

Nama : Aryadil Diangka  
NIM : 20210801179  
Mata Kuliah : Keamanan Informasi  
Hari/tanggal : Selasa, 22 Juli 2025

1. Studi Kasus : Manajemen Inventaris Kantor Dalam Memonitoring Aset dan Peminjaman Barang.

PT Zirru adalah sebuah Perusahaan swasta yang bergerak di bidang layanan teknologi dan memiliki banyak aset fisik berupa peralatan kantor seperti komputer, printer, meja dan perangkat pendukung lainnya. Selama ini, proses pengelolaan inventaris dan peminjaman barang dilakukan secara manual menggunakan kertas atau file excel. Peminjaman tersebut kerap kali menimbulkan masalah seperti data aset yang tidak akurat, sulit menelusuri Riwayat peminjaman barang, dan keterlambatan pembuatan laporan aset yang mengakibatkan efisiensi manajemen data aset menurun, pengeluaran anggaran berlebih dan pengambilan keputusan menjadi kurang tepat oleh bagian administrasi. Sehingga PT Zirru membutuhkan sistem berbasis web yang dapat membantu admin kantor dalam mengelola dan memantau seluruh barang yang tersedia, dipinjam, dan barang rusak.

Analisis Studi Kasus

Kebutuhan fungsional

- a. Manajemen data barang
  - Sistem dapat mencatat data barang inventaris yang dapat diedit, dihapus dan ditambahkan.
  - Sistem dapat menampilkan status barang yang aktif, sedang dipinjam dan rusak.
- b. Peminjaman Barang
  - Sistem dapat mencatat peminjaman barang oleh karyawan
  - Sistem dapat menyimpan Riwayat pinjaman
  - Sistem dapat memperbarui status pinjaman
  - Sistem dapat mencegah peminjaman barang yang statusnya sedang dipinjam.
- c. Laporan
  - Sistem dapat menampilkan seluruh barang.
  - Sistem dapat menampilkan laporan barang per kondisi dan lokasi.
  - Sistem dapat menampilkan Riwayat peminjaman

Kebutuhan nonfungsional

- a. Keamanan
  - Sistem harus melindungi data barang untuk menghindari manipulasi data asset kantor agar jumlah dan status data barang tidak dapat diubah.
  - Data login harus dienkripsi dan akses sistem harus dibatasi berdasarkan hak akses.
  - Sistem juga dapat melindungi data karyawan yang sedang meminjam barang.
- b. Performa website

- Sistem harus merespons setiap aksi dalam waktu kurang dari 3 detik pada jaringan local
- c. Ketersediaan
  - Sistem harus dapat diakses selama jam operasional kantor tanpa downtime yang mengganggu.

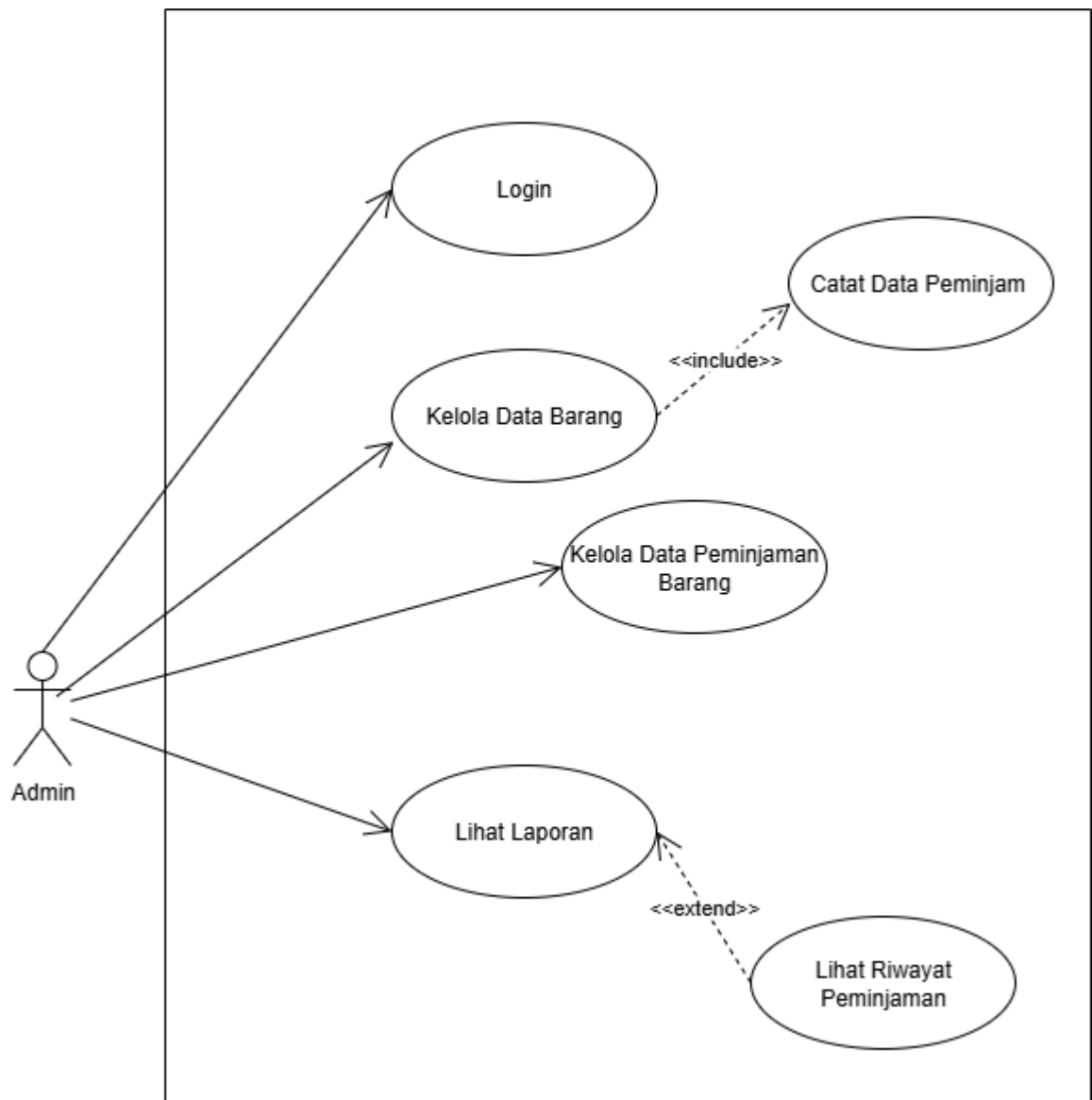
Actor yang terlibat dalam sistem hanyalah admin.

- a. Admin
  - Pengguna utama yang dapat mengelola seluruh data inventaris dan pengguna lain.

Hak akses admin

- a. Mengelola data barang
- b. Mengelola data peminjaman barang
- c. Mengelola laporan aset dan peminjaman
- d. Melihat semua status barang
- e. Lihat data barang berdasarkan lokasi atau kondisi.
- f. Input data peminjam barang
- g. Melihat Riwayat peminjam.

Use Case Diagram



#### Admin

- Aktor Tunggal yang melakukan semua aktivitas sistem dari login, Kelola data barang, data peminjam dan melihat laporan.

#### Login

- Memasukkan username dan password untuk memonitoring aset kantor dan peminjaman barang yang telah disediakan.

#### Kelola data barang

- Admin dapat menambah barang baru, menghapus barang yang tidak digunakan dan mengedit barang.

#### Kelola data peminjaman barang

- Mencatat tanggal pinjam dan Kembali
- Mengubah status barang menjadi dipinjam, telah Kembali dan rusak.

Include catat data peminjam

- Mencatat data peminjam mulai dari nama, nomor telepon dan email.

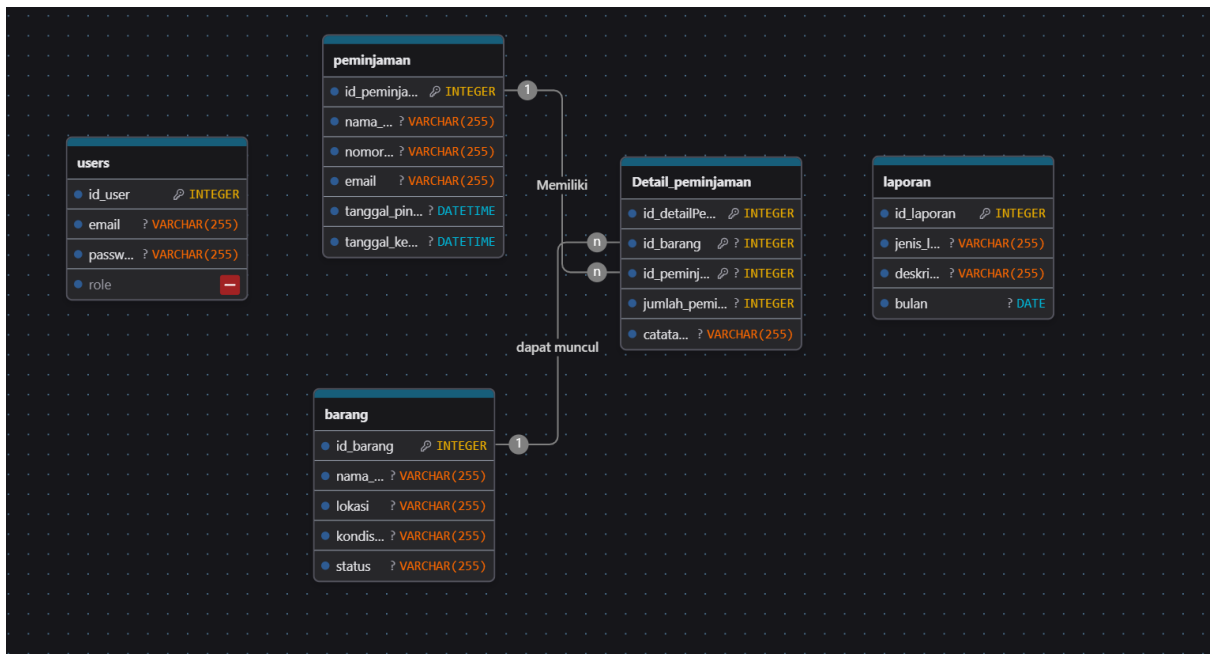
Lihat laporan

- Melihat jumlah barang
- Melihat status barang (aktif, rusak, dipinjam)

Extend lihat Riwayat peminjaman

- Melihat data peminjam barang

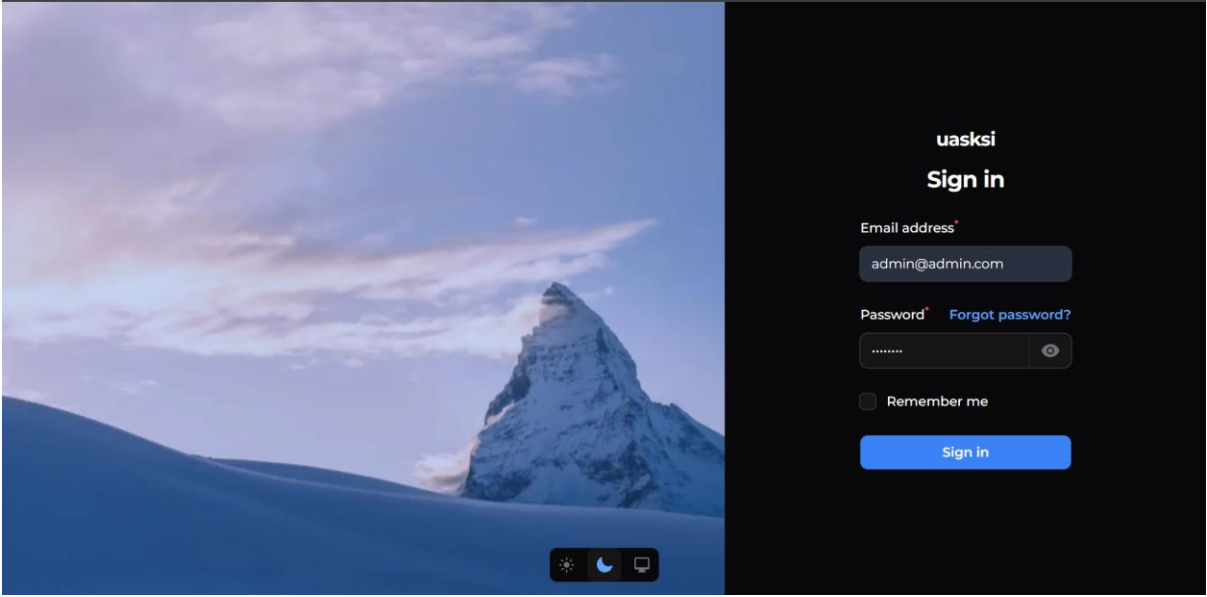
Entity Relationship Diagram



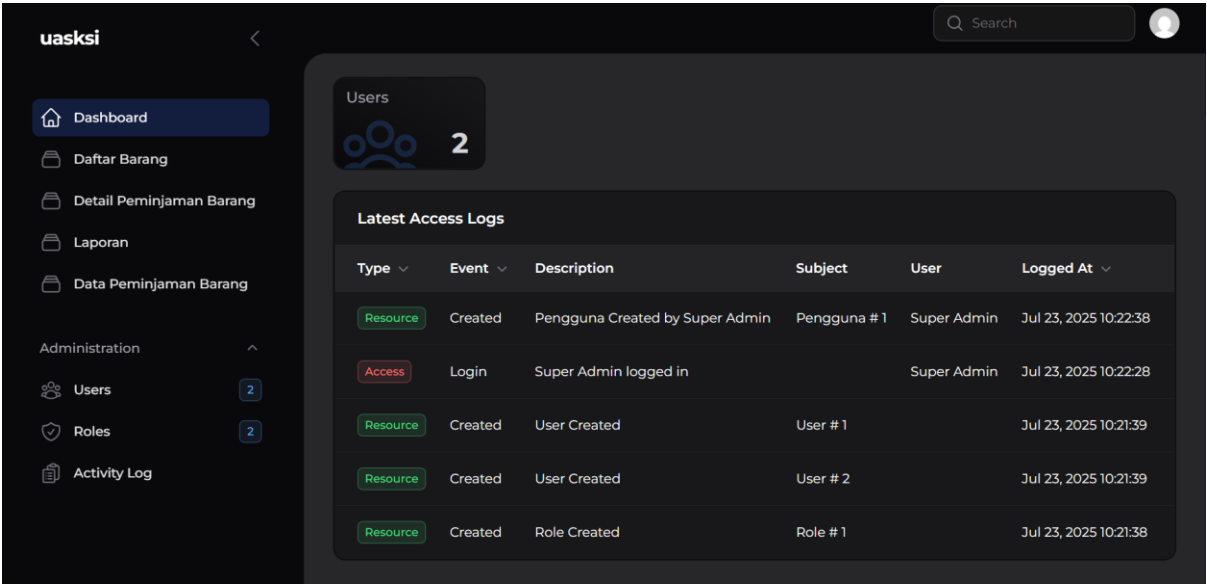
Dari gambar diatas, aplikasi Manajemen Inventaris Kantor Dalam Memonitoring Aset dan Peminjaman Barang memiliki 5 tabel yang terdiri dari *users* (pengguna), *peminjaman*, *barang*, *detail peminjaman* dan *laporan*. Dari tabel diatas memiliki 2 relasi antara *peminjaman* dengan *detail peminjaman* yang berarti satu peminjaman memiliki banyak detail peminjaman sehingga satu peminjam dapat meminjam lebih dari satu barang (*one to many*). Dan relasi antara *barang* dengan *detail peminjaman* yang berarti satu jenis barang dapat muncul di banyak detail barang (*one to many*).

## 2. Aplikasi Manajemen Inventaris Kantor Dalam Memonitoring Aset dan Peminjaman Barang

a. Form Login



b. Dashboard



c. Tabel Daftar Barang

uasksi

Dashboard

Daftar Barang

Detail Peminjaman Barang

Laporan

Data Peminjaman Barang

Administration

Users2

Roles2

Activity Log

Daftar Barang

New daftar barang

Search

<input type="checkbox"/>	Nama barang	Kondisi barang	Status	Total Barang	
<input type="checkbox"/>	Laptop ASUS ROG	baik	aktif	5	<a href="#">Edit</a>
<input type="checkbox"/>	Printer Epson L3110	baik	aktif	2	<a href="#">Edit</a>
<input type="checkbox"/>	Kursi Kantor Ergonomis	baik	aktif	10	<a href="#">Edit</a>
<input type="checkbox"/>	Meja Kerja Kayu	baik	aktif	3	<a href="#">Edit</a>
<input type="checkbox"/>	Proyektor BenQ	baik	hilang	1	<a href="#">Edit</a>

Per page10

d. Form Create & Edit Daftar Barang

uasksi

Dashboard

Daftar Barang

Detail Peminjaman Barang

Laporan

Data Peminjaman Barang

Administration

Users2

Roles2

Activity Log

Daftar Barang > Create

Create Daftar Barang

Nama barang\*

Kondisi barang\*

Status\*

Total Barang\*

Cancel

Create & create another

Create

uasksi

Dashboard

Daftar Barang

Detail Peminjaman Barang

Laporan

Data Peminjaman Barang

Administration

Users2

Daftar Barang > Edit

Edit Daftar Barang

Nama barang\*

Kondisi barang\*

Status\*

Total Barang\*

Cancel

Save changes

Delete

e. Tabel Laporan

Laporan > List

Laporan

New laporan

Q Search

⋮

<input type="checkbox"/>	Periode bulan ▾	Jenis laporan	Deskripsi laporan	
<input type="checkbox"/>	Jul 24, 2025	Laporan Kehilangan	Proyektor BenQ hilang ditelan bumi	<a href="#">Edit</a>

Per page 10 ▾

f. Form Create & Edit Laporan

uasksi

<

Dashboard

Daftar Barang

Detail Peminjaman Barang

Laporan

Data Peminjaman Barang

Administration

Users2

Roles2

Activity Log

Laporan > Create

Create Laporan

Periode bulan\*

dd/mm/yyyy

Jenis laporan\*

Deskripsi laporan\*

Cancel

Create & create another

Create

uasksi

<

Dashboard

Daftar Barang

Detail Peminjaman Barang

Laporan

Data Peminjaman Barang

Administration

Users2

Roles2

Activity Log

Laporan > Edit

Edit Laporan

Periode bulan\*

24/07/2025

Jenis laporan\*

Laporan Kehilangan

Deskripsi laporan\*

Proyektor BenQ hilang ditelan bumi

Cancel

Save changes

Delete

g. Tabel Data Peminjaman Barang

uasksi

Dashboard

Daftar Barang

Detail Peminjaman Barang

Laporan

Data Peminjaman Barang

Administration

Users

2

Roles

2

Activity Log

Data Peminjaman Barang > List

New peminjaman barang

Search

	Nama	Nomor telepon	Email	Tanggal pinjam	Tanggal kembali	
	Aryadil	086564	aryadildiangka24@gmail.com	Jul 23, 2025	Jul 25, 2025	<div>Edit</div>

Per page

10

h. Form Create & Edit Peminjaman Barang

uasksi

Dashboard

Daftar Barang

Detail Peminjaman Barang

Laporan

Data Peminjaman Barang

Administration

Users

2

Roles

2

Activity Log

Data Peminjaman Barang > Create

Create Peminjaman Barang

Nama

Nomor telepon

Email

Tanggal pinjam

dd/mm/yyyy

Tanggal kembali

dd/mm/yyyy

Cancel

Create & create another

Create

uasksi

Dashboard

Daftar Barang

Detail Peminjaman Barang

Laporan

Data Peminjaman Barang

Administration

Users

2

Roles

2

Activity Log

Data Peminjaman Barang > Edit

Edit Peminjaman Barang

Delete

Nama

Aryadil

Nomor telepon

086564

Email

aryadildiangka24@gmail.com

Tanggal pinjam

23/07/2025

Tanggal kembali

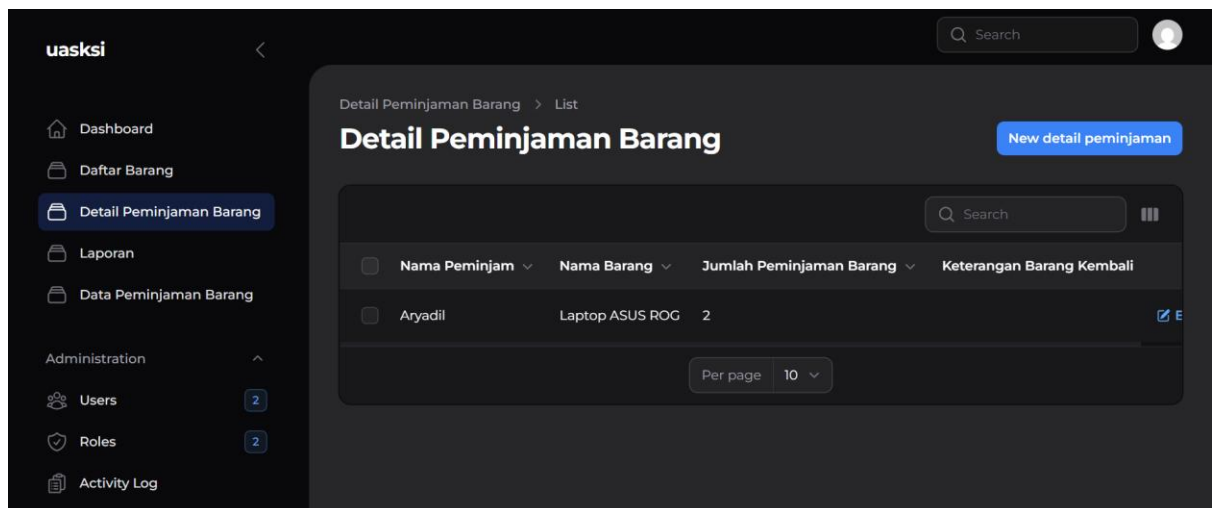
25/07/2025

Cancel

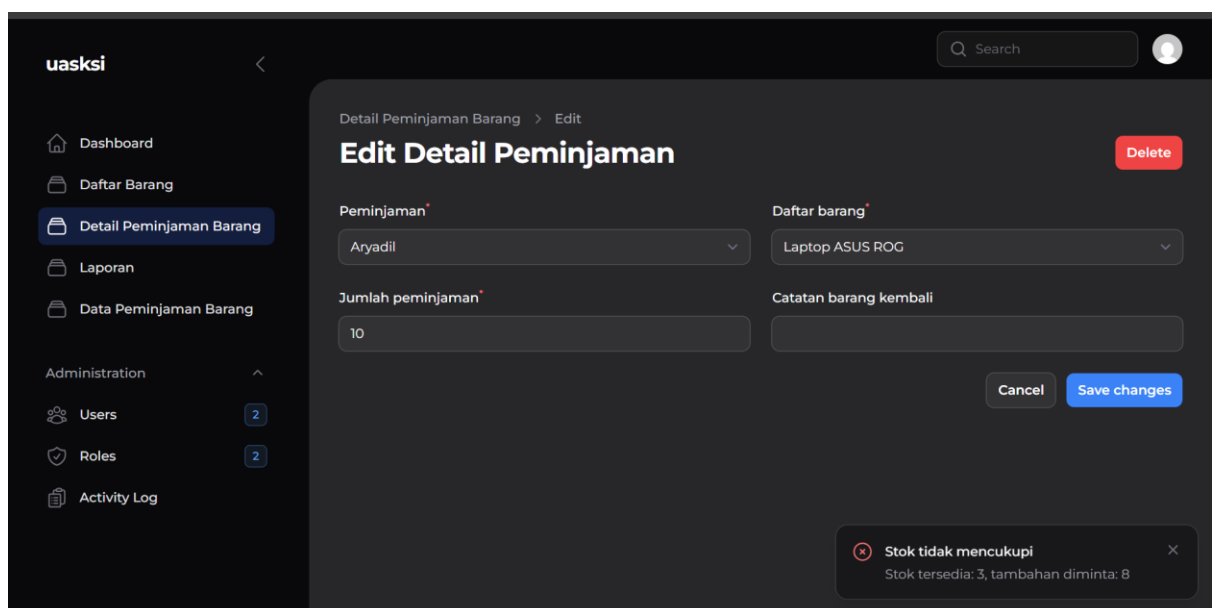
Save changes

i. Tabel Detail Peminjaman Barang





j. Form Create & Edit Detail Peminjaman Barang



uasksi

Dashboard

Daftar Barang

Detail Peminjaman Barang

Laporan

Data Peminjaman Barang

Administration

Users

Roles

Activity Log

Detail Peminjaman Barang > Edit

Edit Detail Peminjaman

Delete

Peminjaman

Aryadil

Daftar barang

Laptop ASUS ROG

Jumlah peminjaman

2

Catatan barang kembali

Cancel

Save changes

k. Tabel dan form edit Users

uasksi

Dashboard

Daftar Barang

Detail Peminjaman Barang

Laporan

Data Peminjaman Barang

Administration

Users

Roles

Activity Log

Users > List

Users

New user

Search

Id	Name	Avatar	Email	Roles	Created at	
1	Super Admin		admin@admin.com	super_admin	Jul 23, 2025	View Edit Delete
2	User Account		user@admin.com	user	Jul 23, 2025	View Edit Delete

Per page 10

uasksi

Dashboard

Daftar Barang

Detail Peminjaman Barang

Laporan

Data Peminjaman Barang

Administration

Users

Roles

Activity Log

Users > Super Admin > Edit

Edit Super Admin

Delete

Name

Super Admin

Avatar

Drag & Drop your files or Browse

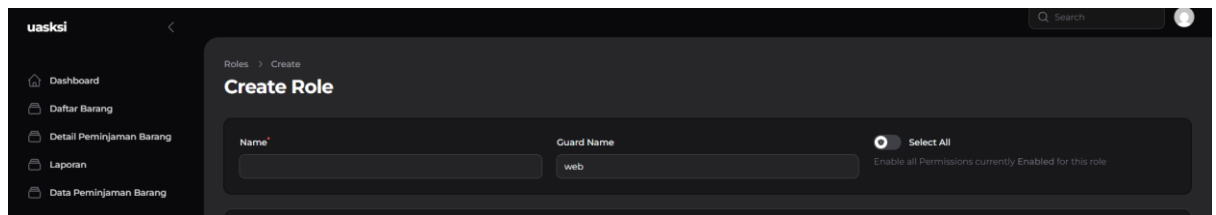
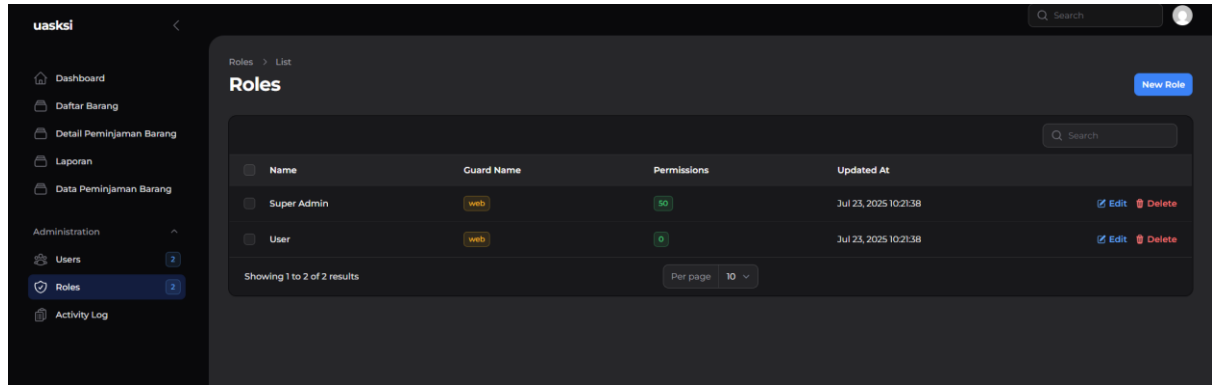
Email

admin@admin.com

Password

Password confirmation

### 1. Form & tabel Role



### 3. Vullnerability Scan

Berikut adalah hasil vulnerability scan terhadap website melalui github ptt website scanner

Vulnerability Scan Report	
<p>[1] Missing security header: X-Content-Type-Options</p> <ul style="list-style-type: none"> <li>- Risk Level: 1 (Low)</li> </ul> <p>Vulnerability Details:</p> <ul style="list-style-type: none"> <li>- Evidence 1: <ul style="list-style-type: none"> <li>- URL: https://politicians-rat-anyone-riders.trycloudflare.com/admin/login</li> <li>- Evidence: Response headers do not include the X-Content-Type-Options HTTP security header Request / Response</li> </ul> </li> <li>- Description: We noticed that the target application's server responses lack the &lt;code&gt;X-Content-Type-Options&lt;/code&gt; header. This header is particularly important for preventing Internet Explorer from misinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header.</li> <li>- Recommendation: We recommend setting the X-Content-Type-Options header such as 'X-Content-Type-Options: nosniff'.</li> </ul>	
<p>[2] Missing security header: Content-Security-Policy</p> <ul style="list-style-type: none"> <li>- Risk Level: 1 (Low)</li> </ul> <p>Vulnerability Details:</p> <ul style="list-style-type: none"> <li>- Evidence 1: <ul style="list-style-type: none"> <li>- URL: https://politicians-rat-anyone-riders.trycloudflare.com/admin/login</li> <li>- Evidence: Response does not include the HTTP Content-Security-Policy security header or meta tag Request / Response</li> </ul> </li> <li>- Description: We noticed that the target application lacks the Content-Security-Policy (CSP) header in its HTTP responses. The CSP header is a security measure that instructs web browsers to enforce specific security rules, effectively preventing the exploitation of Cross-Site Scripting (XSS) vulnerabilities.</li> <li>- Recommendation: Configure the Content-Security-Policy header to be sent with each HTTP response in order to apply the specific policies needed by the application.</li> </ul>	
<p>[3] Missing security header: Strict-Transport-Security</p> <ul style="list-style-type: none"> <li>- Risk Level: 1 (Low)</li> </ul> <p>Vulnerability Details:</p> <ul style="list-style-type: none"> <li>- Evidence 1: <ul style="list-style-type: none"> <li>- URL: https://politicians-rat-anyone-riders.trycloudflare.com/admin/login</li> <li>- Evidence: Response headers do not include the HTTP Strict-Transport-Security header Request / Response</li> </ul> </li> <li>- Description: We noticed that the target application lacks the HTTP Strict-Transport-Security header in its responses. This security header is crucial as it instructs browsers to only establish secure (HTTPS) connections with the web server and reject any HTTP connections.</li> <li>- Recommendation: The Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows: 'Strict-Transport-Security: max-age=&lt;seconds&gt;[; includeSubDomains]' The parameter 'max-age' gives the time frame for requirement of HTTPS in seconds and should be chosen quite high, e.g. several months. A value below 7776000 is considered as too low by this scanner check. The flag 'includeSubDomains' defines that the policy applies also for sub domains of the sender of the response.</li> </ul>	
<p>[4] Missing security header: Referrer-Policy</p> <ul style="list-style-type: none"> <li>- Risk Level: 1 (Low)</li> </ul> <p>Vulnerability Details:</p> <ul style="list-style-type: none"> <li>- Evidence 1: <ul style="list-style-type: none"> <li>- URL: https://politicians-rat-anyone-riders.trycloudflare.com/admin/login</li> <li>- Evidence: Response headers do not include the Referrer-Policy HTTP security header as well as the &lt;meta&gt; tag with name 'referrer' is not present in the response. Request / Response</li> </ul> </li> <li>- Description: We noticed that the target application's server responses lack the &lt;code&gt;Referrer-Policy&lt;/code&gt; HTTP header, which controls how much referrer information the browser will send with each request originated from the current web application.</li> <li>- Recommendation: The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value 'no-referrer' of this header instructs the browser to omit the Referrer header entirely.</li> </ul>	
<p>[5] Server software and technology found</p> <ul style="list-style-type: none"> <li>- Risk Level: 1 (Low)</li> </ul> <p>Vulnerability Details:</p> <ul style="list-style-type: none"> <li>- Evidence 1: <ul style="list-style-type: none"> <li>- Software / Version: Alpine.js 3.14.9</li> <li>- Category: JavaScript frameworks</li> </ul> </li> <li>- Evidence 2: <ul style="list-style-type: none"> <li>- Software / Version: Bunny</li> <li>- Category: CDN</li> </ul> </li> <li>- Evidence 3: <ul style="list-style-type: none"> <li>- Software / Version: Filamentphp</li> <li>- Category: Development</li> </ul> </li> <li>- Evidence 4: <ul style="list-style-type: none"> <li>- Software / Version: Bunny Fonts</li> <li>- Category: Font scripts</li> </ul> </li> <li>- Evidence 5: <ul style="list-style-type: none"> <li>- Software / Version: Livewire</li> <li>- Category: Web frameworks, Miscellaneous</li> </ul> </li> <li>- Evidence 6: <ul style="list-style-type: none"> <li>- Software / Version: Laravel</li> <li>- Category: Web frameworks</li> </ul> </li> <li>- Evidence 7: <ul style="list-style-type: none"> <li>- Software / Version: PHP</li> <li>- Category: Programming languages</li> </ul> </li> <li>- Evidence 8: <ul style="list-style-type: none"> <li>- Software / Version: Cloudflare</li> <li>- Category: CDN</li> </ul> </li> <li>- Description: We noticed that server software and technology details are exposed, potentially aiding attackers in tailoring specific exploits against identified systems and versions.</li> <li>- Recommendation: We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.</li> </ul>	
<p>[6] Robots.txt file found</p> <ul style="list-style-type: none"> <li>- Risk Level: 1 (Low)</li> </ul> <p>Vulnerability Details:</p> <ul style="list-style-type: none"> <li>- Evidence 1: <ul style="list-style-type: none"> <li>- URL: https://politicians-rat-anyone-riders.trycloudflare.com/robots.txt</li> </ul> </li> <li>- Description: We found the robots.txt on the target server. This file instructs web crawlers what URLs and endpoints of the web application they can visit and crawl. Website administrators often misuse this file while attempting to hide some web pages from the users.</li> <li>- Recommendation: We recommend you to manually review the entries from robots.txt and remove the ones which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).</li> </ul>	
<p>[7] Login Interface Found</p> <ul style="list-style-type: none"> <li>- Risk Level: 0 (Info)</li> </ul> <p>Vulnerability Details:</p> <ul style="list-style-type: none"> <li>- Evidence 1: <ul style="list-style-type: none"> <li>- URL: https://politicians-rat-anyone-riders.trycloudflare.com/admin/login</li> <li>- Evidence: &lt;input autocomplete="on" autofocus="autofocus" class="fi-input block w-full border-none py-1.5 text-base text-gray-950 transition duration-75 placeholder:text-gray-400 focus:ring-0 disabled:text-gray-500 disabled:[-webkit-text-fill-color:theme(colors.gray.500)] disabled:placeholder:[-webkit-text-fill-color:theme(colors.gray.400)] dark:text-white dark:placeholder:text-gray-500 dark:disabled:text-gray-400 dark:disabled:[-webkit-text-fill-color:theme(colors.gray.400)] dark:disabled:placeholder:[-webkit-text-fill-color:theme(colors.gray.500)] sm:text-sm sm:leading-6 lg:white/0 ps-3 pe-3" id="data_email" required="required" tabindex="1" type="email" wire:model="data_email"/&gt; &lt;input autocomplete="current-password" class="fi-input block w-full border-none py-1.5 text-base text-gray-950 transition duration-75 placeholder:text-gray-400 focus:ring-0 disabled:text-gray-500 disabled:[-webkit-text-fill-color:theme(colors.gray.500)] disabled:placeholder:[-webkit-text-fill-color:theme(colors.gray.400)] dark:text-white dark:placeholder:text-gray-500 dark:disabled:text-gray-400 dark:disabled:[-webkit-text-fill-color:theme(colors.gray.400)] dark:disabled:placeholder:[-webkit-text-fill-color:theme(colors.gray.500)] sm:text-sm sm:leading-6 lg:white/0 ps-3 pe-3" id="data_password" required="required" tabindex="2" wire:model="data_password" &gt;-bind: type="password" isPasswordRevealed ? 'text' : 'password'"/&gt; &lt;button class="fi-btn relative grid-flow-col items-center justify-center font-semibold outline-none transition duration-75 focus-visible:ring-2 rounded-lg fi-color-cust... (truncated)" Request / Response</li> </ul> </li> <li>- Description: We have discovered that the target application presents a login interface that could be a potential target for attacks. While login interfaces are standard for user authentication, they can become vulnerabilities if not properly secured.</li> <li>- Recommendation: Ensure each interface is not bypassable using common knowledge of the application or leaked credentials using occasional password audits.</li> </ul>	
<p>[8] Security.txt file is missing</p> <ul style="list-style-type: none"> <li>- Risk Level: 0 (Info)</li> </ul> <p>Vulnerability Details:</p> <ul style="list-style-type: none"> <li>- Evidence 1: <ul style="list-style-type: none"> <li>- URL: Missing: https://politicians-rat-anyone-riders.trycloudflare.com/.well-known/security.txt</li> </ul> </li> <li>- Description: We have noticed that the server is missing the security.txt file, which is considered a good practice for web security. It provides a standardized way for security researchers and the public to report security vulnerabilities or concerns by outlining the preferred method of contact and reporting procedures.</li> <li>- Recommendation: We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.</li> </ul>	

Hasil pemindaian keamanan menunjukkan bahwa beberapa header penting belum dikonfigurasi pada aplikasi web.

1. Header seperti Strict-Transport-Security, Content-Security-Policy, X-Content-Type-Options, dan Referrer-Policy tidak ditemukan dalam respons server. Ketiadaan header-header ini dapat membuka peluang terhadap risiko serangan seperti XSS (Cross-Site Scripting), sniffing MIME type, atau kebocoran informasi referer.
2. Selain itu, informasi mengenai perangkat lunak dan teknologi (server software and technology) yang digunakan oleh server masih terlihat secara publik, termasuk framework dan bahasa pemrograman. Hal ini dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk mengidentifikasi potensi celah keamanan yang spesifik.
3. File robots.txt juga ditemukan, dapat berisiko jika digunakan untuk menyembunyikan direktori atau halaman sensitif.
4. Antarmuka login terdeteksi sebagai bagian dari sistem dan dapat menjadi target eksploitasi jika tidak dilindungi dengan benar.
5. file security.txt yang tidak ditemukan, file security.txt merupakan standar yang memungkinkan peneliti keamanan melaporkan kerentanan dengan cara yang tepat. Terakhir, metode HTTP OPTIONS masih diaktifkan, yang dapat memberikan informasi tambahan kepada penyerang potensial mengenai metode HTTP yang diizinkan oleh server.

```
[9] HTTP OPTIONS enabled
    - Risk Level: 0 (Info)

Vulnerability Details:
- We did a HTTP OPTIONS request. The server responded with a 200 status code and the header: 'Allow: GET,HEAD' Request / Response:
  - URL: https://politicians-rat-anyone-riders.trycloudflare.com/admin/login
  - Method: OPTIONS

- Description: We have noticed that the webserver responded with an Allow HTTP header when an OPTIONS HTTP request was sent. This method responds to requests by providing information about the methods available for the target resource.
- Recommendation: We recommend that you check for unused HTTP methods or even better, disable the OPTIONS method. This can be done using your webserver configuration.

[10] Website is accessible.
[11] Nothing was found for vulnerabilities of server-side software.
[12] Nothing was found for client access policies.
[13] Nothing was found for use of untrusted certificates.
[14] Nothing was found for enabled HTTP debug methods.
[15] Nothing was found for secure communication.
[16] Nothing was found for directory listing.
[17] Nothing was found for passwords submitted unencrypted.
[18] Nothing was found for error messages.
[19] Nothing was found for debug messages.
[20] Nothing was found for code comments.
[21] Nothing was found for passwords submitted in URLs.
[22] Nothing was found for domain too loose set for cookies.
[23] Nothing was found for mixed content between HTTP and HTTPS.
[24] Nothing was found for cross domain file inclusion.
[25] Nothing was found for internal error code.
[26] Nothing was found for HttpOnly flag of cookie.
[27] Nothing was found for Secure flag of cookie.
[28] Nothing was found for secure password submission.
[29] Nothing was found for sensitive data.
[30] Nothing was found for unsafe HTTP header Content Security Policy.
[31] Nothing was found for OpenAPI files.
[32] Nothing was found for file upload.
[33] Nothing was found for SQL statement in request parameter.
[34] Nothing was found for password returned in later response.
[35] Nothing was found for Path Disclosure.
[36] Nothing was found for Session Token in URL.
[37] Nothing was found for API endpoints.
[38] Nothing was found for emails.
[39] Nothing was found for missing HTTP header - Rate Limit.
```

```
+----- TEST summary -----+
|
| URL: https://politicians-rat-anyone-riders.trycloudflare.com/admin/login|
| High Risk Findings: 0
| Medium Risk Findings: 0
| Low Risk Findings: 6
| Info Risk Findings: 33
| Start time: 2025-07-23 09:55:00
| End time: 2025-07-23 09:55:34
|
+-----+

→ ptt git:(main) cloudflared tunnel --url https://uasksi.test:443 --no-tls-verify
2025-07-23T06:53:58Z INF Thank you for trying Cloudflare Tunnel. Doing so, without a Cloudflare account, is a quick way to e
xperiment and try it out. However, be aware that these account-less Tunnels have no uptime guarantee, are subject to the Clo
udflare Online Services Terms of Use (https://www.cloudflare.com/website-terms/), and Cloudflare reserves the right to inves
tigate your use of Tunnels for violations of such terms. If you intend to use Tunnels in production you should use a pre-cre
ated named tunnel by following: https://developers.cloudflare.com/cloudflare-one/connections/connect-apps
2025-07-23T06:53:58Z INF Requesting new quick Tunnel on trycloudflare.com...
2025-07-23T06:54:03Z INF +-----+
2025-07-23T06:54:03Z INF | Your quick Tunnel has been created! Visit it at (it may take some time to be reachable): |
2025-07-23T06:54:03Z INF | https://politicians-rat-anyone-riders.trycloudflare.com |
2025-07-23T06:54:03Z INF +-----+
```

Sementara itu, Hasil pemindaian menunjukkan bahwa secara umum aplikasi web telah memenuhi sebagian besar standar keamanan dasar. Tidak ditemukan kerentanan yang berkaitan dengan perangkat lunak sisi server, kebijakan akses klien, sertifikat yang tidak terpercaya, metode debug HTTP yang aktif, maupun komunikasi yang tidak aman. Selain itu, tidak ada informasi sensitif seperti password yang dikirim tanpa enkripsi, error message yang terbuka, komentar kode, atau data sensitif lainnya yang terdeteksi dalam respons.

#### 4. Pengamanan data

Melakukan pengamanan data melalui model untuk membantu mencegah serangan Mass Assignment, di mana penyerang bisa mencoba mengisi kolom yang seharusnya tidak bisa diisi. Kemudian Menggunakan Eloquent seperti `DaftarBarang::create()` atau `update()` secara tidak langsung membantu mencegah serangan SQL Injection, karena Eloquent menggunakan *prepared statements* secara default.

```
class DaftarBarang extends Model
{
    protected $fillable=[
        'nama_barang', 'kondisi_barang', 'kondisi', 'status', 'jumlah'
    ];

    public function DetailPeminjaman(){
        $this->hasMany(DetailPeminjaman::class, 'id_barang');
    }
}
```

```
class DaftarBarangController extends Controller
{
    public function store(Request $request)
    {
        $validated = $request->validate([
            'nama_barang' => 'required|string|max:255',
            'kondisi_barang' => 'required|in:baik,rusak,servis',
            'status' => 'required|in:aktif,dipinjam,hilang,rusak',
            'jumlah' => 'required|integer|min:0',
        ]);

        DaftarBarang::create($validated);

        return response()->json(['message' => 'Barang berhasil ditambahkan']);
    }
}
```