Tugas Software Security

Perancangan Mekanisme Pengamanan Pengaksesan Data via Jaringan

Oleh:
Jonathan Ery Pradana / 23512038
Muhammad Ghufron Mahfudhi / 23512066
Emeraldy Widiyadi / 23512182

Pendahuluan

Desain yang akan diimplementasikan yaitu pengaksesan file pada server melalui client browser oleh client user. Wujud tampilan utama pada client browser terdiri atas tiga tampilan, yakni tampilan login, dashboard, dan file editor. Aspek security diterapkan pada sisi client dan server dari mulai login hingga logout.

Skema Pengaksesan

Case : Login

Pertama kali client user melakukan pengaksesan web, client user dihadapkan pada login form untuk dapat melakukan pengaksesan file. Session pada saat client user mengakses halaman depan web disimpan pada cookies. Session tersebut akan digunakan untuk memastikan
bahwa client user merupakan orang yang sama saat proses-proses berikutnya. Terkait dengan kebutuhan autentikasi client user, user account data (username dan password) yang telah dikenakan proses hashing disimpan pada suatu file dalam secured directory di server.

Berikut ini langkah detil proses “login”:

1. Client user mengakses web page. Cookies pada client browser menyimpan access session.
2. Client user mengirimkan user account data (username dan password) menuju server. Sebelum data dikirim, client browser melakukan hashing terhadap data tersebut.
3. Server menerima hashed user account data dan melakukan pencocokkan dengan hashed user account data yang terdapat pada server.
4. Jika pencocokkan valid, maka server mengirim daftar file milik client user dan memperbolehkan client user mengakses dashboard.
5. Client user mengakses dashboard.

Detail hashing dan salting dijelaskan pada rencana implementasi.

Case : File CRUD

Plain file disimpan di dalam server. File tersebut disimpan di dalam folder yang dimiliki oleh client user secara terbatas, yakni satu folder hanya dimiliki satu client user. Daftar identitas client user yang dapat mengakses file disimpan dalam whitelist pada server. Sesuai dengan penjelasan sebelumnya, ketika client user ingin mengakses file miliknya, client user harus melakukan login terlebih dahulu. Server akan menanggapi permintaan pengaksesan file dan mengirim daftar file yang beratasnamakan client user untuk ditampilkan di client browser. Setelah client memilih file pada daftar file dan permintaannya diterima oleh server, server akan mengambil client file yang dipilih.

Berikut ini langkah detil proses “file CRUD”:

CREATE

1. Client user mengirim request CREATE. Client browser menampilkan text editor.
2. Client user memilih simpan file. Client browser mengenkripsi file yang disimpan client user.
3. Client user mengirim request SAVE.
4. Plain file hasil dekripsi disimpan pada direktori milik client user dalam server.
5. Server mengirim status terbaru direktori client user. Client browser melakukan closing editor dan refreshing dashboard.

READ

1. Client user mengirim request READ.
2. Server menanggapi request dengan mengambil file dalam direktori client user pada server.
3. Client browser menampilkan teks editor yang berisi plain file content.

UPDATE

1. Proses READ.
2. Client user memilih simpan file baik itu dilakukan perubahan ataupun tidak.
3. Client user mengirim request SAVE.

4. File dicocokkan dengan file yang
   disimpan pada direktori milik client user dalam server. File dengan metadata sama (cocok) dikenakan proses overwrite.
5. Server mengirim status terbaru direktori client user. Client browser melakukan closing editor dan refreshing dashboard.

DELETE

1. Client user mengirim request DELETE dan identitas file yang ingin dihapus.

2. Server mengirim status terbaru direktori user client. Client browser melakukan refreshing dashboard.

Rencana Implementasi

Implementasi akan dilakukan menggunakan bahasa PHP dan framework Code Igniter. Sejumlah algoritma yang diterapkan menggunakan algoritma yang pernah ada yang disesuaikan dengan platform penggunaan. File disimpan pada server CPU dalam wujud sistem
folder biasa.

Rencana hashing menggunakan fungsi hash SHA1.

Justifikasi

1. Desain ini cukup andal untuk menangani serangan:
   - Injection, karena perintah-perintah yang digunakan relatif sederhana dan dikenakan aspek security (validasi perintah) serta penanganan data yang disimpan di server tidak menggunakan basis data yang biasa terserang oleh serangan jenis ini.
   - Repeating attack, karena setiap proses yang dilakukan oleh client user diamankan oleh mekanisme serupa dengan parameter yang berbeda-beda.

- ○ XSS, XSSI, CSRF, karena diterapkan whitelist untuk setiap resource (javascript) yang diambil dari situs luar.
- ○ Insecure direct object references, karena menggunakan fungsi yang telah disediakan oleh framework CI.

2. Aturan login:
   - Username minimal terdiri dari 4 karakter
   - Password terdiri dari minimal 8 karakter