**REPORT**

**EXAM MERDEKA SIBER**

Nama Peserta :

BATCH :

# Ringkasan Eksekutif

Berikut adalah ringkasan temuan celah keamanan pada aplikasi Lab Merdeka Siber dengan kategori website sebagai berikut.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Nama Temuan** | **Object** | **Severity Level** | **Status** |
| 1 | XSS Stored via File Upload  “Contoh” | Website | **HIGH** | **Open** |
|  |  |  |  |  |

**Note:** Tingkat keparahan (severity level) dari setiap temuan wajib diurutkan mulai dari **Critical** hingga **Low** dalam laporan akhir.

# Temuan

## Temuan Domain http://exam.merdekasiber.com/

### XSS Stored – Edit Profile [CONTOH]

|  |  |
| --- | --- |
| XSS Stored – Edit Profile | |
| Severity | **HIGH** |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N |
| Deskripsi | XSS atau cross site scripting adalah sebuah kerentanan yang terjadi pada sebuah aplikasi website, mobile apps, dan dekstop, dimana XSS Stored dapat terjadi saat pengguna diizinkan untuk memasukan data yang akan ditampilkan kembali dan telah disisipi malicious code. |
| Affected URL | https://XYZ.id |
| Dampak | 1. Eksekusi skrip berbahaya: Jika serangan berhasil, file berbahaya yang diunggah dapat berisi kode JavaScript atau skrip lain yang berbahaya. Ketika file tersebut diakses oleh pengguna lain, skrip tersebut dapat dieksekusi di browser mereka, mengizinkan penyerang untuk melakukan serangan XSS, mencuri informasi pribadi, atau mengubah tampilan halaman web. 2. Pengambilan kendali sistem: Jika serangan berhasil memanfaatkan kelemahan dalam aplikasi, penyerang dapat menggunakan file yang diunggah untuk mengambil kendali sistem atau server tempat aplikasi dijalankan. Ini dapat mengarah pada kerentanan yang lebih besar dan serangan lanjutan seperti injeksi perintah. 3. Pencurian data sensitif: Jika pengunggahan file berbahaya berhasil, penyerang dapat menggunakan file tersebut untuk mencuri data sensitif yang disimpan di server atau mengakses informasi pribadi pengguna lain yang terhubung dengan aplikasi yang rentan. |
| Kategori | Website |
| Rekomendasi | 1. Melakukan implementasi fungsi htmlspecialchars() yang berfungsi sebagai filter dan melakukan encode semua Tag HTML dan spesial karakter. 2. Melakukan validasi input yang berfungsi untuk mencegah XSS dari penggunaan spesial karakter. 3. Menggunakan implementasi CSP (Content Security Policy). |
| Referensi | https://cheatsheetseries.owasp.org/cheatsheets/Cross\_Site\_Scripting\_Prevention\_Cheat\_Sheet.html |
| **Bukti Temuan** | |
| Pada aplikasi terdapat sebuah fitur ‘Upload File yang dapat dimanfaatkan oleh penyerang menyisipkan file berbahaya.   * https://images.XYZ.id/assets/portal-assets/product/images/ | |
| **Status** | |