REPUBLIK INDONESIA
KEMENTERIAN HUKUM

SURAT PENCATATAN CIPTAAN

Dalam rangka pelindungan ciptaan di bidang ilmu pengetahuan, seni dan sastra berdasarkan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, dengan ini menerangkan:

Nomor dan tanggal permohonan	:	EC00202505781, 14 Januari 2025
Pencipta		
Nama	:	**Ratna Ujiandari, Fauzi Alfadhillah dkk**
Alamat	:	Komplek Puri Kartika Blok F1 No. 17, RT004 RW008, Tajur,, Ciledug, Tangerang, Banten, 15152
Kewarganegaraan	:	Indonesia
Pemegang Hak Cipta		
Nama	:	**Direktorat Riset dan Pengabdian kepada Masyarakat Universitas Budi Luhur**
Alamat	:	Jl. Ciledug Raya, RT.10/RW.2, Petukangan Utara, Pesanggrahan, Jakarta Selatan, DKI Jakarta, 12260
Kewarganegaraan	:	Indonesia
Jenis Ciptaan	:	**Karya Tulis**
Judul Ciptaan	:	**Metode Evaluasi Keamanan Siber Portal Akademik Berbasis OWASP Dan Threat Modeling**
Tanggal dan tempat diumumkan untuk pertama kali di wilayah Indonesia atau di luar wilayah Indonesia	:	13 Januari 2025, di Jakarta Selatan
Jangka waktu pelindungan	:	Berlaku selama 50 (lima puluh) tahun sejak Ciptaan tersebut pertama kali dilakukan Pengumuman.
Nomor pencatatan	:	000845144

adalah benar berdasarkan keterangan yang diberikan oleh Pemohon.
Surat Pencatatan Hak Cipta atau produk Hak terkait ini sesuai dengan Pasal 72 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

a.n. MENTERI HUKUM
DIREKTUR JENDERAL KEKAYAAN INTELEKTUAL
u.b
Direktur Hak Cipta dan Desain Industri

Agung Damarsasongko,SH.,MH.
NIP. 196912261994031001

Disclaimer:
Dalam hal pemohon memberikan keterangan tidak sesuai dengan surat pernyataan, Menteri berwenang untuk mencabut surat pencatatan permohonan.

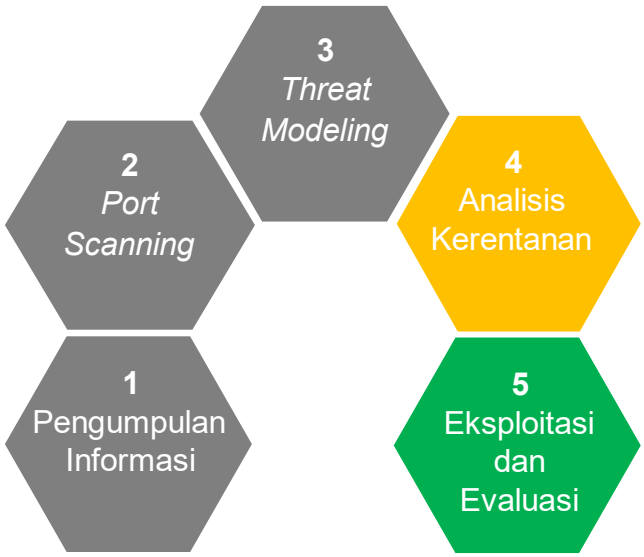
LAMPIRAN PENCIPTA

No	Nama	Alamat
1	Ratna Ujiandari	Komplek Puri Kartika Blok F1 No. 17, RT004 RW008, Tajur,, Ciledug, Tangerang
2	Fauzi Alfadhillah	Jl. Palem V No. 24, RT003 RW008, Petukangan Utara,, Pesanggrahan, Jakarta Selatan
3	Teja Endra Eng Tju	Alam Sutera Buana III No. 12 A, RT001 RW009, Pakulonan, Serpong Utara, Tangerang Selatan

Metode Evaluasi Keamanan Siber Portal Akademik
Berbasis OWASP dan *Threat Modeling*

Ciptaan ini merupakan metode komprehensif untuk mengidentifikasi dan mengevaluasi potensi kerentanan keamanan pada portal akademik mahasiswa. Portal ini merupakan sistem utama yang digunakan mahasiswa untuk mengakses layanan akademik, seperti pendaftaran mata kuliah, pengelolaan data pribadi, dan melihat hasil studi. Menggunakan kerangka OWASP (*Open Web Application Security Project*), metode ini dirancang untuk menjawab kebutuhan mendesak akan perlindungan data sensitif di sektor pendidikan. Ciptaan ini juga mengintegrasikan pendekatan berbasis *threat modeling*, yang memberikan penilaian strategis dan teknis mengenai kerentanan yang ditemukan. Tahapan metode dirancang untuk menghasilkan rekomendasi langkah mitigasi yang spesifik dan efektif untuk diterapkan. Dengan tingginya urgensi keamanan siber dalam sektor pendidikan, metode ini hadir untuk memastikan kerahasiaan, integritas, dan ketersediaan data dalam menghadapi ancaman siber yang semakin kompleks.

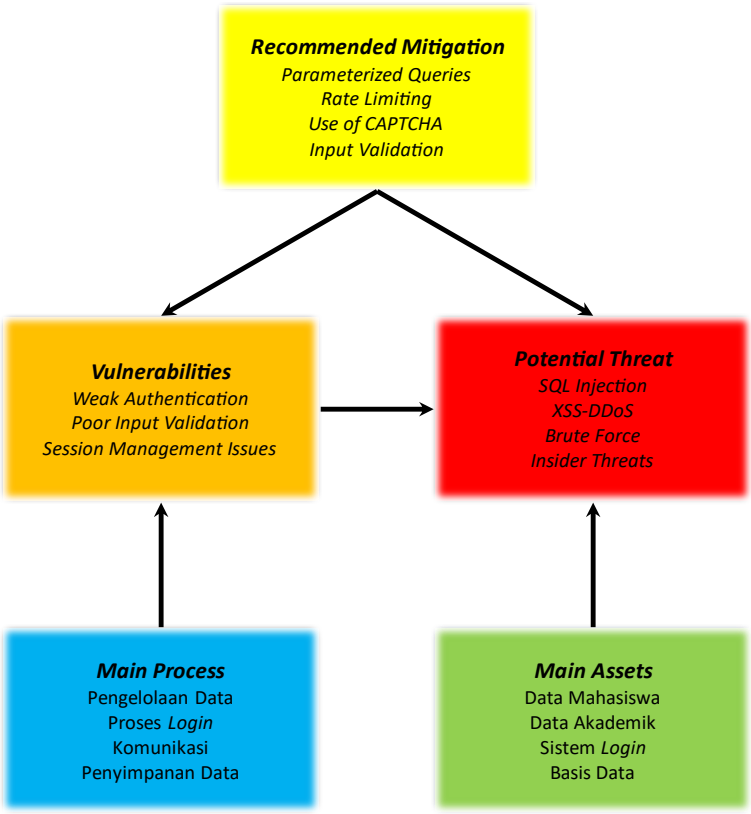
Metode ini sangat relevan dalam meningkatkan keamanan portal akademik, khususnya di era digital saat ancaman siber semakin berkembang. Keunggulannya meliputi penggunaan *tools open-source* yang terus diperbarui, integrasi analisis mendalam berbasis simulasi serangan nyata, serta fokus pada sektor pendidikan. Ciptaan memberikan langkah-langkah sistematis seperti ditunjukkan pada Gambar 1.



Gambar 1. Adaptasi Tahapan OWASP.

Langkah-langkah sistematis ciptaan:

1. **Pengumpulan Informasi**:
    - Menggunakan *tools* seperti WhoIs untuk mengidentifikasi detail domain dan IP server portal akademik. Proses ini bertujuan untuk memahami lingkungan teknis target dan mempersiapkan strategi pengujian lanjutan.
    - Hasilnya berupa data domain, pendaftaran awal, server yang digunakan, dan informasi terkait pihak ketiga yang mengelola sistem.
2. ***Port Scanning***:
    - Menggunakan perangkat lunak Nmap untuk mendeteksi *port* yang terbuka pada *server* portal. Analisis ini mengidentifikasi layanan aktif, seperti FTP, HTTP, HTTPS, MySQL, dan SSH, yang berpotensi menjadi pintu masuk ancaman.
    - Hasil *port scanning* ini divisualisasikan dalam tabel serta mendukung analisis lanjutan.
3. ***Threat Modeling***:
    - Membantu mengidentifikasi, memahami, dan mengevaluasi potensi ancaman terhadap portal. Metode ini memetakan aset-aset penting yang harus dilindungi, ancaman potensial, dan langkah mitigasi yang tepat.
    - Diagram *threat modeling* memberikan gambaran visual potensi ancaman dan kerentanan portal (ditampilkan dalam Gambar 2).
4. **Analisis Kerentanan**:
    - Menggunakan OWASP ZAP untuk memindai sistem terhadap kerentanan keamanan seperti SQL *Injection*, *Cross-Site Scripting* (XSS), dan konfigurasi yang tidak aman.
    - Hasil analisis ini diperkuat dengan pengujian eksploitasi manual untuk memverifikasi kerentanan yang terdeteksi.
5. **Eksploitasi dan Evaluasi**:
    - Dilakukan dengan menggunakan Metasploit *Framework* untuk mensimulasikan serangan nyata pada sistem yang diuji. Simulasi ini membantu memahami dampak kerentanan dan memberikan rekomendasi mitigasi yang relevan.
    - Evaluasi pasca-eksploitasi memastikan efektivitas perbaikan yang telah diterapkan dan mencegah munculnya celah baru.



Gambar 2. Diagram *Threat Modeling* Portal Akademik Mahasiswa.

Keunggulan dan Kebaruan Ciptaan:

1. **Fokus pada Sektor Pendidikan**:
   - Portal akademik sering menjadi target serangan siber karena menyimpan data sensitif. Ciptaan ini dirancang khusus untuk menjawab kebutuhan keamanan di sektor pendidikan yang sering kali terabaikan.
2. **Pendekatan Berbasis Metode Mutakhir**:
   - Mengintegrasikan metode OWASP yang terus diperbarui dengan teknologi modern seperti OWASP ZAP dan Metasploit Framework untuk memberikan hasil analisis yang akurat dan relevan.
3. **Diagram Visual untuk Pemahaman Mendalam**:
   - Ciptaan mencakup diagram seperti Gambar 2 (Tahapan OWASP) dan Gambar 5 (Threat Modeling) yang membantu menggambarkan langkah-langkah evaluasi keamanan.

4. **Pendekatan Holistik**:
    - Tidak hanya mengidentifikasi kerentanan, tetapi juga menyediakan langkah mitigasi berbasis hasil eksploitasi untuk memastikan keamanan sistem secara menyeluruh.
5. **Dukungan Keberlanjutan**:
    - Rekomendasi hasil penelitian dapat diterapkan secara praktis untuk meningkatkan keamanan portal, dengan potensi adaptasi di institusi pendidikan lainnya.

Ciptaan ini diharapkan menjadi referensi utama dalam pengembangan strategi keamanan siber portal akademik, berpotensi memberikan kontribusi penting dalam literatur keamanan siber di sektor pendidikan, selain memberikan solusi praktis untuk institusi yang menghadapi tantangan serupa. Dengan implementasi metode ini, ancaman siber seperti phishing, malware, dan serangan lainnya dapat diminimalkan, sehingga meningkatkan kepercayaan pengguna dan menjaga kerahasiaan data sensitif mahasiswa.