

7 Maret 2025

Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia



# **Laporan Perbaikan Hasil ITSA** Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia

Pada hari Senin, 3 Maret 2025 s/d Jumat, 7 Maret 2025 telah dilaksanakan kegiatan IT *Security Assessment* pada sistem elektronik milik Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia. Berikut adalah hasil perbaikan terhadap temuan yang ada:

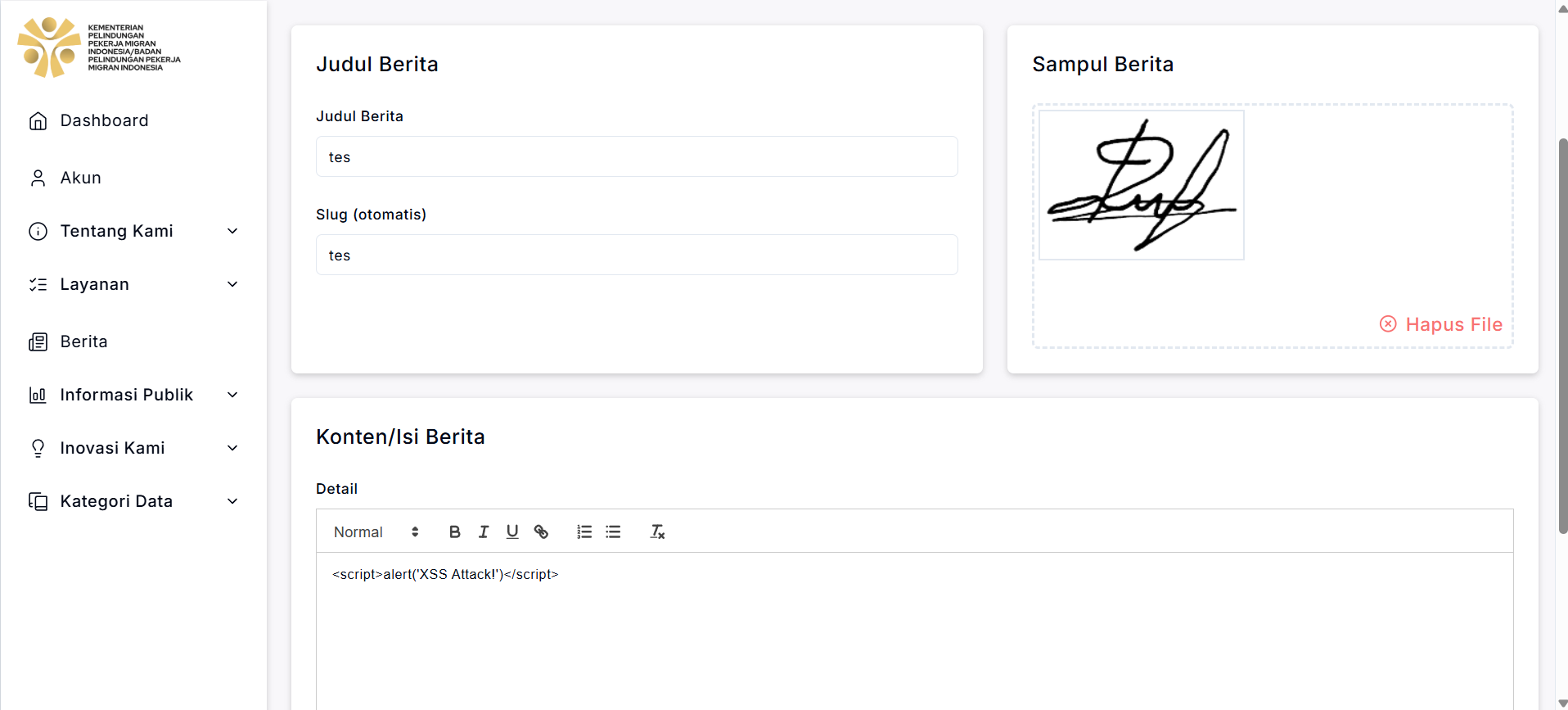
**Temuan ITSA pada Website BP3MI Sumatera Selatan**

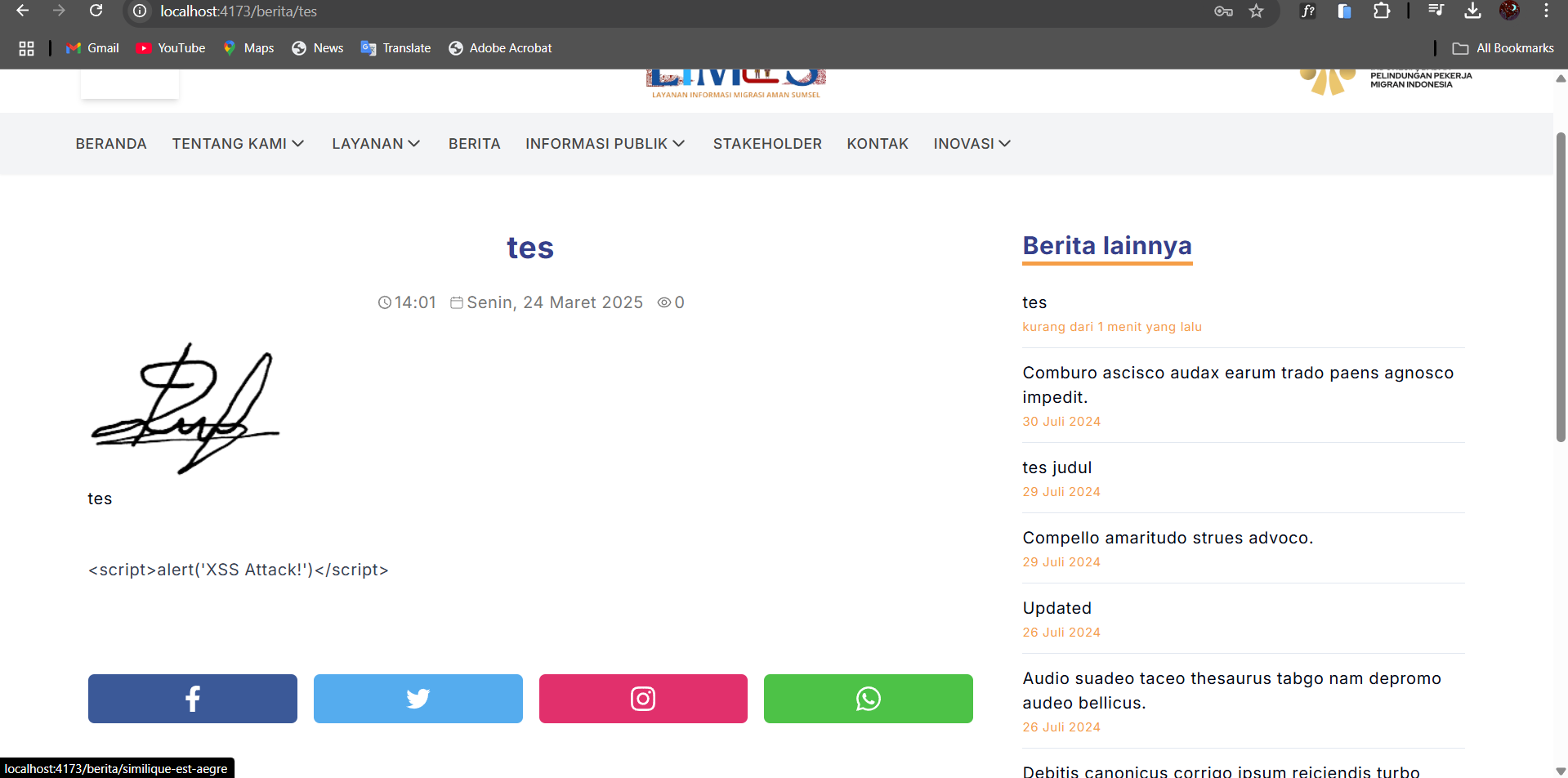
|  |  |
| --- | --- |
| Alamat URL | https://sumsel.bp2mi.go.id/ |
| Alamat IP | 10.56.0.169 |
| Versi | 1.0.0 |
| *Environment* | *Production*  *Staging*  *Development* |

| No | Jenis Kerentanan | Severity | Lokasi | Hasil Remediasi |
| --- | --- | --- | --- | --- |
| 1 | Stored Cross-Site Scripting (XSS) via 'Tambah Konten' | High | POST /api/news POST /api/p3mi (cek path lain) |  |
| 2 | Broken Access Control | High | GET /dashboard |  |
| 3 | Stored Cross-Site Scripting (XSS) via 'File Upload' | Medium | POST /api/news POST /api/job-vacancies (cek path lain) |  |
| 4 | No Rate Limit | Medium | POST /api/users/login |  |
| 5 | User Enumeration | Low | POST /api/users/login |  |

**Penjelasan Perbaikan Kerentanan pada Website BP3MI Sumatera Selatan**

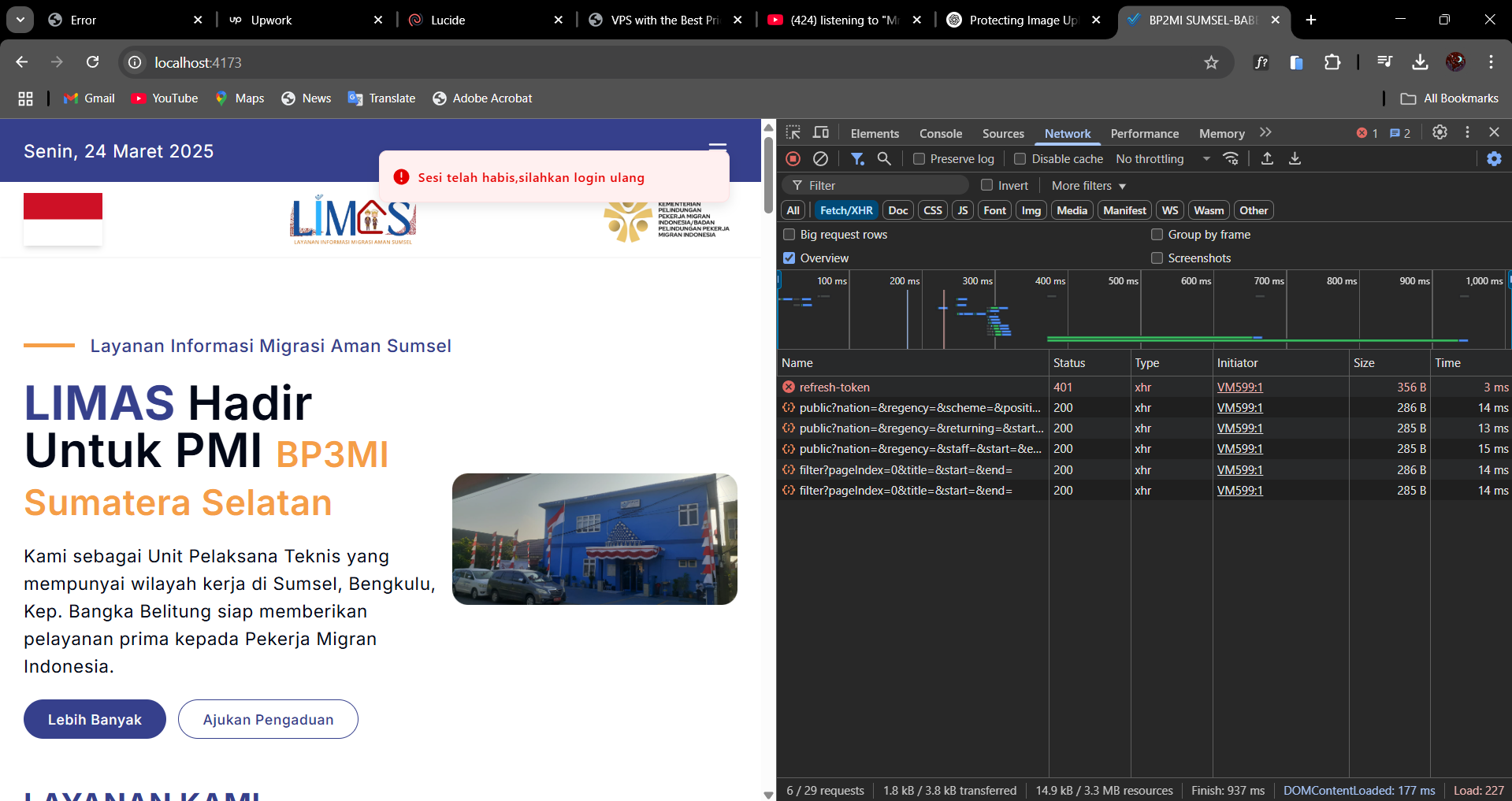
Berikut adalah cara pemilik sistem elektronik untuk menutup celah kerentanan hasil ITSA.

***Bukti 1  
***



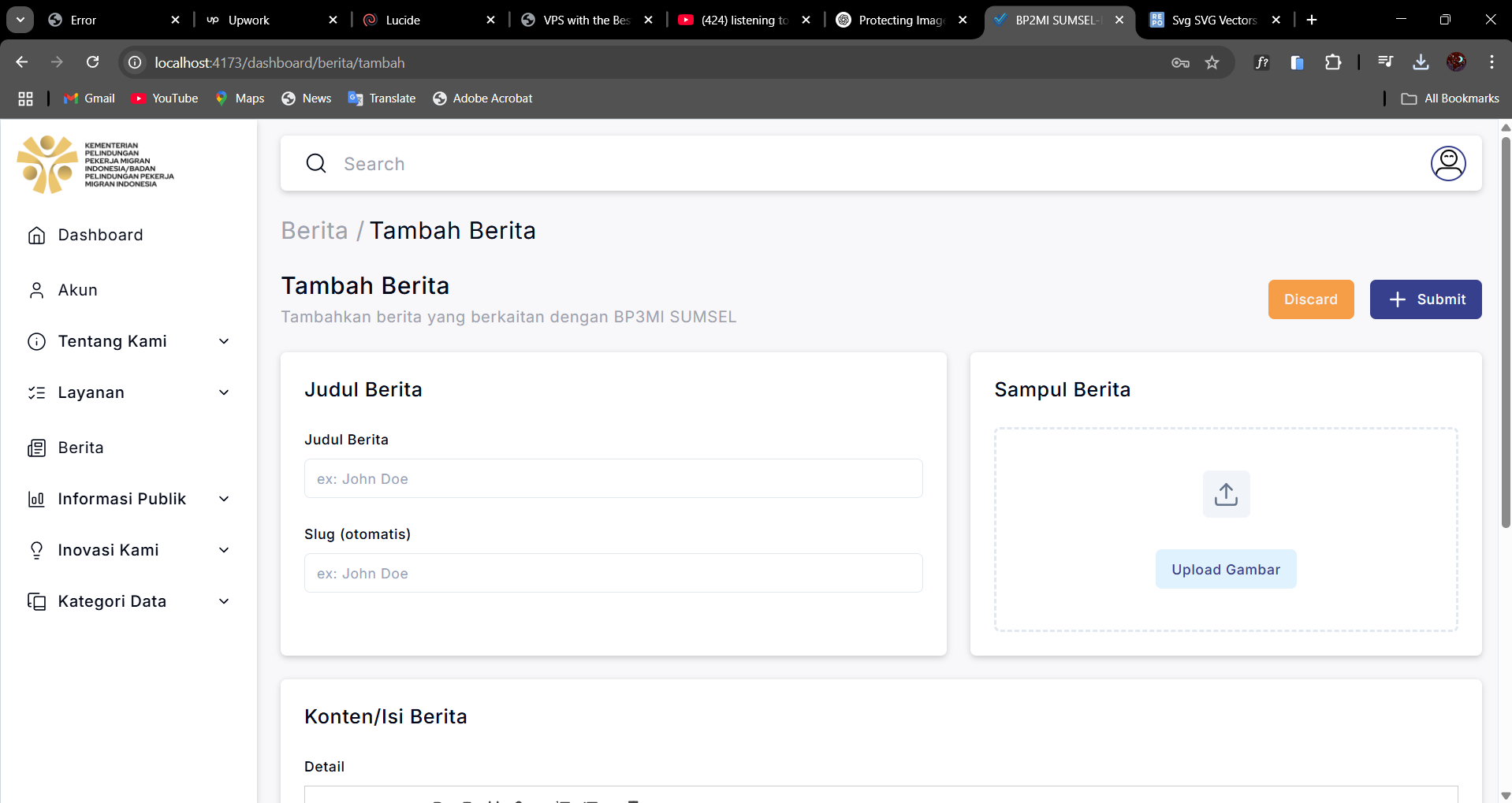
Keterangan   
Untuk menghindari isu Stored Cross-Site Scripting (XSS) via 'Tambah Konten', kami melakukan sanitasi terhadap Input WYSIWYG yang terdapat pada beberapa form. Dengan ini, script yang berbahaya tidak akan tereksekusi dan hanya dianggap sebagai teks biasa

***Bukti 2***



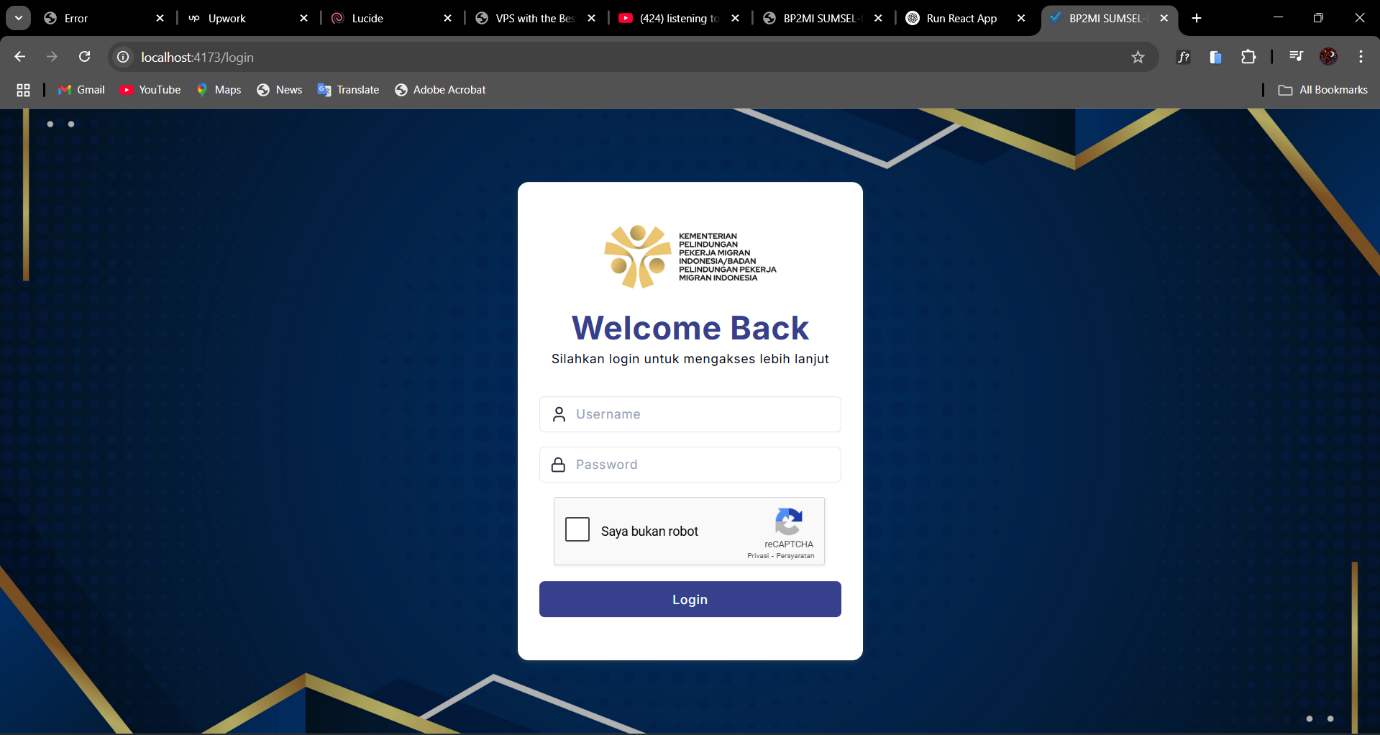
Keterangan   
Untuk menghindari isu Broken Access Control, kami akan langsung memblokir akses ke /dashboard dan halaman yang terproteksi lainnya ketika user tidak sedang terautentikasi, sehingga user sama sekali tidak bisa mengunjungi halaman yang tidak diinginkan. Data yang terproteksi juga tidak akan tampil sama sekali untuk user. Note : data diatas berupa public?... merupakan data public yang memang didapat untuk user tanpa autentikasi sama sekali.

***Bukti 3***



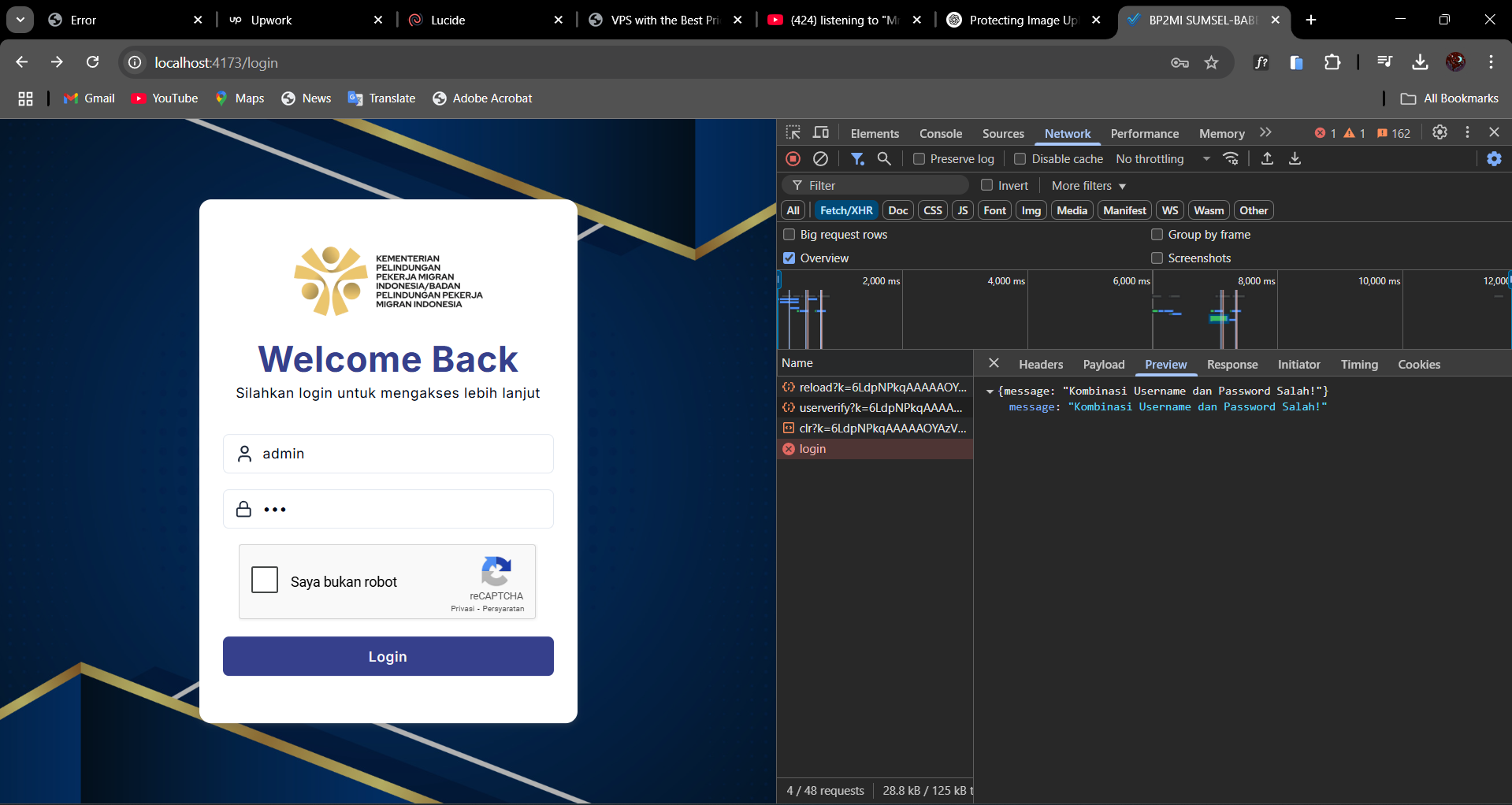
Keterangan   
Untuk menghindari isu Stored Cross-Site Scripting (XSS) via 'File Upload', kami menerapkan Solusi agar form File Upload hanya dapat menerima ekstensi file berupa gambar berupa JPG, PNG, JPEG, dan lainnya, terkecuali ektensi SVG dan ICO, karena kedua ekstensi tersebut dapat disusupi script didalamnya, dan kami juga memikirkan bahwa gambar dengan ekstensi SVG atau ICO terbilang sangat jarang digunakan dalam content management.

***Bukti 4***



Keterangan :  
Untuk menghindari isu No Rate Limit pada halaman login, kami menerapkan solusi berupa permintaan validasi reCaptcha pada kedua sisi FrontEnd & BackEnd, sehingga menghindari kemungkinan request spam dan isu terkait lainnya.

***Bukti 5***



Keterangan :  
Untuk menghindari isu User Numeration pada halaman login, kami hanya akan mengembalikan pesan berisi “Kombinasi Username dan Password Salah” saat ada user yang mencoba login dengan username ataupun password yang tidak tepat.

Bersama laporan ini kami sampaikan perbaikan hasil IT *Security Assessment* pada sistem elektronik milik Kementerian Pelindungan Pekerja Migran Indonesia/Badan Pelindungan Pekerja Migran Indonesia.

|  |  |
| --- | --- |
|  | Jakarta, 7 Maret 2025 Mengetahui,  Stakeholder  Nama PIC Stakeholder  Golongan / Ruang  NIP. 19680530 199001 1 001 |