

Mata Kuliah: CIE406 – Keamanan Informasi

Dosen	: 7800 – Dr. Hani Dewi Ariessanti S.Kom, M.Kom	
Mahasiswa	: Jiwanta Nabhan Alauddin	
NIM	: 20230801384	
Hari	: Selasa	Waktu : 24 Jam
Tanggal	: 22 Juli 2025	Seksi : KJ003
Sifat Ujian	: 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
users	id (PK)	1 : 1 user_profiles 1 : N → staff_salaries , attendances , leaves	Identitas karyawan & kredensial login	users	id (PK)	1 : 1 user_profiles 1 : N → staff_salaries , attendances , leaves
user_profiles	user_id (PK & FK)	1 : 1 ← users	Data bio + jabatan, departemen, foto	user_profiles	user_id (PK & FK)	1 : 1 ← users
departments	id	1 : N ← user_profiles	Mengelompokkan karyawan	departments	id	1 : N ← user_profiles

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
staff_salaries	<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 string , bukan decimal.
users	<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

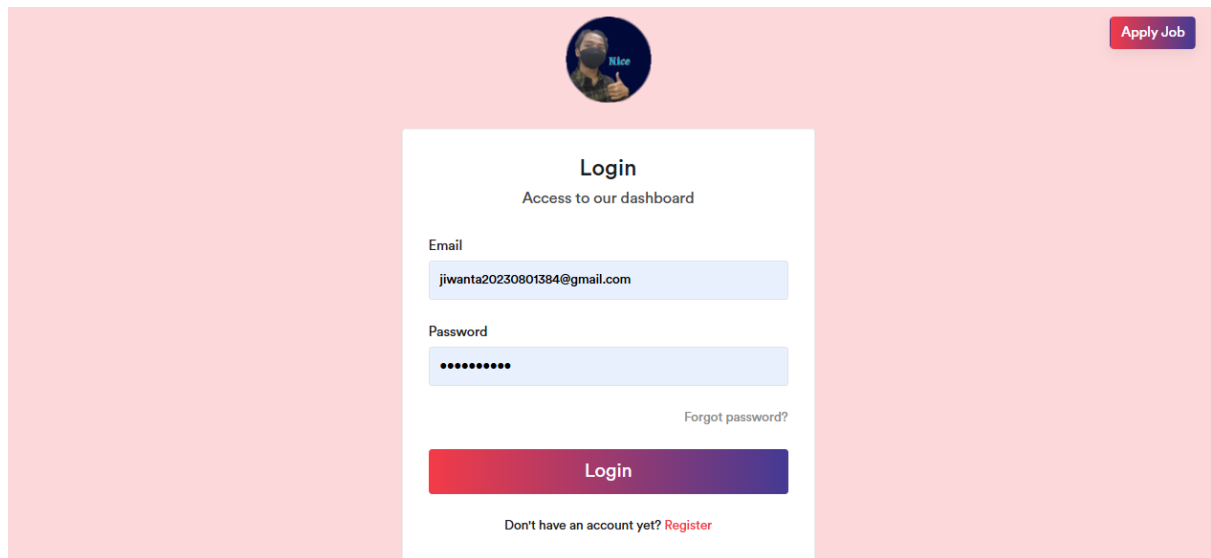
	lalu simpan ke staff_salaries.deleteRecord() - hapus gaji.reportPdf() / reportExcel() - ekspor laporan per karyawan.
app/Exports/SalaryExcel.php + resources/views/report_template/salary_excel.blade.php	Menyusun file .xlsx via Maatwebsite Excel.
resources/views/payroll/*.blade.php	UI input / daftar gaji,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

Alur kerja “Employee Salary”

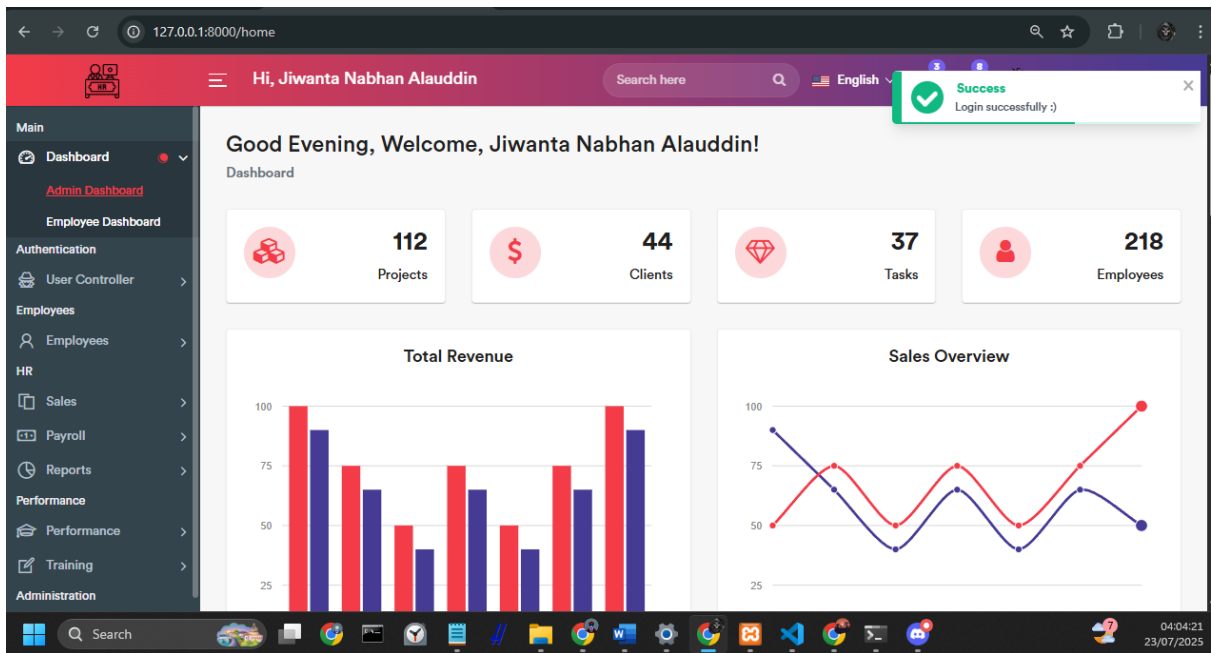
1. **HR/Admin** buka menu **Payroll** → **Salary**
2. Form “Add Staff Salary” memuat daftar karyawan (select) dan semua komponen gaji.
3. Nilai disimpan ke **staff_salaries**. Jika record sudah ada, **updateRecord()** dipakai.
4. Halaman daftar menampilkan kolom-kolom tersebut dan menyediakan tombol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

2. Buatlah aplikasinya, solusi:

Maka mulai dari Admin:



Tampilan Login admin



Tampilan dashboard admin

A screenshot of the 'Employee Salary' management page. It includes a sidebar with navigation links for Main, Authentication, Employees, HR, Sales, Payroll, Reports, Performance, Training, and Administration. The main content area displays a form to add or search for employee salaries, a table of existing salary entries, and a pagination control.

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	Generate Slip
Irfan Fharthan	KH-0004	lrfans@gmail.com	Tue, Jul 22, 2025 8:29 PM	Employee	\$141	Generate Slip

Tampilan Admin untuk Employee Salary

127.0.0.1:8000/form/salary/page

Hi, Jiwanta Nabhan Alauddin

Employee Salary
Dashboard / Salary

Employee Name

Show 10 entries

Employee

Chandra Sadewa

Irfan Fharthan

Showing 1 to 2 of 2 entries

Add Staff Salary

Select Staff: -- Select --

Net Salary: Enter net salary

Earnings

Basic: Enter basic

DA(40%): Enter DA(40%)

HRA(15%): Enter HRA(15%)

Conveyance: Enter conveyance

Allowance: Enter allowance

Medical Allowance: Enter medical allowance

Deductions

TDS: Enter TDS

ESI: Enter ESI

PF: Enter PF

Leave: Enter leave

Prof. Tax: Enter Prof. Tax

Loan: Enter Loan

Submit

Salary

Payslip

Action

Generate Slip

Previous 1 Next

04:07:46
23/07/2025

Tampilan admin dalam mengisi gaji karyawan

127.0.0.1:8000/form/salary/page

Hi, Jiwanta Nabhan Alauddin

Employee Salary
Dashboard / Salary

Employee Name

Show 10 entries

Employee

Chandra Sadewa

Irfan Fharthan

Showing 1 to 2 of 2 entries

Add Staff Salary

Select Staff: Chandra Sadewa

Net Salary: 221

Earnings

Basic: 200

DA(40%): 12

HRA(15%): 11

Conveyance: 14

Allowance: 12

Medical Allowance: 21

Deductions

TDS: 22

ESI: 12

PF: 2

Leave: 4

Prof. Tax: 1

Loan: 2

Submit

Salary

Payslip

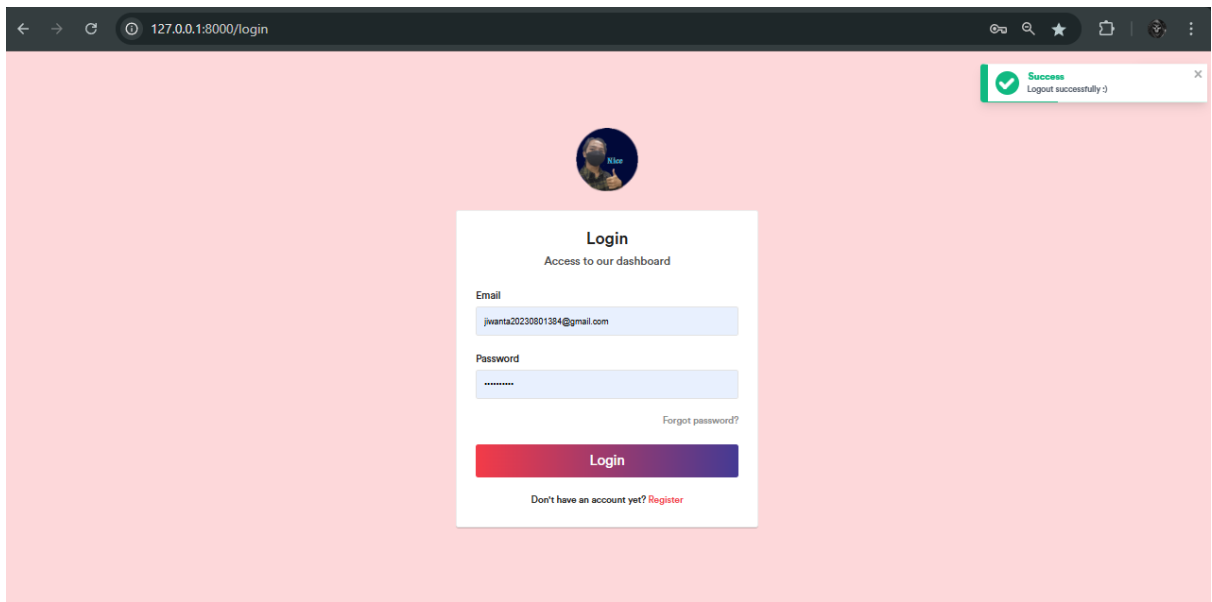
Action

Generate Slip

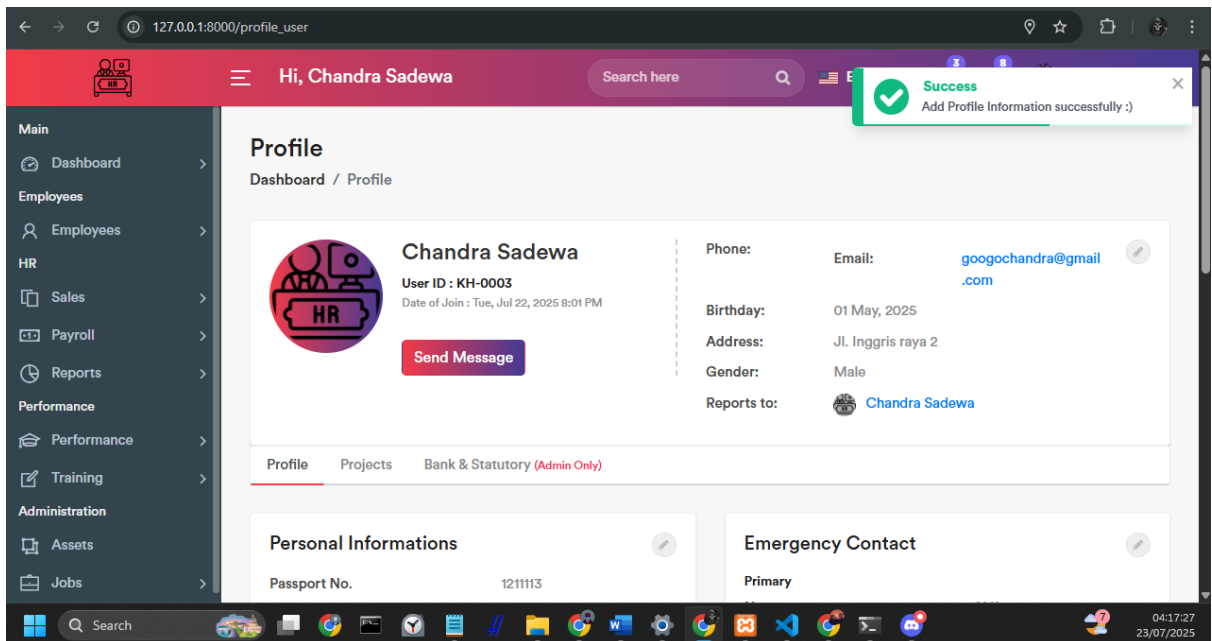
Previous 1 Next

04:09:19
23/07/2025

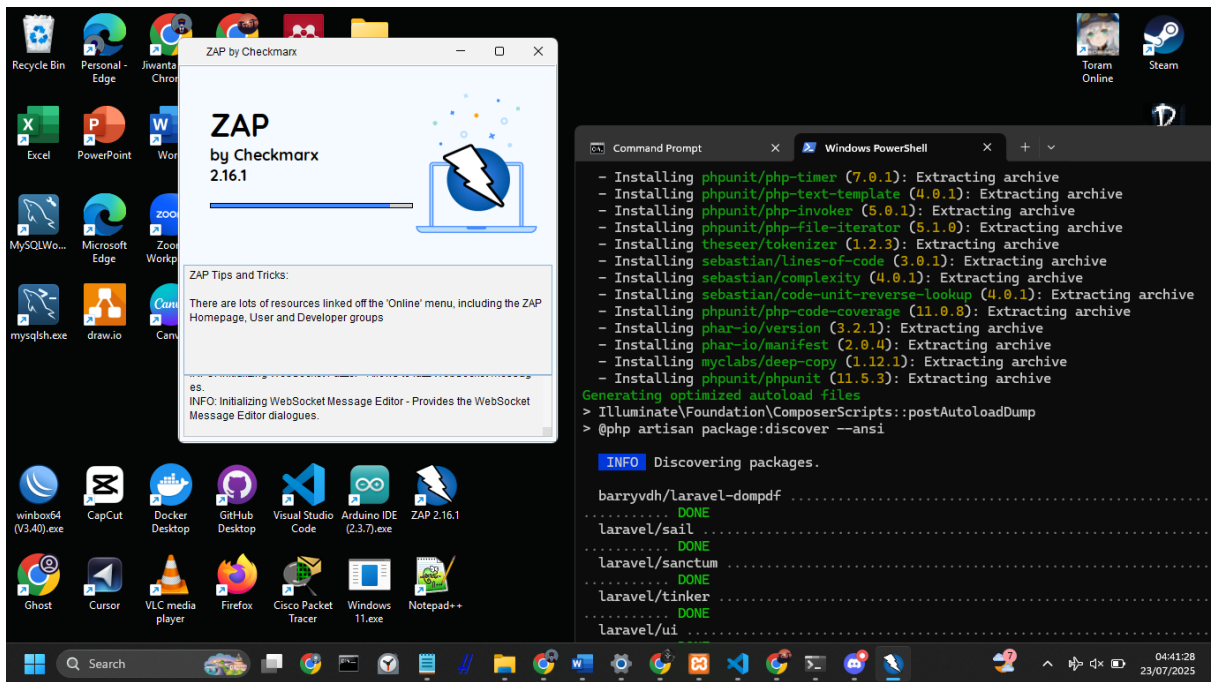
Admin mengisi gaji dolar karyawan dalam perorangan



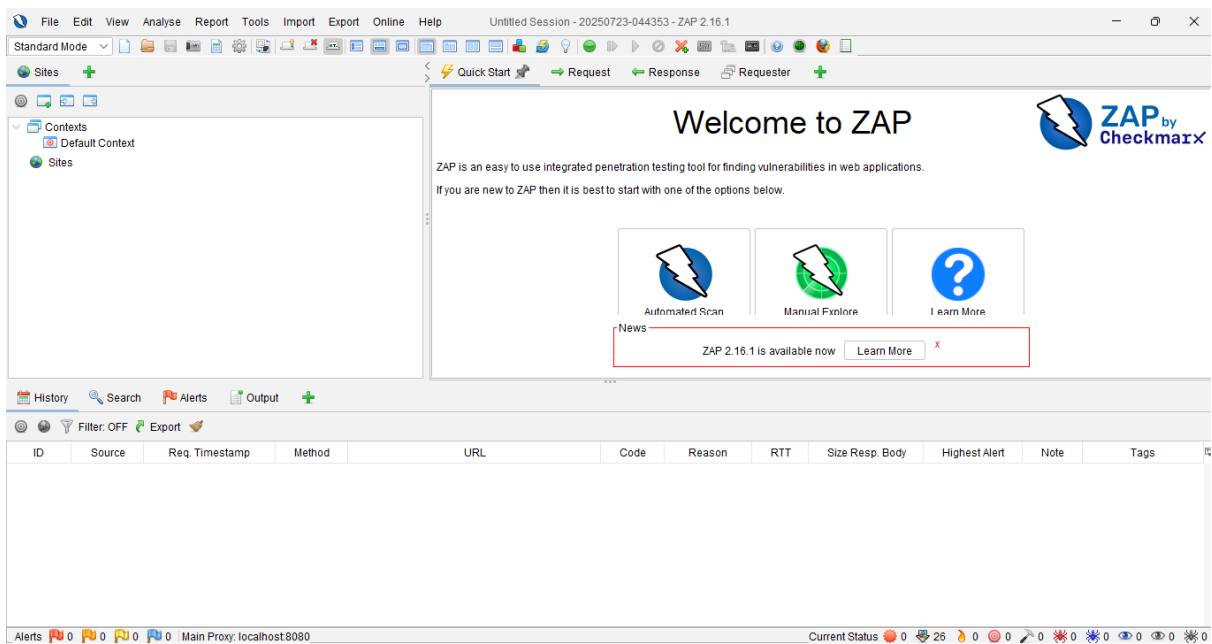
Tampilan admin logout



Tampilan profil user

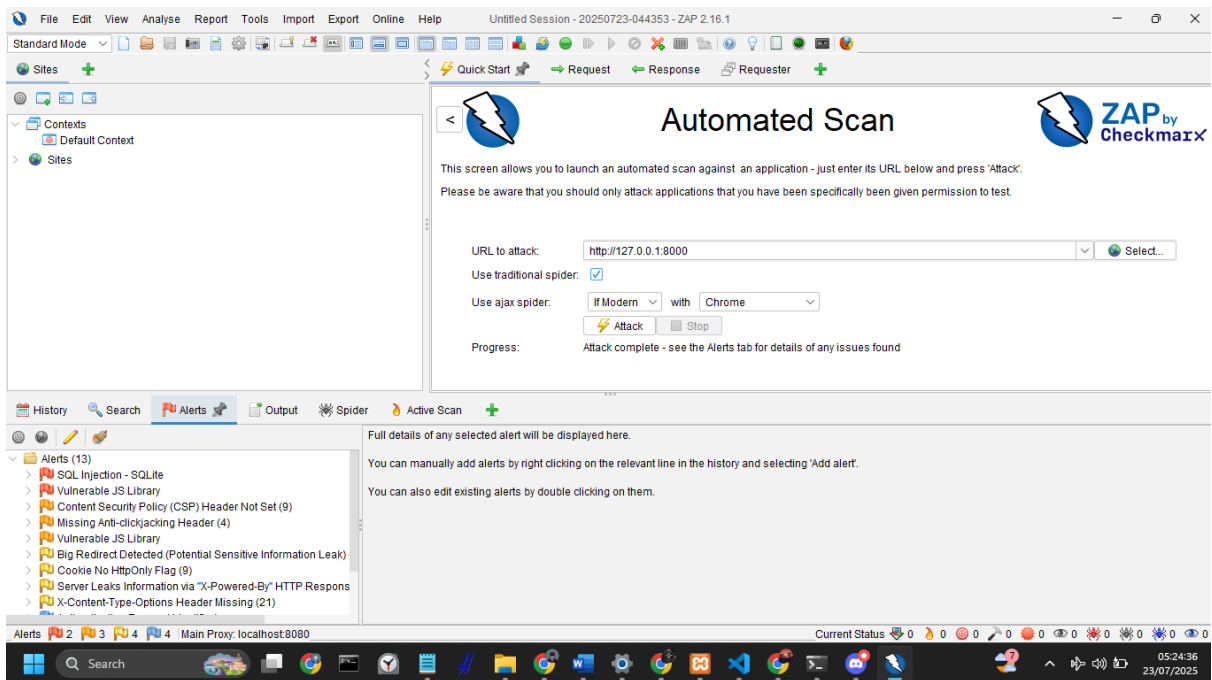


Melakukan persiapan peluncuran ZAP untuk web

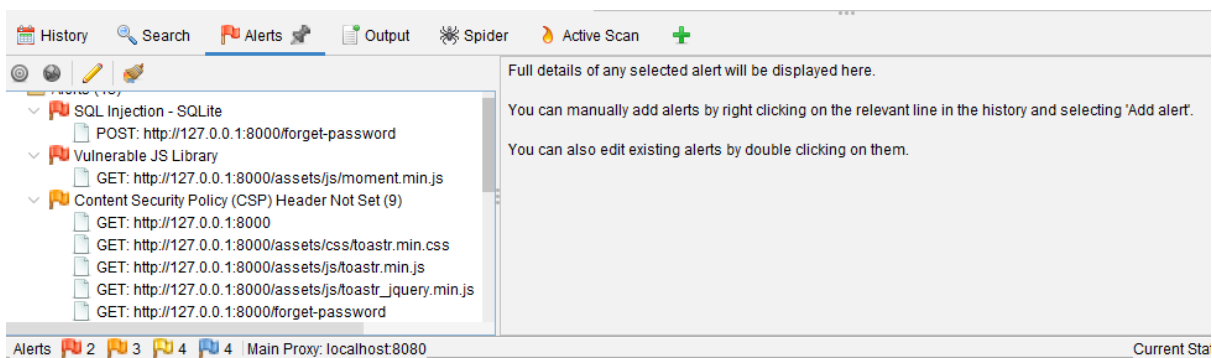


Tampilan awal ZAP

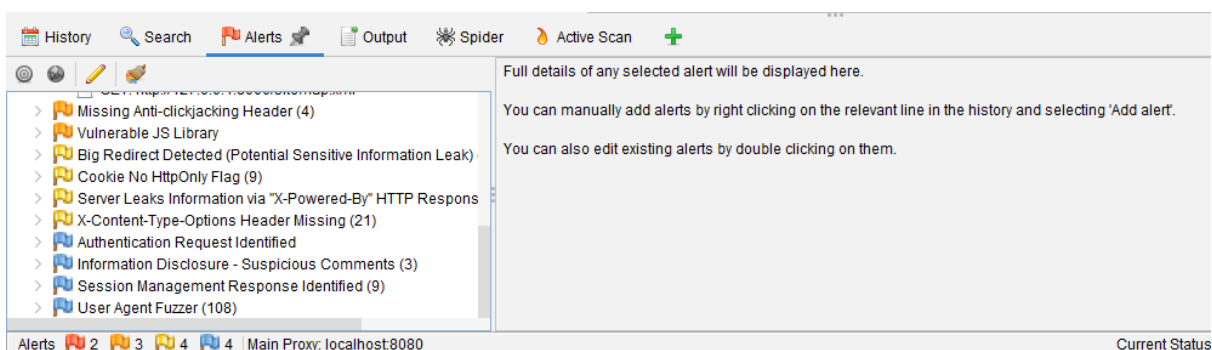




Hasil dari scan pada bagian “alerts” menunjukkan dari warnah merah yang urgent hingga ke biru yang tidak terlalu urgent



Sejauh ini tidak ada “alerts” yang menunjukkan akan kebocoran data gaji terhadap data karyawan, melainkan hanya menunjukkan autentifikasi saja



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:

Dikarenakan pada hasil scan yang urgent bukanlah data gaji karyawan melainkan library pada bagian /register di 127.0.0.1:60525 [404]: Get /assestes/css – No such file or directory. Maka saya mengupdatenya pada powershell untuk di update sebagaimana output berikut ini:


```
2025-07-23 05:11:38 /register ..... 573.09ms
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
```

Maka hasil report yang didapat:

ZAP by Checkmarx Scanning Report (Jiwanta)

Generated with  ZAP on Wed 23 Jul 2025, at 05:36:22

ZAP Version: 2.16.1

ZAP by  Checkmarx

Contents

- [About This Report](#)
 - [Report Parameters](#)
- [Summaries](#)
 - [Alert Counts by Risk and Confidence](#)
 - [Alert Counts by Site and Risk](#)

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				
		User				
		Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	2 (2.4%)	0 (0.0%)	2 (2.4%)
	Medium	0 (0.0%)	1 (2.7%)	2 (3.4%)	0 (0.0%)	3 (6.1%)
	Low	0 (0.0%)	0 (0.0%)	4 (3.8%)	0 (0.0%)	4 (3.8%)
	Informational	0 (0.0%)	1 (0.0%)	2 (0.4%)	1 (0.7%)	4 (1.1%)
	Total	0 (0.0%)	2 (2.7%)	10 (10.0%)	1 (0.7%)	13 (13.4%)

Hasil presentase setelah diperbaiki pada bagian update ataupun penambahan library

▶ GET http://127.0.0.1:8000

Vulnerable JS Library (1)

▶ GET http://127.0.0.1:8000/assets/js/bootstrap.min.js

Risk=Low, Confidence=Medium (4)

http://127.0.0.1:8000 (4)

Big Redirect Detected (Potential Sensitive Information Leak) (1)

▶ GET http://127.0.0.1:8000/form/job/list

Cookie No HttpOnly Flag (1)

▶ GET http://127.0.0.1:8000

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

▶ GET http://127.0.0.1:8000

X-Content-Type-Options Header Missing (1)

▶ GET http://127.0.0.1:8000

Rincian risk data pada library

Appendix

Alert Types

This section contains additional information on the types of alerts in the report.

SQL Injection - SQLite

Source	raised by an active scanner (SQL Injection - SQLite)
CWE ID	89
WASC ID	19
Reference	<ul style="list-style-type: none">▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	1395
Reference	<ul style="list-style-type: none">▪ https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Informasi terkait Appendix js library