penelitian	20
B. Waktu Dan Tempat	22
C. Variabel Yang Diteliti	22
D. Instrumen Penelitian	22
E. Desain Alur Penelitian	23
F. Prosedur Analisis Celah Keamanan Website	23
BAB IV HASIL PENELITIAN	27
A. Data Penelitian	27
B. Analisis Hasil	27
1. Pindai Port (<i>Port Scanning</i>)	27

2.	Penentuan Sampel Uji Keamanan <i>Domain</i> dan <i>Sub-domain</i>	29
3.	Uji <i>Brute Force</i>	31
4.	Uji <i>SQL Injection Nmap</i>	32
5.	<i>Full Scanning Acunetix</i>	41
BAB V PENUTUP.....		52
A.	Kesimpulan.....	52
B.	Saran	52
DAFTAR PUSTAKA		54
LAMPIRAN		56



DAFTAR TABEL

Tabel 4.1 Data Daftar hasil <i>Port Scanning Domain</i> dan <i>Sub-domain</i> Pemerintah Kabupaten Banyumas	28
Tabel 4.2 Detail Jumlah <i>Port</i> Terbuka	29
Tabel 4.3 Sample Uji Keamanan <i>domain</i> dan <i>sub-domain website</i> pemerintah Kabupaten Banyumas	30
Tabel 4.4 Hasil Uji <i>Brute Force</i>	31
Tabel 4.5 Hasil scan acunetix kategori jumlah kerentanan	45
Tabel 4.6 Hasil scan acunetix kategori jumlah jenis kerentanan tinggi	46
Tabel 4.7 Hasil scan acunetix kategori jumlah jenis kerentanan sedang	47
Tabel 4.8 Hasil scan acunetix kategori jumlah jenis kerentanan rendah	50

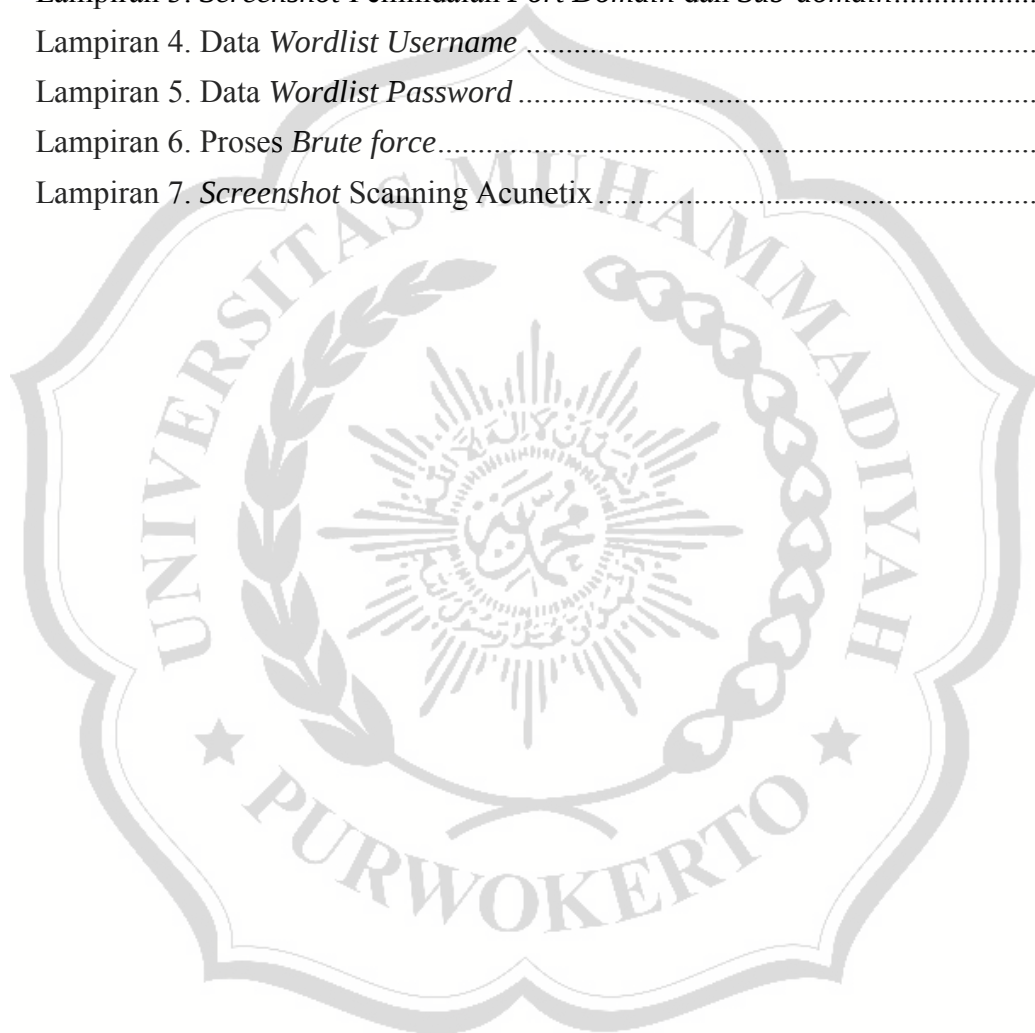


DAFTAR GAMBAR

Gambar 3.1 Metode <i>Port Scanning</i>	20
Gambar 3.2 Metode <i>Port Scanning</i>	23
Gambar 3.3 Tahapan Mendapatkan Celah Keamanan <i>Website</i>	23
Gambar 4.1 Contoh Proses Pengujian <i>SQL injection</i> menggunakan <i>Nmap</i>	32
Gambar 4.2 Lanjutan Contoh Proses Pengujian <i>SQL injection</i> menggunakan <i>Nmap</i>	32
Gambar 4.3 Contoh Alamat <i>website</i> Memiliki Kerentanan <i>Query</i>	33
Gambar 4.4 Pengujian pada <i>banyumaskab.go.id</i>	34
Gambar 4.5 Pengujian pada <i>rsudajibaranag.banyumaskab.go.id</i>	35
Gambar 4.6 Pengujian pada <i>dinperkim.banyumaskab.go.id</i>	35
Gambar 4.7 Pengujian pada <i>rsud.banyumaskab.go.id</i>	36
Gambar 4.8 Pengujian pada <i>bkd.banyumaskab.go.id</i>	37
Gambar 4.9 Pengujian pada <i>dindik.banyumaskab.go.id</i>	37
Gambar 4.10 Pengujian pada <i>dpmptsp.banyumaskab.go.id</i>	38
Gambar 4.11 Pengujian pada <i>dinkes.banyumaskab.go.id</i>	39
Gambar 4.12 Pengujian pada <i>dinnakerkopukm.banyumaskab.go.id</i>	39
Gambar 4.13 Pengujian pada <i>dindukcapil.banyumaskab.go.id</i>	40
Gambar 4.14 Pengujian pada <i>banyumas.kemenag.go.id</i> a.....	41
Gambar 4.15 Tampilan login <i>acunetix</i>	42
Gambar 4.16 <i>Sidebar acunetix</i>	42
Gambar 4.17 <i>Popup form target</i>	43
Gambar 4.18 Tampilan sebelum <i>scanning acunetix</i>	43
Gambar 4.19 <i>Popup scanning option</i>	44
Gambar 4.20 Tampilan proses <i>scanning acunetix</i>	44
Gambar 4.21 Tampilan selesai proses <i>scanning acunetix</i>	45

DAFTAR LAMPIRAN

Lampiran 1. Surat Perizinan.....	57
Lampiran 2. Data <i>Domain</i> dan <i>Sub-domain</i> Pemerintah Kabupaten Banyumas .	59
Lampiran 3. Tabel Kunjungan Bulan Desember.....	60
Lampiran 3. <i>Screenshot</i> Pemindaian <i>Port Domain</i> dan <i>Sub-domain</i>	61
Lampiran 4. Data <i>Wordlist Username</i>	74
Lampiran 5. Data <i>Wordlist Password</i>	75
Lampiran 6. Proses <i>Brute force</i>	91
Lampiran 7. <i>Screenshot</i> Scanning Acunetix.....	102



ABSTRAK

Website pemerintah Kabupaten Banyumas ini dibuat dengan mengikuti perkembangan zaman dimana masyarakat membutuhkan kemudahan dalam mengakses informasi mengenai hal-hal yang berkaitan dengan pemerintah Banyumas ataupun informasi umum yang ada di sekitar Kabupaten Banyumas. Tujuan penelitian ini adalah untuk menganalisis celah keamanan *website* untuk dijadikan rujukan evaluasi keamanan pada *website* tersebut. Metode penelitian yang digunakan dalam analisis celah keamanan web ini adalah metode penelitian kualitatif berupa analisis eksperimen menggunakan metode *port scanning* untuk memindai port dan *brute force* serta *SQL Injection* untuk *penetration testing*. Perangkat lunak untuk analisis yaitu nmap dan hydra. Hasil penelitian ini menunjukkan tingkat keamanan *website* pemerintah Kabupaten Banyumas terhadap *penetration testing* dengan *brute force* dan *SQL Injection*. Hasil akhir penelitian ini memberikan ulasan dan evaluasi terhadap keamanan *website* pemerintah Kabupaten Banyumas, sehingga dapat dijadikan rujukan untuk menambah keamanan *website* pemerintah Kabupaten Banyumas.

Kata Kunci : Celah Keamanan, *Website*, *Port Scanning*

ABSTRACT

The Banyumas Regency government website is based on information on the development of the era in which people need information about matters relating to the Banyumas government or general information in Banyumas Regency. The purpose of this study is to analyze the security holes of the website to be used as a reference for security evaluation on the website. The research methodology used in this web security vulnerability analysis is a qualitative research method consisting of research analysis using the port scan method for port and brute force investigation and SQL Injection for penetration testing. The software for analysis is nmap and hydra. The results of this study indicate the level of security of the Banyumas Regency government website against penetration testing with brute force and SQL Injection. The Final Results of this study provides a review and evaluation of the Banyumas Regency government website, so that it can be used as a reference for adding Banyumas district government website.

Keywords: Security Vulnerable, Website, Port Scanning