Analisis Studi Kasus Sistem Informasi Data Nilai Mahasiswa dengan Pengamanan NIM dan Data Nilai

Latar Belakang Masalah

Nomor Induk Mahasiswa (NIM) merupakan identitas unik setiap mahasiswa di perguruan tinggi yang digunakan sebagai penanda resmi identitas akademik dan administratif. Bersama dengan data nilai, seperti nilai ujian dan Indeks Prestasi Kumulatif (IPK), NIM menjadi elemen penting dalam seluruh aktivitas akademik.

Kebocoran data NIM maupun data nilai dapat menimbulkan risiko serius, antara lain penyalahgunaan identitas mahasiswa, pemalsuan data, manipulasi nilai akademik, hingga pelanggaran kerahasiaan informasi pribadi. Oleh karena itu, diperlukan suatu sistem informasi akademik yang mampu mengelola data nilai secara terpusat dengan pengamanan berlapis, agar kerahasiaan NIM dan data nilai tetap terjaga.

Rumusan Masalah

1. Bagaimana merancang sistem informasi akademik yang mampu mengelola data NIM dan nilai mahasiswa secara aman?
2. Bagaimana menerapkan mekanisme enkripsi pada data NIM dan nilai agar tidak dapat diakses secara langsung melalui basis data?
3. Bagaimana mencatat seluruh aktivitas perubahan atau akses data NIM dan nilai agar jejak audit (log) dapat dipertanggungjawabkan?
4. Bagaimana membatasi hak akses pengguna agar hanya pihak yang berwenang (admin/dosen) yang dapat melihat atau memperbarui data NIM dan nilai mahasiswa?

Tujuan

1. Membangun sistem informasi nilai mahasiswa berbasis web dengan Laravel & Filament versi 3.3.
2. Menerapkan teknik enkripsi pada atribut data NIM dan nilai guna menjaga kerahasiaan di tingkat basis data.
3. Menyediakan fitur pencatatan log setiap aktivitas perubahan atau akses terhadap data NIM dan nilai.
4. Menerapkan autentikasi dan otorisasi pengguna untuk membatasi akses sesuai dengan peran yang ditentukan.

Relasi antar entitas

1. Students → Grades: Satu mahasiswa memiliki banyak catatan nilai.
2. Grades → GradeLogs: Satu catatan nilai dapat memiliki banyak riwayat perubahan.

Manfaat

1. Menjamin kerahasiaan dan integritas data NIM serta data nilai mahasiswa.

2. Mencegah potensi penyalahgunaan atau manipulasi oleh pihak yang tidak berwenang.
3. Memberikan bukti audit yang sah dalam kasus perselisihan data akademik.
4. Mempermudah pihak admin akademik dan dosen dalam mengelola data mahasiswa secara terpusat, aman, dan terkontrol.

+--+

| Vulnerability Scan Report |

+--+

[1] Missing security header: Strict-Transport-Security

- Risk Level: 1 (Low)

Vulnerability Details:

- Evidence 1:

- URL: https://mission-importantly-frontier-actions.trycloudflare.com/

- Evidence: Response headers do not include the HTTP Strict-Transport-Security header
Request / Response

- 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.

- 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>[; 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.

[2] Missing security header: Referrer-Policy

- Risk Level: 1 (Low)

Vulnerability Details:

- Evidence 1:

  - URL: https://mission-importantly-frontier-actions.trycloudflare.com/

  - Evidence: Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response. Request / Response

- Description: We noticed that the target application's server responses lack the <code>Referrer-Policy</code> HTTP header, which controls how much referrer information the browser will send with each request originated from the current web application.

- 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 Referer header entirely.

[3] Missing security header: Content-Security-Policy

- Risk Level: 1 (Low)

Vulnerability Details:

- Evidence 1:

  - URL: https://mission-importantly-frontier-actions.trycloudflare.com/

  - Evidence: Response does not include the HTTP Content-Security-Policy security header or meta tag Request / Response

- 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.

- Recommendation: Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

[4] Missing security header: X-Content-Type-Options

- Risk Level: 1 (Low)

Vulnerability Details:

- Evidence 1:

- URL: https://mission-importantly-frontier-actions.trycloudflare.com/

- Evidence: Response headers do not include the X-Content-Type-Options HTTP security header Request / Response

- Description: We noticed that the target application's server responses lack the <code>X-Content-Type-Options</code> header. This header is particularly important for preventing Internet Explorer from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header.

- Recommendation: We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff`.

[5] Server software and technology found

- Risk Level: 1 (Low)

Vulnerability Details:

- Evidence 1:

- Software / Version: Alpine.js 3.14.9

- Category: JavaScript frameworks

- Evidence 2:

- Software / Version: Bunny

- Category: CDN

- Evidence 3:

- Software / Version: Filamentphp

- Category: Development

- Evidence 4:
    - Software / Version: Bunny Fonts
    - Category: Font scripts

- Evidence 5:
    - Software / Version: Livewire
    - Category: Web frameworks, Miscellaneous

- Evidence 6:
    - Software / Version: Laravel
    - Category: Web frameworks

- Evidence 7:
    - Software / Version: PHP
    - Category: Programming languages

- Evidence 8:
    - Software / Version: Cloudflare
    - Category: CDN

- Description: We noticed that server software and technology details are exposed, potentially aiding attackers in tailoring specific exploits against identified systems and versions.

- 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.

[6] Robots.txt file found

- Risk Level: 1 (Low)

Vulnerability Details:

- Evidence 1:

    - URL: https://mission-importantly-frontier-actions.trycloudflare.com/robots.txt

- 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.

- 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).

[7] Login Interface Found

- Risk Level: 0 (Info)

Vulnerability Details:

- Evidence 1:

    - URL: https://mission-importantly-frontier-actions.trycloudflare.com/admin/login

    - Evidence: `<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 bg-white/0 ps-3 pe-3" id="data.email" required="required" tabindex="1" type="email" wire:model="data.email"/> <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 bg-white/0 ps-3 pe-3 [&::-ms-reveal]:hidden" id="data.password" required="required" tabindex="2" wire:model="data.password" x-bind:type="isPasswordRevealed ? 'text' : 'password'"/> <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

- 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.

- Recommendation: Ensure each interface is not bypassable using common knowledge of the application or leaked credentials using occasional password audits.

[8] Security.txt file is missing

- Risk Level: 0 (Info)

Vulnerability Details:

- Evidence 1:

- URL: Missing: https://mission-importantly-frontier-actions.trycloudflare.com/.well-known/security.txt

- 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.

- 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.

[9] Website is accessible.

[10] Nothing was found for vulnerabilities of server-side software.

[11] Nothing was found for client access policies.

[12] Nothing was found for use of untrusted certificates.

[13] Nothing was found for enabled HTTP debug methods.

[14] Nothing was found for enabled HTTP OPTIONS method.

[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.

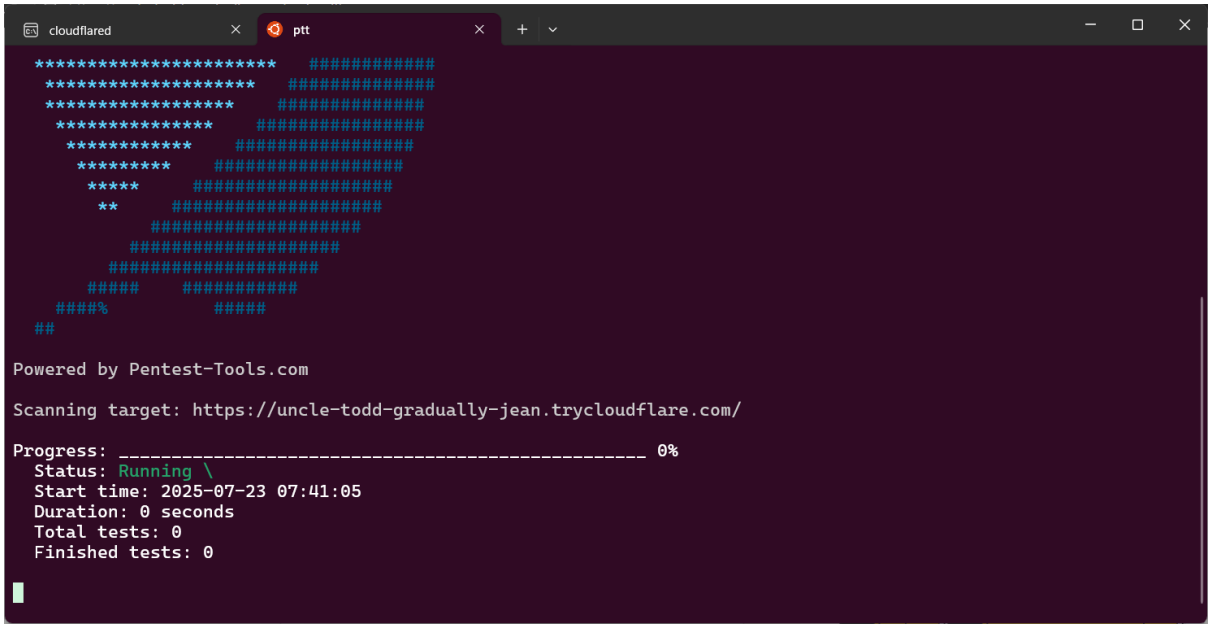
[35] Nothing was found for Path Disclosure.

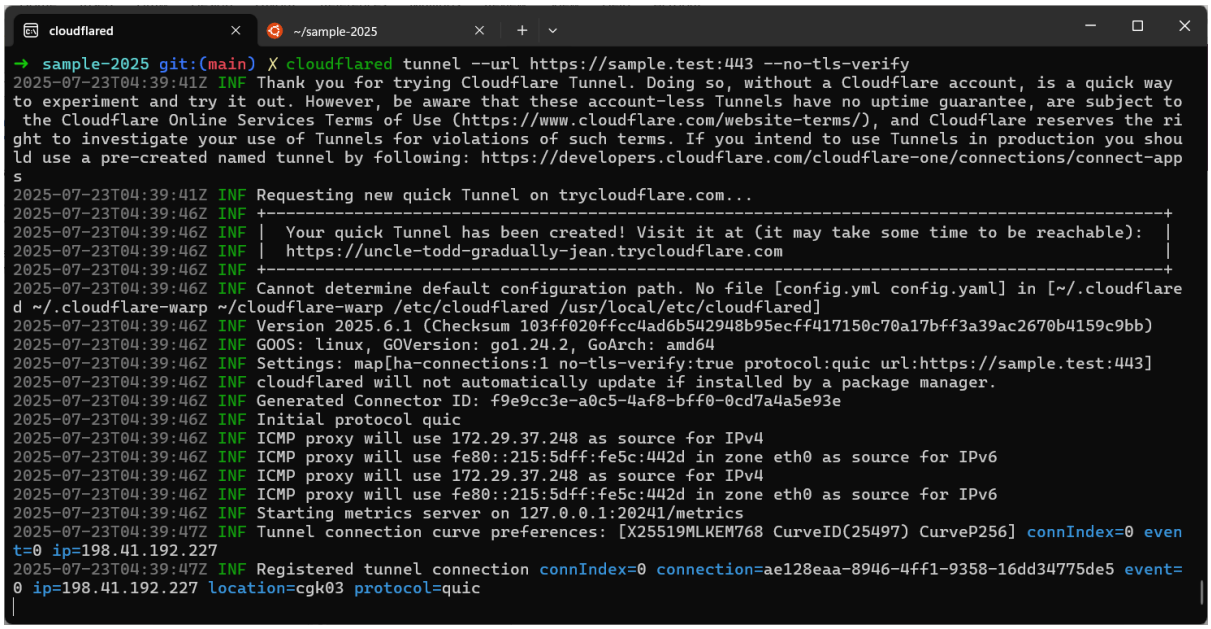
[36] Nothing was found for Session Token in URL.

[37] Nothing was found for API endpoints.

[38] Nothing was found for emails.

[39] Nothing was found for missing HTTP header - Rate Limit.


cloudflared
ptt
Powered by Pentest-Tools.com
Scanning target: https://uncle-todd-gradually-jean.trycloudflare.com/
Progress: 0%
Status: Running \
Start time: 2025-07-23 07:41:05
Duration: 0 seconds
Total tests: 0
Finished tests: 0


cloudflared
~/sample-2025
➜ sample-2025 git:(main) X cloudflared tunnel --url https://sample.test:443 --no-tls-verify
2025-07-23T04:39:41Z INF Thank you for trying Cloudflare Tunnel. Doing so, without a Cloudflare account, is a quick way to experiment and try it out. However, be aware that these account-less Tunnels have no uptime guarantee, are subject to the Cloudflare Online Services Terms of Use (https://www.cloudflare.com/website-terms/), and Cloudflare reserves the right to investigate your use of Tunnels for violations of such terms. If you intend to use Tunnels in production you should use a pre-created named tunnel by following: https://developers.cloudflare.com/cloudflare-one/connections/connect-apps
2025-07-23T04:39:41Z INF Requesting new quick Tunnel on trycloudflare.com...
2025-07-23T04:39:46Z INF Your quick Tunnel has been created! Visit it at (it may take some time to be reachable):
2025-07-23T04:39:46Z INF https://uncle-todd-gradually-jean.trycloudflare.com
2025-07-23T04:39:46Z INF Cannot determine default configuration path. No file [config.yml config.yaml] in [~/.cloudflared ~/.cloudflare-warp ~/cloudflare-warp /etc/cloudflared /usr/local/etc/cloudflared]
2025-07-23T04:39:46Z INF Version 2025.6.1 (Checksum 103ff020ffcc4ad6b542948b95ecff417150c70a17bff3a39ac2670b4159c9bb)
2025-07-23T04:39:46Z INF GOOS: linux, GOVersion: go1.24.2, GoArch: amd64
2025-07-23T04:39:46Z INF Settings: map[ha-connections:1 no-tls-verify:true protocol:quic url:https://sample.test:443]
2025-07-23T04:39:46Z INF cloudflared will not automatically update if installed by a package manager.
2025-07-23T04:39:46Z INF Generated Connector ID: f9e9cc3e-a0c5-4af8-bff0-0cd7a4a5e93e
2025-07-23T04:39:46Z INF Initial protocol quic
2025-07-23T04:39:46Z INF ICMP proxy will use 172.29.37.248 as source for IPv4
2025-07-23T04:39:46Z INF ICMP proxy will use fe80::215:5dff:fe5c:442d in zone eth0 as source for IPv6
2025-07-23T04:39:46Z INF ICMP proxy will use 172.29.37.248 as source for IPv4
2025-07-23T04:39:46Z INF ICMP proxy will use fe80::215:5dff:fe5c:442d in zone eth0 as source for IPv6
2025-07-23T04:39:46Z INF Starting metrics server on 127.0.0.1:20241/metrics
2025-07-23T04:39:47Z INF Tunnel connection curve preferences: [X25519MLKEM768 CurveID(25497) CurveP256] connIndex=0 event=0 ip=198.41.192.227
2025-07-23T04:39:47Z INF Registered tunnel connection connIndex=0 connection=ae128eaa-8946-4ff1-9358-16dd34775de5 event=0 ip=198.41.192.227 location=cgk03 protocol=quic