BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

4.1. Penentuan Ruang Lingkup (*Scope*)

Peneliti menerapkan ruang lingkup penelitian pada Web KRS Daring untuk menjadi target pengujian merujuk pada daftar hasil penilaian risiko pada penelitian sebelumnya (Yuhaz, 2018). Hasil yang ingin dicapai peneliti adalah pencarian akun milik mahasiswa.

4.2. Pengintaian Sistem (*Reconnaissance*)

Tahap pengintaian ini dilakukan untuk mencari informasi dasar target dan melakukan *port scanning* menggunakan *Nmap*. Pada *Nmap* terdapat dua cara dalam melakukan *port scanning* yaitu yang pertama dengan *command prompt / terminal* atau yang kedua dengan *Zenmap* yang memiliki GUI untuk mempermudah peneliti melakukan *port scanning*. Peneliti hanya tinggal mengetikan target pengujian dan memilih *profile scan* yang diinginkan. Pada pengujian ini memilih menggunakan *profile scan "slow comprehensive scan"* di mana *Zenmap* akan melakukan pemindai secara menyeluruh untuk mendapatkan informasi tentang *port* seperti pada **Gambar 4.1**.

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

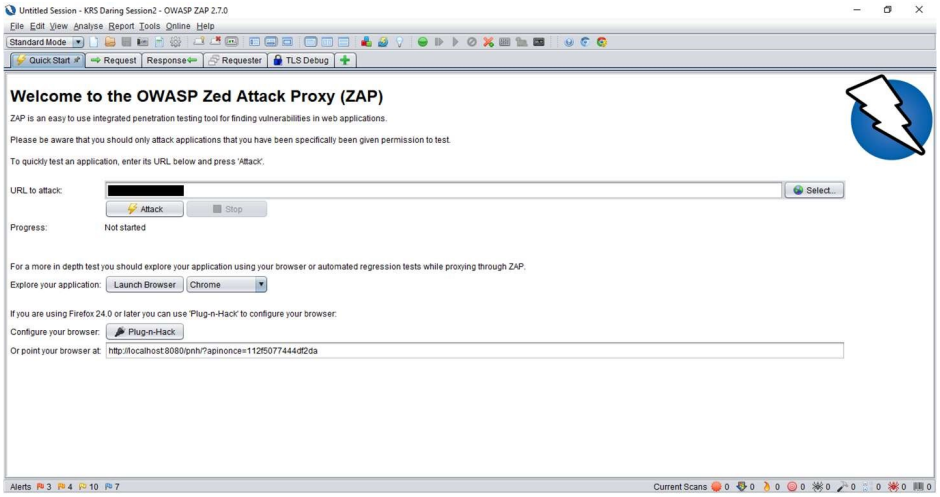
Port	Protocol	State	Service	Version
80	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
443	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
445	tcp	open	microsoft-ds	
3389	tcp	open	ms-wbt-server	
49155	tcp	open	msrpc	Microsoft Windows RPC

Gambar 4. 1 *Port* yang terbuka

4.3. Pencarian Kerentanan Keamanan (*Vulnerability Detection*) Menggunakan *Tools Software* OWASP ZAP

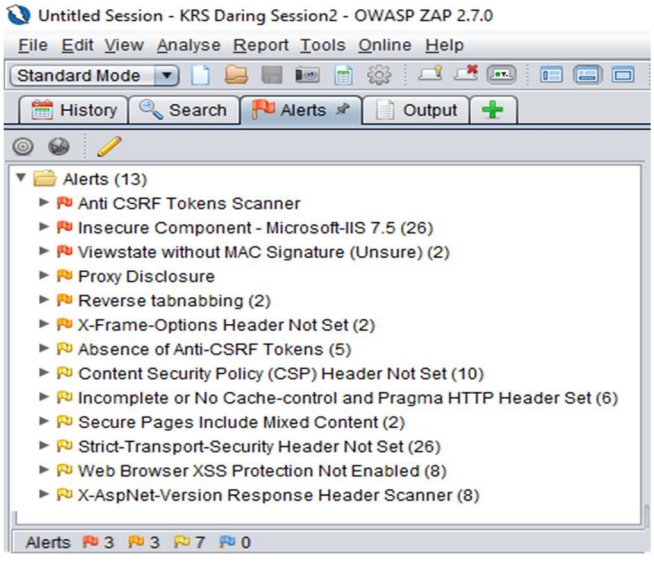
Pada tahap pencarian kerentanan keamanan akan dilakukan *Vulnerability Scanning* menggunakan OWASP ZAP (*Open Web Application Security Project*

Zed Attack Proxy). Tujuan dilakukan *vulnerability scanning* adalah untuk mencari kerentanan keamanan pada Web KRS Daring. Hasil pencarian kerentanan keamanan digunakan sebagai bahan untuk melakukan *penetration testing*. Pencarian kerentanan keamanan dilakukan dengan cara memasukkan URL KRS Daring di tampilan awal pada OWASP ZAP di **Gambar 4.2**.



Gambar 4. 2 Tampilan awal OWASP ZAP

Setelah itu langsung tekan tombol "*Attack*" dan tunggu proses pemindaian selesai. Setelah proses pemindaian selesai pada **Gambar 4.3** muncul daftar kerentanan keamanan di bagian *Tab Menu* "*Alert*".



Gambar 4. 3 Daftar Kerentanan Keamanan KRS Daring

Pada hasil pencarian kerentanan menggunakan OWASP ZAP terdapat salah satu kerentanan pada Web KRS Daring yaitu *Anti CSRF Tokens Scanner*, kerentanan ini memiliki *level High*, kerentanan ini mengindikasikan tidak ada mekanisme perlindungan *token* keamanan pada halaman web tersebut, untuk lebih lengkapnya ada pada **Tabel 4.1** di bawah ini.

Tabel 4. 1 Penjelasan kerentanan keamanan pada KRS Daring

No.	Nama Kerentanan	*Level*	Deskripsi
1	*Anti CSRF Tokens Scanner*	*High*	Kerentanan ini mengindikasikan tidak ada mekanisme perlindungan token keamanan pada halaman web.
2	*Insecure Component – Microsoft-IIS 7.5*	*High*	Kerentanan ini mengindikasikan IIS masih menggunakan versi 7.5, saat ini IIS sudah versi 10.
3	*Viewstate without MAC Signature (Unsure)*	*High*	Kerentanan ini mengindikasikan situs web ini menggunakan ASP.NET *Viewstate* mungkin tanpa MAC (*Message Authentication Code*).
4	*Proxy Disclosure*	*Medium*	Kerentanan ini mengindikasikan satu *proxy server* terdeteksi informasi ini potensial membantu penyerang untuk menentukan: a. Daftar target untuk serangan terhadap aplikasi. b. Potensi kerentanan pada *server proxy* yang melayani aplikasi. c. Ada atau tidak adanya komponen yang mungkin menyebabkan serangan terhadap aplikasi untuk di deteksi, di cegah, atau dikurangi.
5	*Reverse Tabnabbing*	*Medium*	Kerentanan ini mengindikasikan halaman Web KRS Daring bisa di kloning untuk serangan berupa *phising*.

No.	Nama Kerentanan	*Level*	Deskripsi
6	*X-Frame-Options Header Not Set*	*Medium*	Kerentanan ini berpotensi terkena serangan *ClickJacking*.
7	*Absence of Anti-CSRF*	*Low*	Kerentanan ini mengindikasikan tidak ada token *Anti-CSRF* yang di temukan pada *HTML Submission Form*.
8	*Content Security Policy (CSP) Header Not Set*	*Low*	Kerentanan ini mengindikasikan pada *Content Security Policy (CSP)* tidak diaktifkan.
9	*Incomplete or No Cache-control and Pragma HTTP Header Set*	*Low*	Kerentanan ini memungkinkan data tersimpan di *cache*.
10	*Secure Pages Include Mixed Content*	*Low*	Kerentanan ini mengindikasikan halaman web dapat diakses melalui HTTP bukan HTTPS.
11	*Strict-Transport-Security Header Not Set*	*Low*	Kerentanan ini mengindikasikan pengalihan akses HTTPS ke HTTP dengan memasukkan sertifikat tidak *valid*.
12	*Web Browser XSS Protection Not Enabled*	*Low*	Kerentanan ini mengindikasikan *XSS Protection* tidak diaktifkan.
13	*X-AspNet-Version Response Header Scanner*	*Low*	Kerentanan ini mengindikasikan rentan terkena *sniffing* apabila menggunakan *web browser Internet Explorer* dan *Google Chrome* versi lama.

4.4. Analisis dan Perencanaan *Penetration Testing*

Pada tahap ini peneliti melakukan analisis untuk menentukan kerentanan yang akan diuji dari hasil pencarian kerentanan pada Web KRS Daring. Peneliti memilih satu kerentanan yang digunakan untuk bahan *penetration testing* yaitu *Secure Pages Include Mixed Content* yang memiliki kerentanan *level Low*, alasan memilih kerentanan ini karena bisa dimanfaatkan untuk mendapatkan akun nama

pengguna dan kata sandi KRS Daring. *Tools* yang digunakan untuk *penetration testing* adalah *Arpspoof* dan *SSLStrip*, untuk pendekatannya menggunakan metode *Social Engineering*.

4.5. *Penetration Testing*

Pada tahap ini peneliti melakukan *penetration testing* berdasarkan hasil analisis dan perencanaan *penetration testing* dan kerentanan keamanan yang dipilih adalah *Secure Pages Include Mixed Content*. Kerentanan keamanan tersebut peneliti melakukan pengujian dengan memanfaatkan kelemahan sistem dari web KRS Daring yang kebanyakan web dirancang memakai https melalui *request http* (*port* 80) atau *https* (*port* 443). Web *port* 80 biasanya hanya sebagai jembatan untuk menuju web yang sebenarnya pada port 443, dengan kata lain http sebagai gerbang menuju https. Pengujian ini menggunakan *tools Moxie Marlinspike SSLStrip* dan *Arpspoof*. SSLStrip adalah *tools* untuk menyerang web yang dilindungi oleh https, cara kerjanya mencegah peralihan web dari *http* ke *https* dengan secara aktif mengubah *response* dari server sehingga pengunjung web akan tetap pada di *protocol http*. Sedangkan *Arpspoof* adalah *tools* untuk memanipulasi paket ARP (*Address Resolution Protocol*) dari *client* target agar semua paket – paket data dari *client* dialihkan ke *hacker* terlebih dahulu, ARP merupakan *protocol* yang bertugas memetakan *IP Address* menjadi *MAC Address* melalui penghubung antara datalink layer dan *IP Layer* pada *TCP/IP* dan bekerja pada *Layer* 2.

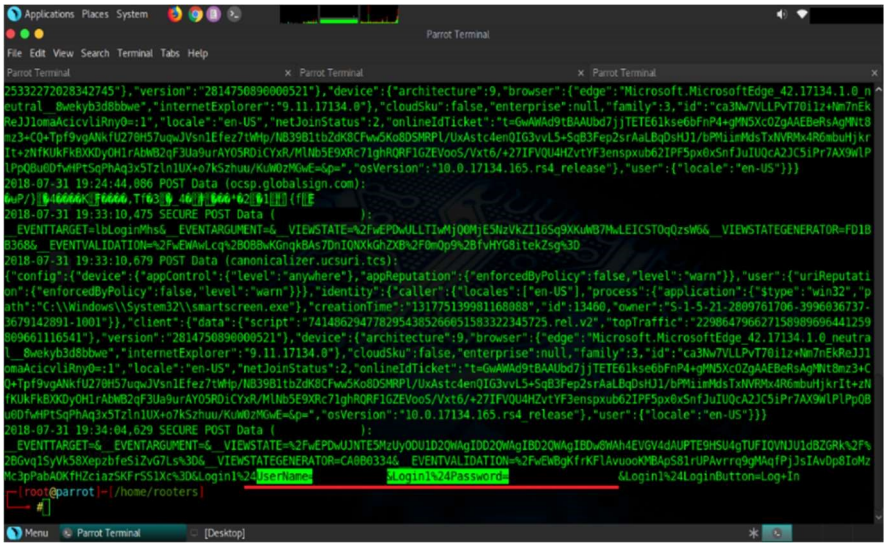
Target yang diinginkan dari peneliti adalah mendapatkan akun nama pengguna dan kata sandi KRS Daring dengan pendekatan *Social Engineering* adalah salah satu metode yang biasa digunakan oleh seorang *hacke*r untuk memperoleh informasi tentang targetnya dengan cara menipu secara halus tanpa disadari sampai bisa meyakinkan si targetnya. Peneliti sudah melakukannya dan mendapatkan dua target mahasiswa yang memiliki akun KRS Daring dari Institusi XYZ dan identitasnya dirahasiakan oleh peneliti. Pendekatan *Social Engineering* yang dilakukan peneliti dengan dua skenario berbeda.

4.5.1. Skenario Pertama Mahasiswa A

Pada skenario ini peneliti mengajak kepada target yaitu Mahasiswa A untuk bertemu di salah satu tempat yang sudah ditentukan oleh peneliti dan Mahasiswa A. Skenarionya peneliti berpura – pura meminta tolong kepada Mahasiswa A tersebut bersedia menjadi responden peneliti untuk mengomentari tampilan web pada KRS Daring sebagai bahan penelitian untuk peneliti, dan Mahasiswa A bersedia meluangkan waktunya dan peneliti meminta Mahasiswa A untuk membawa laptopnya pada hari-H.

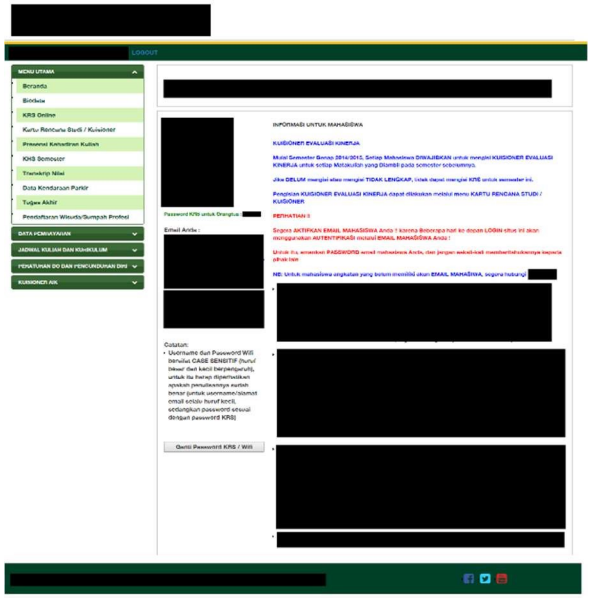
Pada hari-H akhirnya peneliti bertemu dengan Mahasiswa A di tempat yang sudah ditentukan, peneliti meminta Mahasiswa A untuk menyiapkan laptopnya dan peneliti sudah mempersiapkan laptopnya juga untuk dilakukan uji penyerangan dengan *tools Arpspoof* dan *SSLStrip* ke laptop Mahasiswa A, pada saat itu juga proses pendekatan *Social Engineering* telah berjalan. Peneliti meminta kepada Mahasiswa A untuk mengakses KRS Daring ke laptopnya dan peneliti mengecek ke laptop Mahasiswa A untuk memastikan bahwa *tools Arpspoof* dan *SSLStrip* berjalan dengan baik dan KRS Daring pada *protocol http* bukan https. Selanjutnya peneliti berpura-pura untuk mewawancarai Mahasiswa A mengenai tampilan pada KRS Daring sampai Mahasiswa A *login* ke KRS Daring dan memasukkan akun nama pengguna dan kata sandi melalui laptopnya sendiri.

Setelah peneliti sudah selesai melakukan pendekatan *Social Engineering* kepada Mahasiswa A ini maka hasilnya adalah mendapatkan akun pengguna dan kata sandi KRS Daring milik Mahasiswa A. Karena pada saat Mahasiswa A login ke KRS Daring nama pengguna dan kata sandi terekam masuk ke *log SSLStrip* di laptop milik peneliti seperti pada **Gambar 4.4**, lalu mencoba *login* ke KRS Daring dengan akun milik Mahasiswa A. Setelah mencoba login akhirnya berhasil *login* dengan akun milik Mahasiswa A seperti pada **Gambar 4.5**, terdapat juga data pribadi pada **Gambar 4.6**, data kendaraan pada **Gambar 4.7**, dan reset kata sandi pada **Gambar 4.8**.



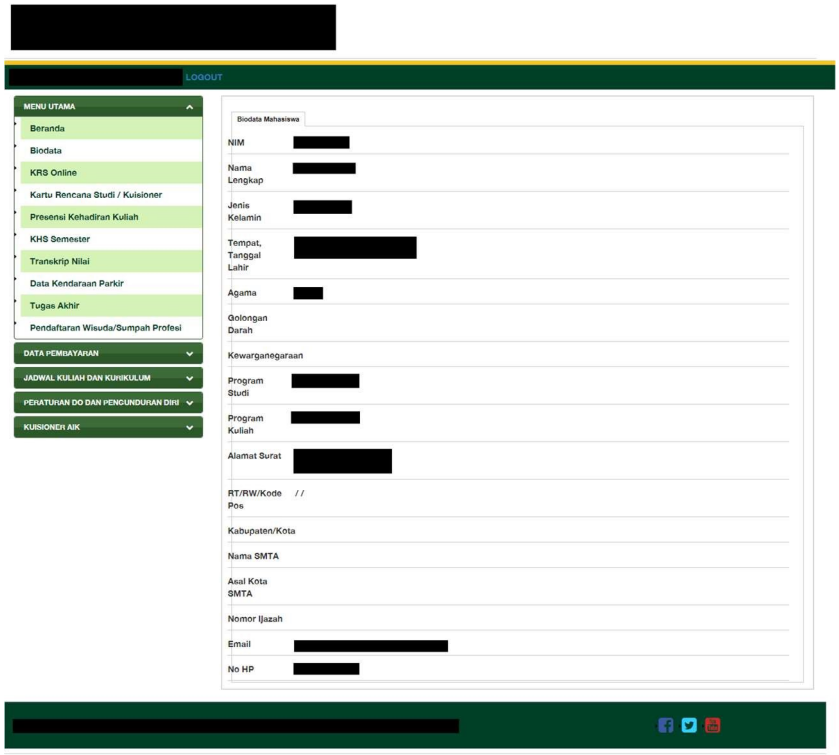
Gambar 4. 4 Hasil log *SSLStrip* pada perangkat milik Mahasiswa A

Pada gambar di atas ini merupakan *log* dari kegiatan Mahasiswa A pada saat membuka *browser* dan mengakses Web KRS Daring, lalu Mahasiswa A memasukkan nama pengguna dan kata sandi Web KRS Daring.



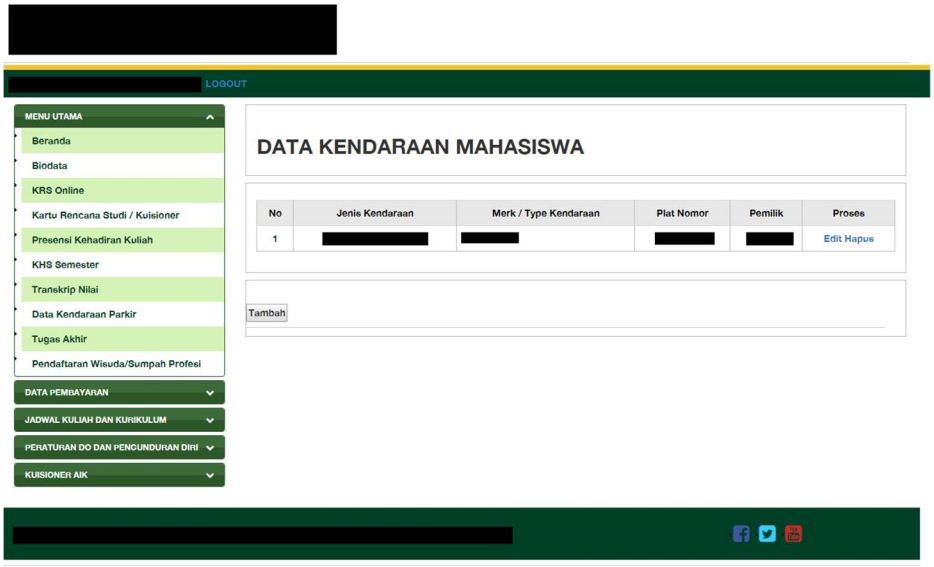
Gambar 4. 5 Tampilan KRS Daring milik Mahasiswa A

Peneliti melakukan *login* untuk memverifikasi bahwa nama pengguna dan kata sandi benar milik Mahasiswa A. Pada gambar diatas merupakan tampilan awal Web KRS Daring milik Mahasiswa A setelah *login*.



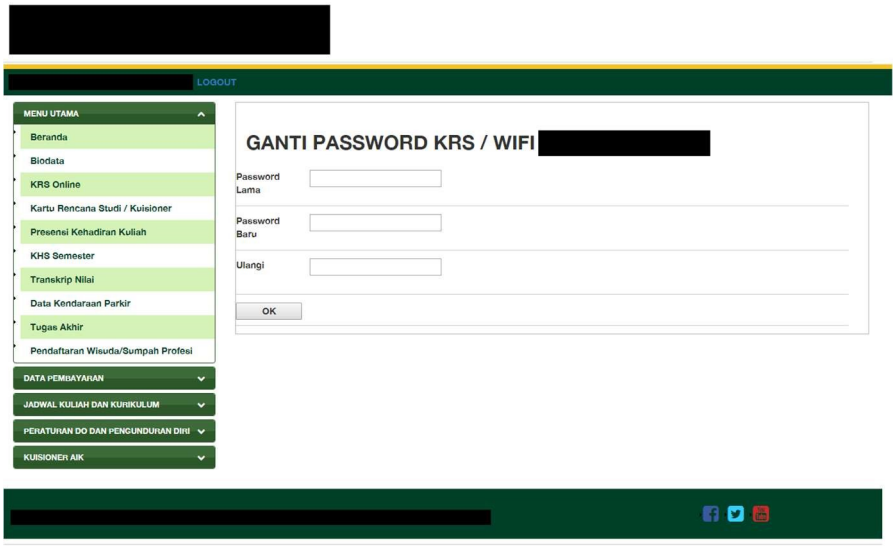
Gambar 4. 6 Data pribadi milik Mahasiswa A

Pada gambar diatas peneliti bisa melihat data pribadi milik Mahasiswa A. Terdapat informasi penting seperti NIM (Nomor Induk Mahasiswa), Nama Lengkap, Tempat Tanggal Lahir, Alamat Rumah, dan Nomor HP.



Gambar 4. 7 Data kendaraan milik Mahasiswa A

Pada gambar diatas peneliti bisa melihat data kendaraan milik Mahasiswa A, terdapat nama Jenis Kendaraan, Merk/Type Kendaraan, Pelat Nomor, dan Pemilik. Peneliti bisa merubah atau menghapus data kendaraan tersebut.



Gambar 4. 8 Reset kata sandi KRS Daring milik Mahasiswa A

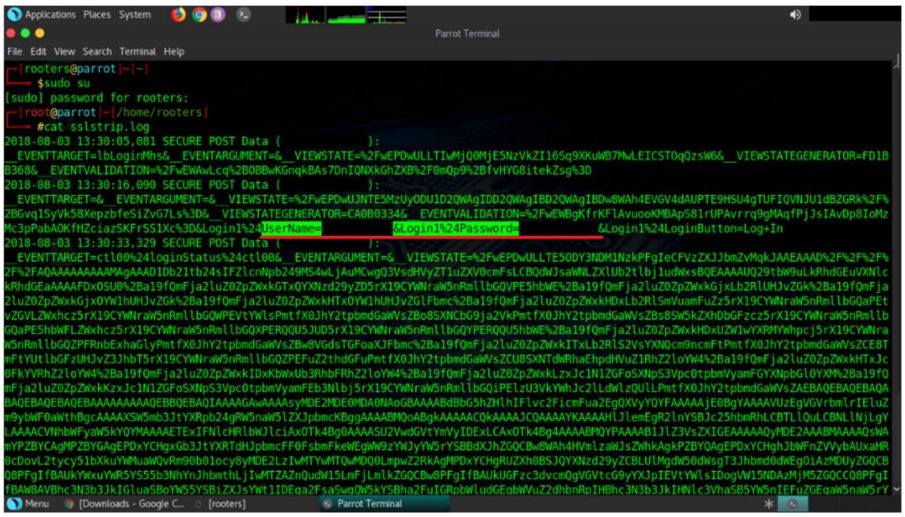
Pada gambar diatas peneliti bisa melakukan reset kata sandi KRS Daring milik Mahasiswa A.

4.5.2. Skenario Kedua Mahasiswa B

Peneliti melakukan pengintaian jaringan secara spontan disalah satu area gedung Institusi Pendidikan XYZ dan melakukan pemindaian untuk mengetahui perangkat apa saja yang terhubung pada jaringan area gedung tersebut. Secara tidak sengaja peneliti mengenali salah satu mahasiswa sedang duduk di area gedung tersebut dan akhirnya peneliti memilih mahasiswa tersebut sebagai target sebut saja Mahasiswa B, pada saat itu juga proses *Social Engineering* berlangsung.

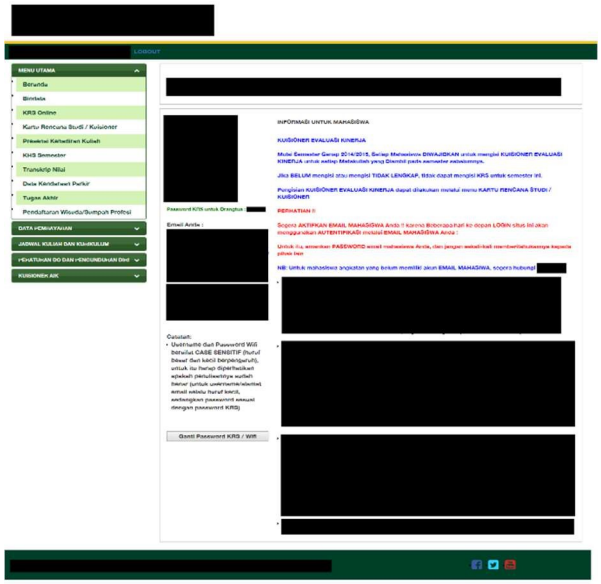
Pada kali ini peneliti meminta mengakses dan menyuruh masuk KRS Daring ke Mahasiswa B dengan alasan ingin mengetahui macam-macam mata kuliah apa saja yang ada di prodinya. Akhirnya Mahasiswa B melakukannya dan Peneliti berhasil mendapatkan akun nama pengguna dan kata sandi KRS Daring pada *log SSLStrip* seperti pada **Gambar 4.9**. Lalu peneliti mencoba *login* ke KRS Daring

dengan akun milik Mahasiswa B. Setelah mencoba *login* akhirnya berhasil login dengan akun milik Mahasiswa B seperti **Gambar 4.10**, terdapat juga data pribadi seperti **Gambar 4.11**, data kendaraan seperti **Gambar 4.12**, dan reset kata sandi seperti **Gambar 4.13**.



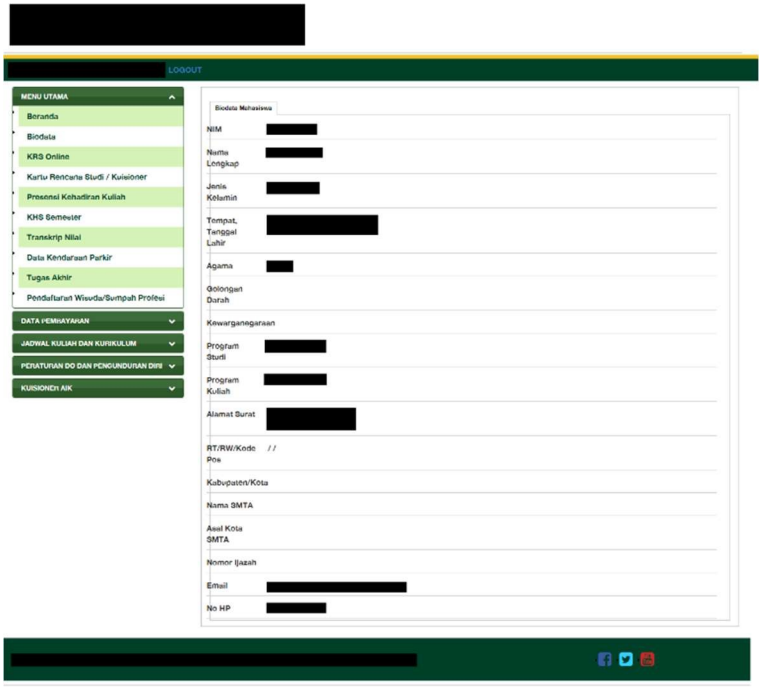
Gambar 4. 9 Hasil log *SSLStrip* pada perangkat milik Mahasiswa B

Pada gambar di atas ini merupakan log dari kegiatan Mahasiswa B pada saat membuka browser dan mengakses Web KRS Daring, lalu Mahasiswa B memasukkan nama pengguna dan kata sandi Web KRS Daring.



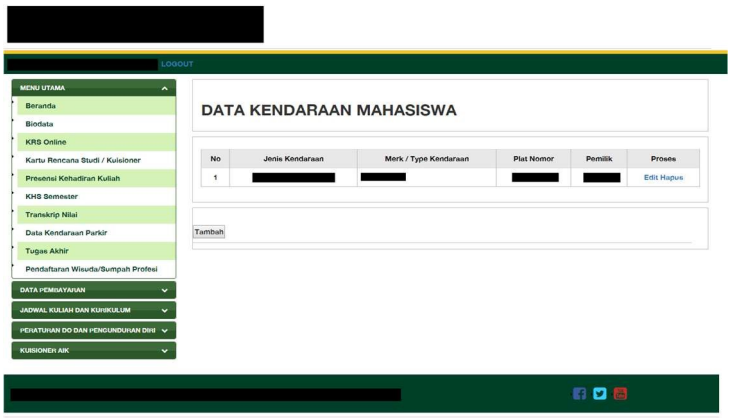
Gambar 4. 10 Tampilan KRS Daring milik Mahasiswa B

Peneliti melakukan *login* untuk memverifikasi bahwa nama pengguna dan kata sandi benar milik Mahasiswa B. Pada gambar diatas merupakan tampilan awal Web KRS Daring milik Mahasiswa B setelah *login*.



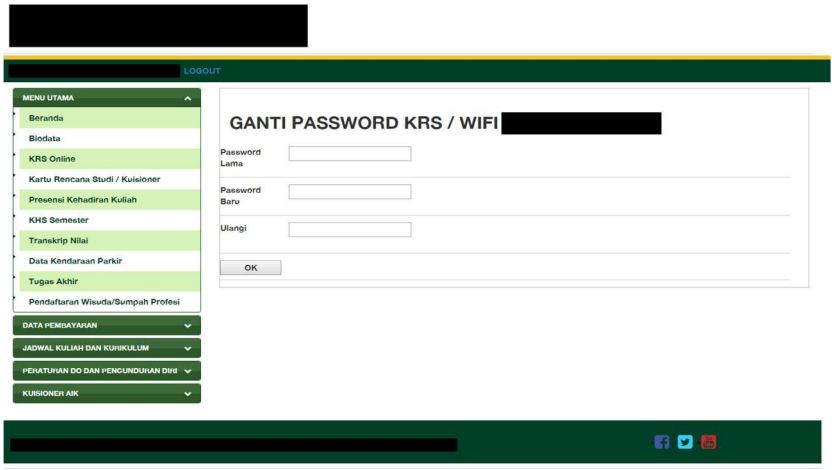
Gambar 4. 11 Data pribadi milik Mahasiswa B

Pada gambar diatas peneliti bisa melihat data pribadi milik Mahasiswa B. Terdapat informasi penting seperti NIM (Nomor Induk Mahasiswa), Nama Lengkap, Tempat Tanggal Lahir, Alamat Rumah, dan Nomor HP.



Gambar 4. 12 Data kendaraan milik Mahasiswa B

Pada gambar diatas peneliti bisa melihat data kendaraan milik Mahasiswa B, terdapat nama Jenis Kendaraan, Merk/Type Kendaraan, Pelat Nomor, dan Pemilik. Peneliti bisa merubah atau menghapus data kendaraan tersebut.



Gambar 4. 13 Reset kata sandi KRS Daring milik Mahasiswa B

Pada gambar diatas peneliti bisa melakukan reset kata sandi KRS Daring milik Mahasiswa B.

4.6. Eksploitasi Kerentanan (*Privilege Escalation*)

Pada tahap eksploitasi kerentanan, peneliti mendapatkan hak akses dari hasil *Social Engineering* pada kedua mahasiswa Institusi Pendidikan XYZ. Ketika diakses peneliti mendapatkan hak akses berupa mengganti data kendaraan mahasiswa dan mereset kata sandi akun Web KRS Daring.

4.7. *Reporting*

Pada tahap ini peneliti melakukan penulisan laporan tentang penelitian. Hasil penulisan laporan akan diberikan kepada Institusi Pendidikan XYZ untuk bahan evaluasi dan perbaikan. Laporan ada pada Lampiran.