Jurnal Computech & Bisnis, Vol. 2, No. 1, Juni 2008, 14-21
ISSN 1978-9629

PENGEMBANGAN PERANGKAT LUNAK DENGAN MENGGUNAKAN PHP

KM. Syarif Haryana
STMIK Mardira Indonesia, Bandung 40235
kmsyarifharyana @yahoo.co.id

Abstract

PHP is a web-based programming language in which the system is implemented on the server side . PHP can be inserted between the HTML language scripts and other server side language arena , with it then PHP will be executed directly on the server . While the browser will execute the web page through which the server will then receive the display " results so " in an HTML form , whereas PHP code itself will not be visible .

Keyword : *PHP, Web, Software, Programming*

Abstrak

PHP merupakan salah satu bahasa pemograman berbasis web dimana sistem yang diterapkan adalah pada sisi server side. PHP dapat disisipkan diantara skrip-skrip bahasa HTML dan arena bahasa server side lainnya, dengan itu maka PHP akan dieksekusi secara langsung pada server. Sedangkan browser akan mengeksekusi halaman web tersebut melalui server yang kemudian akan menerima tampilan "hasil jadi" dalam bentuk HTML, sedangkan kode PHP itu sendiri tidak akan dapat terlihat.

Kata Kunci : PHP, Web, Perangkat Lunak, Pemograman

Pendahuluan

Pengembangan perangkat lunak yang semakin meluas dan beragam dipengaruhi oleh beragamnya bahasa pemograman dan aplikasi bantu yang menjanjikan kemudahan dalam mengembangkan perangkat lunak. Selain itu ketergantungan akan penulisan baris-baris perintah pemograman sebagian besar telah di ubah dengan adanya pemograman Visual, sehingga tampilan antar muka sebuah perangkat lunak dapat dengan mudah dan dibentuk dengan lebih menarik.

Namun dari keberagaman bahasa pemograman dan janji-janji kemudahan pengoperasiannya dan berbagai fitur yang lengkap ternyata masih belum dilengkapi tersedianya fasilitas keamanan pengembangan perangkat lunak itu sendiri. Salah satu kajian yang akan dikupas pada paper ini adalah aspek keamanan pemograman menggunakan skrip PHP.

Kelebihan-kelebihan PHP yaitu:

1. Web menggunakan PHP dapat dengan mudah dibuat dan memiliki kecepatan akses yang cukup tinggi.
2. Skrip-skrip PHP dapat berjalan dalam web server yang berbeda dan dalam system operasi yang berbeda pula.

PHP dapat berjalan disistem operasi UNIX, windows dan macintosh.

3. PHP diterbitkan secara gratis.
4. PHP juga dapat berjalan pada web server Microsoft Personal Web Server, Apache, IIS, Xitami dan sebagainya.
5. PHP adalah termasuk bahasa embedded (bisa ditempel atau diletakan dalam tag HTML)
6. PHP termasuk server side programming

Sistem database yang didukung oleh PHP

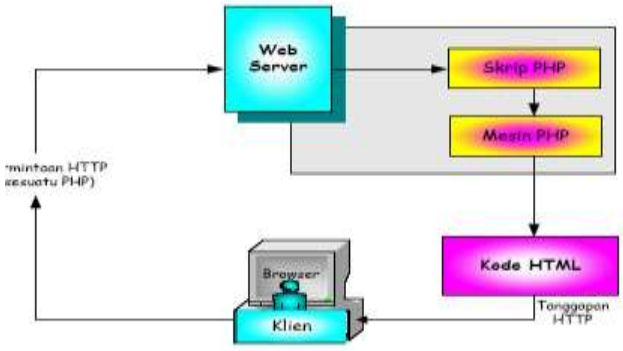
a. Oracle
b. Sybase
c. mSQL
d. MySQL
e. Solid
f. Generic ODBC
g. Postgres SQL

PHP juga mendukung komunikasi dengan layanan lain melalui protokol IMAP, SNMP, NNTP, POP3 dan HTTP. Fungsi-fungsi yang ada di PHP tidak case sensitive tetapi variabelnya case sensitive (membedakan hurup besar dan kecil). Kode PHP diawali dengan tanda lebih kecil (<) dan diakhiri dengan tanda lebih besar (>).

Konsep kerja HTML diawali dengan permintaan suatu halaman web oleh browser. Berdasarkan URL (Uniform Resource Locator) ataudikenal dengan internet, browser mendapat alamat dari web server, mengidentifikasi halaman yang dikehendaki, dan menyampaikan segala informasi yang dibutuhkan oleh web server.

Selanjutnya, web server akan mencarikan berkas yang diminta dan membrikan isinya ke browser. Browser yang mendapatkan isinya segera melakukan proses penerjemahan kode HTML dan menampilkannya ke layar pemakai (klien).

Pada PHP prinsip kerjanya sama, hanya saja ketika berkas PHP yang diminta didapatkan oleh web server, isinya segera dikirimkan ke mesin PHP dan mesin inilah yang memproses dan memberikan hasilnya (berupa kode HTML) ke web server. Selanjutnya, web server menyampaikannya ke klien.



Gambar: Konsep Kerja PHP

Vulnerabilities

Berjuta-juta halaman Web dapat kita temui saat ini di Internet. Perkembangannya sangat cepat. Telah banyak perusahaan yang menampilkan diri di Internet melalui Web. Begitu juga dengan berbagai jenis Web yang lain yang kini telah menjadi bagian tak terpisahkan dari Internet. Web sedemikian populer karena mudah dibuat dan banyak menawarkan keuntungan. Banyak sekali informasi yang disediakan oleh Web-Web yang ada dan dapat diakses oleh siapa saja. Bahkan saat ini banyak pula perusahaan-perusahaan yang menyediakan transaksi melalui Web mereka. Web telah dijadikan satu bagian

penting untuk promosi maupun layanan kepada pelanggan.

Jenis Jenis Serangan

Berikut adalah 10 (sepuluh) dafttar celah yang dapat menyebabkan website terancam :

1. *Cross Site Scripting* (XSS)
   Celah XSS, adalah saat pengguna web aplikasi dapat memasukkan data dan mengirimkan ke web browser tanpa harus melakukan validasi dan encoding terhadap isi data tersebut, Celah XSS mengakibatkan penyerang dapat menjalankan potongan kode (script) miliknya di browser target, dan memungkinkan untuk mencuri user session milik target, bahkan sampai menciptakan Worm.

2. *Injection Flaws*
   Celah Injeksi, umumnya injeksi terhadap SQL (database) dari suatu aplikasi web. Hal ini mungkin terjadi apabila pengguna memasukkan data sebagai bagian dari perintah (query) yang menipu interpreter untuk menjalankan perintah tersebut atau merubah suatu data.

3. *Malicious File Execution*
   Celah ini mengakibatkan penyerang dapat secara remote membuat file yang berisi kode dan data untuk di eksekusi, salah satunya adalah *Remote file inclusion* (RFI).

4. *Insecure Direct Object Reference*
   Adalah suatu celah yang terjadi saat pembuat aplikasi web merekspos referensi internal penggunaan objek, seperti file, direktori, database record, dll

5. *Cross Site Request Forgery* (CSRF)
   Celah ini akan memaksa browser target yang sudah log-in untuk mengirimkan "pre-authenticated request"terhadap aplikasi web yang diketahui memiliki celah, dan memaksa browser target untuk melakukan hal yang menguntungkan penyerang.

6. *Information Leakage and Improper Error Handling*
   Penyerang menggunakan informasi yang didapatkan dari celah yang di akibatkan oleh informasi yang diberikan oleh web aplikasi seperti pesan kesalahan (error) serta konfigurasi yang bisa di lihat.

7. *Broken Authentication and Session Management*
   Celah ini merupakan akibat buruknya penanganan proses otentikasi dan manajemen sesi, sehingga penyerang bisa mendapatkan password, atau key yang di gunakan untuk otentikasi.

8. *Insecure Cryptographic Storage*
   Aplikasi web umumnya jarang menggunakan fungsi kriptografi untuk melindungi data penting yang dimiliki, atau menggunakan fungsi kriptografi

yang di ketahui memiliki kelemahan.

9. *Insecure Communications*
   Sedikit sekali aplikasi web yang mengamankan jalur komunikasinya, hal inilah yang dimanfaatkan oleh penyerang sebagai celah untuk mendapatkan informasi berharga.

10. *Failure to Restrict URL Access*
    Seringkali, aplikasi web hanya menghilangkan tampilan link (URL) dari pengguna yang tidak berhak, tetapi hal ini dengan sangat mudah dilewati dengan mengakses URL tersebut secara langsung.

Pembahasan Php

PHP dapat dijalankan sama seperti aplikasi CGI (Common Gateway Interface) seperti web server yang terintegrasi. Interpreter PHP mempunyai kemampuan untuk mengakses hampir semua host- file system, network interfaces, IPC, dan lain-lain. Konsekwensinya PHP potensial mendapat serangan dari attacker. Untuk meminimalkan serangan programmer harus menyadari dan mengetahui hal-hal yang tidak diharapkan (merusak) saat program dijalankan, yaitu pengetahuan kelemahan suatu sistem dan modus serangan secara umum yang diarahkan untuk mengganggu keamanan program tersebut Lubang keamanan yang paling umum di dalam skrip PHP dan tak terkecuali pada aplikasi web yang manapun, adalah berkaitan dengan User Input. Banyak skrip menggunakan informasi user yang legal dalam bentuk format web dan memproses informasi ini dengan berbagai cara. Jika user input ini dilegalkan tanpa batasan, maka user input potensial menyisipkan perintah-perintah yang tidak diinginkan dalam skrip.

Cross Site Scripting

Suatu Jenis Serangan dengan cara memasukkan code/script HTML (javascript) kedalam suatu web site dan dijalankan melalui browser di client Contoh :

```
<script>alert(document.cookie
)</script>
```

Dengan skrip di atas maka akan mendapatkan Cookies yang berisi info berharga milik client yang digunakan oleh server untuk proses authentikasi. Salah satu type lubang keamanan sistem yang biasa ditemukan di web based applications dengan melakukan code injections dengan malicious web pengguna kepada halaman web yang dilihat oleh user lainnya dimana memungkinkan penyerang untuk mencuri cookies, menipu user dengan memberikan credentials mereka, memodifikasi penampilan page, mengeksekusi seluruh sort dari malicious java- script code.

Information Disclosure

Predictable resource location : Jenis serangan dengan menebak letak resource yang disembunyikan dan umum di gunakan oleh web aplikasi.

Contoh :
– /admin/

– /backup/
– /logs/
– /PhpMyadmin/
– admin.php
– login.php

Path Traversal

Suatu jenis vulnerabilities yang mengakibatkan user dapat melihat secara lengkap path suatu direktori atau file dari suatu situs/website, Contoh :

http://target.com/appx/Sources/Admin.php

Fatal error: Call to undefined function: is_admin() in /var/www/html/user/target/appx/Sources /Admin.ph p on line 32

Diketahui bahwa halaman web target.com terletak di
/var/www/html/
user/target

Kegunaan bagi attacker

- Mempersingkat waktu untuk mencari letak web direktori target
- Informasi tambahan jika telah memiliki akses ke server.
- = ‘pwd’ pada situs target

SQL injection

Suatu Cara untuk Mengexploitasi Web Application yang menggunakan suatu database , dan memasukan command sql, sehingga membentuk suatu query yang akan dieksekusi dan dijalankan oleh sql server.

Contoh: http://victim.com/login.asp
yang menerima input user dan pass
attacking input user = test ‘OR ‘1’=‘1
&& input pass
=test
Syntax SQL : select * from users where pass=‘test’ and user = ‘test’or’1’=‘1’

SQL Injection termasuk kedalam metode yang memanfaatkan kelemahan pada mesin server SQLnya, misalnya server yg menjalankan aplikasi tersebut. Hal ini dilakukan dengan mencoba memasukkan suatu script untuk menampilkan halaman error di browser, dan biasanya halaman error akan menampilkan paling tidak struktur dari hirarki server dan logika program. Metode ini memasukan “karakter” query tertentu pada sebuah “text area” atau di address browser dengan perintah-perintah dasar SQL seperti SELECT, WHERE, CREATE, UPDATE, dan lain-lain.

Pada dasarnya terdapat beberapa metode yang digunakan penyerang untuk melakukan SQL Injection, biasanya targetnya adalah database yang digunakan untuk menyimpan data. Saat ini terdapat beberapa metode seperti 1-tier, 2-tier layer pengaksesan dari web server ke DB. Jadi request dari client tidak akan langsung ke DB namun diterjemahkan oleh web server dan diquery-kan oleh web applications. Kelemahan yang biasanya dicoba adalah di bagian web server dengan menyerang Daemon web servernya, Web Applications dengan menginject bahasanya, dan DB yang digunakan (Oracle, Postgress, MySQL, SQL Server, dan lain-lain). Query-query yang sering diinjection, seperti ;

- 'anything' OR 'x'='x';
- 'x' AND email IS NULL; --';
- 'x' AND userid IS NULL; --';
- 'x' AND 1=(SELECT COUNT(*) FROM tabname); --';
- 'bob@example.com' AND passwd = `hello123';

Berikut ini adalah query pada SQL yang sering kita pergunakan dalan SQL injection :

Insert
INSERT INTO namatabel (field1 [, field2 [, …]]) VALUES (nilai1 [,nilai2 [,…]]);
Select
SELECT{* field1 [, field2 [,…]]} FROM namatabel
[where kondisi];

SQL inejction

Contoh dari SQL statement :
select id, forename, surname from authors

Perintah ini akan menghasilkan kolom 'id', 'forename' dan 'surname' dari tabel 'authors', dengan menghasilkan semua baris pada setiap kolom yang relevan SQL Injection dapat terjadi ketika seseorang dapat memasukkan serangkaian perintah SQL dalam query dengan memanipulasi data pada aplikasi database. Kita akan membahas beberapa teknik SQL injection yang umum ditemukan pada Microsoft Internet Information Server/Active Server Pages/SQL Server platform. Terdapat beberapa cara dimana SQL dapat diinjeksikan pada sebuah aplikasi.

Hasil yang diinginkan dapat lebih spesifik dengan menyebutkan 'author' seperti di bawah ini : select id, forename, surname from authors where forename = 'john' and surname = 'smith'. Hal utama yang perlu dicatat adalah kita telah memiliki batas-batas dalam pencarian yakni dengan menyebutkan 'john' sebagai forename dan 'smith' sebagai surename. Seakan-akan 'forename' and 'surname' field telah didapatkan dari user yang memberikan input.

Seorang attacker dapat menginjeksikan beberapa SQL dalam query ini dengan memasukkan nilai pada aplikasi seperti dibawah ini :
Forename: john
Surname: smith

Query akan menjadi seperti ini :
select id, forename, surname from authors where forename = 'jo'hn' and surname = 'smith'

Ketika database menjalankan query,akan menghasilkan suatu kesalahan seperti yang ditunjukkan berikut ini :

Server: Msg 170, Level 15, State 1, Line 1
Line 1: Incorrect syntax near 'hn'.

Ini disebabkan karena dimasukkannya karakter single quote (tanda petik satu) yang menyatakan breaks out. Selanjutnya database akan mencoba untuk mengeksekusi 'hn' dan gagal juga.

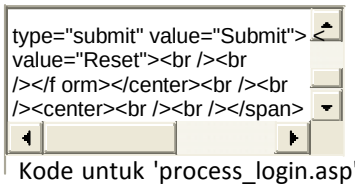
Jika attacker menspesifikasi data seperti ini :
Forename: jo'; drop table authors--
Surname:

Akan menyebakan tabel penulis akan dihapus. Ini dapat memberikan gambaran bahwa beberapa metoda seperti membuang single quote dari input atau dengan mengabaikan mereka dalam beberapa hal dapat memecahkan kasus ini. Tapi tidak semua itu benar, karena masih terdapat beberapa kesulitan dalam aplikasinya. Pertama, tidak semua user memasukkan data bertipe string. Jika user dapat memilih author dengan 'id'(yang biasanya berupa angka), kita akan memiliki query seperti di bawah ini :

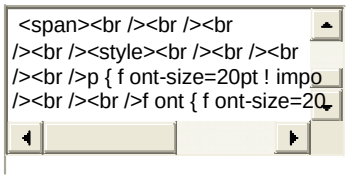
select id, forename, surname from authors where id=1234

Pada siatuasi seperti ini seorang attacker dapat dengan sederhana menambahkan perintah SQL pada akhir dari input yang berupa angka. Beberapa delimiter juga digunakan pada dialek (perintah khusus) SQL lainnya, seperti pada Microsoft Jet DBMS, tanggal dapat diakhiri dengan karakter '#' character. Kedua, mengabaikan single quote tidak permasalahan yang gampang. Kita akan mengilustrasikan kasus di atas lebih jauh lagi dengan menggunakan Active Server Pages (ASP) atau PHP untuk 'login' , dengan mengakses SQL Server database dan mencoba untuk masuk dengan autentifikasi yang tidak mungkin rasanya terjadi. Berikut ini adalah kode dari halaman

'form' page, dimana user akan memasukkan username dan password :



Kode untuk 'process_login.asp' :



Poin terpenting disini adalah misalnya bagian dari 'process_login.asp' dengan query string :

```
var sql = "select * from users where
username = '" +
username + "' and password = '" +
password + "'";
```

Jika user memasukkan hal berikut ini :

```
Username: '; drop table users—
Password:
```

Tabel user akan terhapus, dan akan memberikan kesempatan sehingga semua user dapat mengakses ke dalam database. Kejadiannya adalah sbb :

- Karakter ';' menandakan akhir dari sebuah query dan awalan dari query yang lainnya.
- Karakter '--' adalah single line comment dalam Transact-SQL. Karakter '--' pada akhir dari kolom username dibutuhkan agar pada bagian ini query tidak menimbulkan erro pada waktu dijalankan.

Attacker dapat log on (masuk) sebagai siapa saja, seakan-akan dia mengetahui username dengan memberikan input sbb :

```
Username: admin'—
```

Attacker dapat juga log on sebagai user yang pertama pada tabel 'user' dengan menggunakan input sbb :

```
Username: ' or 1=1—
```

Attacker juga dapat log in seakan-akan terdapat user yang sebenarnya tidak ada di database dengan memasukkan input sbb :

```
Username: ' union select 1,
'fictional_user',
'some_password', 1—
```

Ini disebabkan karena aplikasi yang kita buat percaya bahwa baris yang konstan dispesifikasikan oleh attacker adalah bagian perintah yang terdapat dalam database itu sendiri.

PHP under attack

Remote File inclusion

Suatu jenis serangan yang dilakukan dengan meng-include-kan halaman web lain kepada suatu situs/web aplikasi.

Contoh

Situs yang vulnerable
http://victim.com/index.php?fil
e=readme.txt URL code :
http://victim.com/index.php?file=http
://echo.or.id

Remote Command Execution

Suatu jenis serangan yang dilakukan dengan meng-include-kan tag-tag bahasa pemrograman secara remote dan mengakibatkan web yang "vulnerable" akan mengeksekusi "request" yang di kirimkan.

Contoh :
Situs yang vulnerable
http://victim.com/viewtopic.php?t=48
URL code:
http://victim.com/viewtopic.php?t=48&hi
ghlight=%25
27.passthru($HTTP_GET_VARS[a]).%2527
&a=id;pwd

Dampak-dampak yang bisa terjadi

A. Defacing

Kegiatan merubah/merusak tampilan suatu website baik halaman utama (index) ataupun halaman lain yang masih terkait dalam satu url dengan website tersebut (folder lain ; file lain). Telah banyak kejadian dan tindakan yang mengarah ke defacing,

meskipun secara materiil mungkin saja tidak berdampak luas, namun secara non-materiil dapat mengakibatkan kerugian yang cukup fatal.

B. Motivasi

Jika kita tinjau dari kebutuhan/kepentingan sisi hacker/cracker, maka dapat dikategorikan ke dalam 6 kategori, yaitu :

- Dendam atau perasaan gak puas*
  Terdapat beberapa kasus yang mengakibatkan tindakan ke arah defacing web server yang dilatarbelakangi oleh perasaan tidak puas atau dendam, misalnya kasus pemilu, kasus partai politik, kasus web seorang tokoh nasional, kasus ambalat, dan masih banyak sebenarnya kasus-kasus lainnya.
- Kenikmatan tersendiri, 'defacer' merasa tertantang.
  Biasanya dilakukan oleh para pemula yang mau mencoba dan memiliki rasa keingintahuan yang sangat besar. Atau terdapat beberapa kasus yang berlatar belakang ingin terkenal atau ingin memproklamirkan diri sebagai hacker.
- Intrik politik, Sosial
  Biasanya dilatarbelakangi oleh persaingan yang tidak sehat sehingga ingin menjatuhkan lawan dengan merubah imej lawan politiknya. Atau dengan secara sengaja melakukan pen-dikreditan seseorang/melakukan cara fitnah, dll.
- Penyampaian pesan
  Dilatarbelakangi oleh keingintahuan dan ingin menyampaikan pesan-pesan tertentu, baik pesan untuk kepentingan umum maupun untuk kepentingan pribadi.
- Keuntungan Materill
  Untuk kasus ini sudah lebih jauh lagi, karena keingintahuan tersebut dilanjutkan dengan kepentingan-kepetingan pribadi. Baik secara pribadi mendapatkan keuntungan dari hasil deface-nya, atau bisa juga mendapat order dari orang lain yang bersedia membayar dari hasil kerjanya.
- *Prestice* dalam kelompok
  Biasanya dilakukan oleh para pemula atau kelompok tertentu yang mau mencoba dan memiliki rasa ingin dikenal atau ingin lebih terkenal. Atau terdapat beberapa kasus yang berlatar belakang ingin terkenal atau ingin memproklamirkan diri sebagai hacker

Kesimpulan

Dilihat dari uraian di atas maka dapat disimpulkan bahwa vulnerabilities aplikasi web yang menggunakan PHP. Terdapat beberapa vulnerabilities pada aplikasi web berbasis PHP seperti Client side attack : xss, cookies stealing, Remote command execution melalui php command.

Daftar Pustaka

Secure Coding: Principles & Practices, G. Graff Mark, R. van Wyk Kenneth, O'Reilly Publisher, 2004

Scambray joel, MIKE SHEMA,Hacking.Exposed.Web.Applicati ons.iNT, McGraw. Hill/Osborne, 2006

http://www.cert.or.id/~budi/courses/ec7010/dikmenjur/thalib-report.pdf

ri32.wordpress.com/2009/07/10/script-keamanan-php