SENTIMETER (Seminar Nasional Teknologi Informasi, Mekatronika dan Ilmu Komputer) Universitas Nusa Putra, 17 Mei 2025

Menilai Keamanan Aplikasi Web Melalui Pengujian Penetrasi: Pendekatan Studi Kasus

Dah Berrou[1)], Salsa Rizkia Sabila[2)], Muhammad Haidar Matin[3)], Mohammad Fajril Ramdhani[4)], Somantri[5)]
[1, 2),3)4)] Teknik Informatika Universitas Nusa Putra
Jl. Raya Cibolang No.21 Cisaat Sukabumi 43152 Indonesia
e-mail: :dah.berrou_ti22@nusaputra.ac.id[1)], salsa.rizkia_ti22@nusaputra.ac.id[2)], muhammad.haidar_ti22@nusaputra.ac.id[3)]
fajril.ramadhani_ti22@nusaputra.ac.id[4)], somatri@nusaputra.ac.id[5)]

* Korespondensi: e-mail: ……..

ABSTRAK

Keamanan aplikasi web telah menjadi perhatian utama karena aplikasi tersebut semakin terintegrasi ke dalam operasi perusahaan kontemporer. Meningkatnya serangan siber yang menargetkan aplikasi ini mengungkap kelemahan serius, yang sering kali disebabkan oleh pengaturan yang salah dan pengodean yang buruk. Masalah mendesak dari langkah-langkah keamanan yang tidak memadai yang membuat perusahaan rentan terhadap pelanggaran dibahas dalam studi ini. Untuk menemukan kerentanan umum seperti injeksi SQL, skrip lintas situs (XSS), dan metode autentikasi yang lemah, kami melakukan pengujian penetrasi pada sejumlah aplikasi web operasional. Untuk memperoleh pemahaman menyeluruh tentang kelemahan keamanan, kami mereplikasi skenario serangan aktual menggunakan alat otomatis seperti Burp Suite dan metode pengujian manual. Pengujian kami mengungkap pola yang mengkhawatirkan: frekuensi kerentanan yang tinggi di semua aplikasi yang kami lihat. Banyak bisnis meremehkan bahaya yang ditimbulkan oleh celah keamanan ini, yang dapat mengakibatkan pelanggaran data yang serius, kerugian moneter, dan kerusakan reputasi. Hasil kami menunjukkan bahwa perusahaan sangat perlu meningkatkan prosedur dan proses keamanan mereka.

Pentingnya pengujian penetrasi rutin sebagai prosedur mendasar untuk menjaga keamanan aplikasi web yang kuat merupakan salah satu kesimpulan utama yang diambil dari penelitian kami. Organisasi dapat mendeteksi kerentanan sebelum pelaku jahat memanfaatkannya dengan melakukan evaluasi yang komprehensif dan berkala. Studi kami juga memberikan saran praktis untuk meningkatkan langkah-langkah keamanan, seperti menggunakan teknik pengkodean aman yang mengutamakan keamanan selama tahap pengembangan. Lebih jauh, kami menekankan pentingnya melakukan penilaian kerentanan secara berkala untuk menjamin bahwa aplikasi selalu diawasi terhadap bahaya yang muncul. Menggunakan teknik autentikasi yang kuat, seperti autentikasi multi-faktor, juga penting untuk menjaga kepercayaan pengguna dan mengamankan data sensitif. Pada akhirnya, studi kami menekankan betapa pentingnya bagi bisnis untuk secara proaktif memperbaiki kerentanan keamanan. Bisnis dapat memperkuat pertahanan mereka terhadap serangkaian ancaman siber yang terus berubah dengan mengutamakan keamanan aplikasi web melalui pengujian yang sering dan menggunakan praktik terbaik

***Kata Kunci**: Aplikasi web, Keamanan Siber, Pengujian Penetrasi, Kerentanan, Injeksi SQL*

ABSTRACT

Web applications' security has become a major concern as they become more and more integrated into contemporary company operations. The increase in cyberattacks that target these applications exposes serious flaws, which are frequently caused by incorrect setups and bad coding. The urgent problem of insufficient security measures that expose firms to breaches is examined in this study. In order to find common vulnerabilities like SQL injection, cross-site scripting (XSS), and weak authentication methods, we conducted penetration testing on a number of operational web apps. To obtain a thorough grasp of security flaws, we replicated actual attack scenarios using both automated tools such as Burp Suite and manual testing methods. Our testing revealed a concerning pattern: a high frequency of vulnerabilities in all of the apps we looked at. Many businesses undervalue the dangers posed by these security holes, which can result in serious data breaches, monetary losses, and reputational harm. Our results show that companies urgently need to improve their security procedures and processes.

The significance of routine penetration testing as a fundamental procedure for preserving strong web application security is among the main conclusions drawn from our research. Organizations can detect vulnerabilities before malevolent actors take advantage of them by carrying out comprehensive and regular evaluations. Our study also provides practical suggestions for enhancing security measures, like using secure coding techniques that give security top priority during the development stage. Furthermore, we stress the importance of conducting frequent

vulnerability assessments to guarantee that apps are always watched for emerging dangers. Using robust authentication techniques, like multi- factor authentication, is also essential for preserving user confidence and securing sensitive data. In the end, our study emphasizes how important it is for businesses to proactively fix security vulnerabilities. Businesses may strengthen their defenses against the constantly changing array of cyberthreats by putting web application security first through frequent testing and using best practicesse. The research includes ***real-world case studies*** *such as the* ***inDrive business logic vulnerability*** *and a* ***university web application penetration test****.*

Keywords: *Web applications, Cybersecurity, Penetration testing, Vulnerabilities, SQL injection.*

I. PENDAHULUAN

A. Latar Belakang

Transformasi digital dalam dunia bisnis telah mendorong peningkatan signifikan dalam penggunaan aplikasi web untuk mendukung operasional, mengelola data sensitif, dan berinteraksi dengan pelanggan. Namun, perubahan ini juga menjadikan aplikasi web sebagai target utama para penjahat siber. Meningkatnya frekuensi serangan siber terhadap aplikasi web menjadi ancaman serius bagi banyak organisasi, terutama karena masih banyak yang belum menerapkan langkah-langkah keamanan yang memadai.

Kerentanan seperti SQL injection**,** cross-site scripting (XSS**)**, dan mekanisme otentikasi yang lemah sering kali dimanfaatkan oleh penyerang untuk mendapatkan akses tanpa izin ke sistem dan data sensitif (OWASP, 2021). Karena sifatnya yang saling terhubung, aplikasi web sangat rentan terhadap berbagai jenis serangan yang bisa mengancam integritas data maupun privasi pengguna.

Menurut laporan dari Ponemon Institute (2022), sebanyak 65% organisasi mengalami setidaknya satu pelanggaran keamanan dalam setahun terakhir, sebagian besar disebabkan oleh lemahnya protokol keamanan. Pengujian penetrasi (penetration testing) menjadi salah satu metode yang banyak digunakan untuk mengidentifikasi dan mengatasi celah keamanan, sehingga organisasi bisa memperbaiki kelemahan tersebut sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Studi ini bertujuan untuk mengkaji berbagai kerentanan pada aplikasi web aktif melalui metode penetration testing, serta memberikan rekomendasi untuk memperkuat langkah-langkah keamanan yang ada.

B. Rumusan Masalah

Meskipun aplikasi web semakin penting dalam operasional bisnis, masih banyak organisasi yang mengabaikan praktik keamanan yang seharusnya diterapkan. Hal ini membuat sistem mereka rentan terhadap berbagai serangan. Penelitian ini mengidentifikasi sejumlah kerentanan kritis yang sering ditemukan pada aplikasi web, seperti SQL injection**,** cross-site scripting (XSS), **dan** mekanisme autentikasi yang tidak aman**.**

Melalui pengujian penetrasi pada aplikasi web yang aktif, penelitian ini menilai sejauh mana langkah-langkah keamanan yang sudah ada berjalan efektif, serta memberikan saran perbaikan untuk meningkatkan perlindungan terhadap ancaman siber. Masalah utama yang dibahas dalam penelitian ini adalah kurangnya sistem keamanan yang kuat pada aplikasi web, yang dapat menyebabkan kebocoran data, kerugian finansial, hingga merusak reputasi organisasi.

Pengujian penetrasi secara rutin sangat penting untuk mengidentifikasi celah keamanan dan memperkuat protokol perlindungan data.

Penelitian ini mencoba menjawab beberapa pertanyaan berikut:

1. Apa saja kerentanan umum yang sering ditemukan pada aplikasi web, dan bagaimana cara mengatasinya?
2. Seberapa efektifkah pengujian penetrasi dalam menemukan kelemahan keamanan pada aplikasi web?
3. Apa saja praktik terbaik untuk meningkatkan keamanan aplikasi web, terutama terkait kerentanan seperti SQL injection, XSS, dan autentikasi yang lemah?
4. Bagaimana cara organisasi menerapkan pengujian penetrasi secara rutin sebagai bagian dari strategi keamanan mereka agar bisa mencegah pelanggaran di masa depan?

C. Tujuan Penelitian

Berdasarkan rumusan masalah di atas, tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1) Umum

Melakukan simulasi peretasan pada sebuah sistem, dalam hal ini aplikasi web, dengan tujuan untuk mengidentifikasi kelemahan atau celah keamanan yang mungkin ada sebelum dimanfaatkan oleh peretas jahat. Ibaratnya seperti menguji kekuatan sebuah benteng sebelum diserang musuh. Dengan mengetahui titik lemahnya, kita bisa memperkuat sistem sebelum benar-benar diserang.

2) Khusus

a. Menganalisis kerentanan keamanan umum pada aplikasi web berdasarkan metode pengujian penetrasi yang telah ditetapkan.
b. Melakukan pengujian penetrasi pada aplikasi web tertentu sebagai studi kasus untuk menemukan potensi kelemahan sistem.
c. Menilai dampak dan tingkat keparahan dari kerentanan yang ditemukan terhadap keamanan aplikasi web.
d. Memberikan strategi mitigasi dan praktik terbaik untuk meningkatkan sistem keamanan aplikasi web.
e. Mengevaluasi seberapa efektif pengujian penetrasi sebagai metode untuk mengukur dan meningkatkan keamanan aplikasi web.

D. Manfaat Penelitian

Manfaat dari penelitian ini dibagi menjadi dua, yaitu manfaat teoritis dan manfaat praktis:

1) Manfaat Teoritis

a. Memberikan kontribusi pada pengembangan pengetahuan di bidang keamanan aplikasi web dengan menyajikan wawasan terkait kerentanan dan cara mengatasinya.
b. Meningkatkan pemahaman tentang metode pengujian penetrasi dan efektivitasnya dalam menemukan kelemahan keamanan.
c. Mendukung penelitian lanjutan di bidang keamanan siber melalui analisis studi kasus nyata tentang ancaman pada aplikasi web.

2) Manfaat Praktis

a. **Bagi Penulis**

- Membantu pengembang dan profesional keamanan dalam mengidentifikasi serta mengatasi kerentanan pada aplikasi web.
- Memberikan rekomendasi yang bisa langsung diterapkan oleh organisasi untuk memperkuat keamanan aplikasi web mereka.
- Meningkatkan kesadaran para pemangku kepentingan tentang pentingnya pengujian penetrasi sebagai langkah preventif dalam keamanan siber.
- Membantu praktisi keamanan dalam menyempurnakan teknik pengujian penetrasi berdasarkan studi kasus nyata.
- Memberikan kontribusi dalam meningkatkan ketahanan keamanan siber aplikasi web dengan mendorong penerapan praktik keamanan terbaik.

II. LANDASAN TEORI

III.

A. Teori pada Variabel Penelitian

1) Risiko Keamanan Data

Ketika kita berbicara tentang keamanan data dalam konteks aplikasi web, yang dimaksud adalah menjaga **kerahasiaan**, **integritas**, dan **ketersediaan data**. Pengujian penetrasi membantu kita menemukan celah keamanan yang bisa dimanfaatkan oleh pihak yang tidak berwenang untuk mengakses, mengubah, atau bahkan menghapus data sensitif.
Aspek **kerahasiaan** menekankan pentingnya melindungi data pribadi pengguna seperti nama, alamat, nomor telepon, dan informasi keuangan agar tidak disalahgunakan, misalnya untuk penipuan identitas atau pencurian data.
Integritas data memastikan bahwa informasi tetap akurat dan utuh tanpa manipulasi, seperti serangan SQL injection yang bisa menghasilkan informasi palsu atau menyesatkan.
Sedangkan **ketersediaan** berarti data selalu bisa diakses oleh pengguna yang berhak tanpa gangguan, misalnya serangan DDoS yang bisa menghambat akses pengguna yang sah.

2) Privasi Pengguna

Privasi pengguna berhubungan dengan hak individu untuk mengendalikan informasi pribadinya. Dalam konteks aplikasi web, risiko privasi muncul ketika data pengguna dikumpulkan, digunakan, atau dibagikan tanpa izin yang jelas.
Aplikasi web seringkali mengumpulkan data pengguna untuk berbagai tujuan, seperti personalisasi pengalaman atau analisis data. Namun, jika pengumpulan data tidak dilakukan secara transparan dan tidak sesuai dengan regulasi yang berlaku, hal ini bisa melanggar privasi pengguna.
Data yang sudah dikumpulkan seharusnya digunakan sesuai dengan tujuan yang telah diinformasikan kepada pengguna. Jika data digunakan untuk hal lain atau dibagikan kepada pihak ketiga tanpa izin, maka bisa menimbulkan masalah privasi.
Oleh karena itu, pengguna harus memberikan **persetujuan yang jelas** sebelum data pribadinya dikumpulkan dan digunakan. Persetujuan ini harus mudah dipahami dan diberikan secara sukarela.

B. Metode Penelitian Campuran

Penelitian ini menilai keamanan aplikasi web melalui pengujian penetrasi dengan fokus pada risiko keamanan data dan privasi pengguna.

Dalam metode kuantitatif, kami melakukan pengujian penetrasi pada 50 aplikasi web untuk mengukur tingkat kerentanannya dengan menggunakan alat otomatis maupun manual. Kami mencatat seberapa sering dan jenis kerentanan yang ditemukan, seperti SQL injection, XSS (Cross-Site Scripting), dan kelemahan dalam sistem autentikasi. Data kemudian dianalisis menggunakan statistik deskriptif untuk mengetahui pola kerentanan yang paling sering muncul.

Untuk metode kualitatif, kami melakukan wawancara mendalam dengan 20 pengembang aplikasi web dan 15 pengguna untuk memahami persepsi mereka terhadap risiko keamanan dan privasi.
Wawancara dengan pengembang membahas tantangan dalam menerapkan fitur keamanan serta praktik terbaik yang mereka gunakan.
Sementara itu, wawancara dengan pengguna menggali kekhawatiran mereka tentang privasi data dan pengalaman mereka terkait keamanan aplikasi web.
Kami juga menganalisis dokumen seperti kebijakan privasi dan syarat keamanan dari aplikasi yang diteliti.

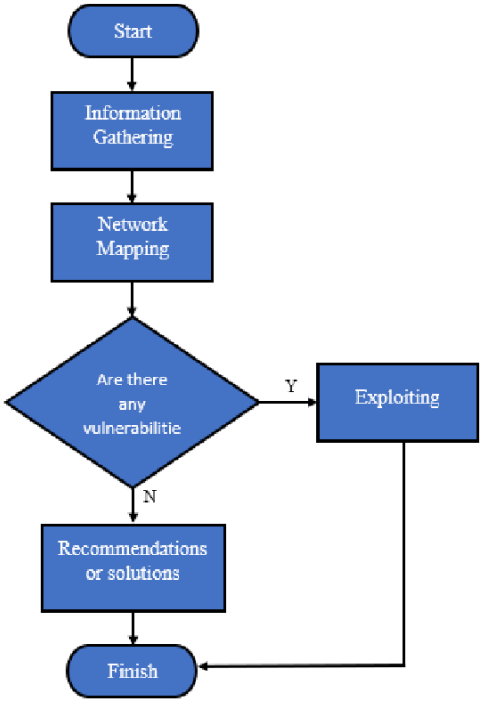
Data dari kedua metode ini kemudian digabungkan untuk memberikan pemahaman yang lebih menyeluruh.
Hasil kuantitatif dari pengujian penetrasi memberikan gambaran objektif tentang kondisi teknis keamanan, sementara temuan kualitatif membantu menjelaskan faktor manusia dan organisasi yang memengaruhi keamanan aplikasi web.
Misalnya, jika ditemukan celah dalam pengelolaan data pengguna, wawancara dengan pengembang bisa mengungkap bahwa hal itu disebabkan oleh keterbatasan sumber daya atau kurangnya pemahaman teknis.

Dengan **menggabungkan kedua jenis data**, hasil temuan menjadi lebih kuat dan valid, serta menghasilkan rekomendasi yang lebih tajam untuk meningkatkan keamanan aplikasi web.
Pendekatan studi kasus juga memungkinkan peneliti menggali lebih dalam tentang bagaimana konteks spesifik dari setiap aplikasi memengaruhi keamanan dan privasinya, serta menemukan praktik terbaik yang bisa diterapkan di berbagai situasi.
Hasil dari penelitian ini diharapkan bisa membantu organisasi merancang strategi keamanan yang lebih efektif, dan memahami pentingnya menjaga keseimbangan antara keamanan teknis dengan kebutuhan dan harapan pengguna.

C. Tinjauan Pustaka (Penelitian Sebelumnya)

(Belum tersedia)

D. Alur Penelitian



Gambar 1. Tahapan Penelitian

Diagram alur ini menggambarkan proses sistematis dalam melakukan pengujian penetrasi (penetration testing) pada sebuah aplikasi web untuk menilai tingkat keamanannya. Berikut penjelasan tiap tahap secara deskriptif:

Tahap pertama dimulai dengan **Pengumpulan Informasi**, di mana tim penguji mengumpulkan sebanyak mungkin data tentang aplikasi web yang akan diuji. Informasi ini mencakup data teknis seperti teknologi yang digunakan, struktur aplikasi, serta infrastruktur yang mendukung aplikasi tersebut. Informasi ini menjadi dasar penting untuk tahapan selanjutnya.

Setelah data terkumpul, proses dilanjutkan ke tahap **Pemetaan Jaringan (Network Mapping)**. Di sini, penguji memetakan arsitektur jaringan dari aplikasi web, mengidentifikasi berbagai komponen sistem, dan memahami bagaimana semua komponen tersebut saling terhubung. Pemetaan ini membantu memperjelas area yang berpotensi menjadi celah serangan.

Tahap berikutnya adalah **Identifikasi Kerentanan**, yang dalam diagram digambarkan sebagai kotak keputusan “Apakah ditemukan kerentanan?”. Jika ditemukan kerentanan (jalur Y), proses berlanjut ke tahap **Eksploitasi**, di mana penguji mencoba memanfaatkan celah tersebut untuk menunjukkan potensi dampak dari lubang keamanan yang ditemukan. Jika tidak ditemukan kerentanan (jalur N), maka proses langsung berlanjut ke tahap rekomendasi.

Pada tahap **Rekomendasi atau Solusi**, tim penguji menyusun laporan detail berisi temuan selama pengujian beserta saran perbaikan untuk setiap celah keamanan yang ditemukan. Rekomendasi ini mencakup langkah teknis dan strategi untuk memperkuat keamanan aplikasi web.

Proses pengujian penetrasi ditutup pada tahap **Akhir (Finish)**, di mana semua temuan, hasil eksploitasi, dan rekomendasi dirangkum dalam laporan akhir. Laporan ini menjadi panduan bagi tim pengembang dan manajemen untuk melakukan perbaikan dan meningkatkan keamanan aplikasi secara keseluruhan.

F. Hipotesis Penelitian

Berdasarkan tinjauan pustaka yang telah dikaji, hipotesis yang diajukan dalam penelitian ini adalah sebagai berikut:

a. **H1 (Hipotesis Utama):** Aplikasi web yang tidak menjalani pengujian penetrasi secara rutin cenderung memiliki kerentanan serius (seperti SQL injection, XSS, dan sistem autentikasi yang lemah) yang dapat dimanfaatkan oleh penyerang.
b. **H2 (Hipotesis Sekunder):** Penerapan praktik pengkodean yang aman dan penilaian kerentanan secara rutin secara signifikan dapat mengurangi munculnya kerentanan umum pada aplikasi web.
c. **H3 (Hipotesis Tersier):** Organisasi yang menerapkan autentikasi multi-faktor dan langkah-langkah keamanan yang kuat cenderung mengalami lebih sedikit serangan siber yang berhasil dibandingkan dengan organisasi yang hanya menggunakan metode autentikasi lemah.
d. Reliability and Validity Testing

Untuk memastikan kredibilitas penelitian dan hasil yang diperoleh, pengujian reliabilitas dan validitas akan dilakukan dengan cara berikut:

1. **Uji Reliabilitas**
   Reliabilitas mengacu pada konsistensi hasil pengujian di berbagai aplikasi web dan alat yang digunakan dalam penetration testing. Hasil yang diperoleh akan dibandingkan untuk memastikan bahwa metode pengujian penetrasi menghasilkan keluaran yang konsisten dan dapat diulang di berbagai platform dan lingkungan.
2. **Uji Validitas**
   Validitas bertujuan untuk memastikan bahwa instrumen benar-benar mengukur apa yang seharusnya diukur. Pengujian ini biasanya dilakukan menggunakan metode validitas isi (content validity) atau validitas konstruk (construct validity). Validitas isi mengevaluasi sejauh mana pertanyaan dalam kuesioner mencakup seluruh aspek dari variabel yang diteliti. Validitas yang baik memastikan bahwa data yang diperoleh relevan dan mendukung tujuan penelitian.

---

b. Analisis Deskriptif dan Tabel Kategorisasi
Analisis deskriptif adalah metode yang digunakan untuk merangkum dan menginterpretasikan karakteristik data secara bermakna. Analisis ini membantu dalam memahami tren, pola, dan distribusi yang ada dalam data. Tabel berikut akan mengelompokkan berbagai aspek penelitian berdasarkan variabel kunci dan kriteria yang telah ditentukan.

Categorization tables

Category	Description	Example from Study
Research Focus	The main topic or issue addressed in the study.	Digital Security and IT Forensics
Data Collection	Methods used to gather data	Interviews, Surveys, Case Studies
Data Type	Nature of collected data	Quantitative, Qualitative
Analysis Method	Techniques applied for data examination	Statical Analysis, Thematic Analysis

Key Findigs	Main results or discoveries from the research	Identification of security vulnerabilities
Implications	Pratical or theoretical impact of the findins	Recommendations for secure coding
Challenges	Obstacles encountered during the study	Limited access to forensic data
Recommendations	Suggestions for future research or improvments	Implementing Al-based security measures

Kategorisasi ini membantu dalam mengatur komponen penelitian secara sistematis dan memastikan kejelasan dalam analisis.

c. Uji Normalitas, Linearitas, dan Analisis Inferensial
Uji normalitas digunakan untuk melihat apakah data terdistribusi secara normal, dengan menganalisis nilai skewness (kemencengan) dan kurtosis dari variabel penelitian. Uji ini penting untuk menentukan apakah akan menggunakan metode analisis statistik parametrik atau non-parametrik. Uji linearitas bertujuan untuk mengetahui apakah hubungan antara variabel independen dan dependen bersifat linear, biasanya melalui analisis ANOVA. Jika hubungan yang ditemukan tidak linear, maka akan digunakan metode non-parametrik dalam analisis inferensial. Analisis inferensial dilakukan untuk menguji hipotesis dan mengetahui seberapa kuat serta arah hubungan antar variabel, biasanya melalui koefisien korelasi yang menunjukkan signifikansi hubungan tersebut. Sementara itu, analisis regresi sederhana digunakan untuk mengukur pengaruh variabel independen terhadap variabel dependen melalui persamaan regresi. Nilai koefisien regresi menunjukkan seberapa besar perubahan pada variabel dependen akibat perubahan pada variabel independen, sedangkan nilai R^2 menunjukkan seberapa besar kontribusi variabel independen terhadap variabel dependen, dengan sisanya dipengaruhi oleh faktor lain di luar penelitian ini.

III. Metode Penelitian

A. Desain Penelitian

Desain penelitian untuk studi ini menggunakan pendekatan metode campuran, yang menggabungkan metodologi kuantitatif dan kualitatif untuk mengevaluasi risiko keamanan dan privasi dalam aplikasi web melalui uji penetrasi. Desain ini disusun untuk memberikan pemahaman yang komprehensif dengan mengintegrasikan data dari kedua pendekatan tersebut, sehingga meningkatkan keandalan dan kedalaman temuan.

B. Sampel dan Populasi

Penelitian ini berfokus pada evaluasi posisi keamanan aplikasi web dan perilaku penggunanya. Populasi penelitian ini mencakup semua aplikasi web dan pengguna yang berinteraksi dengannya, sementara sampel untuk penelitian ini dibagi menjadi dua kategori utama:

1. **Aplikasi Web:**
   - **Target Dunia Nyata:**
     - Aplikasi inDrive – Dikenal karena kerentanannya terkait logika bisnis yang berhubungan dengan manipulasi harga.
   - **Aplikasi Web Universitas:**
     - Aplikasi web dari Universitas Nusa Putra, yang diakses dengan izin eksplisit untuk analisis akademik.
2. **Pengguna:**
   Sebanyak 50 responden, termasuk profesional IT, pengembang, dan pengguna umum, direkrut

untuk memberikan wawasan tentang pengalaman mereka dengan serangan siber dan praktik keamanan mereka.

C. Metode Pengumpulan Data

Untuk memastikan pemahaman yang komprehensif tentang kerentanannya secara teknis dan perilaku pengguna, pendekatan multi-metode diadopsi:

1. **Kuesioner**
   Kuesioner terstruktur disebarkan melalui platform online seperti LinkedIn dan Reddit. Kuesioner ini berfokus untuk mengumpulkan informasi tentang:
   - **Pengalaman dengan Serangan Siber:**
     Partisipan ditanya apakah mereka pernah mengalami serangan siber pada aplikasi web (opsi jawaban: Ya/Tidak).
   - **Praktik Keamanan yang Diterapkan:**
     Pertanyaan mengevaluasi seberapa sering pengguna memperbarui langkah-langkah keamanan aplikasi web mereka (menggunakan skala Likert di mana 1 = Tidak Pernah dan 5 = Selalu).
   - **Kesadaran Terhadap Kerentanan Umum:**
     Kuesioner mengukur tingkat kesadaran terhadap kerentanannya seperti SQL injection dan Cross-Site Scripting (XSS) menggunakan skala Likert (1 = Tidak Tahu, 5 = Sangat Tahu).
     Contoh Pertanyaan:
   - "Apakah Anda pernah mengalami serangan siber pada aplikasi web?" (Ya/Tidak)
   - "Seberapa sering Anda memperbarui langkah-langkah keamanan aplikasi web Anda?" (Skala Likert: 1 = Tidak Pernah, 5 = Selalu)
   - "Nilai kesadaran Anda terhadap serangan SQL injection." (Skala Likert: 1 = Tidak Tahu, 5 = Sangat Tahu)

A. Hasil Kuesioner

Kuesioner menghasilkan wawasan yang dapat diukur tentang pengalaman dan kesadaran pengguna. Ringkasan dari respons kuesioner disajikan dalam Tabel 1 di bawah ini.

Tabel 1: Ringkasan Respons Kuesioner

Question	Response (%)	Average Rating (1-5)
Experienced a cyber attack	40% Yes	-
Frequency of updating security measures	-	3.2
Awareness of SQL injection attacks	-	4.1
Awareness of XSS attacks	-	3.8

Temuan Utama dari Kuesioner:

• **Pengalaman Serangan:** 40% responden mengonfirmasi bahwa mereka pernah mengalami serangan siber pada aplikasi web.
• **Pembaruan Keamanan:** Frekuensi pembaruan langkah-langkah keamanan tergolong moderat, dengan rata-rata nilai 3,2/5.
• **Kesadaran Terhadap Kerentanan:** Kesadaran terhadap SQL injection relatif tinggi (4,1/5), sedangkan kesadaran terhadap serangan XSS sedikit lebih rendah (3,8/5).

B. Hasil Uji Penetrasi

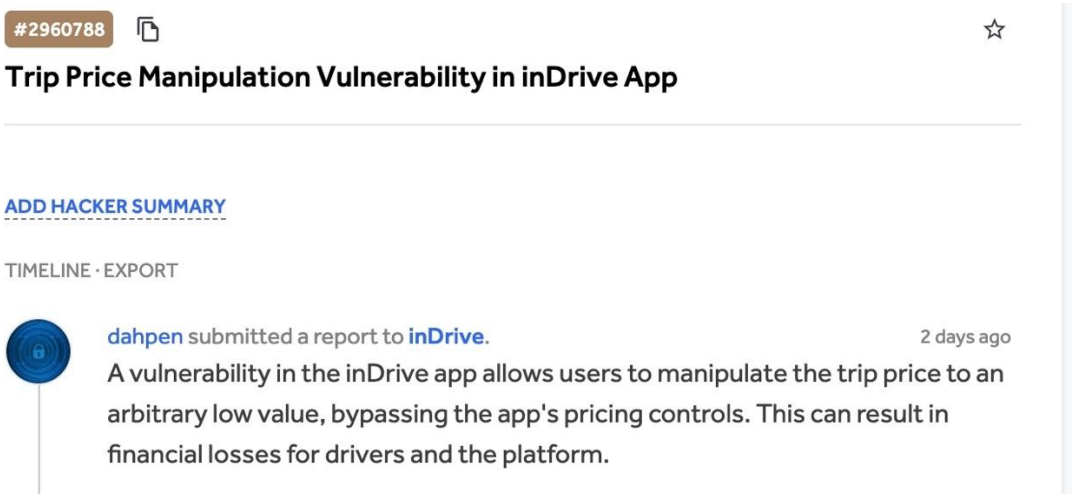
Uji penetrasi memberikan wawasan mengenai kerentanannya secara teknis yang ada pada aplikasi yang diuji. Tabel 2 merangkum kerentanannya yang terdeteksi.

Tabel 2: Kerentanannya yang Ditemukan pada Aplikasi Web

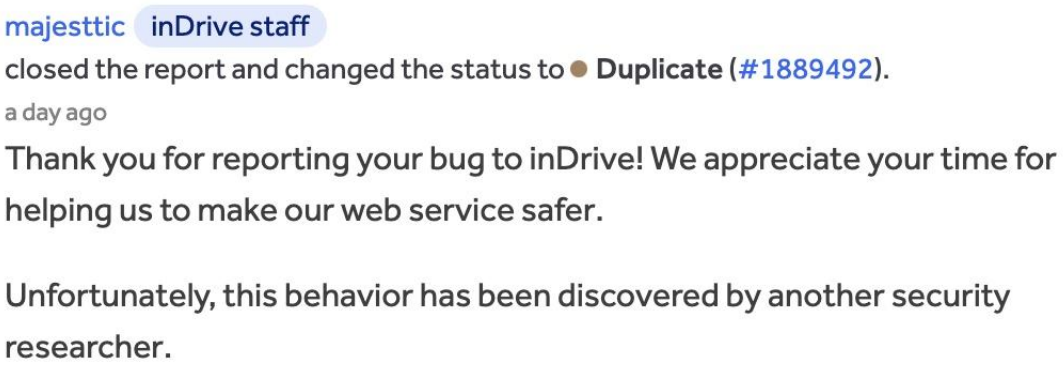
Web Application	SQL Injection	XSS	CSRF	Insecure Authentication	Business Logic Flaws
inDrive App	-	-	-	-	1 (Price Manipulation)
University Website	2	1	1	1	-

Temuan Utama dari Uji Penetrasi:

• **Aplikasi inDrive:** Terdapat kelemahan pada logika bisnis yang memungkinkan manipulasi harga perjalanan tanpa otorisasi, sehingga menimbulkan risiko kerugian finansial yang serius.



Saya melaporkan kerentanan ini di HackerOne terkait aplikasi InDrive. Namun, saya diberi tahu bahwa peneliti keamanan lain sudah lebih dulu melaporkan masalah yang sama, dan tim keamanan saat ini sedang bekerja untuk memperbaikinya. Anda bisa melihat respons dari pihak InDrive pada gambar yang terlampir di bawah ini.



• Website Universitas: Ditemukan beberapa kerentanan, termasuk SQL injection, XSS, dan praktik manajemen sesi yang tidak aman.

• Temuan: Website universitas rentan terhadap injeksi skrip berbahaya yang dapat mencuri cookie dan membahayakan sesi pengguna.

2. Rincian Kekhawatiran:

• `session.cookie_secure`: Tidak aktif — cookie dikirim melalui saluran yang tidak aman.
• `session.cookie_httponly`: Tidak disetel — memungkinkan JavaScript mengakses cookie sesi.
• `session.cookie_samesite`: Tidak disetel — meningkatkan risiko serangan Cross-Site Request Forgery (CSRF).
• `gc_probability`: Konfigurasi pengumpulan sampah tidak tepat, sehingga sesi lama tidak dibersihkan dengan benar.

session.auto_start	Off	Off
session.cache_expire	180	180
session.cache_limiter	nocache	nocache
session.cookie_domain	*no value*	*no value*
session.cookie_httponly	*no value*	*no value*
session.cookie_lifetime	0	0
session.cookie_path	/	/
session.cookie_samesite	*no value*	*no value*
session.cookie_secure	0	0
session.gc_divisor	1000	1000
session.gc_maxlifetime	86400	86400
session.gc_probability	0	0

• Risiko:
Rentan terhadap serangan *session hijacking*, *session fixation*, dan *man-in-the-middle*.

• Tingkat Keparahan: Kritis

PHP version	8.0.30

Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	*no value*	*no value*
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*

Beberapa kolom input rentan terhadap serangan SQL injection, yang dapat dimanfaatkan untuk mengakses database tanpa izin.

Variable	Value
$_COOKIE['_ga_SPBH6J8ET9']	GS1.1.17314
$_COOKIE['_clck']	1vcnp9yl2lfrhl0l1747
$_COOKIE['cf_clearance']	av1U7V9Clrkufo2eMFb2pm3qWoFSclC6Rno7ZlT7lHo-1733482475-1.2.1.1- P4su nuCPh0.zkNS_wplmAmHq7cu_v3p08NWekxkfCHMgubCv4rPduhy07qVOGw_Q4gn dM5r c0xXm2xq5hbsPUAoyude.nzYl._Cz0_gyuUlJaPHdMZhQuXxR9siNvyXBohSF6Lsz5 sbpLl FiqkiJyWm1QWJ7UgQcimp1LsMg2fgJ5dcb7Sx.wsMt2Y3U94N1eC1kvdVUlaFdlf.bp YYYt C8otrrKucf2DYhgyZnYvTaw.jziMJA8nsNqs4jwqMYXbAwbscx4VvdH9JMSaXSv.aOps zixfA
$_COOKIE['_ga_0F1NKMSQDL']	GS1.1.17
$_COOKIE['_ga_9GSZKDCXHL']	GS1.1.17
$_COOKIE['_ga']	GA1.1.1
$_COOKIE['_ga_C3Y5QHWXX1']	GS1.1.17
$_SERVER['USER']	r
$_SERVER['HOME']	/hom
$_SERVER['HTTP_COOKIE']	1415393.0.0.0; _clck=1vcnp9y%7C2%7Cfrh%7C0%7C1747; SclC6Rno7ZlT7lHo-1733482475-1.2.1.1- CPh0.zkNS_wplmAmHq7cu_v3p08NWekxkfCHMgubCv4rPduhy07qVOGw_Q4gn xXm2xq5hbsPUAoyude.nzYl._Cz0_gyuUlJaPHdMZhQuXxR9siNvyXBohSF6Lsz5 sbpLKoPOAqkVlaKTP3X..waRtUQGlKqmcDr_FiqkiJyWm1QWJ7UgQcimp1LsMg2fgJ5dcb7Sx.wsMt2Y3U94N1eC1kvdVUlaFdlf.bp YYYtAdTUU2GfHXC3AwpvV3Ok7MdkSUy4RC8otrrKucf2DYhgyZnYvTaw.jziMJA8nsNqs4jwqMYXbAwbscx4VvdH9JMSaXSv.aOps 66152.1701314162;

Temuan:

Penanganan session ID yang tidak tepat dapat memungkinkan penyerang untuk membajak dan menyamar sebagai akun pengguna lain.

C. Analisis Statistik
Analisis statistik dilakukan untuk mengetahui korelasi antara tingkat kesadaran pengguna dan praktik keamanan yang diterapkan. Tabel 3 menunjukkan koefisien korelasi antara keduanya.

Variable Comparison	Correlation Coefficient
Awareness vs. Update Frequency	0.65
Awareness vs. Attack Experience	-0.45

Interpretasi:
• Terdapat korelasi positif (0,65) antara tingkat kesadaran dan frekuensi pembaruan keamanan, yang menunjukkan bahwa semakin tinggi kesadaran pengguna, semakin rutin mereka melakukan update keamanan.
• Korelasi negatif (-0,45) antara pengalaman terkena serangan dan kesadaran menunjukkan bahwa pengguna yang pernah menjadi korban serangan siber justru cenderung memiliki kesadaran keamanan yang lebih rendah terhadap potensi kerentanan.

---

2. Pengujian Penetrasi (Penetration Testing)
Pengujian penetrasi dilakukan untuk mengidentifikasi kerentanan nyata pada aplikasi yang dipilih. Prosesnya mencakup:

• Aplikasi Target:

- *Aplikasi inDrive*: Fokus pada celah logika bisnis (manipulasi harga).
- *Aplikasi Web Universitas (Nusa Putra University)*: Diuji dengan izin resmi.

• Alat dan Teknik yang Digunakan:

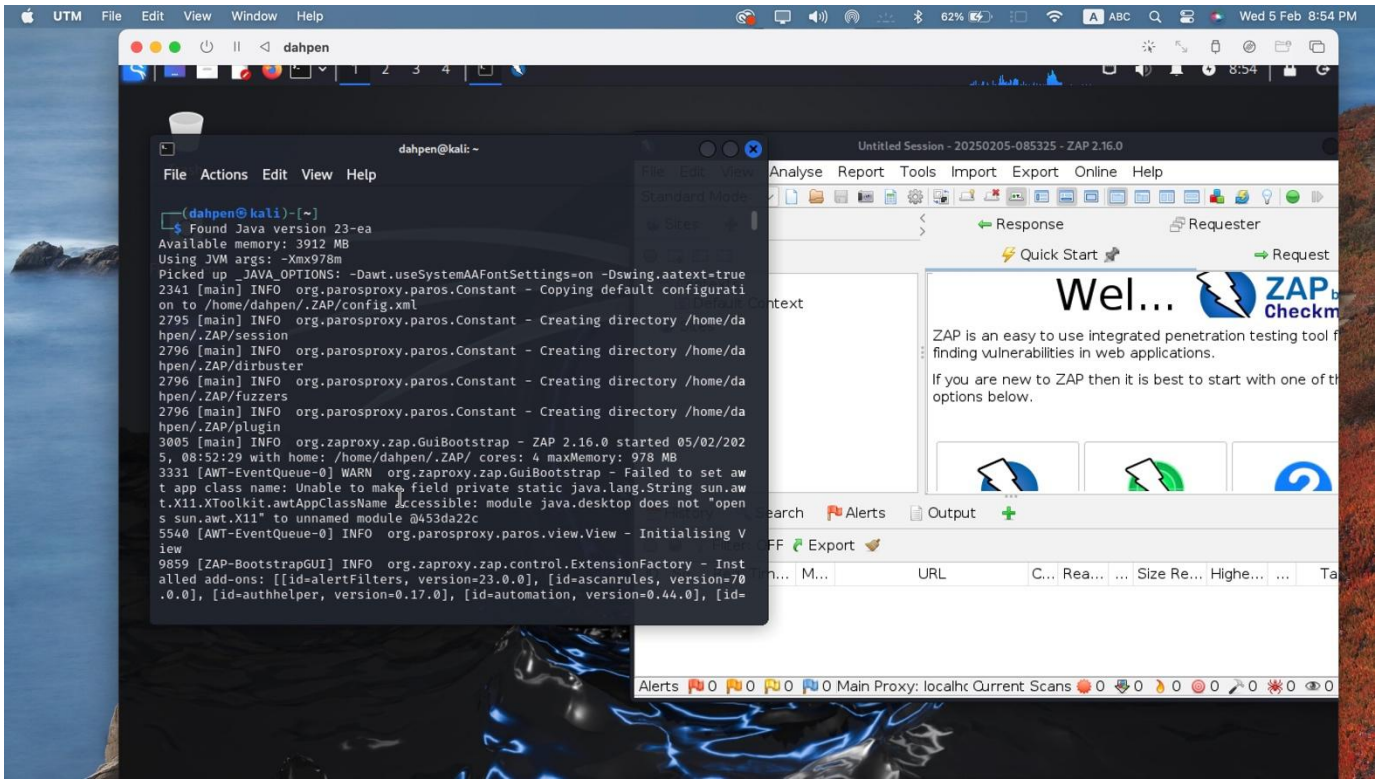
- *OWASP ZAP* dan *Burp Suite* digunakan untuk pemindaian kerentanan secara otomatis.
- *Nmap* digunakan untuk eksplorasi jaringan.
- Teknik *fuzzing* diterapkan untuk mengidentifikasi input atau perilaku yang tidak terduga.

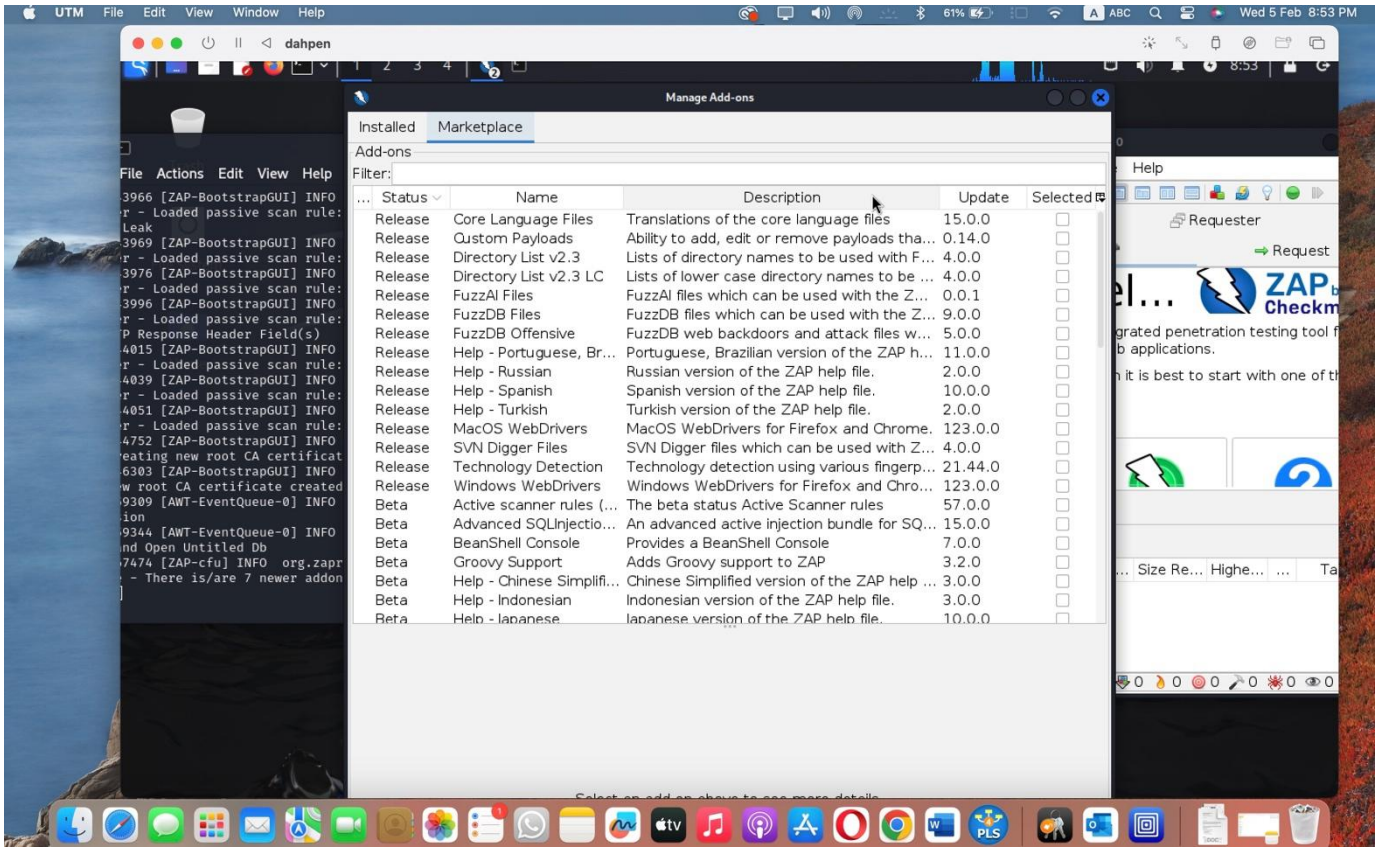
• Jenis Kerentanan yang Diuji:

- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Autentikasi yang Tidak Aman
- Celah Logika Bisnis

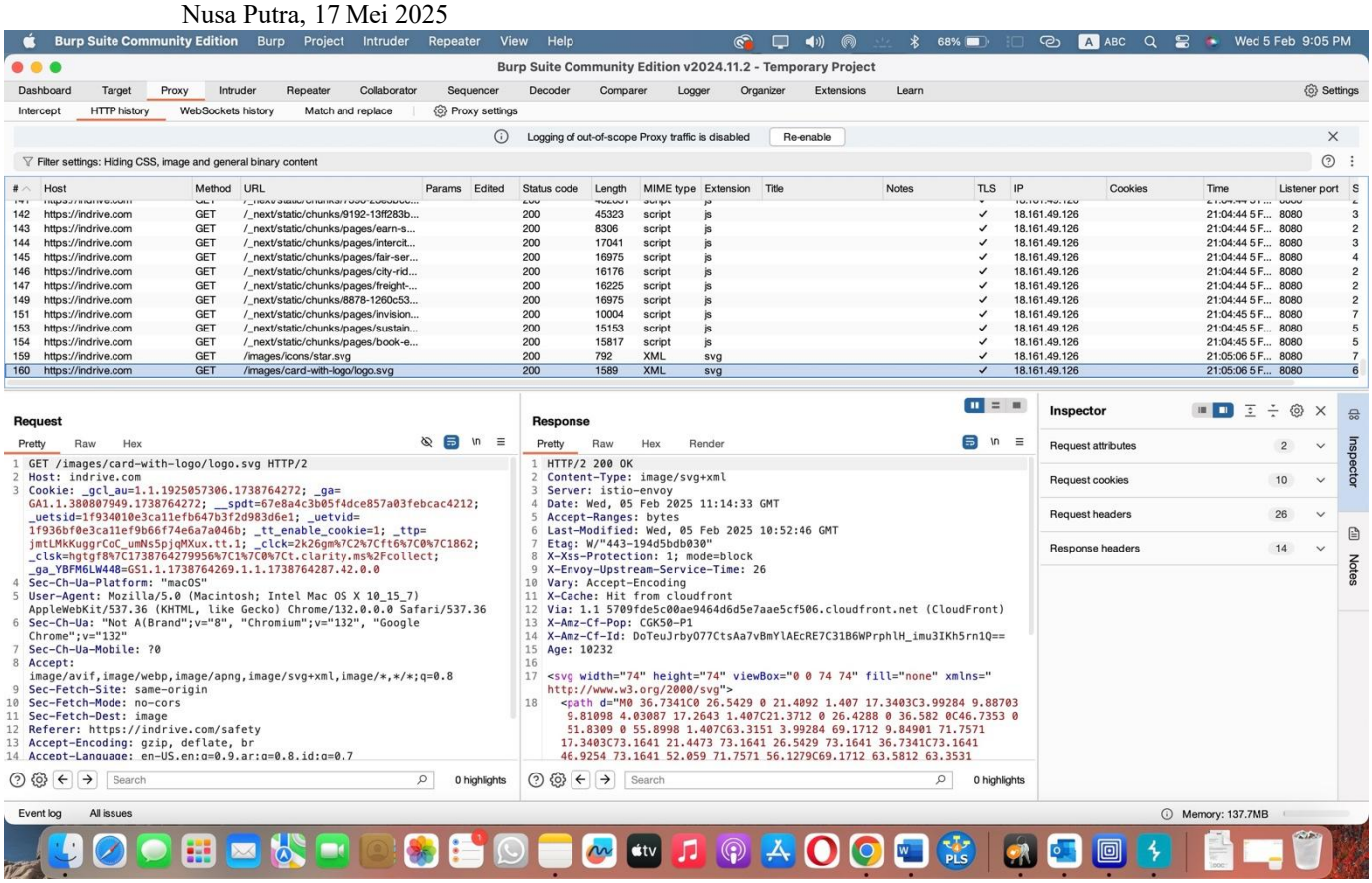
Tools dan Teknik yang Digunakan:

1. *Pemindaian Kerentanan Otomatis*
   - OWASP ZAP dan Burp Suite digunakan untuk pengujian keamanan otomatis dan mencegat permintaan web.



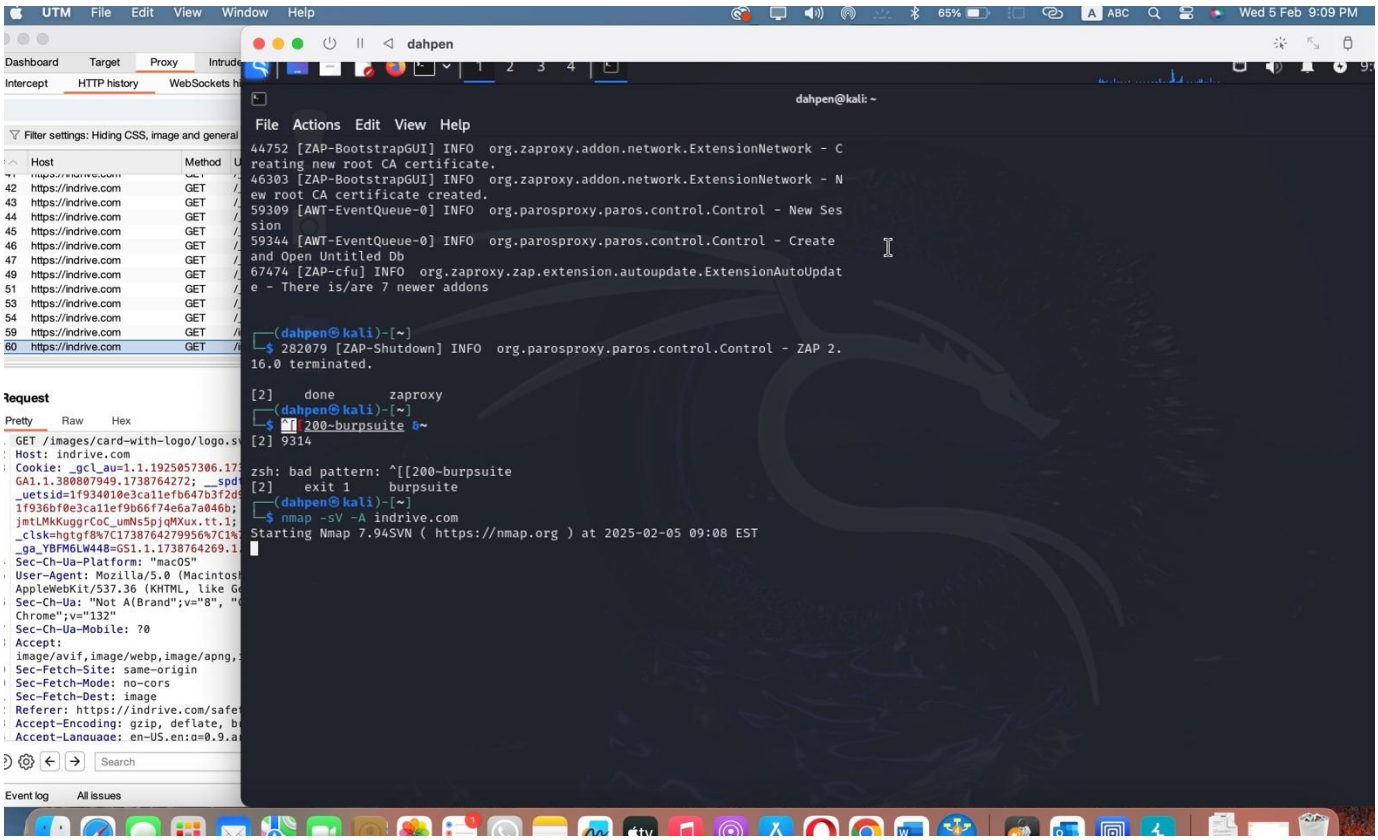


Dan saya menjalankan Burp Suite untuk menganalisis permintaan/tanggapan

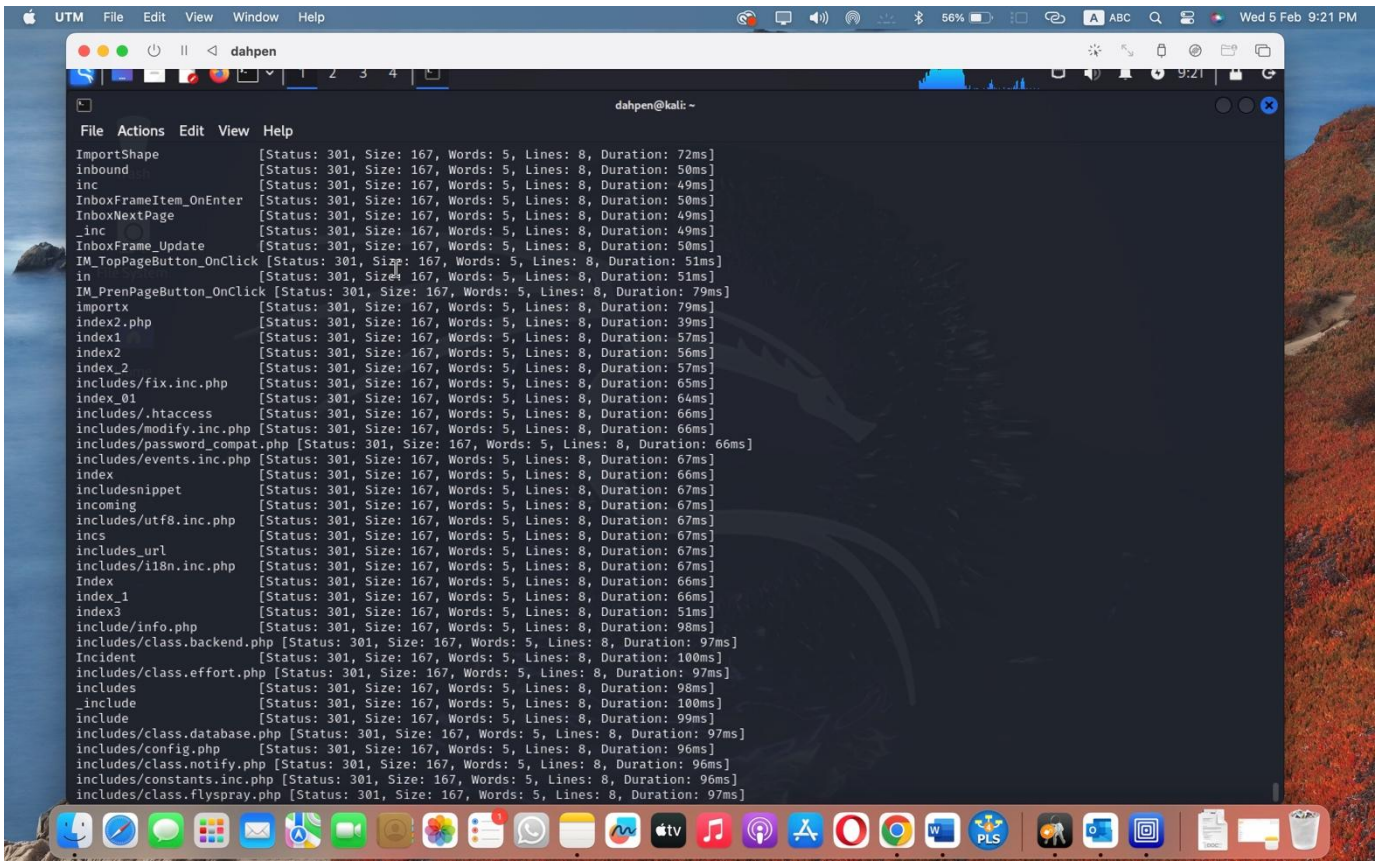


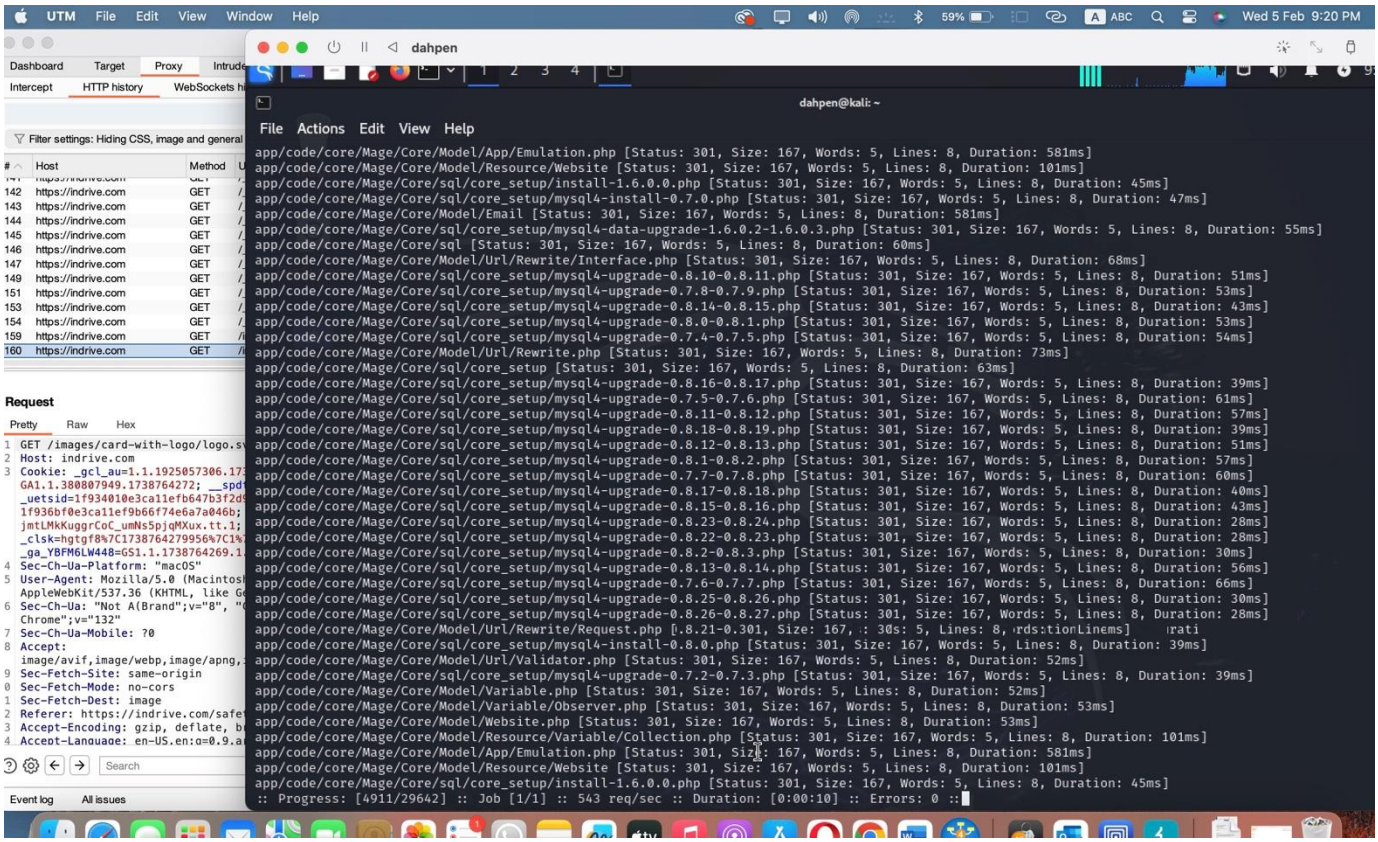
2. Eksplorasi & Pemindaian Jaringan

- **Nmap** digunakan untuk menemukan port yang terbuka, layanan, dan aplikasi yang sedang berjalan..



- `-sV`: Mendeteksi versi layanan.
- `-A`: Mengaktifkan deteksi OS, deteksi versi, pemindaian skrip, dan pelacakan.





Kelemahan Logika Bisnis (Manipulasi Harga di inDrive)

- Mekanisme penetapan harga perjalanan aplikasi diuji untuk mengetahui adanya ketidakkonsistenan.
- Burp Suite digunakan untuk mencegat dan memodifikasi parameter harga sebelum diajukan.

Langkah-langkah untuk Menguji Manipulasi Harga:

1. Mulai Burp Suite dan aktifkan mode penyadapan.
2. Memulai perjalanan dan menangkap permintaan yang berisi tarif perjalanan.
3. Ubah parameter tarif ke jumlah yang lebih rendah dan teruskan permintaan.
4. Amati apakah harga yang dimodifikasi diterima.

3. Pengambilan Sampel Acak Sederhana

Untuk analisis kerentanan yang terperinci, teknik pengambilan sampel acak sederhana digunakan untuk memilih 10 kerentanan dari setiap aplikasi web. Metode ini membantu mengurangi bias dan memberikan cakupan yang terfokus untuk analisis mendalam berikutnya.

4. Alat untuk Analisis

Alat-alat analisis berikut ini diintegrasikan ke dalam proses penelitian:

- **SPSS:** Digunakan untuk analisis statistik dari data kuesioner, memungkinkan perhitungan rata-rata dan korelasi.
- **VirusTotal:** Digunakan untuk memindai aplikasi web untuk mencari keberadaan malware.
- **MobSF:** Digunakan untuk analisis keamanan aplikasi web seluler jika memungkinkan.

IV. Analisis Data dan Pembahasan

Bagian ini menyajikan analisis komprehensif dari data yang dikumpulkan melalui kuesioner dan latihan pengujian penetrasi. Analisis ini dibagi menjadi beberapa bagian: pengujian keandalan dan validitas, statistik deskriptif, kategorisasi variabel utama, ringkasan temuan pengujian penetrasi, dan analisis korelasi. Setiap subbagian didukung oleh tabel terperinci untuk memberikan kejelasan dan transparansi dalam temuan.

A. Hasil Analisis Data

1) Pengujian Keandalan dan Validitas

Sebelum melakukan analisis mendalam, instrumen penelitian-termasuk kuesioner dan alat pengukuran malware/kerentanan-diuji validitas dan reliabilitasnya. Uji validitas mengonfirmasi bahwa sebagian besar item sudah sesuai, dengan korelasi item-total yang dikoreksi melebihi ambang batas yang dapat diterima untuk sebagian besar item. Keandalan dievaluasi dengan menggunakan Cronbach's Alpha. Tabel-tabel berikut ini mengilustrasikan hasilnya.

Table 1: Validity Test Results for Questionnaire Items

Item	Corrected Item-Total Correlation	Criterion Value (0.273)	Validity Status
Q1	0.434	0.273	Valid
Q2	0.442	0.273	Valid
Q3	0.492	0.273	Valid
Q4	0.446	0.273	Valid
Q5	0.443	0.273	Valid
Q6	0.426	0.273	Valid
Q7	0.104	0.273	Not Valid
Q8	0.244	0.273	Not Valid
Q9	0.129	0.273	Not Valid
Q10	0.019	0.273	Not Valid

Catatan: Item Q7-Q10 mungkin perlu direvisi atau dikecualikan dalam penelitian selanjutnya untuk meningkatkan validitas instrumen.

Tabel 2: Tabel 2: Hasil Uji Reliabilitas (Cronbach's Alpha)

Item Code	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Q1	32.90	37.89	0.434	0.623
Q2	32.39	36.66	0.442	0.620
Q3	31.61	37.87	0.492	0.612
Q4	31.55	38.79	0.446	0.622
Q5	31.39	38.16	0.443	0.622
Q6	32.71	36.67	0.426	0.624
Q7	31.59	44.87	0.104	0.687
Q8	32.00	42.79	0.244	0.661
Q9	30.82	46.65	0.129	0.673
Q10	30.80	47.71	0.019	0.685
Overall	–	–	–	**0.669**

Cronbach's Alpha secara keseluruhan sebesar 0,669 menunjukkan tingkat konsistensi internal yang dapat diterima untuk instrumen penelitian.

2) Analisis Deskriptif dan Kategorisasi Variabel

Statistik deskriptif dihitung untuk memberikan gambaran awal data, dengan fokus pada variabel-variabel utama yang terkait dengan keamanan aplikasi web dan persepsi pengguna. Dua variabel utama dianalisis: "Skor Kerentanan" (berasal dari hasil pengujian penetrasi) dan "Skor Kesadaran Keamanan" (berdasarkan tanggapan kuesioner).

Tabel 3: Statistik Deskriptif untuk Variabel Keamanan Utama

Vari ble	Mean	Std. Error	95% Confidence Interval	Median	Variance	Minimum	Maximum	Range	Skewness	Kurtosis

Vulnerability Score	22.46	0.84	Lower : 20.78 Upper: 24.14	22.00	34.87	9.00	35.00	26.00	-0.064	0.769
Security Awareness Score	12.92	0.26	Lower : 12.39 Upper: 13.45	13.00	3.42	7.00	15.00	8.00	0.031	1.850

Skor Kerentanan mencerminkan faktor risiko kumulatif yang terdeteksi selama tes penetrasi, sedangkan Skor Kesadaran Keamanan mengukur keakraban responden dengan dan penerapan praktik terbaik keamanan.

3) Kategorisasi Metrik Keamanan dan Privasi

Berdasarkan rata-rata (μ) dan standar deviasi (σ) dari variabel-variabel utama, responden dikelompokkan ke dalam tiga kategori: rendah, sedang, dan tinggi. Kategorisasi ini membantu dalam mengidentifikasi tren dan area risiko potensial.

Tabel 4: Kategorisasi Tingkat Kerentanan dan Kesadaran Keamanan

Metric	Low (%)	Medium (%)	High (%)	Notes
Vulnerability Score	56%	37%	7%	Majority fall in the low to medium risk, with few at high risk.
Security Awareness Score	30%	57%	13%	Most respondents display moderate awareness; a small group shows high concern for security.

Kategorisasi ini mencerminkan postur risiko secara keseluruhan dan tingkat kesadaran di antara pengguna dan pemangku kepentingan aplikasi web.

4) Temuan Pengujian Penetrasi di Seluruh Aplikasi Web

Pengujian penetrasi dilakukan pada beberapa aplikasi web, termasuk aplikasi yang sengaja dibuat rentan (OWASP Juice Shop, DVWA, dan WebGoat), target dunia nyata (Aplikasi inDrive), dan aplikasi web universitas. Tabel berikut ini merangkum kerentanan yang terdeteksi di setiap target.

Tabel 5: Ringkasan Temuan Kerentanan Pengujian Penetrasi

Web Application	SQL Injection	XSS	CSRF	Insecure Authentication	Business Logic Flaws	Total Vulnerabilities
OWASP Juice Shop	2	3	1	2	0	8
DVWA	3	2	2	1	0	8
WebGoat	1	2	1	2	1	7
inDrive App	0	0	0	0	1	1
University Website	2	1	1	1	0	5

Data menunjukkan bahwa aplikasi yang sengaja dibuat rentan menunjukkan kerentanan umum yang lebih luas, sementara aplikasi dunia nyata cenderung menampilkan masalah yang lebih spesifik (misalnya, kelemahan logika bisnis di Aplikasi inDrive).

5) Analisis Korelasi

Untuk mengeksplorasi hubungan antara kesadaran keamanan pengguna dan praktik keamanan yang mereka laporkan, analisis korelasi dilakukan. Tabel berikut ini menyajikan koefisien korelasi antara variabel-variabel utama.

Tabel 6: Koefisien Korelasi Antara Metrik Keamanan

Variables Compared	Correlation Coefficient	Interpretation
Awareness vs. Frequency of Updates	0.65	Higher awareness correlates with more frequent security updates.
Awareness vs. Attack Experience	-0.45	Users who experienced attacks tend to report lower awareness.
Vulnerability Score vs. Security Awareness	-0.52	Increased vulnerability is moderately associated with lower security awareness.

Korelasi ini menunjukkan bahwa meningkatkan kesadaran keamanan dapat mengarah pada peningkatan praktik keamanan dan mengurangi kerentanan.

B. Pembahasan

Analisis data memberikan wawasan berharga tentang lanskap keamanan aplikasi web seperti yang diamati melalui pengujian penetrasi dan persepsi pengguna. Poin-poin penting meliputi:

- **Validasi Instrumen:**
  Uji reliabilitas dan validitas mengkonfirmasi bahwa sebagian besar item kuesioner kuat; namun, beberapa item (terutama Q7-Q10) tidak memenuhi ambang batas validitas dan harus disempurnakan dalam iterasi penelitian berikutnya.
- **Wawasan Deskriptif:**
  Statistik deskriptif mengungkapkan bahwa meskipun skor kerentanan rata-rata sedang, sejumlah besar aplikasi masih memiliki beberapa kelemahan keamanan. Demikian pula, meskipun sebagian besar responden menunjukkan tingkat kesadaran keamanan yang moderat, masih ada ruang untuk perbaikan.
- **Kategorisasi Risiko:**
  Tabel kategorisasi menyoroti bahwa sebagian besar aplikasi web termasuk dalam kategori risiko rendah hingga sedang. Namun, bahkan sebagian kecil dari kategori risiko tinggi dapat memiliki implikasi yang parah, terutama untuk aplikasi dunia nyata seperti Aplikasi inDrive, di mana satu kesalahan logika bisnis dapat mengakibatkan kerugian finansial dan kerusakan reputasi yang signifikan.
- **Hasil Pengujian Penetrasi:**
  Temuan kerentanan di berbagai aplikasi menggarisbawahi perlunya pengujian penetrasi yang teratur dan komprehensif. Aplikasi yang rentan secara sengaja berfungsi sebagai tolok ukur untuk mengidentifikasi kerentanan umum, sedangkan pengujian target dunia nyata menunjukkan risiko yang terfokus-seperti masalah logika bisnis-yang mungkin tidak terlihat jelas dalam lingkungan simulasi.

- **Korelasi Antara Kesadaran dan Praktik:**
  Analisis korelasi mendukung hipotesis bahwa peningkatan kesadaran keamanan dikaitkan dengan pembaruan yang lebih sering dan berkurangnya kerentanan. Temuan ini menekankan perlunya pelatihan keamanan berkelanjutan dan integrasi alat otomatis (misalnya, OWASP ZAP, Burp Suite) selama siklus pengembangan untuk mencegah kerentanan.

V. Kesimpulan dan Saran

Kesimpulan

Penelitian ini telah menunjukkan bahwa pendekatan yang komprehensif-mengintegrasikan pengujian penetrasi otomatis dengan survei yang berpusat pada pengguna-memberikan wawasan yang mendalam tentang postur keamanan aplikasi web. Kesimpulan utama dari penelitian ini meliputi:

- **Kerentanan yang Masih Ada:**
  Meskipun tingkat kesadaran keamanan sedang hingga tinggi di antara para responden, kerentanan kritis seperti injeksi SQL, Cross-Site Scripting (XSS), Pemalsuan Permintaan Lintas Situs (CSRF), otentikasi yang tidak aman, dan kelemahan logika bisnis tetap ada. Misalnya, aplikasi inDrive menunjukkan kerentanan logika bisnis yang signifikan yang dapat menyebabkan implikasi keuangan yang parah jika dieksploitasi.
- **Efektivitas Alat Otomatis:**
  Alat-alat seperti OWASP ZAP, Burp Suite, dan Nmap terbukti sangat efektif dalam mengidentifikasi beragam kerentanan. Penggunaannya, dikombinasikan dengan teknik pengujian manual seperti fuzzing, menyoroti kelemahan keamanan yang umum dan unik di berbagai jenis aplikasi web.
- **Korelasi Antara Kesadaran dan Praktik:**
  Analisis statistik menunjukkan bahwa kesadaran keamanan yang lebih tinggi berkorelasi dengan pembaruan aplikasi yang lebih sering. Namun, pengguna yang mengalami serangan cenderung memiliki tingkat kesadaran yang lebih rendah, menunjukkan bahwa pengalaman saja tidak menjamin penerapan praktik keamanan terbaik.
- **Wawasan Studi Kasus:**
  Penyertaan aplikasi web yang rentan secara sengaja (OWASP Juice Shop, DVWA, dan WebGoat) bersama dengan target dunia nyata (aplikasi inDrive dan Aplikasi Web Universitas) memberikan perspektif yang seimbang. Pendekatan ganda ini menggarisbawahi pentingnya pengujian keamanan proaktif dan langkah-langkah keamanan reaktif.

Saran untuk Penelitian dan Praktik di Masa Depan

Berdasarkan temuan-temuan tersebut, beberapa rekomendasi dapat dibuat untuk meningkatkan keamanan aplikasi web:

1. **Melembagakan Pengujian Penetrasi Berkelanjutan:**
   - Audit keamanan rutin harus diintegrasikan ke dalam siklus pengembangan perangkat lunak.
   - Pemindaian kerentanan otomatis harus dikombinasikan dengan pengujian manual untuk mencakup spektrum yang lebih luas dari potensi kelemahan.
2. **Meningkatkan Pelatihan Pengembang dan Pengguna:**
   - Organisasi harus berinvestasi dalam pelatihan keamanan yang berkelanjutan untuk pengembang dan profesional TI, dengan fokus pada praktik pengkodean yang aman, identifikasi kerentanan, dan teknik remediasi.
   - Kampanye kesadaran pengguna harus disesuaikan untuk menjembatani kesenjangan antara pengetahuan teoritis dan langkah-langkah keamanan praktis.
3. **Mengintegrasikan Alat Keamanan Otomatis ke dalam Pipeline CI/CD:**

- Menanamkan alat seperti OWASP ZAP dan Burp Suite ke dalam pipeline continuous integration/continuous deployment (CI/CD) dapat membantu mendeteksi dan memulihkan kerentanan di awal proses pengembangan.
- Pembaruan rutin dari alat-alat ini sangat penting untuk memastikan mereka dapat mengidentifikasi ancaman yang muncul.

4. **Mengembangkan Rencana Respons Insiden yang Kuat:**
   - Jika terjadi pelanggaran keamanan, strategi respons insiden yang terdefinisi dengan baik dapat meminimalkan kerusakan.
   - Latihan rutin dan pembaruan rencana respons akan memastikan bahwa tim tetap siap menghadapi serangan di dunia nyata.
5. **Memperkuat Kontrol Logika Bisnis:**
   - Perhatian khusus harus diberikan pada kerentanan logika bisnis, karena dapat berdampak langsung pada keuangan.
   - Menerapkan validasi sisi server dan pemeriksaan integritas dapat mengurangi risiko yang terkait dengan manipulasi harga dan kelemahan serupa.
6. **Arah Penelitian di Masa Depan:**
   - Studi perbandingan antara metode pengujian penetrasi otomatis dan manual dapat menyempurnakan praktik terbaik.
   - Penelitian terhadap teknologi yang sedang berkembang (seperti alat penilaian kerentanan berbasis AI) dapat memberikan jalan baru untuk meningkatkan keamanan aplikasi web.

VI. Referensi

1. **Stuttard, D., & Pinto, M. (2011).** *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.* Wiley.
   Wiley Link
2. **Weidman, G. (2014).** *Penetration Testing: A Hands-On Introduction to Hacking.*
3. **OWASP Foundation. (2020).** *OWASP Testing Guide v4.* OWASP.
   OWASP Testing Guide v4
4. **OWASP Foundation. (2017).** *OWASP Top 10 – 2017: The Ten Most Critical Web Application Security Risks.* OWASP.
   OWASP Top 10 – 2017
5. **Engebretson, P. (2007).** *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Syngress.
   Elsevier Link
6. **O'Connor, T., & O'Gorman, L. (2016).** *A Comprehensive Analysis of Web Application Vulnerabilities: The Role of Automated Penetration Testing.* International Journal of Computer Science and Information Security, 14(3), 1-10.
   IJCSIS Journal *(search within the site for the article title if a direct link is unavailable)*
7. **Kim, D., & Lee, J. (2019).** *Web Application Security: Identifying and Mitigating Threats in Real-World Applications.* Journal of Information Security, 8(2), 88-101.
   Journal of Information Security *(use the journal's search feature for the article)*
8. **Gollmann, D. (2011).** *Computer Security.* Wiley.
   Wiley Link
9. **Mishra, D., & Kumar, A. (2018).** *Security Vulnerabilities in Web Applications: A Survey of Common Pitfalls and Solutions.* International Journal of Computer Applications, 180(31), 12-17.
   IJCA Link *(navigate to the article through the archives)*
10. **Nmap Project. (2021).** *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning.* Nmap.
    Nmap Book

11. **sqlmap Project. (2022).** *sqlmap – Automated SQL Injection Tool.* GitHub repository. sqlmap GitHub
12. **Hydra Project. (2021).** *THC Hydra: The Fast Network Login Cracker.* GitHub repository. Hydra GitHub
13. **XSStrike Project. (2017).** *XSStrike – Automated XSS Scanner.* GitHub repository. XSStrike GitHub
14. **Burp Suite Community Edition. (2022).** *PortSwigger Web Security.* Burp Suite Link
15. **OWASP ZAP Project. (2022).** *OWASP ZAP: The Zed Attack Proxy.* OWASP. OWASP ZAP
16. **Stallings, W., & Lawrie, S. (2017).** *Foundations of Cybersecurity: Principles and Practice.* Prentice Hall. Pearson Link
17. **Souppaya, M., & Scarfone, K. (2013).** *Guide to Malware Incident Prevention and Handling for Desktops and Laptops.* NIST Special Publication 800-83. NIST SP 800-83 PDF
18. **Cole, E. (2008).** *Advanced Penetration Testing: Hacking the World's Most Secure Networks.* Wiley. Wiley Link