



***PENETRATION TESTING TERHADAP SISTEM MANAJEMEN  
DATA SUMBER TERBUKA CKAN MENGGUNAKAN  
METODE OWASP TOP 10***

**SKRIPSI**

**HANNA NABILA CANTHY PELAWI**

**1810511022**

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN**

**JAKARTA**

**FAKULTAS ILMU KOMPUTER**

**PROGRAM STUDI INFORMATIKA**

**2022**



***PENETRATION TESTING TERHADAP SISTEM MANAJEMEN  
DATA SUMBER TERBUKA CKAN MENGGUNAKAN  
METODE OWASP TOP 10***

**SKRIPSI**

**Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar  
Sarjana Komputer**

**HANNA NABILA CANTHY PELAWI**

**1810511022**

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN  
JAKARTA**

**FAKULTAS ILMU KOMPUTER  
PROGRAM STUDI INFORMATIKA**

**2022**

## PERNYATAAN ORSINALITAS

Tugas Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun yang dirujuk saya nyatakan dengan benar.

Nama : Hanna Nabila Canthy Pelawi

NIM : 1810511022

Tanggal : 3 Juni 2022

Bilamana dikemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 3 Juni 2022

Yang Menyatakan,



*Hanna Nabila Canthy Pelawi*

(Hanna Nabila Canthy Pelawi)

## PERNYATAAN PERSETUJUAN PUBLIKASI

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan dibawah ini:

Nama : Hanna Nabila Canthy Pelawi

NIM : 1810511022

Fakultas : Ilmu Komputer

Program Studi : S1-Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non-Exchange Royalty Free Right*) atas karya ilmiah saya yang berjudul:

*Penetration Testing Terhadap Sistem Manajemen Data Sumber Terbuka CKAN Menggunakan Metode OWASP Top 10*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti di Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formalitas, mengelola dalam bentuk pengkalan data (Basis Data), merawat dan mempublikasi Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta, Demikian Pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 3 Juni 2022

Yang Menyatakan,



(Hanna Nabila Canthy Pelawi)

# LEMBAR PENGESAHAN

Dengan ini menyatakan bahwa skripsi berikut:

Nama : Hanna Nabila Canthy Pelawi

NIM : 1810511022

Program Studi : S1 Informatika

Judul : *Penetration testing Terhadap Sistem Manajemen Data*

Sumber Terbuka Ckan Menggunakan Metode Owasp Top 10

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



**Henki Bavu Seta, S.Kom, MTL**

Penguji 1



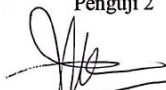
**Yuni Widiastiwi, S.Kom, M.Si**

Penguji 2



**Bayu Hananto S.Kom., M.Kom.**

Pembimbing 1



**I Wawan Widi P., S.Kom., MTL**

Pembimbing 2



**Dr. Ernatta, M.Kom.**

Dekan



**Desta Sandya Prasvita, S.Kom., M.Kom.**

Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal pengesahan : 5 Juli 2022



***PENETRATION TESTING TERHADAP SISTEM MANAJEMEN  
DATA SUMBER TERBUKA CKAN MENGGUNAKAN  
METODE OWASP TOP 10***

**HANNA NABILA CANTHY PELAWI**

**ABSTRAK**

Keamanan dalam mengakses dan menggunakan data menjadi hal yang penting ditengah perkembangan pengolahan informasi. Kebutuhan akan data yang semakin meningkat menjadi salah satu hal yang melatarbelakangi hadirnya berbagai platform *portal* data. *Portal* data dikembangkan untuk menyediakan layanan akses data secara terbuka untuk memenuhi kebutuhan akan data yang menunjang perkembangan teknologi. Sistem manajemen data seperti *CKAN* membutuhkan jaminan dari sisi keamanan, karena *CKAN* memberikan layanan akses data yang terbuka untuk berbagai pihak. *Penetration testing* menjadi salah satu upaya yang dapat dilakukan untuk menganalisis keamanan sistem, terdapat berbagai macam teknik dalam melakukan uji penetrasi. Salah satu metode yang banyak digunakan adalah *OWASP TOP 10*. *OWASP TOP 10* merupakan salah satu produk dari *OWASP* (Open Web Application Security Project) yang merupakan sebuah platform pengembangan keamanan aplikasi mulai dari metodologi, alat bantu, dokumentasi, dan lain-lain. *OWASP TOP 10* sendiri merupakan 10 kategori teratas celah/kerentanan keamanan suatu aplikasi. Penelitian ini bertujuan untuk melakukan uji penetrasi terhadap salah satu *website portal* data yang menggunakan *CKAN* untuk kemudian dianalisis hasilnya menggunakan metode *OWASP TOP 10* dengan berbagai alat bantu.

Kata Kunci : *CKAN, Penetration Testing, OWASP Top 10*

# ***PENETRATION TESTING OF CKAN OPEN SOURCE DATA MANAGEMENT SYSTEM USING OWASP TOP 10 METHOD***

**HANNA NABILA CANTHY PELAWI**

## **ABSTRACT**

Security in accessing and using data is *important* in the midst of the development of information processing. The increasing need for data is one of the things behind the presence of various data *portal* platforms. The data *portal* was developed to provide open data access services to meet the need for data that *supports* technological developments. Data management systems such as *CKAN* require guarantees in terms of security, because *CKAN* provides data access services that are open to various parties. *Penetration testing* is one of the efforts that can be done to analyze system security, there are various kinds of techniques in conducting penetration tests. One of the widely used methods is *OWASP TOP 10*. *OWASP TOP 10* is one of the products of *OWASP* (Open Web Application Security Project) which is an application security development platform ranging from methodologies, *tools*, documentation, and others. *OWASP TOP 10* itself is the *Top 10* categories of security gaps/vulnerabilities of an application. This study aims to conduct a penetration test on one of the data *portal websites* that uses *CKAN* to then analyze the results using the *OWASP TOP 10* method with various *tools*.

**Keyword:** *CKAN, Penetration Testing, OWASP Top 10*

## KATA PENGANTAR

Syukur alhamdulillah atas kehadiran Allah SWT karena berkat rahmat dan hidayah-Nya peneliti dapat menyelesaikan perkuliahan dan tugas akhir yang berjudul **“PENETRATION TESTING TERHADAP SISTEM MANAJEMEN DATA SUMBER TERBUKA CKAN MENGGUNAKAN METODE OWASP TOP 10”**. Shalawat beriring salam kepada junjungan alam Nabi Muhammad SAW yang menjadi panutan, pedoman, dan pemberi syafaat di akhirat kelak. Skripsi ini merupakan salah satu syarat kelulusan untuk menyelesaikan perkuliahan dan meraih gelar sarjana pada Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta. Berbagai macam bantuan, dukungan, saran, kritik, dan doa dari berbagai pihak sangat membantu peneliti dalam menyelesaikan skripsi ini. Izinkan peneliti dengan segala hormat dan kerendahan hati mengucapkan terima kasih kepada:

1. Bunda tercinta (Rini Djumiati Surbakti) dan Bapak tersayang (Herman Pelawi) yang selalu memberikan doa, dorongan, dan nasihat dalam tiap langkah hidup peneliti.
2. Corine Nur Fadhilah Pelawi, Azizah Ramadhan Pelawi, dan Kynan Ahmad Sembiring Pelawi yang merupakan adik peneliti yang setia memberi dukungan dan semangat kepada peneliti dalam menyelesaikan skripsi.
3. Vania Millenia Melinda sahabat sejiwa beserta Bintaro Family yang senantiasa menemani perjuangan peneliti dan saling memberi masukan, doa, dan dukungan.
4. Bapak Bayu Hananto S.Kom., M.Kom. dan Bapak I Wayan Widi S.Kom., MTI selaku dosen pembimbing skripsi yang senantiasa membimbing dan memberi masukan dan saran untuk menyelesaikan skripsi ini.
5. Ibu dan Bapak Dosen Informatika serta seluruh staff Fakultas Ilmu Komputer UPN Veteran Jakarta atas ilmu yang telah diberikan semasa kuliah.
6. Sahabat semasa perkuliahan, Anti Bambang Grup, Kelas A TI 2018, Kwetiau Goreng Basah yang telah mewarnai masa perkuliahan peneliti dengan canda tawa dan penuh sukacita.



7. Tya, Hasan, Drian, Shasa, Daniello, Mail, Fio, Fia, dan teman-teman peneliti yang tidak dapat disebutkan satu persatu.
8. Senior Informatika dan KSM Robotika yang telah menjadi keluarga di rantau dan memberi masukan dan pengalaman belajar yang menyenangkan selama perkuliahan.
9. Seluruh teman dan keluarga yang selalu ada hingga saat ini yang memberi semangat, dukungan, serta doa terbaik yang tidak bisa disebutkan satu persatu.

Jakarta, 29 Mei 2022



Hanna Nabila Canthy Pelawi

## DAFTAR ISI

PERNYATAAN ORSINALITAS .....	iii
PERNYATAAN PERSETUJUAN PUBLIKASI .....	iv
LEMBAR PENGESAHAN .....	v
ABSTRAK .....	vi
ABSTRACT .....	vii
KATA PENGANTAR .....	viii
DAFTAR ISI .....	x
DAFTAR GAMBAR .....	xiii
DAFTAR TABEL .....	xiv
DAFTAR SIMBOL .....	xv
BAB I PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Tujuan Penelitian .....	2
1.4 Batasan Masalah .....	3
1.5 Ruang Lingkup .....	3
1.6 Manfaat Penelitian .....	3
1.7 Sistematika Penulisan .....	4
BAB II TINJAUAN PUSTAKA .....	5
2.1 Open Data .....	5
2.2 CKAN .....	5
2.3 <i>Penetration testing</i> .....	7
2.4 <i>Open Web Application Security Project (OWASP)</i> .....	9
2.5 <i>OWASP Top 10</i> .....	9
2.5.1 <i>Broken Access Control</i> .....	9
2.5.2 <i>Cryptographic Failures</i> .....	10
2.5.3 <i>Injection</i> .....	10
2.5.4 <i>Insecure Design</i> .....	10
2.5.5 <i>Security Misconfiguration</i> .....	10
2.5.6 <i>Vulnerable and Outdated Components</i> .....	11
2.5.7 <i>Identification and Authentication Failures</i> .....	11

2.5.8	<i>Software and Data Integrity Failures</i>	11
2.5.10	<i>Server-Side Request Forgery</i>	12
2.6	<i>Discovery Tools</i>	12
2.7	<i>Attack Tools</i>	13
2.8	Penelitian Terkait	14
BAB III METODELOGI PENELITIAN		19
3.1	Alur Penelitian	19
3.2	Identifikasi Masalah	20
3.3	Pengumpulan Data	20
3.3.1	Studi Literatur	20
3.3.2	Observasi	20
3.4	Tahapan <i>Penetration testing</i>	21
3.4.1	<i>Planning</i>	21
3.4.2	Discovery	21
3.4.3	Attacking	21
3.4.4	<i>Reporting</i>	21
3.5	Analisis Hasil Pengujian	22
3.6	Alat dan Kebutuhan Penelitian	22
3.7	Jadwal Penelitian	22
BAB IV HASIL PENELITIAN		24
4.1	<i>Planning</i>	24
4.2	<i>Discovery</i>	24
4.2.1	<i>Whatweb</i>	24
4.2.2	<i>Whois</i>	26
4.2.3	<i>OWASP ZAP</i>	27
4.2.4	<i>Nmap</i>	28
4.3	<i>Attack</i>	28
4.3.1	<i>Broken Access Control</i>	28
4.3.2	<i>Cryptographic Failures</i>	29
4.3.3	<i>Insecure Design</i>	30
4.3.4	<i>Security Misconfiguration</i>	31
4.3.5	<i>Vulnerable and Outdated Components</i>	33
4.3.6	<i>Injection</i>	36
4.4	<i>Reporting</i>	42

BAB V PENUTUP.....	44
5.1    Simpulan.....	44
5.2    Saran.....	45
DAFTAR PUSTAKA .....	46
RIWAYAT HIDUP.....	48
LAMPIRAN.....	49

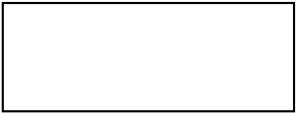
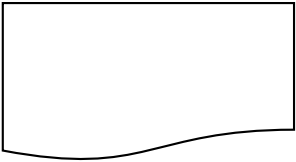


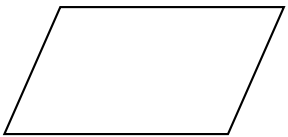
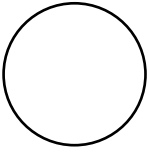
## DAFTAR GAMBAR

Gambar 2.1 Struktur Fungsional CKAN.....	6
Gambar 2.2 OWASP TOP 10 2021 .....	9
Gambar 3.1 Alur Penelitian.....	19
Gambar 4.5 Hasil <i>Whatweb</i> .....	25
Gambar 4.6 Hasil <i>Whatweb</i> Versi CKAN .....	25
Gambar 4.1 Hasil <i>Whois</i> .....	26
Gambar 4.2 Hasil <i>Whois 2</i> .....	26
Gambar 4.3 Hasil <i>Whois Personal Information</i> .....	26
Gambar 4.4 Hasil <i>Whois Personal Information 2</i> .....	27
Gambar 4.7 <i>Report Scanning OWASP Zap</i> .....	27
Gambar 4.8 Hasil <i>Nmap</i> .....	28
Gambar 4.9 Hasil <i>Dirb</i> Direktori Website Pemerintah ABC .....	29
Gambar 4.10 Hasil Broken Access Control .....	29
Gambar 4.11 Pengamanan <i>Password</i> .....	30
Gambar 4.16 <i>Injection Script Login Page</i> .....	33
Gambar 4.17 Hasil <i>Injection Script Login Page</i> .....	34
Gambar 4.18 Hasil <i>Injection Script Kolom Search</i> .....	34
Gambar 4.19 Proses <i>Xsser</i> .....	35
Gambar 4.20 Hasil <i>Xsser</i> pada Website Pemerintah ABC.....	35
Gambar 4.21 Hasil <i>SQLmap</i> pada Website Pemerintah ABC.....	36
Gambar 4.24 <i>Code Injection Website</i> dengan OWASP ZAP.....	38
Gambar 4.25 Hasil <i>Code Injection OWASP ZAP</i> .....	39
Gambar 4.26 Hasil <i>Logging and Monitoring Attack</i> .....	39
Gambar 4.28 Menu <i>Burpclickbandit</i> .....	40
Gambar 4.29 <i>Script Burpclickbandit</i> .....	41
Gambar 4.30 <i>Burpclickbandit Menu Bar</i> .....	41
Gambar 4.31 Hasil serangan <i>clickjacking</i> pada laman <i>login</i> .....	42

## DAFTAR TABEL

Tabel 3.1 Jadwal Penelitian.....	23
Tabel 4.2 Hasil Uji Penetrasi Terhadap <i>website</i> Target.....	42

## DAFTAR SIMBOL

Simbol	Nama Simbol	Keterangan
	Simbol Proses	Menggambarkan Proses
	Simbol Dokumen	Dokumen yang dibutuhkan dalam proses sistem
	Simbol arah data atau arus data	Sebagai petunjuk arah data dan arus data pada proses
	Simbol Terminator	Simbol untuk permulaan atau akhir dari suatu kegiatan
	Simbol Data	Simbol sebagai masukan atau keluaran data untuk suatu proses
	Simbol konektor	Simbol untuk sambungan pada halaman yang sama