

**IMPLEMENTASI PENILAIAN KERENTANAN DAN  
PENGUJIAN PENETRASI BERBASIS PTES PLATFORM  
EDUTECH SKILL UPKIDS UNTUK MENGIDENTIFIKASI  
KERENTANAN KEAMANAN APLIKASI WEB**

**SKRIPSI**

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



disusun oleh

**RENDY ADITIYA PUTRA KURNIAWAN**

**22.83.0890**

Kepada

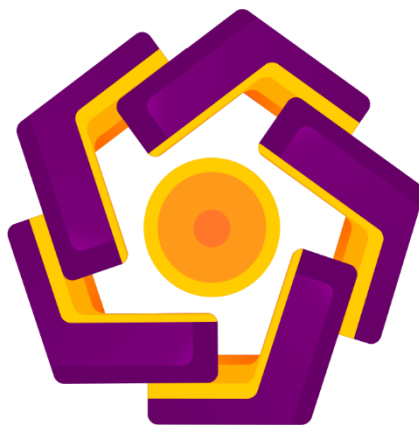
**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2026**

**IMPLEMENTASI PENILAIAN KERENTANAN DAN  
PENGUJIAN PENETRASI BERBASIS PTES UNTUK  
MENGIDENTIFIKASI KERENTANAN KEAMANAN PADA  
SITUS WEB**

**SKRIPSI**

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



disusun oleh

**RENDY ADITIYA PUTRA KURNIAWAN**

**22.83.0890**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2026**

**HALAMAN PERSETUJUAN  
SKRIPSI**

**IMPLEMENTASI PENILAIAN KERENTANAN DAN  
PENGUJIAN PENETRASI BERBASIS PTES PLATFORM  
EDUTECH SKILL UPKIDS UNTUK MENGIDENTIFIKASI  
KERENTANAN KEAMANAN APLIKASI WEB**

yang disusun dan diajukan oleh

**Rendy Aditya Putra Kurniawan**

**22.83.0890**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 22 Januari 2026

**Dosen Pembimbing,**



**Senie Destya, ST., M.Kom.**

**190302312**

HALAMAN PENGESAHAN  
SKRIPSI

IMPLEMENTASI PENILAIAN KERENTANAN DAN PENGUJIAN  
PENETRASI BERBASIS PTES PLATFORM EDUTECH SKILL UPKIDS  
UNTUK MENGIDENTIFIKASI KERENTANAN KEAMANAN APLIKASI  
WEB

yang disusun dan diajukan oleh

**Rendy Aditiya Putra Kurniawan**

22.83.0890

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 20 Februari 2026

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

Andika Agus Slameto, S.Kom., M.Kom.  
NIK. 190302109

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

Senie Destya, S.T., M.Kom.  
NIK. 190302312



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 20 Februari 2026

**DEKAN FAKULTAS ILMU KOMPUTER**



Prof. Dr. Kusriani, M.Kom.  
NIK. 190302106

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Rendy Aditya Putra Kurniawan  
NIM : 22.83.0890

Menyatakan bahwa Skripsi dengan judul berikut:

### **IMPLEMENTASI PENILAIAN KERENTANAN DAN PENGUJIAN PENETRASI BERBASIS PTES PLATFORM EDUTECH SKILL UPKIDS UNTUK MENGIDENTIFIKASI KERENTANAN KEAMANAN APLIKASI WEB**

Dosen Pembimbing : Senie Destya, ST., 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, 20 Februari 2026

Yang Menyatakan,



Rendy Aditya Putra K

## HALAMAN PERSEMBAHAN

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa karena atas rahmat dan karunia-Nya, penulis dapat menyelesaikan skripsi yang berjudul “Implementation of PTES-Based Vulnerability Assessment and Penetration Testing to Identify Security Vulnerabilities on Websites” dengan baik. Skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan program pendidikan Strata Satu (S1).

Dalam proses penyusunan skripsi ini, penulis menyadari bahwa keberhasilan penyelesaian penelitian tidak terlepas dari bantuan, dukungan, serta bimbingan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Ibu Senie Destya, ST., M.Kom. selaku Dosen Pembimbing, yang telah meluangkan waktu, memberikan bimbingan, arahan, serta motivasi kepada penulis dengan penuh kesabaran selama proses penyusunan skripsi ini.
2. Bapak/Ibu Tim Dosen Penguji, yang telah memberikan kritik, saran, dan masukan yang membangun demi penyempurnaan skripsi ini.
3. Pihak PT Anak Hebat Nusantara, khususnya pengelola platform Skill Upkids, yang telah memberikan izin dan dukungan sehingga penelitian ini dapat dilaksanakan dengan baik.
4. Kedua orang tua penulis yang senantiasa memberikan doa, dukungan moral, serta motivasi tanpa henti selama penulis menempuh pendidikan hingga penyelesaian skripsi ini.
5. Angel Jeannette Gretha Saputra, yang telah memberikan dukungan, perhatian, dan semangat kepada penulis selama proses penyusunan skripsi ini.
6. Seluruh pihak yang tidak dapat disebutkan satu per satu yang telah membantu penulis dalam menyelesaikan skripsi ini.

Penulis menyadari bahwa skripsi ini masih memiliki keterbatasan dan kekurangan. Oleh karena itu, penulis mengharapkan kritik dan saran yang bersifat membangun guna penyempurnaan di masa mendatang. Semoga skripsi ini dapat memberikan manfaat dan kontribusi bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan informasi dan pengujian keamanan aplikasi web.

## KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga skripsi yang berjudul **“Implementasi Penilaian Kerentanan Dan Pengujian Penetrasi Berbasis Ptes Platform Edutech Skill Upkids Untuk Mengidentifikasi Kerentanan Keamanan Aplikasi Web”** dapat diselesaikan dengan baik sebagai salah satu syarat memperoleh gelar Sarjana Komputer pada Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta.

Penulis menyampaikan terima kasih kepada Ibu **Senie Destya, S.T., M.Kom.** selaku Dosen Pembimbing atas bimbingan dan arahnya, kepada seluruh dosen serta pihak terkait yang telah mendukung proses penyusunan skripsi ini, serta kepada kedua orang tua dan Angel Jeannette Gretha Saputra atas doa dan dukungan yang diberikan.

Penulis menyadari bahwa skripsi ini masih memiliki keterbatasan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi penyempurnaan di masa mendatang.

Yogyakarta, 20 Februari 2026

Penulis

Rendy Aditiya Putra K

## DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI .....	iii
HALAMAN PERSEMBAHAN .....	v
KATA PENGANTAR .....	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR .....	x
DAFTAR SINGKATAN .....	xi
INTISARI.....	xiii
<i>ABSTRACT</i> .....	xv
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian .....	3
1.5 Manfaat Penelitian .....	4
1.6 Sistematika Penulisan .....	4
BAB II TINJAUAN PUSTAKA.....	6
2.1 Studi Literatur .....	6
2.2 Dasar Teori.....	11
2.3 Keamanan Informasi (CIA Triad).....	11
2.4 Pengujian Penetrasi (Penetration Testing) .....	12
2.5 Metode BlackBox.....	13
2.6 Information Gathering.....	15
2.8 Vulnerability Scanning.....	17
2.9 Exploitation.....	18
2.10 Post-Exploitation.....	19

2.11 Reporting.....	20
2.12 Analisis.....	20
2.13 Perangkat Lunak Pemindai Kerentanan (Acunetix & Burp Suite) .....	21
2.14 CVSS (Sistem Penelitian Kerentanan).....	23
2.15 Penetration Testing Execution Standard (PTES) .....	24
<b>BAB III METODE PENELITIAN.....</b>	<b>26</b>
3.1 Objek Penelitian .....	27
3.2 Alur Penelitian .....	29
3.3 Alat dan Bahan .....	34
3.4 Alat Penelitian.....	35
3.5 Bahan Penelitian.....	36
3.6 Perencanaan Pengujian.....	37
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>	<b>39</b>
4.1 Tahap Pengujian.....	39
4.2 Information Gathering.....	42
4.3 Threat Modelling.....	48
4.4 Vulnerability Analysis .....	53
4.5 Exploitation .....	58
4.6 Post-Exploitation.....	65
4.7 Reporting.....	66
<b>BAB V PENUTUP.....</b>	<b>71</b>
5.1 Kesimpulan .....	71
5.2 Saran.....	73
<b>REFERENSI .....</b>	<b>75</b>
<b>LAMPIRAN.....</b>	<b>77</b>

## DAFTAR TABEL

Tabel 2. 1 Keaslian Penelitian	8
Tabel 3. 1 Spesifikasi Alat dan Bahan	34
Tabel 4. 1 Hasil Information Gathering	47
Tabel 4. 2 Threat Modelling	52
Tabel 4. 3 Vulmerability Analysis	56
Tabel 4. 4 Berhasil Exploitation	64
Tabel 4. 5 Hasil Reporting dan Rekomendasi Mitigasi	68



## DAFTAR GAMBAR

Gambar 1. 1 Proses Pentesting	2
Gambar 3. 1 Alur Penelitian	30
Gambar 4. 1 Informasi WHOIS Domain skillupkids.id	43
Gambar 4. 2 Arsitektur Infranstruktur Aplikasi Web Skill Upkids	44
Gambar 4. 3 Hasil Pemindaian Port IP Cloudflare Domain Skillupkids.id	45
Gambar 4. 4 Hasil Pemindaian Port IP Origin Domain skillupkids.id	46
Gambar 4. 5 Hasil Identifikasi Teknologi Web dengan Wappalyzer	47
Gambar 4. 6 Halaman Login Member Tanpa Proteksi CAPTCHA	51
Gambar 4. 7 Hasil Pemindaian Vulnerability Menggunakan Acunetix	54
Gambar 4. 8 Daftar Kerentanan yang Teridentifikasi oleh Acunetix	55
Gambar 4. 9 Bukti Berhasil Exploitation Session Hijacking	60
Gambar 4. 10 Halaman Lupa Password	61
Gambar 4. 11 Perubahan Kata Sandi Tanpa Verifikasi Identitas (OTP)	62
Gambar 4. 12 Verifikasi Login Menggunakan Kata Sandi Baru Hasil	63
Gambar 4. 13 Tampilan atau Pengguna Setelah Berhasil Login	64



## DAFTAR SINGKATAN

### **CIA Triad**

Confidentiality, Integrity, dan Availability, yaitu tiga prinsip dasar dalam keamanan informasi yang digunakan untuk menilai tingkat perlindungan data dan sistem.

### **CSRF (Cross-Site Request Forgery)**

Jenis serangan pada aplikasi web yang memanfaatkan kepercayaan pengguna untuk menjalankan permintaan tidak sah tanpa sepengetahuan pengguna.

### **CVSS (Common Vulnerability Scoring System)**

Standar penilaian tingkat keparahan kerentanan keamanan sistem berdasarkan skor numerik.

### **Edutech (Education Technology)**

Pemanfaatan teknologi informasi dan komunikasi untuk mendukung proses pembelajaran dan pendidikan.

### **GCP (Google Cloud Platform)**

Layanan komputasi awan yang digunakan sebagai infrastruktur hosting aplikasi web.

### **HTTP (Hypertext Transfer Protocol)**

Protokol komunikasi jaringan yang digunakan untuk pertukaran data pada aplikasi web tanpa enkripsi.

### **HTTPS (Hypertext Transfer Protocol Secure)**

Versi aman dari HTTP yang menggunakan enkripsi untuk melindungi data yang dikirimkan.

### **IP Address (Internet Protocol Address)**

Alamat unik yang digunakan untuk mengidentifikasi perangkat dalam jaringan komputer.

### **Nmap (Network Mapper)**

Perangkat lunak pemindaian jaringan yang digunakan untuk mendeteksi port terbuka dan layanan aktif.

**OpenVAS (Open Vulnerability Assessment System)**

Alat pemindaian kerentanan yang digunakan untuk mengidentifikasi kelemahan keamanan pada sistem dan jaringan.

**PoC (Proof of Concept)**

Bukti teknis yang menunjukkan bahwa suatu kerentanan dapat dieksploitasi.

**PTES (Penetration Testing Execution Standard)**

Standar internasional yang digunakan sebagai metodologi dalam pelaksanaan penetration testing.

**VA/PT (Vulnerability Assessment and Penetration Testing)**

Metode pengujian keamanan sistem yang bertujuan untuk mengidentifikasi dan mengevaluasi kerentanan serta dampaknya.

**WAF (Web Application Firewall)**

Sistem keamanan yang berfungsi untuk melindungi aplikasi web dari serangan berbasis HTTP/HTTPS.

**WHOIS**

Layanan pencarian informasi kepemilikan dan administrasi domain internet.

**XSS (Cross-Site Scripting)**

Jenis kerentanan aplikasi web yang memungkinkan penyerang menyisipkan skrip berbahaya ke dalam halaman web

## INTISARI

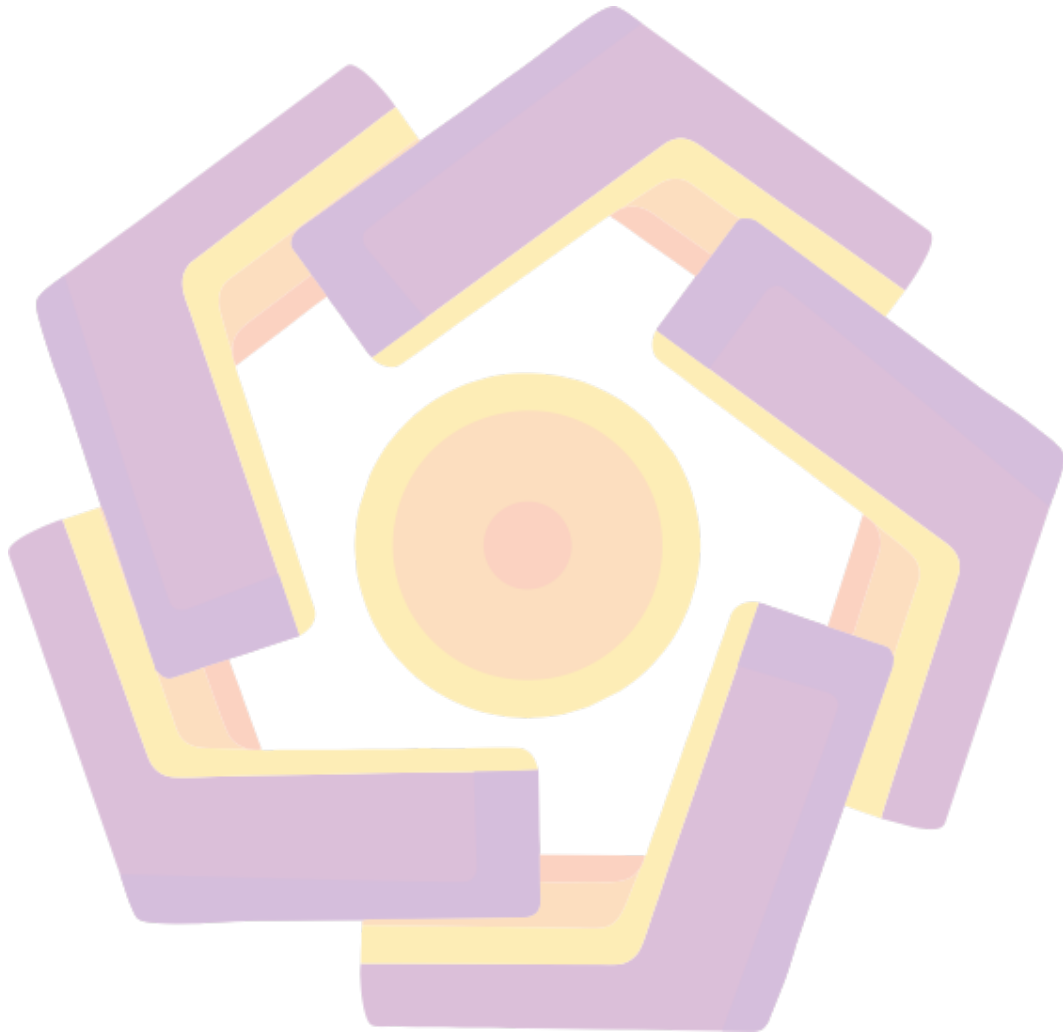
Perkembangan platform teknologi pendidikan berbasis web di Indonesia mengalami peningkatan signifikan seiring dengan transformasi digital di sektor pendidikan. Namun, peningkatan ini juga diiringi dengan risiko keamanan siber, khususnya pada platform yang mengelola data pribadi anak-anak sebagai kelompok pengguna rentan. Platform Skill Upkids milik PT ANAK HEBAT NUSANTARA merupakan salah satu aplikasi edutech yang menyimpan dan memproses data sensitif pengguna. Ketiadaan audit keamanan sistem yang terstandarisasi berpotensi menimbulkan kerentanan keamanan yang dapat berdampak pada kebocoran data, pengambilalihan akun, serta gangguan terhadap kerahasiaan dan integritas sistem.

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan keamanan pada aplikasi web Skill Upkids dengan menerapkan metode Vulnerability Assessment dan Penetration Testing (VA/PT) berbasis Penetration Testing Execution Standard (PTES). Metode penelitian dilakukan menggunakan pendekatan Blackbox testing melalui tujuh tahapan PTES, yaitu pre-engagement interactions, intelligence gathering, threat modelling, vulnerability analysis, exploitation, post-exploitation, dan reporting. Proses pengujian didukung oleh penggunaan alat bantu seperti OpenVAS, Burp Suite, Nmap, WHOIS, dan Wappalyzer, serta pengujian manual untuk memvalidasi temuan teknis.

Hasil penelitian menunjukkan adanya 5 kerentanan kritis, yaitu session hijacking akibat manajemen sesi yang lemah, mekanisme reset kata sandi tanpa verifikasi identitas, ketiadaan token CSRF pada formulir input, cookie sesi tanpa atribut keamanan, serta terbukanya port backend yang menggunakan protokol HTTP tanpa enkripsi. Temuan ini menunjukkan bahwa sistem belum menerapkan kontrol keamanan dasar secara optimal. Penelitian ini diharapkan dapat dimanfaatkan oleh pengembang aplikasi edutech, tim keamanan siber, serta institusi pendidikan sebagai acuan dalam meningkatkan keamanan aplikasi web dan melindungi data pengguna anak-anak. Penelitian lanjutan disarankan untuk

mencakup pengujian keamanan berkelanjutan dan evaluasi kebijakan keamanan sistem.

**Kata kunci:** Keamanan Siber, Standar Eksekusi Pengujian Penetrasi, Penilaian Kerentanan, Pengujian Penetrasi, Aplikasi Web.



## **ABSTRACT**

*The rapid growth of web-based educational technology platforms in Indonesia has been accompanied by increasing cybersecurity risks, particularly for systems that manage children's personal data as a vulnerable user group. Skill Upkids, an edutech platform developed by PT ANAK HEBAT NUSANTARA, processes and stores sensitive user information that requires strong security protection. The absence of standardized security audits may lead to undetected vulnerabilities, potentially resulting in data breaches, account takeover, and violations of confidentiality and system integrity.*

*This study aims to identify and analyze security vulnerabilities in the Skill Upkids web application by implementing Vulnerability Assessment and Penetration Testing (VA/PT) based on the Penetration Testing Execution Standard (PTES). The research adopts a black box testing approach and follows the seven PTES phases: pre-engagement interactions, intelligence gathering, threat modelling, vulnerability analysis, exploitation, post-exploitation, and reporting. The testing process is supported by automated and manual security tools, including OpenVAS, Burp Suite, Nmap, WHOIS, and Wappalizer, to ensure comprehensive vulnerability identification and validation.*

*The results reveal several critical security issues, including session hijacking caused by weak session management, password reset mechanisms without identity verification, the absence of Cross-Site Request Forgery (CSRF) tokens in input forms, insecure session cookies lacking security attributes, and exposed backend ports using unencrypted HTTP protocols. These findings indicate insufficient implementation of fundamental web security controls. This research contributes practical guidance for edutech developers, cybersecurity practitioners, and educational institutions to strengthen web application security and protect children's personal data. Future research is recommended to focus on continuous security testing and the evaluation of long-term security policies.*

**Keywords:** *Cyber Security, Penetration Testing Execution Standard, Vulnerability Assessment, Penetration Testing, Web Application.*