

Forum:[Hack Forums](#)

Thread: [WSO2 shell | Educational Purposes](#)

Light Yagami - August 26, 2014, 3:46 am

Removed for security purpose

Hope you all enjoy ^^

Th3PonyWizard - August 26, 2014, 6:57 am

I'd recommend everybody to always review manually any PHP shells they're using. Nothing is more difficult than spotting a backdoor in these codes :\

Light Yagami - August 26, 2014, 7:11 am

(Aug 26, 2014 06:57 AM)Sonder Wrote: [\[CITE\]](#) I'd recommend everybody to always review manually any PHP shells they're using. Nothing is more difficult than spotting a backdoor in these codes :\

I will also check these files, thanks for writing this!

hoer- - August 26, 2014, 8:30 am

File is corrupted! (I wanted to find the backdoor)

I can see the start and they have used

Code

```
\x65\x76\x61\x6C\x28\x67\x7A\x69\x6E\x66\x6C\x61\x74\x65\x28\x62\x61\x73\x65\x36\x34\x5F\x64\x65\x63\x6F\x64\x65\x28
```

which is

Code `eval(gzinflate(base64_decode(`

Any attempt to hide code so much would suggest it's a backdoor'd.

Light Yagami - August 26, 2014, 8:33 am

(Aug 26, 2014 08:30 AM)hoer- Wrote: [\[CITE\]](#) File is corrupted! (I wanted to find the backdoor)

I can see the start and they have used

Code

```
\x65\x76\x61\x6C\x28\x67\x7A\x69\x6E\x66\x6C\x61\x74\x65\x28\x62\x61\x73\x65\x36\x34\x5F\x64\x65\x63\x6F\x64\x65\x28
```

which is

Code `eval(gzinflate(base64_decode(`

Any attempt to hide code so much would suggest it's a backdoor'd.

I am sorry, I will remove this post