

Mata Kuliah: CIE406 – Keamanan Informasi

<b>Dosen</b>	: 7800 – Dr. Hani Dewi Ariessanti S.Kom, M.Kom	
<b>Mahasiswa</b>	: Jiwanta Nabhan Alauddin	
<b>NIM</b>	: 20230801384	
<b>Hari</b>	: Selasa	Waktu : 24 Jam
<b>Tanggal</b>	: 22 Juli 2025	Seksi : KJ003
<b>Sifat Ujian</b>	: Take Home	

Solusi Pada Soal Studi Kasus:

1. Buatlah analisisnya dengan kasus yang anda tentukan sendiri, solusi:

Dikarenakan pada praktikum semester lalu saya terdapat website penggajian karyawan, maka saya akan menggunakannya untuk studi kasus ini, yang Di mana saya merubah datanya yang berfokus pada basic salary (gaji) si karyawan dan admin dalam pembuatan data gaji. Berikut ini dasar kodingan pada data yang akan dikembangkan:

Entitas	Kolom kunci	Relasi utama	Fungsi	Entitas	Kolom kunci	Relasi utama
<b>users</b>	id (PK)	1 : 1 <b>user_profiles</b> 1 : N → <b>staff_salaries</b> , <b>attendances</b> , <b>leaves</b>	Identitas karyawan & kredensial login	<b>users</b>	id (PK)	1 : 1 <b>user_profiles</b> 1 : N → <b>staff_salaries</b> , <b>attendances</b> , <b>leaves</b>
<b>user_profiles</b>	user_id (PK & FK)	1 : 1 ← <b>users</b>	Data bio + jabatan, departemen, foto	<b>user_profiles</b>	user_id (PK & FK)	1 : 1 ← <b>users</b>
<b>departments</b>	id	1 : N ← <b>user_profiles</b>	Mengelompokkan karyawan	<b>departments</b>	id	1 : N <b>user_profiles</b> ←

**Inti hubungan:**

`users.id` dengan `staff_salaries.user_id`

Setiap karyawan hanya *seharusnya* punya **satu** baris di `staff_salaries`. Tabel lain (`attendance`, `leave`) ikut menunjang payroll—mis. script perhitungan gaji bisa:

Struktur file phpnya:

Tabel	Kolom utama terkait gaji	Catatan
<b>staff_salaries</b>	<code>salary</code> , <code>basic</code> , <code>da</code> , <code>hra</code> , <code>conveyance</code> , <code>allowance</code> , <code>medical_allowance</code> , <code>tds</code> , <code>esi</code> , <code>pf</code> , <code>leave</code> , <code>prof_tax</code> , <code>labour_welfare</code> , <code>user_id</code>	Satu baris per karyawan (relasi ke <code>users.user_id</code> ). Semua kolom disimpan sebagai <b>string</b> , bukan decimal.
<b>users</b>	<code>user_id</code> , <code>name</code> , <code>email</code> , <code>dsb.</code>	Identitas karyawan.

**Lapisan aplikasinya:**

File / Kelas	Fungsi kunci
<code>app/Models/StaffSalary.php</code>	Model Eloquent; \$fillable sesuai kolom di atas.
<code>app/Http/Controllers/PayrollController.php</code>	<code>salary()</code> - menampilkan daftar & form gaji. <code>saveRecord()</code> / <code>updateRecord()</code> - validasi

	lalu simpan ke <b>staff_salaries.deleteRecord()</b> - hapus gaji.reportPdf() / reportExcel() - ekspor laporan per karyawan.
app/Exports/SalaryExcel.php + resources/views/report_template/salary_excel.blade.php	Menyusun file .xlsx via Maatwebsite Excel.
resources/views/payroll/*.blade.php	UI input / daftar gaji, termasuk modal “Add Staff Salary”.

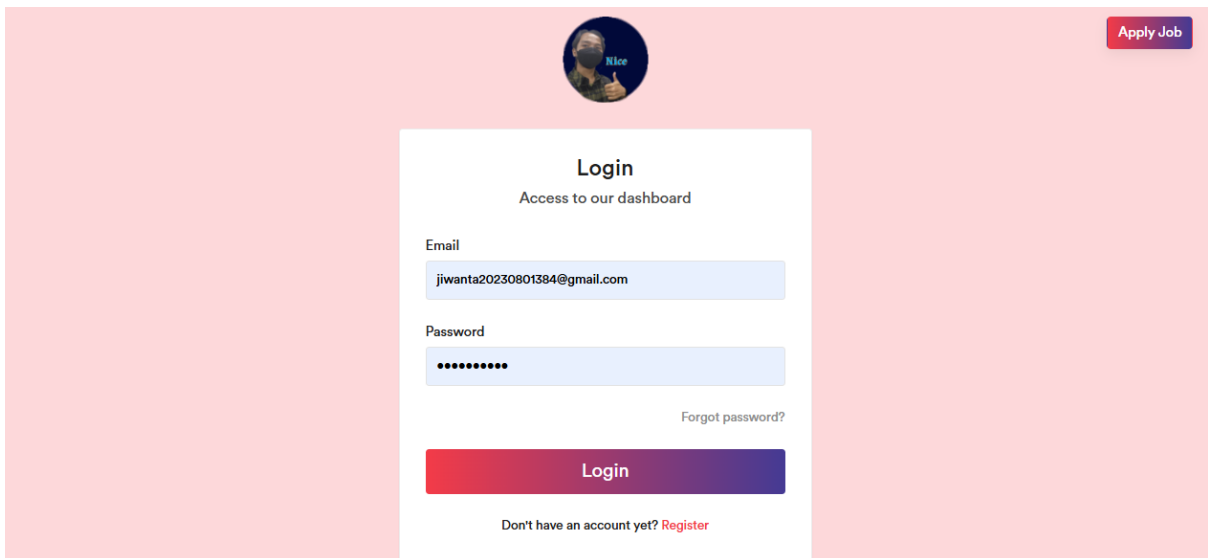
### Alur kerja “Employee Salary”

1. **HR/Admin** buka menu **Payroll** → **Salary**
2. Form “Add Staff Salary” memuat daftar karyawan (select) dan semua komponen gaji.
3. Nilai disimpan ke **staff\_salaries**. Jika record sudah ada, **updateRecord()** dipakai.
4. Halaman daftar menampilkan kolom-kolom tersebut dan menyediakan tombol PDF/Excel per karyawan.
5. Ekspor memakai view Blade → diunduh sebagai **ReportDetailSalary.pdf/xlsx**.

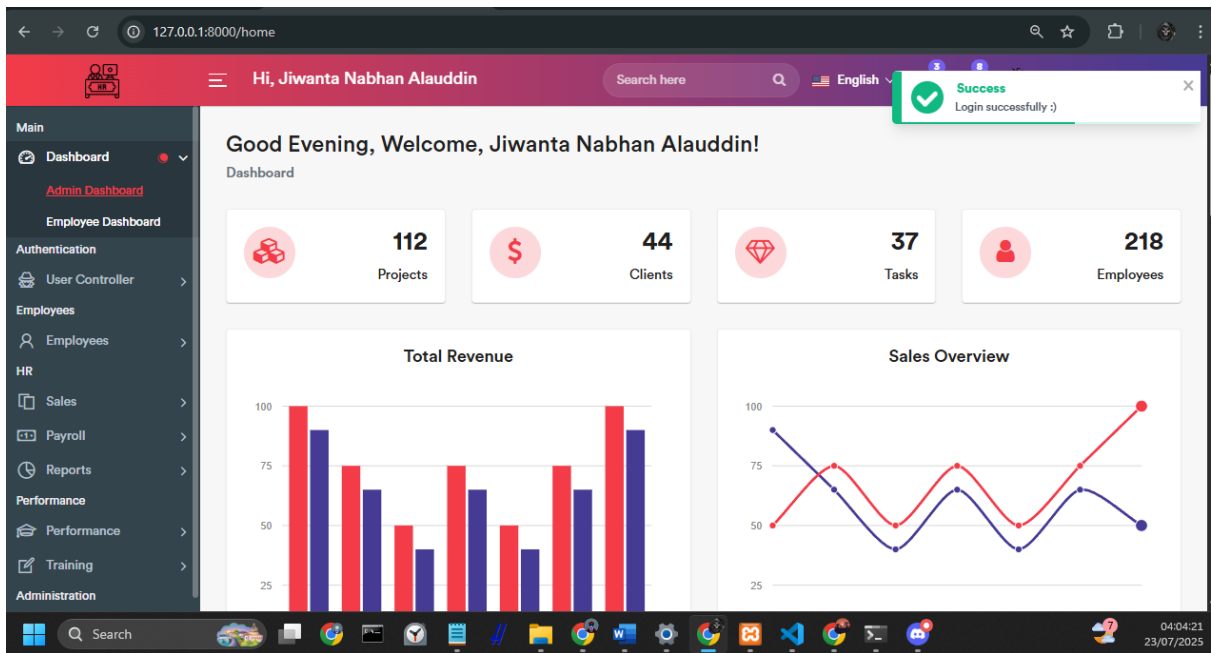
Sehingga hal-hal di atas merupakan dasar dalam pembuatan website, ada pula nanti perkembangan website ke depannya untuk ditambahkan berbagai macam fitur yang berkaitan dengan data kegiatan dari si kepegawaian.

2. Buatlah aplikasinya, solusi:

Maka mulai dari Admin:



Gambar 1. Tampilan Login admin



Gambar 2. Tampilan dashboard admin

The screenshot shows the "Employee Salary" management page. The header bar is identical to the dashboard. The left sidebar highlights the "Payroll" section, with "Employee Salary" selected. The main content area features a "Dashboard / Salary" breadcrumb and an "Add Salary" button. Below this is a search form with fields for "Employee Name", "Role" (a dropdown menu), "Leave Status" (a dropdown menu), "From" (a date picker), and "To" (a date picker), followed by a green "SEARCH" button. A "Show 10 entries" link is present. The table below lists employee salary data with columns: Employee, Employee ID, Email, Join Date, Role, Salary, and Payslip. Two entries are shown: Chandra Sadewa (KH-0003) with a salary of \$208 and Irfan Fharthan (KH-0004) with a salary of \$141. Each entry has a "Generate Slip" button. At the bottom, a pagination bar shows "Showing 1 to 2 of 2 entries" and navigation buttons for "Previous", "1", and "Next". The Windows taskbar at the bottom shows the system clock as 04:06:07 on 23/07/2025.

Employee	Employee ID	Email	Join Date	Role	Salary	Payslip
Chandra Sadewa	KH-0003	googochandra@gmail.com	Tue, Jul 22, 2025 8:01 PM	Employee	\$208	<a href="#">Generate Slip</a>
Irfan Fharthan	KH-0004	lrfans@gmail.com	Tue, Jul 22, 2025 8:29 PM	Employee	\$141	<a href="#">Generate Slip</a>

Gambar 3. Tampilan Admin untuk Employee Salary

**Add Staff Salary**

Select Staff:

Net Salary:

**Earnings**

Basic:

DA(40%):

HRA(15%):

Conveyance:

Allowance:

Medical Allowance:

**Deductions**

TDS:

ESI:

PF:

Leave:

Prof. Tax:

Loan:

**Submit**

Gambar 4. Tampilan admin dalam mengisi gaji karyawan

**Add Staff Salary**

Select Staff:

Net Salary:

**Earnings**

Basic:

DA(40%):

HRA(15%):

Conveyance:

Allowance:

Medical Allowance:

**Deductions**

TDS:

ESI:

PF:

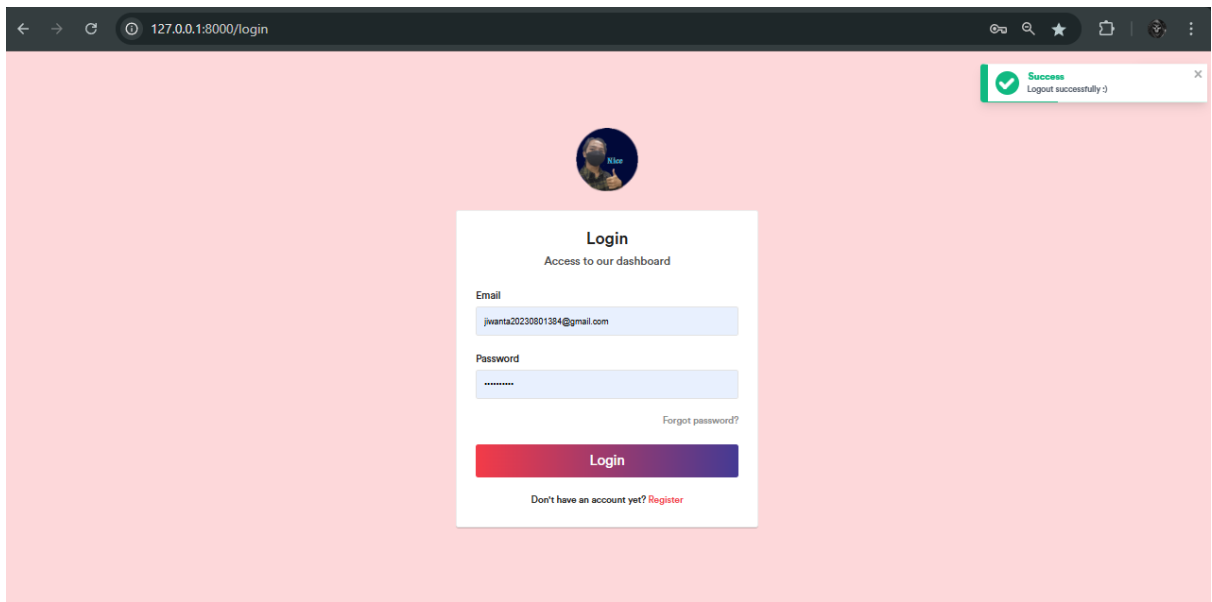
Leave:

Prof. Tax:

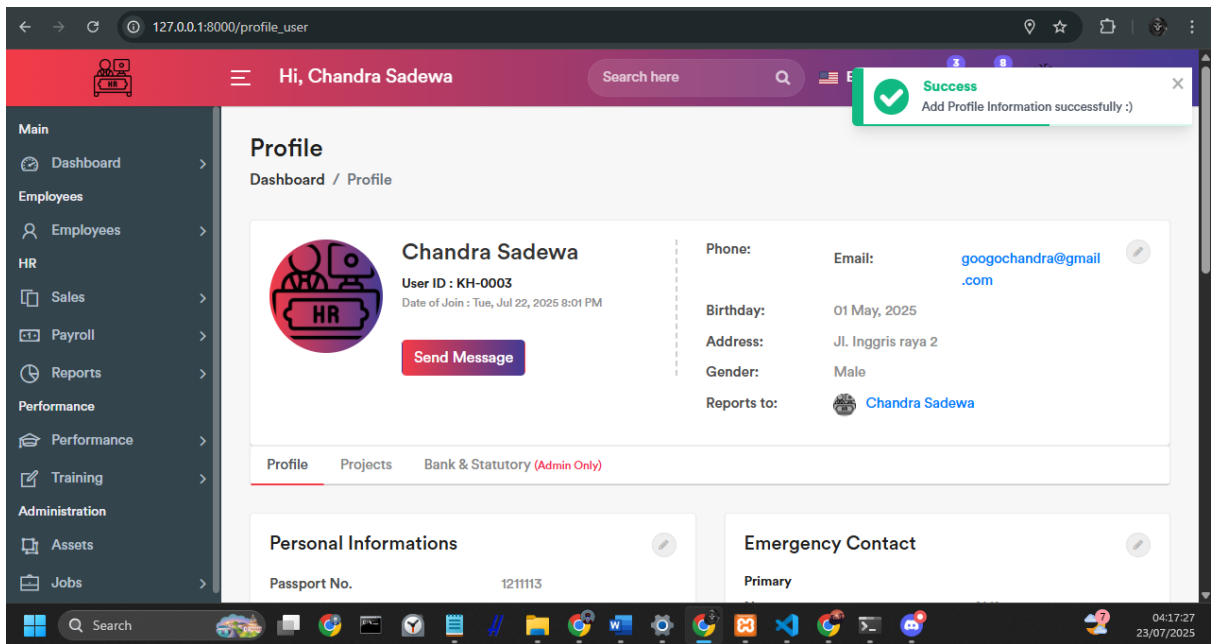
Loan:

**Submit**

Gambar 5. Admin mengisi gaji dolar karyawan dalam perorangan



Gambar 6. Tampilan admin logout




Gambar 7. Tampilan profil user

**Payslip**  
Dashboard / Payslip

Excel PDF Print

PAYSLIP FOR THE MONTH OF JUL 2025

**PAYSLIP #49029**  
Salary Month: Jul , 2025



Chandra Sadeva  
Jl. Inggris raya 2  
Indonesia

Chandra Sadeva  
Employee ID: KH-0003  
Joining Date: Tue, Jul 22, 2025 8:01 PM

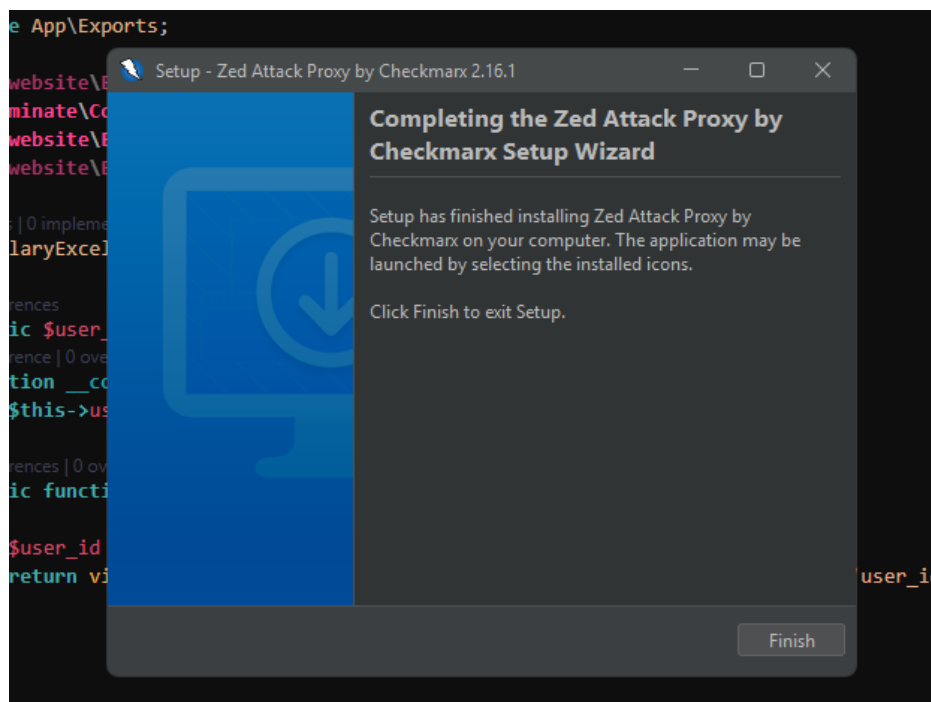
Earnings		Deductions	
Basic Salary	\$150	Tax Deducted at Source (T.D.S.)	\$10
House Rent Allowance (H.R.A.)	\$22	Provident Fund	\$2
Conveyance	\$12	ESI	\$3
Other Allowance	\$7	Loan	\$3
<b>Total Earnings</b>	<b>\$191</b>	<b>Total Deductions</b>	<b>\$18</b>

**Net Salary: \$208** (Fifty nine thousand six hundred and ninety eight only)

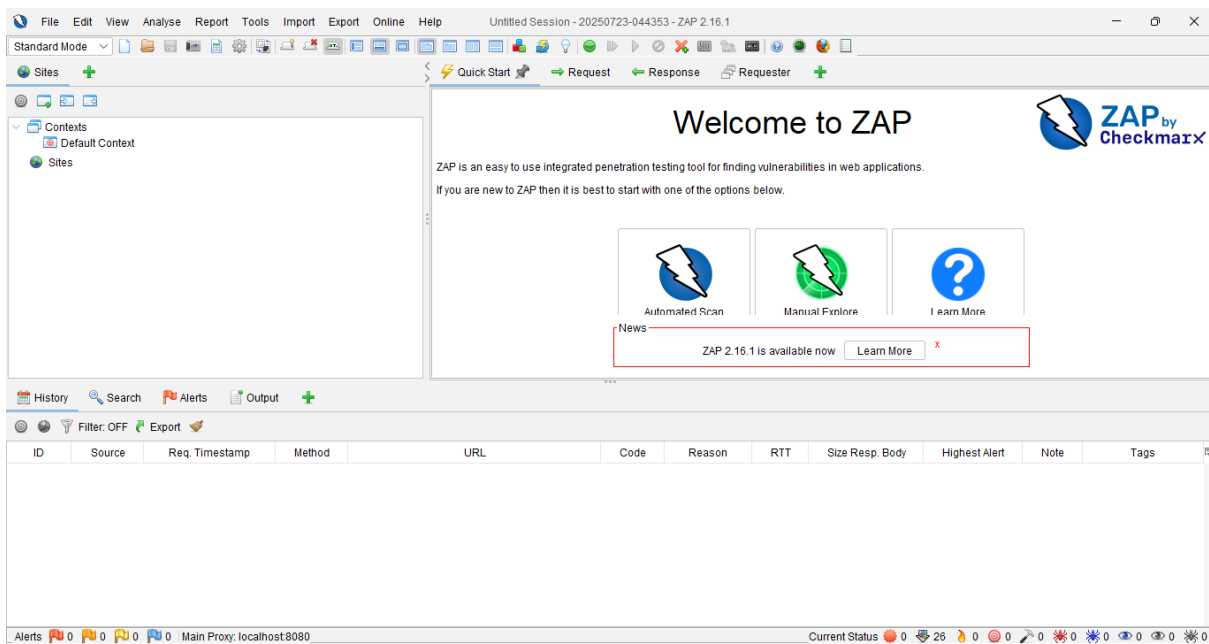
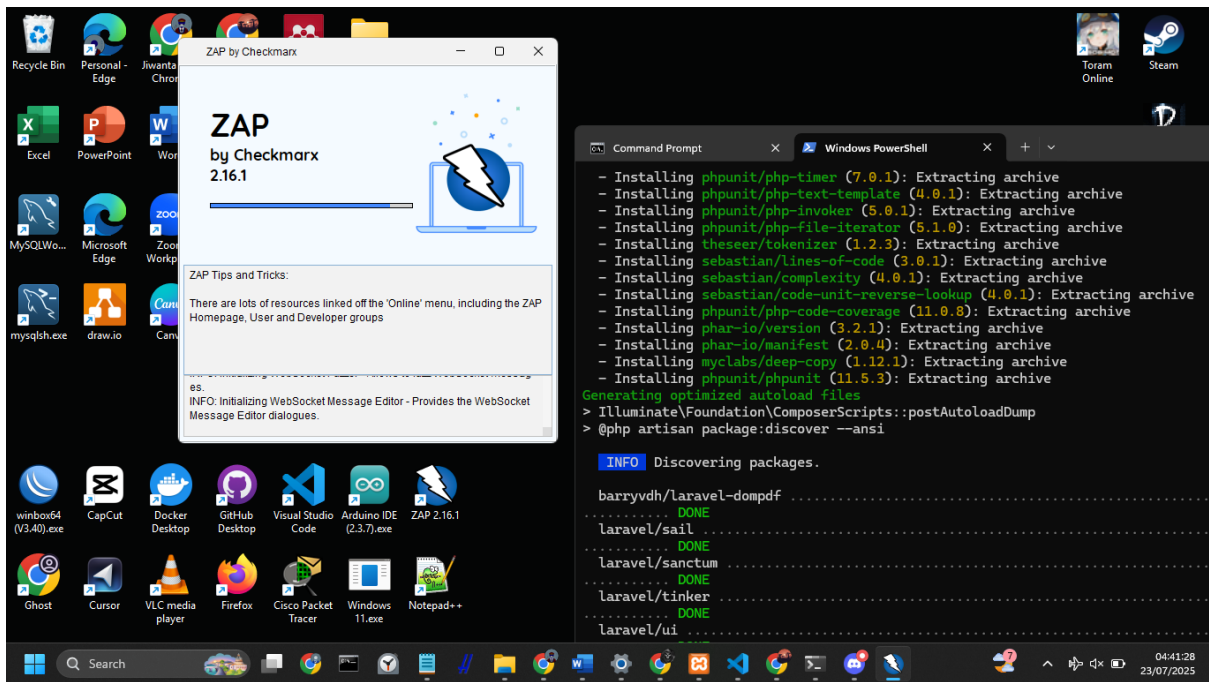
Gambar 8. Hasil tampilan gaji untuk Chandra sebagai employee

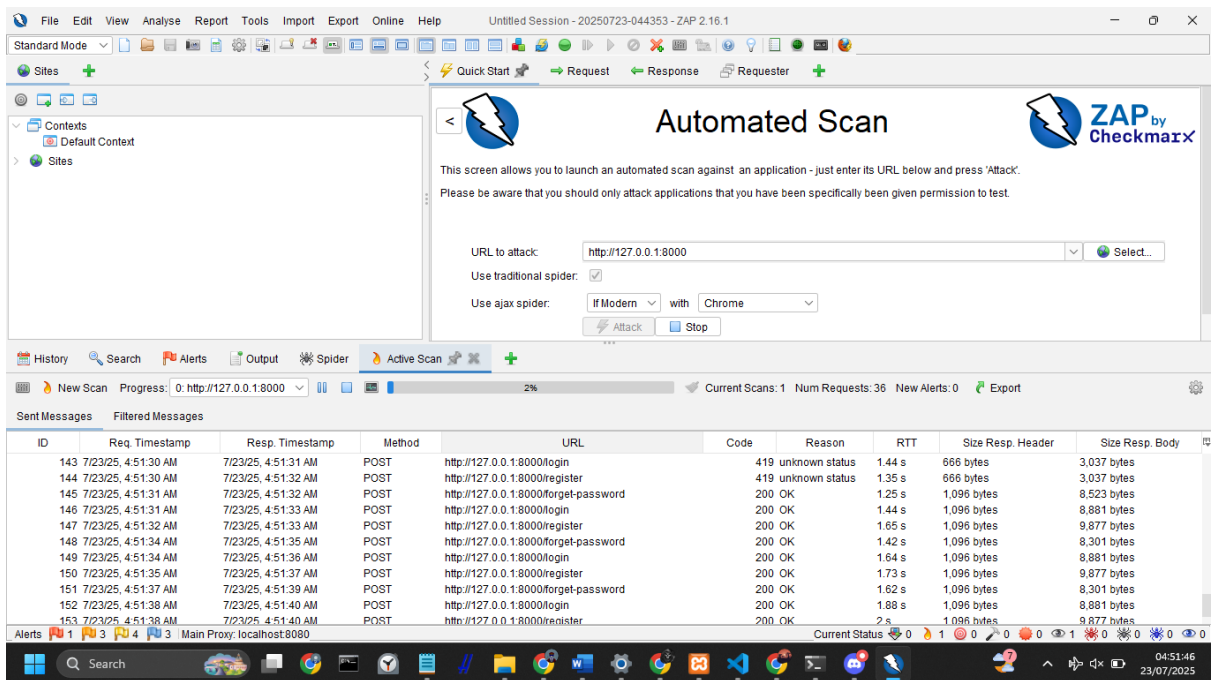
### 3. Lakukan Vulnerability Assesment terhadap aplikaasi yang dibikin, solusi:

Sesudah membuat aplikasi sesuai dengan tujuan awal dibuat, maka selanjutnya saya menggunakan Vulnerability Assesment, dengan Zed Attack Proxy dalam pencarian sistem yang rentan terhadap data karyawan maupun gaji.

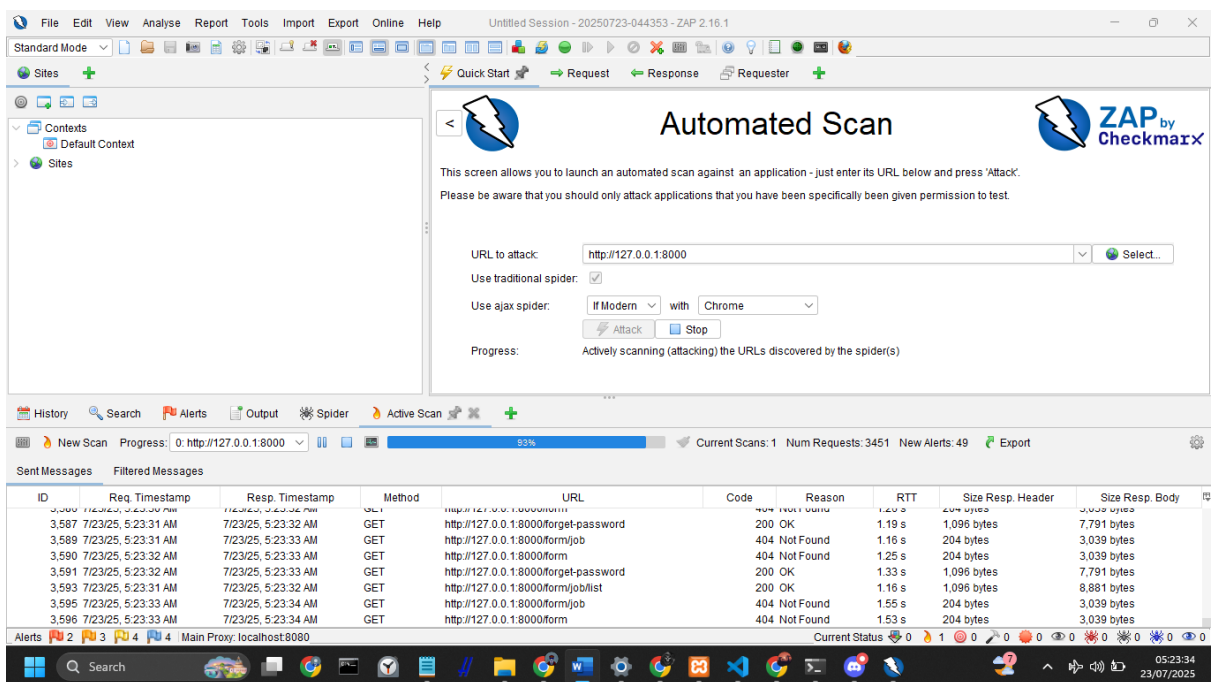


Gambar 9. Setup ZAP



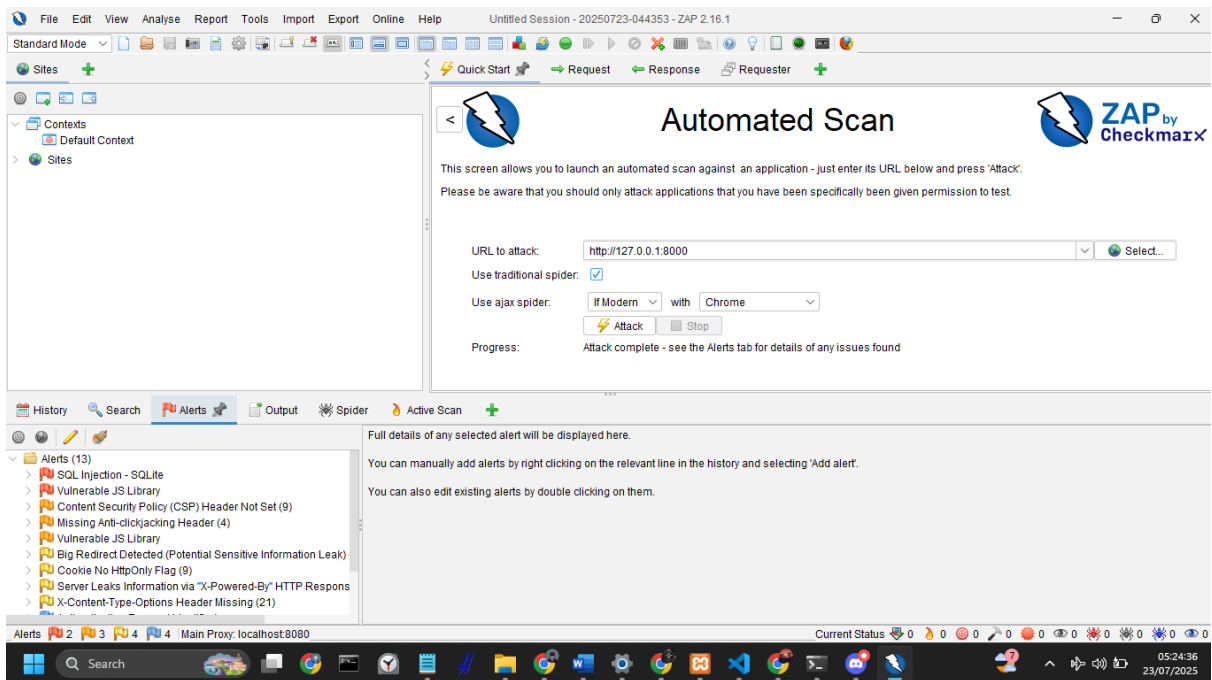


Gambar 12. ZAP sedang mengscan aplikasinya terhadap potensi kerentanan suatu data

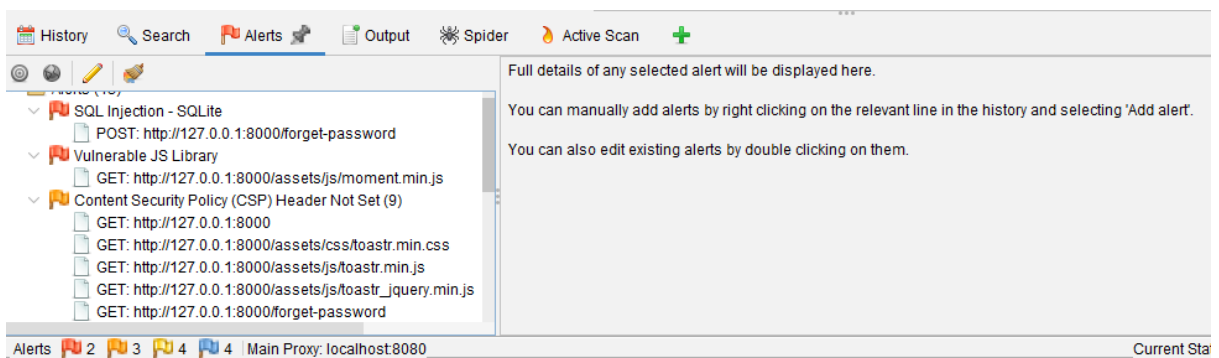


Gambar 13. Proses scan ini memerlukan puluhan menit

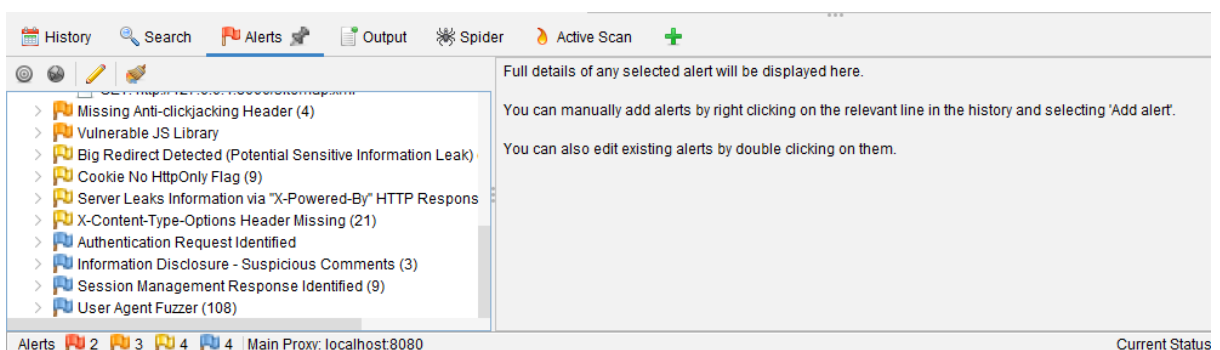




Gambar 14. Hasil dari scan pada bagian “alerts” menunjukkan dari warnah merah yang urgent hingga ke biru yang tidak terlalu urgent



Gambar 15. Se jauh ini tidak ada “alerts” yang menunjukkan akan kebocoran data gaji terhadap data karyawan, melainkan hanya menunjukkan autentifikasi saja



Gambar 16. Selain itu pada Laravel 11 ini, ada beberapa library yang perlu saya update

4. Lakukan pengamanan data-datanya sesuai dengan kasus yang anda tentukan sendiri, solusi:

```
Command Prompt X Windows PowerShell X + ^ v
2025-07-23 05:11:38 /register ..... ~ 573.89ms
2025-07-23 05:11:39 /register ..... ~ 0.77ms
2025-07-23 05:11:39 /register ..... ~ 15.84ms
2025-07-23 05:11:40 /register ..... ~ 579.97ms
2025-07-23 05:11:40 /register ..... ~ 505.49ms
2025-07-23 05:11:41 /register ..... ~ 522.15ms
2025-07-23 05:11:41 /register ..... ~ 526.48ms
2025-07-23 05:11:42 /register ..... ~ 504.38ms
2025-07-23 05:11:42 /register ..... ~ 512.99ms
2025-07-23 05:11:43 /register ..... ~ 509.41ms
2025-07-23 05:11:43 /register ..... ~ 520.29ms
2025-07-23 05:11:44 /register ..... ~ 518.91ms
2025-07-23 05:11:44 /register ..... ~ 513.73ms
2025-07-23 05:11:45 /register ..... ~ 701.89ms
2025-07-23 05:11:45 /register ..... ~ 513.92ms
2025-07-23 05:11:46 /register ..... ~ 516.24ms
2025-07-23 05:11:47 /register ..... ~ 517.66ms
2025-07-23 05:11:47 /register ..... ~ 540.41ms
2025-07-23 05:11:48 /register ..... ~ 0.19ms
2025-07-23 05:11:48 /register ..... ~ 512.41ms
2025-07-23 05:11:49 /register ..... ~ 1s
2025-07-23 05:11:49 /register ..... ~ 521.33ms
2025-07-23 05:11:50 /register ..... ~ 536.53ms
2025-07-23 05:11:50 /register ..... ~ 1.06ms
2025-07-23 05:11:51 /register ..... ~ 506.82ms
2025-07-23 05:11:51 /register ..... ~ 519.79ms
2025-07-23 05:11:52 /register ..... ~ 516.29ms
2025-07-23 05:11:52 /register ..... ~ 514.77ms
2025-07-23 05:11:53 /register ..... ~ 501.50ms
2025-07-23 05:11:53 /register ..... ~ 509.45ms
2025-07-23 05:11:54 /register ..... ~ 508.19ms
2025-07-23 05:11:54 /register ..... ~ 0.15ms
127.0.0.1:60525 [404]: GET /assets - No such file or directory
2025-07-23 05:11:54 ..... ~ 0.38ms
127.0.0.1:60526 [404]: GET /assets/css - No such file or directory
```

Selain itu 404 pada /assets/css hanyalah *broken link*, bukan kerentanan kritikal. Temuan yang benar-benar “urgent” menurut ZAP ialah:

Risk	URL / Objek	Aksi perbaikan singkat
<b>High – SQL Injection</b>	POST /forget-password (_token parameter)	Pastikan endpoint memakai Eloquent / Query Builder dengan binding; jika sudah, verifikasi input-validation dan CSRF.
<b>Medium – Vulnerable JS Library</b>	assets/js/moment.min.js (versi lama)	Ganti ke versi terbaru (npm i moment@latest) atau ganti <b>day.js</b> .
<b>Medium – CSP Header Not Set</b>	Seluruh respon	Tambahkan middleware “SecureHeaders” → set Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, HSTS.
<b>Low – Cookie No HttpOnly</b>	Cookie sesi	Di config/session.php: 'http_only' => true, 'secure' => true.
<b>Informational – X-Powered-By</b>	HTTP header	php.ini → expose_php = Off.

Sehingga Kerentanan prioritas tertinggi adalah **SQL Injection** di endpoint /forget-password. Solusinya saya melakukan: refactor query menjadi Eloquent dengan parameter binding dan tambahkan validasi email + token. Selanjutnya perbarui *moment.js* ke versi terbaru untuk menutup CVE-2025-31129, aktifkan header CSP & X-Frame-Options via middleware, dan set flag HttpOnly + Secure pada cookie sesi agar data gaji & karyawan tidak bisa di-eksfiltrasi melalui XSS atau session hijacking. Setelah patch, jalankan ulang ZAP untuk memastikan temuan High/Medium hilang.

Maka hasil report yang didapat:



Gambar 18. Hasil report

**Summaries**

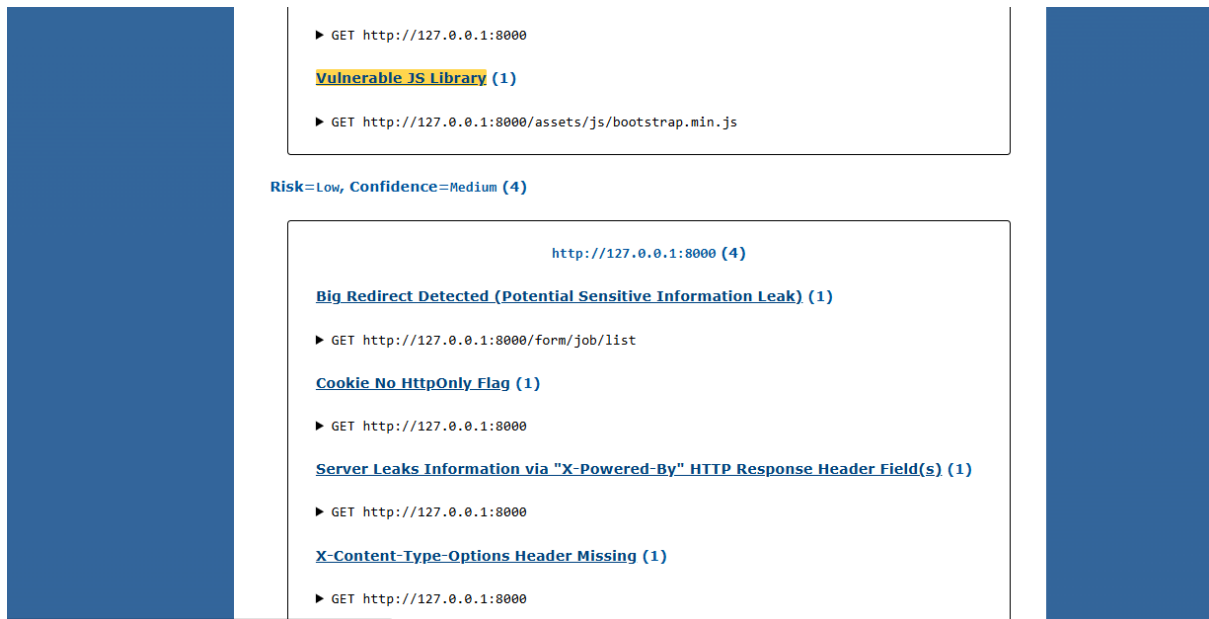
**Alert Counts by Risk and Confidence**

This table shows the number of alerts for each level of risk and confidence included in the report.

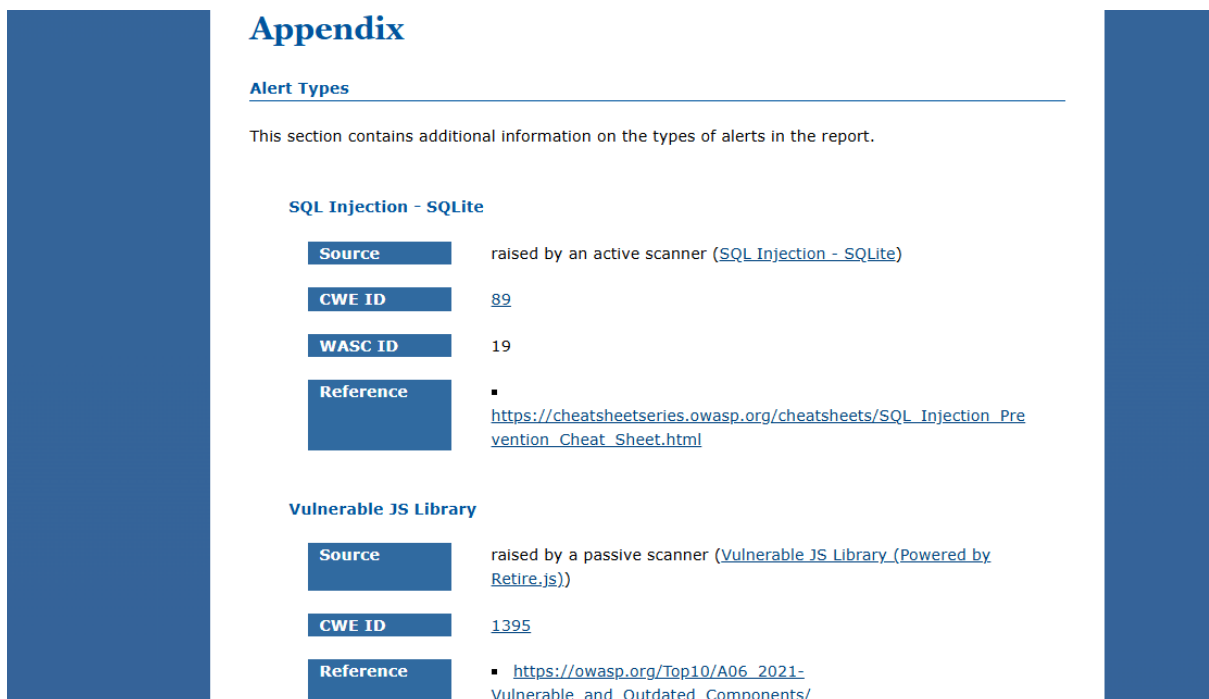
(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence			
Risk	User	Confirmed	High	Medium	Low
	High	0 (0.0%)	0 (0.0%)	2 (2.4%)	0 (0.0%)
	Medium	0 (0.0%)	1 (2.7%)	2 (3.4%)	0 (0.0%)
	Low	0 (0.0%)	0 (0.0%)	4 (3.8%)	0 (0.0%)
	Informational	0 (0.0%)	1 (0.0%)	2 (0.4%)	1 (0.7%)
	Total	0 (0.0%)	2 (2.7%)	10 (10.0%)	1 (0.7%)
		Total			
		0 (0.0%)	2 (2.7%)	10 (10.0%)	1 (0.7%)

Gambar 19. Hasil presentase setelah diperbaiki pada bagian update ataupun penambahan library



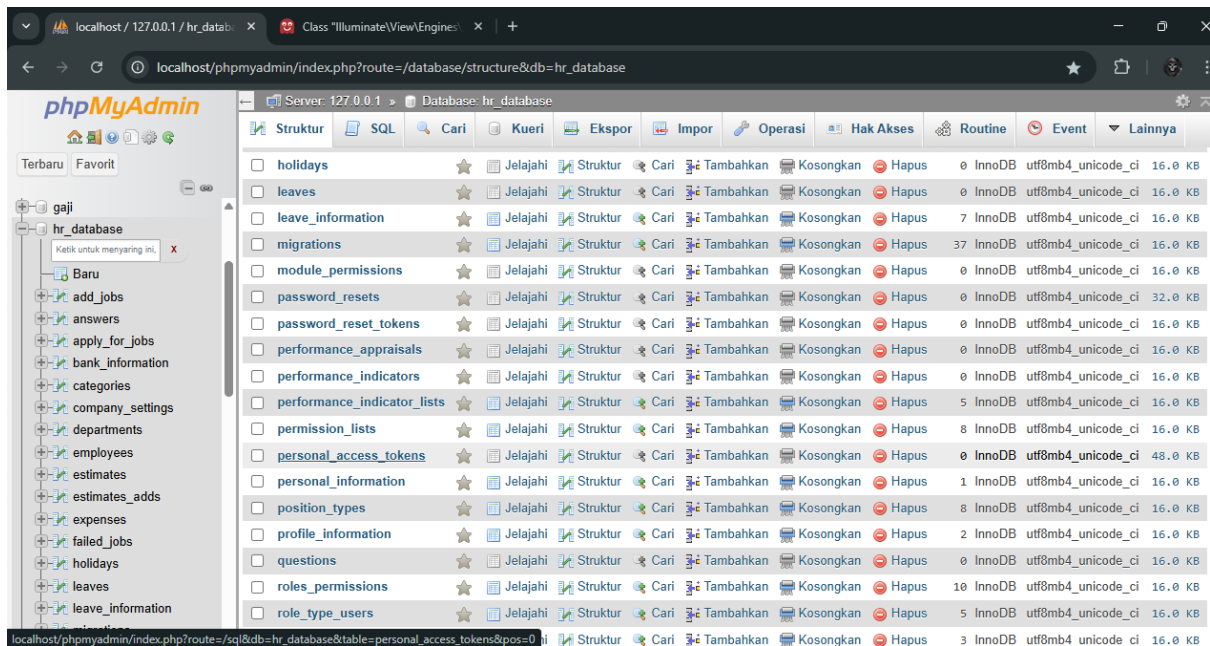
Gambar 20. Rincian risk data pada library



Gambar 21. Informasi terkait Appendix js library

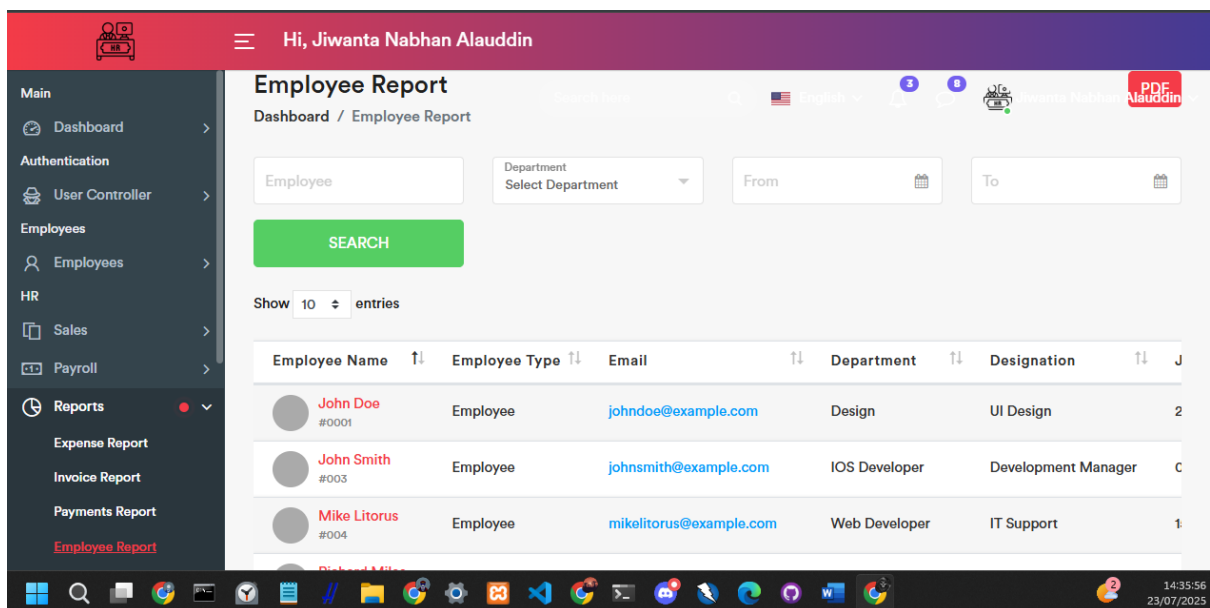
Hasil akhir pada link github: [https://github.com/Jiwanta384/Project\\_Untuk\\_UAS\\_KSI.git](https://github.com/Jiwanta384/Project_Untuk_UAS_KSI.git)

Update aplikasi pasca scan dalam mengurangi “Alert” pada aplikasi. Pada database saya menambahkan beberapa logaritma untuk penggunaan tokennya sebagaimana “alert” yang dilaporkan pada ZAP Scanner. Sehingga beberapa database Token bisa kita lihat sebagai berikut:



Gambar 22. Penambahan beberapa fitur token terhadap “forget\_password”

Selain itu karena ini berkaitan dengan gaji karyawan, maka website ini dikembangkan pada bagian kinerja karyawan beserta jabatannya, sehingga pada bagian admin kita bisa melihat:



Gambar 23. (Update) Admin pada bagian laporan karyawan dalam menangani pekerjaan

127.0.0.1:8000/form/employee/reports/page

Hi, Jiwanta Nabhan Alauddin

SEARCH

	Contact Number	Emergency Contact Details	Experience	Status
chester Township, NJ, 08759	9876543210	7894561235	0 years 4 months and 9 days	Active
chester Township, NJ, 08759	9876543210	7894561235	0 years 3 months and 21 days	Active
chester Township, NJ, 08759	9876543210	7894561235	0 years 1 months and 9 days	Active
chester Township, NJ, 08759	9876543210	7894561235	0 years 5 months and 24 days	Active
chester Township, NJ, 08759	9876543210	7894561235	0 years 0 months and 24 days	Active

Left Sidebar: Main, Dashboard, Authentication, User Controller, Employees, HR, Sales, Payroll, Reports (selected), Expense Report, Invoice Report, Payments Report, Employee Report.

Gambar 24. Selain itu kita bisa melihat pengalaman si karyawan kita

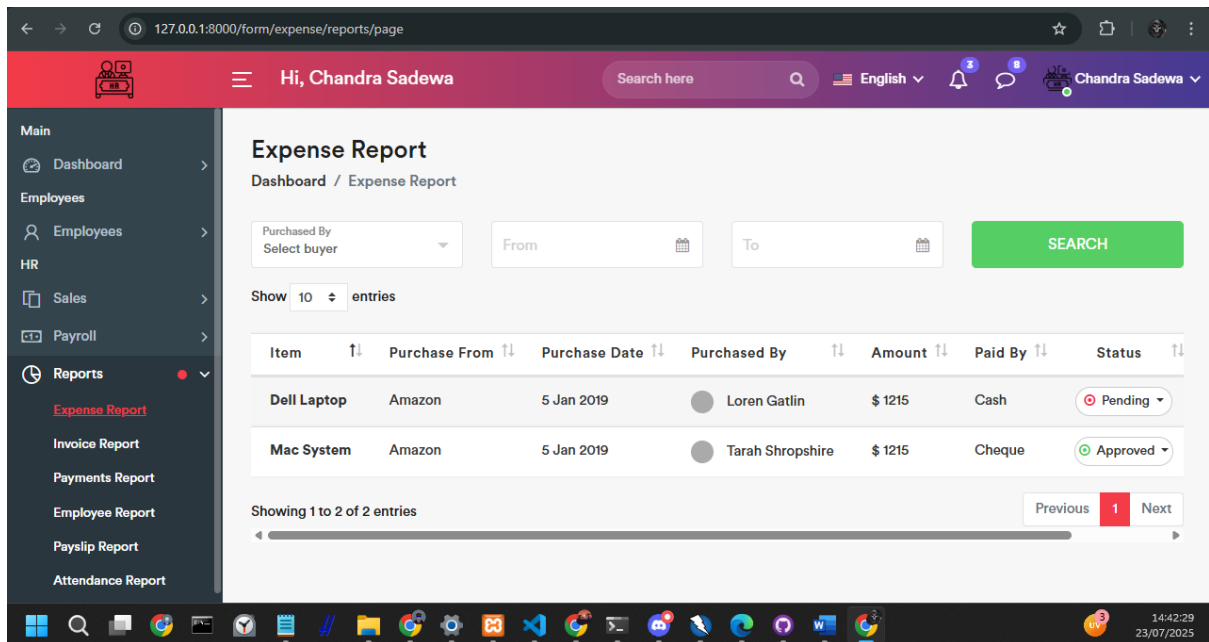
Hi, Jiwanta Nabhan Alauddin

Show 10 entries

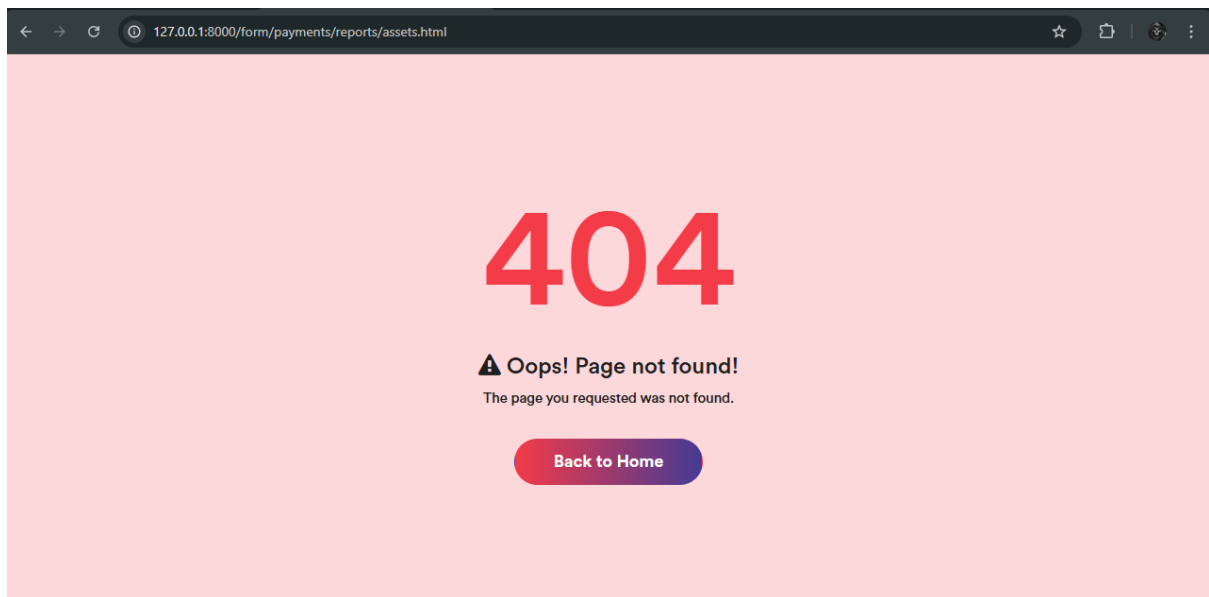
Scheduled Shift	Fri 21	Sat 22	Sun 23
Bernardo Galaviz Web Developer	6:30 am - 9:30 pm (14 hrs 15 mins) Web Designer - SMARTHTR	+	+
Jeffrey Warden Web Developer	+	+	+
John Doe Web Designer	6:30 am - 9:30 pm (14 hrs 15 mins) Web Designer - SMARTHTR	+	+
John Smith Android Developer	+	+	6:30 am - 9:30 pm (14 hrs 15 mins) Web Designer - SMARTHTR
Mike Litorus IOS Developer	+	+	+

Left Sidebar: Main, Dashboard, Authentication, User Controller, Employees, All Employees, Holidays, Leaves (Admin), Leaves (Employee), Leave Settings, Attendance (Admin), Attendance (Employee), Departments.

Gambar 25. Admin juga dapat memantau jadwal dan hal yang dilakukan oleh employee serta mengatur jadwalnya



Gambar 26. Lalu pada bagian employee (Chandra sadewa) kita bisa melihat pekerjaan kita dan melakukan decesion terhadap penerimaan pekerjaan yang akan dilakukan



Gambar 27. Beberapa fitur akan diupdate selain pada data gaji (karena sekarang fokusnya pada bagian pengamanan data gaji karyawan).