

Forum:[Hack Forums](#)

Thread: [Deface using JSP shell](#)

adios1 - July 19, 2016, 4:05 am

Hey guys I just rooted or uploaded a laudanum jsp shell.

Now I wanna know what this shell can do. Is it possible to deface that website? or upload/download any file to/from server? the server is Windows.

my shell looks like this

[img]http://[censored].com/r/x6edl5/9[/img]
[quote='adios1' pid='51733189' dateline='1468926308']
Hey guys I just rooted or uploaded a laudanum jsp shell.

Now I wanna know what this shell can do. Is it possible to deface that website? or upload/download any file to/from server? the server is Windows.

my shell looks like this

NOTE: This is not my actual shell. I just googled it

[img]http://4.bp.blogspot.com/-U6lwurVS-hQ/UQquad-LV6I/AAAAAAAAACw/RJHw9MBlh80/s1600/Laudanum-5.png[/img]

Gee4rce - July 19, 2016, 8:02 am

It does what a shell is meant to be for,
it provides you an interface which offers you command execution functionality on the server (if you have the permissions to).

So if that server is a linux server, you could use following (OS) commands to gather information about your system: id, pwd, ls -la, etc.

For windows that'll rather be "cmd /c dir" for example to make use of the "dir" command. If you are lucky and have root privileges, then you can do anything you want with the server.

Cheers, Gee.

Im gone brah - July 19, 2016, 12:58 pm

Understanding that you have a basic understanding of Linux commands and knows how to execute arbitrary commands using your shell.

Located the index file and switch it out or edit it to your liking, lol.

adios1 - July 19, 2016, 5:31 pm

(Jul 19, 2016 08:02 AM)Gee4rce3 Wrote: [\[CITE\]](#) It does what a shell is meant to be for,
it provides you an interface which offers you command execution functionality on the server (if you have the permissions to).

So if that server is a linux server, you could use following (OS) commands to gather information about your system: id, pwd, ls -la, etc.

For windows that'll rather be "cmd /c dir" for example to make use of the "dir" command. If you are lucky and have root privileges, then you can do anything you want with the server.

Cheers, Gee.

(Jul 19, 2016 12:58 PM)Zayne Wrote: [\[CITE\]](#) Understanding that you have a basic understanding of Linux commands and knows how to execute arbitrary commands using your shell.

Located the index file and switch it out or edit it to your liking, lol.

It's a Windows OS server. And it uses tomcat. Im trying to find the database of it. I checked every files but i cant find the databases of user&pass of administrator accounts. I also googled how to enable remote desktop using cmd, It says command operated successfully, but whenever I tried to connect to it via Remote desktop, it just doesn't connect. Is there Anyway that I can upload/download files using cmd? I know that in linux there is wget command. but i don't think that there is such command on windows. im not sure tho

Gee4rce - July 20, 2016, 12:53 am

Since it's a Windows, your typical shell that you usually can archive with bash commands is not working here,

and there is no "generic" solution for Windows Servers with cmd.exe commands only. But there are solutions,

doing a quick google how to shell with windows native cms.exe commands a guy came up with a solution via FTP:

https://www.sans.edu/student-files/presentations/ftp_nslookup_withnotes.pdf

Another option would be to install Netcat for windows on the target machine, then you could open a sock there with "nc -l 123",

from which you can connect to remotely and send commands. But installing something on the machine could cause attention by the Server admins.

Best solution here in my eyes would be checking if there is any Perl/Ruby/Python supported on the server, if yes you can write your own backdoor script with just a 2 - 5 lines of code.

If your JSP shell has root, then i'd eventually leave it already by that, unless there is a support for one of the above 3 mentioned scripting languages.

Cheers, Gee.

adios1 - July 20, 2016, 6:17 am

(Jul 20, 2016 12:53 AM)Gee4rce3 Wrote: [\[CITE\]](#) Since it's a Windows, your typical shell that you usually can archive with bash commands is not working here,

and there is no "generic" solution for Windows Servers with cmd.exe commands only. But there are solutions,

doing a quick google how to shell with windows native cms.exe commands a guy came up with a solution via FTP:

https://www.sans.edu/student-files/presentations/ftp_nslookup_withnotes.pdf

Another option would be to install Netcat for windows on the target machine, then you could open a sock there with "nc -l 123",

from which you can connect to remotely and send commands. But installing something on the machine could cause attention by the Server admins.

Best solution here in my eyes would be checking if there is any Perl/Ruby/Python supported on the server, if yes you can write your own backdoor script with just a 2 - 5 lines of code.

If your JSP shell has root, then i'd eventually leave it already by that, unless there is a support for one of the above 3 mentioned scripting languages.

Cheers, Gee.

I checked every single folder of the server. I didn't see any perl/ruby/python supported in the server. I'll just gonna explore more about this ftp thingy. But my JSP shell has root privilege. thank you for your reply

Im gone brah - July 21, 2016, 1:11 pm

(Jul 20, 2016 06:17 AM)adios1 Wrote: [\[CITE\]](#) I checked every single folder of the server. I didn't see any perl/ruby/python supported in the server. I'll just gonna explore more about this ftp thingy. But my JSP shell has root privilege. thank you for your reply You can't have root privileges on a windows machine. Send me the shell and I'll help you escalate your privileges.