

Re: PHP Directory Transversal

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-03/0046.html>

From: Andres Molinetti (*andymolinetti_at_hotmail.com*)

Date: 03/10/05

To: securityfocus@felikz.net

Date: Thu, 10 Mar 2005 14:48:28 +0000

I'm sure that I'm adding the exact number of "../" because I was able to retrieve phpinfo.php and there I have the DOCUMENT_ROOT server variable...

It's under user Apache...but anyway...it is accessing the files for reading, and all users have privileges to access the passwd file for reading...

thanks,
Andy

>From: Felikz <securityfocus@felikz.net>

>To: Andres Molinetti <andymolinetti@hotmail.com>

>CC: pen-test@securityfocus.com, webappsec@securityfocus.com

>Subject: Re: PHP Directory Transversal

>Date: Thu, 10 Mar 2005 14:44:17 +0000

>

>Have you tried <http://www.example.com/static.php?page=/etc/passwd>

>

>?????

>

>Also, the issue you may be hitting is that the website root may be in a

>deeper directory that you think, therefore you may need to do more

>../..../

>

>It's worth giving a thought to the fact that Apache/PHP may/should be

>running as an underprivileged user and therefore shouldn't have the ability

>to traverse that far.

>

>Andres Molinetti wrote:

>

>>Hi,

>>

>>Working on a Web app testing...I have found that it uses the

>>so-vulnerable method of including files requested by php parameters:

>>

>>www.example.com/static.php?page=hello.htm

>>(htm files are in /templates dir)

>>

SecurityFocus Penetration: Re: PHP Directory Transversal

>>A the page in the parameter is requested statically, I did a
>>www.example.com/static.php?page=../static.php and I got that page source
>>code.

>>

>>Therefore, I tried doing a

>>www.example.com/static.php?page=../../../../etc/passwd

>>but I get an error saying that file doesn't exist.

>>

>>I user the same source code in my server, and I could retrieve the

>>file...what can be happening? I don't think it is under a chroot jail...

>>

>>I'm working with Apache 2.0.48 and PHP 4.3.4

>>and the real server has Apache 2.0.52 an PHP 4.3.9....

>>

>>Thanks in advance,

>>Andy

>>

>>

>>Descarga gratis la Barra de Herramientas de MSN

>><http://www.msn.es/usuario/busqueda/barra?XAPID=2031&DI=1055&SU=http%3A/www.hotmail.com&HL=LIN>

>>

>>

Acepta el reto MSN Premium: Protección para tus hijos en internet.

Descárgalo y pruébalo 2 meses gratis.

http://join.msn.com?XAPID=1697&DI=1055&HL=Footer_mailsenviados_proteccioninfantil