

## PHP Security Dasar

PHP Security digunakan untuk melindungi source php dari serangan-serangan hacker ke dalam aplikasi website yang dibangun dengan menggunakan PHP. Adapun beberapa hal dasar yang dapat dipelajari lebih lanjut adalah:

### 1. Encryption

Digunakan untuk melindungi data yang dikirim, dengan enkripsi detail maka data tidak dapat dilihat dengan mata kosong. Pada dasarnya enkripsi digunakan untuk password namun berjalan sesuai pengembangan enkripsi digunakan ke semua data yang dikirim dari client ke server ataupun sebaliknya. Adapun enkripsi PHP yang sering digunakan adalah:

- Md5 (tidak memiliki decrypt)
- CRC32 (tidak memiliki decrypt)
- Crypt (tidak memiliki decrypt)
- SHA1 (tidak memiliki decrypt)
- base64\_encode (memiliki decrypt yaitu base64\_decode)

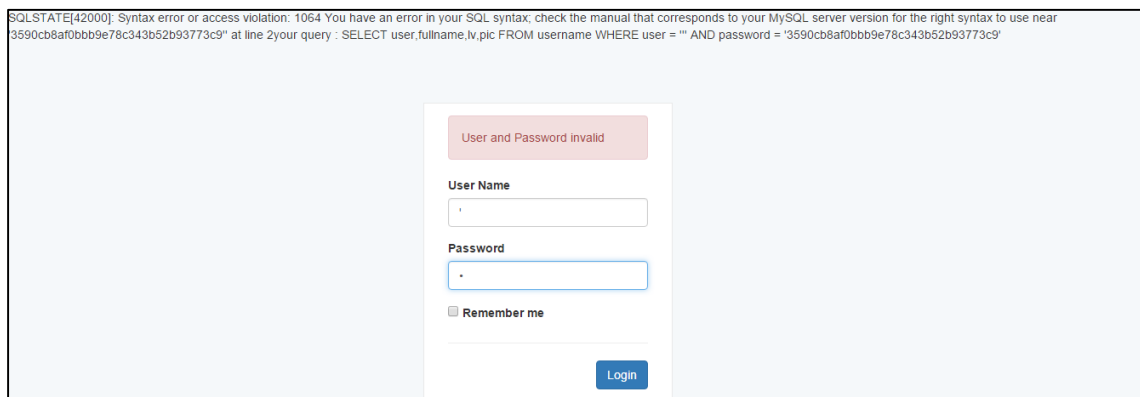
Setiap enkripsi memiliki algoritma yang berbeda-beda, namun untuk lebih baik menggunakan enkripsi yang telah dibuat berbeda dengan yang lain atau menggabungkan beberapa enkripsi yang tersedia.

### 2. SQL Injection

SQL Injection memiliki makna yaitu sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi. Celah ini terjadi ketika masukan pengguna (dari form) tidak disaring secara benar dari karakter-karakter pelolos bentukan string yang diimbuhkan dalam pernyataan SQL atau masukan pengguna tidak bertipe kuat dan karenanya dijalankan tidak sesuai harapan. Ini sebenarnya adalah sebuah contoh dari sebuah kategori celah keamanan yang lebih umum yang dapat terjadi setiap kali sebuah bahasa pemrograman atau skrip diimbuhkan di dalam bahasa yang lain. SQL injection adalah jenis aksi hacking pada keamanan komputer di mana seorang penyerang bisa mendapatkan akses ke basis data di dalam sistem.

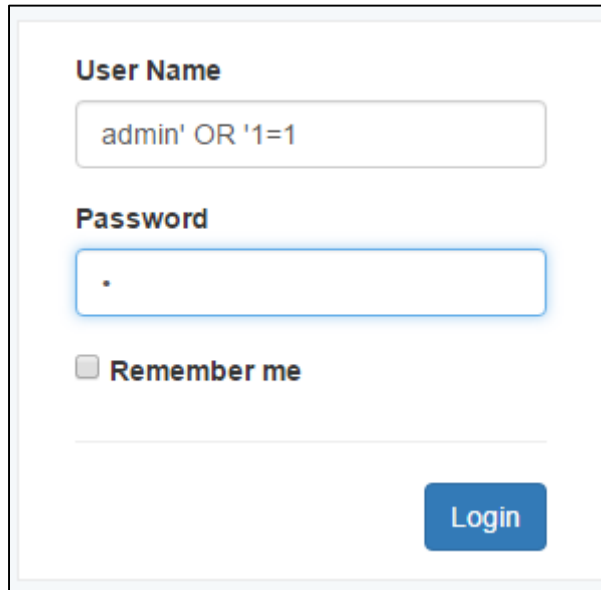
#### Contoh SQL Injection:

- Buka Aplikasi PHONE BOOK yang telah kita buat
- Pada saat login masukkan karakter ' (petik atas) pada text box username dan password maka akan muncul error seperti dibawah ini:



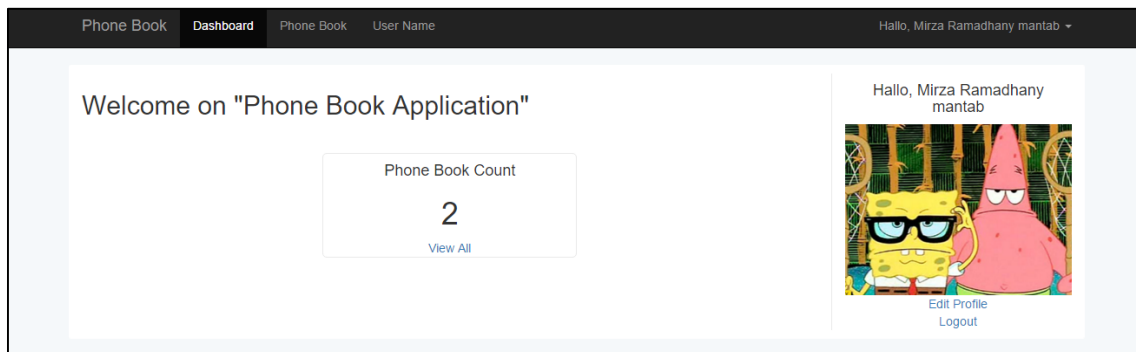
Error diatas menandakan aplikasi dapat ditembus degan menggunakan sql injection, para hacker dapat mengakses database kita dengan sql injection ataupun login meggunakan sql injection, dibawah ini langkah-langkah untuk login menggunakan sql injection:

- Pada username masukkan tulisan dibawah ini



The screenshot shows a login form with two input fields: 'User Name' and 'Password'. The 'User Name' field contains the text 'admin' OR '1=1'. The 'Password' field contains a single dot '.'. Below the password field is a checkbox labeled 'Remember me'. At the bottom right of the form is a blue 'Login' button.

- Login dan akan masuk halaman administrator



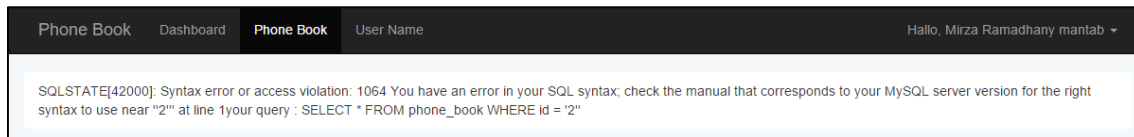
SQL Injection juga dapat diserang melalui melalui metode \$\_GET tepatnya pada URL bar yang terdapat kata kunci dari sebuah data (pada saat view / edit data). Contoh dapat kita coba langkah-langkah dibawah ini:

- Setelah login
- Masuk Phonebook
- Lalu edit salah satu data
- Lihat pada URL yang tercipta pada saat kita edit data

[localhost/sapeltu\\_team/github/modul\\_php/5.PHONE\\_BOOK/index.php?cpage=pb/update&cid=2](localhost/sapeltu_team/github/modul_php/5.PHONE_BOOK/index.php?cpage=pb/update&cid=2)

Pada URL dapat kita lihat tulisan cid secara kasat mat cid merupakan kata kunci untuk mengakes database.

- Pada cid=2 tambahkan tanda ' (petik atas) menjadi cid=2', lalu tekan enter maka system akan error seperti dibawah ini:



### Cara mengatasi SQL Injection:

Ada beberapa cara untuk mengatasi SQL Injection, disini kita akan mencoba mengatasi SQL Injection dengan proteksi menggunakan kode PHP adapun kodenya adalah sebagai berikut:

- Pada Aplikasi PHONE BOOK, buka file connection.php pada folder connection
- Tambahkan fungsi data\_secure() dibawah ini:

```
<?php
session_name("PHONE_BOOK");
session_start("");
require_once 'pdo.mysql.php'; //memanggil / menghubungkan pdo.mysql.php
$mydb = new mydb(); //deklarasi koneksi
$mydb->connect("localhost","root","","learning_pb"); //mengaktifkan koneksi ke database learning

function data_secure($data){
    $parse = (stripslashes(strip_tags(htmlspecialchars($data, ENT_QUOTES))));
    return $parse;
}
?>
```

- Sebelum fungsi data\_secure() tambahkan kode seperti dibawah ini:

```
<?php
session_name("PHONE_BOOK");
session_start("");
require_once 'pdo.mysql.php'; //memanggil / menghubungkan pdo.mysql.php
$mydb = new mydb(); //deklarasi koneksi
$mydb->connect("localhost","root","","learning_pb"); //mengaktifkan koneksi ke database learning

foreach($_POST as $key => $value){
    ..... $_POST[$key] = data_secure($value);
}
foreach($_GET as $key => $value){
    ..... $_GET[$key] = data_secure($value);
}

function data_secure($data){
    $parse = (stripslashes(strip_tags(htmlspecialchars($data, ENT_QUOTES))));
    return $parse;
}
?>
```

- Lalu coba kembali SQL Injection yang telah kita bahas diatas maka SQL Injection tidak dapat bekerja

User and Password invalid

**User Name**

admin' OR '1=1

**Password**

.

☐ Remember me

Login

Pada login area

localhost/sapeltu\_team/github/modul\_php/5.PHONE\_BOOK/index.php?page=pb/update&cid=2

Phone Book Dashboard Phone Book User Name

Hallo, Mirza Ramadhany mantab

Update Data

**First Name**

Mirza

**Last Name**

Ramadhanyuhuu

**Address**

singosari Malang ifa ibriz

**Email**

signo@masadf.com

**Phone**

099998

**Company**

asdfasdf

**Positon**

CEOCTO

### 3. Framework PHP

Framework adalah kerangka kerja. Framework juga dapat diartikan sebagai kumpulan script (terutama class dan function) yang dapat membantu developer/programmer dalam menangani berbagai masalah-masalah dalam pemrograman seperti koneksi ke database, pemanggilan variabel, file, dll sehingga developer lebih fokus dan lebih cepat membangun aplikasi. Dapat juga dikatakan Framework adalah komponen pemrograman yang siap re-use kapan saja, sehingga programmer tidak harus membuat skrip yang sama untuk tugas yang sama. Untuk saat ini semua programmer dianjurkan menguasai framework, kelebihan framework antara lain sebagai berikut:

- Ringan dan cepat. Framework hanya melakukan pemanggilan pustaka/kelas yang dibutuhkan sehingga meminimalkan resource yang diperlukan sehingga ketika kita me-load sebuah halaman akan menjadi ringan dan cepat.

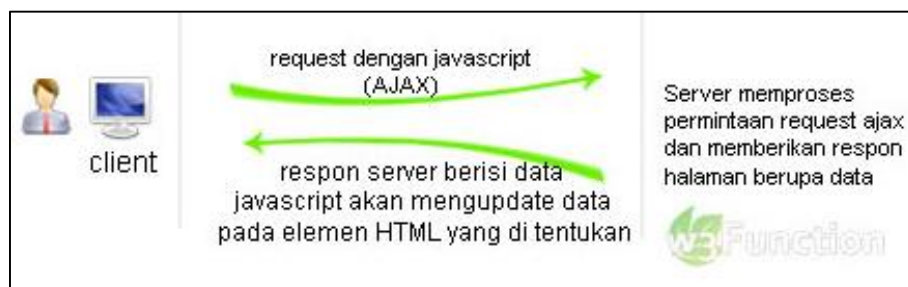
- Menggunakan metode MVC. Seperti yang telah dijelaskan sebelumnya, dengan metode MVC akan mempermudah kita dalam memahami alur pemrograman karena untuk bagian tampilan, logika dan query database telah dipecah sedemikian rupa.
- Mayortitas mendukung berbagai jenis database.
- Dapat mengikuti perkembangan
- Terstruktur dan manajemen pembagian tugas antar programmer lebih baik
- Keamanan lebih tangguh dari pada PHP Dasar

Berikut beberapa contoh PHP FRAMEWORK yang dapat dipelajari:

- [Laravel](#)
- [CodeInteger](#)
- [Yii](#)
- [Zend](#)

#### 4. AJAX

Pada website tradisional biasa jika kita mengklik suatu tombol/link tertentu maka browser akan melakukan refresh dimana document HTML akan di baca dari awal dan layar browser akan menjadi blank sesaat karena pada saat itu browser sedang meminta/merequest data dari web server dan hal itulah yang membuat aplikasi website menjadi kurang interaktif dan responsif. Ajax digunakan untuk memecahkan masalah tersebut, Ajax membuat aplikasi website menjadi lebih interaktif dan responsif serta memiliki kecepatan dalam memproses request ke server. Saat ini Ajax sudah menjadi teknologi yang wajib diterapkan bagi website dan website aplikasi modern.



#### 5. SSL

SSL (dan TLS) adalah protokol standar Web untuk mengenkripsi komunikasi antara user dan SSL (secure socket layer). Data yang dikirim melalui sambungan SSL dilindungi oleh enkripsi, suatu mekanisme yang mencegah eavesdropping dan sabotase data yang ditransmisikan apapun. SSL menyediakan bisnis dan konsumen dengan keyakinan bahwa data pribadi yang dikirim ke situs Web, seperti nomor kartu kredit, akan dijaga kerahasiaannya. Sertifikat server web (juga dikenal sebagai aman sertifikat server atau sertifikat SSL) yang diperlukan untuk menginisialisasi sesi SSL. SSL Certificate kunci dalam browser user Anda tahu kapan mereka memiliki sesi SSL dengan situs Web ketika browser mereka menampilkan gembok emas kecil dan panel alamat dimulai dengan https bukan http. Sertifikat SSL dapat digunakan pada Internet webserver keamanan dan mail server seperti imap, pop3 dan smtp untuk mail pengumpulan / pengiriman keamanan.



# HTTP vs HTTPS

