EAS MANAJEMEN KEAMANAN IT

Disusun guna memenuhi EAS mata kuliah Manajemen Keamanan IT

Dosen Pengampu:
Dr. Ir. Mohammad Idhom, SP, S. Kom., MT

Disusun oleh:

Fauzan Ilyas Almeyda

(23081010188)

PROGRAM STUDI INFORMATIKA

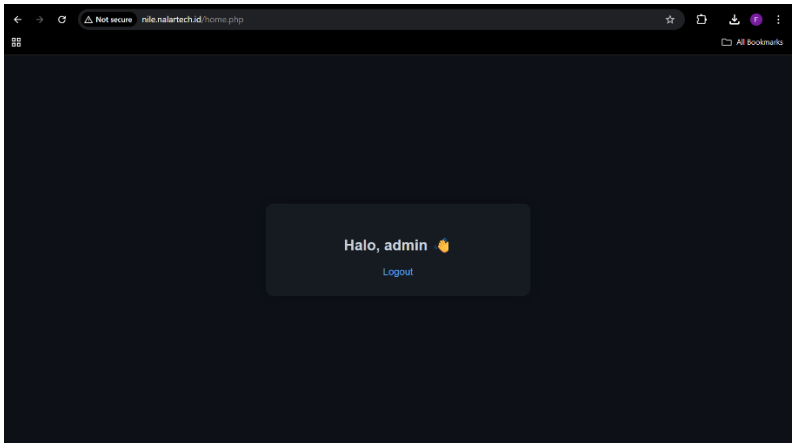
FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAWA TIMUR

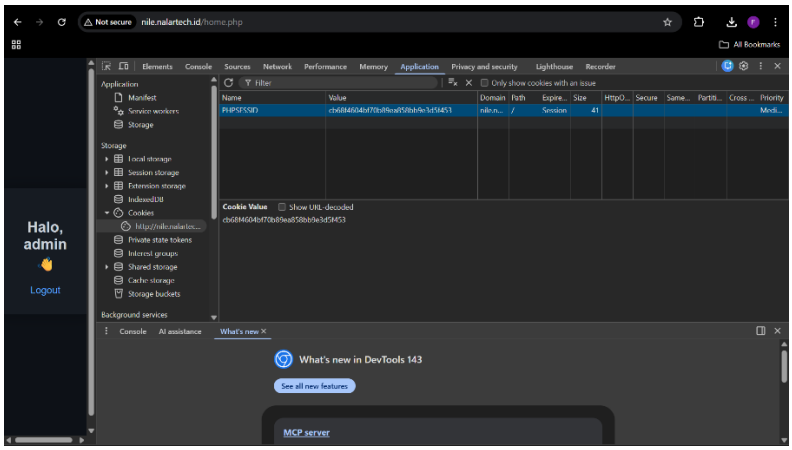
TAHUN 2025

1. Bagian A (Identifikasi Session dan Cookie)

- Screenshot Halaman Home



- Screenshot Devtools cookie



- Hasil Observasi

Kriteria Audit	Hasil	Aman?	Penjelasan Resiko
Session ID dapat dilihat di halaman	Ya	**Ya/Tidak** Tidak	Session ID (PHPSESSID) tersimpan pada browser dan dapat dilihat melalui DevTools pada bagian Application → Cookies. Penyimpanan Session ID di sisi client memiliki potensi risiko, karena apabila pihak tidak berwenang berhasil mengakses browser pengguna (XSS,Shared Pc), maka session dapat disalahgunakan yang mengakibatkan terjadinya session hijacking.
Cookie memiliki HttpOnly flag	Tidak	**Ya/Tidak** Tidak **Kenapa penting?** Tanpa HttpOnly flag memungkinkan	Berbahaya karena dapat beresiko terkena serangan XSS dapat dimanfaatkan untuk mencuri session id (PHPSESSID) untuk menguasai sesi pengguna.

		cookie diakses oleh skrip di sisi client.	
Cookie memiliki Secure flag	Tidak	**Ya/Tidak** Tidak **Apa resikonya di wifi publik?** Data yang dikirim melalui koneksi HTTP tanpa Secure flag dapat dengan mudah disadap oleh pihak lain yang berada pada jaringan yang sama.	Beresiko karena penyerang dapat melakukan penyadapan lalu lintas data (sniffing) atau serangan Man-in-the-Middle (MITM) untuk mencuri nilai PHPSESSID, sehingga memungkinkan terjadinya pengambilalihan sesi pengguna.
Session ID berubah setelah login	Tidak	**Ya/ Tidak** Tidak **Dampak Fixation** Session fixation berpotensi mengakibatkan pengambilalihan akun, karena penyerang dapat memanfaatkan Session ID yang identik dengan milik korban setelah proses autentikasi berhasil dilakukan.	Penyerang dapat menetapkan atau mengetahui Session ID terlebih dahulu, kemudian memanfaatkan Session ID tersebut setelah korban melakukan autentikasi. Penyerang memperoleh akses tanpa perlu mengetahui kredensial login.
Session ID berubah setelah logout	Tidak	**Ya/Tidak** Tidak **Potensi Reuse Session** Ya, Session lama berpotensi dapat digunakan kembali oleh pihak yang tidak bertanggung jawab karena tidak dihancurkan/ diganti setelah proses logout.	Session id yang sama dan dapat digunakan kembali sangat berisiko terutama pada penggunaan perangkat bersama atau komputer umum, karena pihak lain dapat memanfaatkan session tersebut untuk mengakses akun pengguna.

2. Bagian B (Analisis Keamanan)
   - **Apa risiko keamanan jika session ID dapat terlihat oleh user di halaman?**
     : Session ID yang dapat diakses di sisi client berisiko dicuri dan disalahgunakan oleh pihak tidak berwenang, sehingga memungkinkan terjadinya session hijacking dan pengambilalihan akun pengguna.

- **Jelaskan risiko Tidak adanya Secure flag pada jaringan HTTP/WiFi publik.**
  : Tanpa Secure flag, cookie dapat dikirim melalui koneksi tidak terenkripsi. Pada WiFi publik, kondisi ini memungkinkan penyadapan data dan pencurian Session ID melalui serangan sniffing atau Man-in-the-Middle.

- **Apa yang terjadi jika session ID tidak berubah setelah login dan logout? (hubungkan dengan session fixation & session reuse attack)**
  : Jika Session ID tidak dibuat ulang setelah login, aplikasi rentan terhadap session fixation. Jika tidak dihapus setelah logout, Session ID lama dapat digunakan kembali oleh penyerang dengan session reuse attack untuk mengakses akun tanpa login ulang.

- **Dari hasil observasi, menurut kamu apa vektor serangan paling berbahaya pada aplikasi ini?**
  : Vektor serangan paling berbahaya adalah session hijacking atau penyalahgunaan session, karena kelemahan pengelolaan session memungkinkan penyerang mengambil alih sesi pengguna dengan mudah.

3. Bagian C (Rekomendasi Mitigasi)

   - **Batasi masa aktif session (session timeout)**
     Session sebaiknya memiliki batas waktu tertentu dan otomatis berakhir jika tidak ada aktivitas pengguna. Hal ini dapat mengurangi risiko penyalahgunaan session yang sudah tidak digunakan.

   - **Aktifkan HTTPS dan atur cookie agar hanya dikirim melalui HTTPS**
     Aplikasi sebaiknya menggunakan HTTPS pada seluruh halaman, serta memastikan cookie session hanya dikirim pada koneksi aman agar Session ID tidak dapat disadap di jaringan publik.

   - **Aktifkan atribut HttpOnly dan Secure pada cookie session**
     Atribut HttpOnly mencegah cookie diakses melalui JavaScript, sedangkan Secure memastikan cookie hanya dikirim melalui koneksi HTTPS, sehingga mengurangi risiko pencurian Session ID.

4. Bagian D (Kesimpulan)

   - **Seberapa aman session aplikasi ini?**
     : Session pada aplikasi ini **kurang aman**, karena mekanisme pengelolaan session masih memiliki celah keamanan, khususnya pada pengaturan cookie dan Session ID yang berpotensi memungkinkan terjadinya pengambilalihan sesi oleh pihak tidak berwenang.

   - **Apa kelemahan paling kritikal?**
     : Kelemahan paling kritikal adalah tidak diterapkannya pengamanan cookie session, seperti Secure dan HttpOnly, serta tidak optimalnya pengelolaan Session ID.

   - **Langkah perbaikan prioritas?**
     : Langkah perbaikan prioritas adalah mengamankan cookie session dan memperbaiki manajemen Session ID, termasuk penggunaan HTTPS dan pengaturan agar session bisa di regenerasi/dibuat ulang.