BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah penulis melakukan pengujian keamanan pada website Prestasi Mahasiswa UPNVJ, didapatkan kesimpulan sebagai berikut:

1. Identifikasi kerentanan dilakukan dengan pengujian keamanan pada asset website Prestasi Mahasiswa UPNVJ. Pengujian dilaksanakan dengan 4 fase pengujian yang dimulai dari fase planning, fase discovery, fase attack, dan diakhiri dengan fase reporting.
2. Kerentanan yang ditemukan pada situs Prestasi Mahasiswa UPNVJ dan telah diuji oleh peneliti terdiri dari:
    - 1 kerentanan A01:2021-Broken Access Control dengan severity medium
    - 3 kerentanan A02:2021-Cryptographic Failures dengan severity low
    - 1 kerentanan A03:2021-Injection dengan severity Medium
    - Tidak ditemukan kerentanan yang valid untuk kategori A04:2021-Insecure Design
    - 4 kerentanan A05:2021-Security Misconfiguration dengan 1 diantaranya memiliki severity medium dan 3 lainnya memiliki severity low
    - 1 kerentanan A06:2021-Vulnerable And Outdated Components dengan severity Medium
    - Tidak ditemukan kerentanan yang valid untuk kategori A07:2021-Identification and Authentication Failures
    - Tidak dilakukan pengujian untuk kerentanan A08:2021-Software and Data Integrity Failures dan kerentanan A09:2021-Security Logging and Monitoring Failures.

- Tidak ditemukan kerentanan A10:2021-Server-Side Request Forgery (SSRF) pada situs target.

3. Setiap kerentanan yang ditemukan dapat diremidiasi dan dimitigasi untuk setiap kerentanannya. Remediasi dan mitigasi yang dapat dilakukan antara lain:
    - Kerentanan A01:2021-Broken Access Control yang ditemukan dapat diremediasi dengan menerapkan kontrol akses yang tepat pada file sensitif.
    - Kerentanan A02:2021-Cryptographic Failures yang ditemukan dapat diremediasi dengan menambahkan header, flag, dan attribute sesuai best practicenya pada response dari web server.
    - Kerentanan A03:2021-Injection yang ditemukan dapat diremediasi dengan menambahkan Header Content Security Policy sesuai dengan Content yang diijinkan untuk dimuat oleh user.
    - Kerentanan A05:2021-Security Misconfiguration yang ditemukan dapat diremediasi dengan menambahkan header, flag, dan attribute sesuai best practicenya pada response dari web server. Untuk kerentanan dimana terpaparnya informasi sensitif pada response header dapat diremediasi dengan mengkonfigurasi web server untuk menghapus atau menyembunyikan informasi versi server pada header HTTP.
    - Kerentanan A06:2021-Vulnerable And Outdated Components yang ditemukan dapat diremediasi dengan melakukan pembaruan libraries Javascript pihak ketiga yang digunakan secara rutin. Diperlukan juga untuk selalu memantau peringatan keamanan terkait libraries yang digunakan.

5.2 Saran

Berdasarkan pada pembahasan dan kesimpulan yang telah penulis dapatkan, penulis memberikan beberapa saran yang dapat diterapkan dimasa depan, antara lain:

1. Penelitian serupa dimasa depan dapat dilakukan dengan menggunakan metode penetration testing lain yang mungkin lebih cocok untuk kasus tertentu. Dapat juga ditambahkan metode Whitebox testing saat melakukan pengujian agar dapat melakukan static code analysis agar setiap aspek dari asset yang diuji dapat tercover sepenuhnya.
2. Sebaiknya dilakukan Kembali pengujian ulang pada website terkait setelah dilakukannya remediasi baik itu fine-tuning maupun hardening, agar dapat dipastikan kerentanan telah diremediasi dengan baik dan tidak timbul adanya kerentanan baru dari remediasi tersebut.
3. Pengujian pada presma.upnvj.ac.id pada penelitian ini hanya salah satu dari banyaknya subdomain yang berada dibawah domain utama upnvj.ac.id. Karena itu, dapat dilakukan penelitian serupa pada subdomain upnvj lain yang dapat menjadi pintu masuk penyerang dalam menyusup ke sistem utama Universitas Pembangunan Nasional Veteran Jakarta.