

Forum:[Hack Forums](#)

Thread: [10 SSI Injection vulnerable sites.](#)

bckslsh - June 20, 2012, 9:55 am

You can use these for practicing, or writing guides.

To get a shell up, just wget the shellcode and make the output something such as "shell.txt".

<http://www.cgibackgrounds.com/Dan.txt> is an example. Not shellcode, though.

Code <http://www.glasshouseimages.com/user/login.shtml>
<http://www.wppionlinecontest.com/user/login.shtml>
www.cgibackgrounds.com/user/login.shtml
www.getstock.com/user/login.shtml
www.estostock.com/user/login.shtml
<http://www.blendimages.com/user/login.shtml>
<http://www.pdnthelook.com/user/login.shtml>
<http://iloveimages.com/user/login.shtml>
<http://www.win-initiative.com/user/login.shtml> (view source to see output)
<http://thegatheringsphotocontest.com/user/login.shtml>

RIPPER - June 20, 2012, 9:56 am

Great tut mate..Keep up the good work...will see how this shit works today

sl4sh3rz - June 20, 2012, 9:59 am

i check this thread when im wake up later.xD

bowhunter - June 21, 2012, 6:55 pm

hey havent been anywhere the computer scene for many years and getting un-rusty since the past year, re-visiting programming knowlege and all. i was still on dial-up the last time i was really into it to give you an idea. im now amazed by the wealth of information/websites available nowadays.

Anyway going to the point. while reading the code is no problem, i have a few questions:

- Why use a php shell? I mean you can run the shell commands from the login/pass fields. is it only because its just easier to do so from the shell or are there additional advantages? (but thanks to ITsecTEam for having one readily available)

- was this vulnerability only available because of the "bin/CkIb"? are these login vulnerabilities still common?

Suved - June 21, 2012, 9:57 pm

Thanks ?Dan for SSI Injection vulnerable sites.

Phizo - June 21, 2012, 10:37 pm

While this is nice and all; I don't see why this should be posted in the SQL Injection Attacks category as it is irrelevant to SQL injection.

bckslsh - June 22, 2012, 12:12 am

(Jun 21, 2012 10:37 PM)Phizo Wrote: [\[CITE\]](#) While this is nice and all; I don't see why this should be posted in the SQL Injection Attacks category as it is irrelevant to SQL injection.

I know it is irrelevant. This was originally posted in the website and forum hacking section, but got moved..

BlackRoas - June 22, 2012, 12:24 am

Thanks ?Dan for SSI Injection vulnerable sites I like it

Zixem - June 22, 2012, 4:16 am

Thank you ?Dan !

~*Zixem ?

fobber - June 22, 2012, 5:56 am

(Jun 21, 2012 10:37 PM)Phizo Wrote: [\[CITE\]](#) While this is nice and all; I don't see why this should be posted in the SQL Injection Attacks category as it is irrelevant to SQL injection.Well. The description to this sub-forum is:

For help and tutorials on SQL injection attacks or other code injection techniques enter this forum.
So it really isn't that wrong, is it?

Thanks for the list, Dan. I'll go practice now! ^.^

Phizo - June 22, 2012, 6:42 am

(Jun 22, 2012 05:56 AM)fobber Wrote: [\[CITE\]](#) Well. The description to this sub-forum is:

For help and tutorials on SQL injection attacks or other code injection techniques enter this forum.
So it really isn't that wrong, is it?

Thanks for the list, Dan. I'll go practice now! ^.^

I suppose so, it got moved here for a reason after all.

TheExclusive - June 22, 2012, 9:11 am

The most of the time

```
<!--#exec cmd="ls -a" --></pre><!--#exec cmd="ls -a" --></pre>
```

 succeed but when i try to inject my shell i fails.

Do you know what i am doing wrong ?

Th3PonyWizard - June 22, 2012, 9:22 am

(Jun 22, 2012 09:11 AM)TheExclusive Wrote: [\[CITE\]](#) The most of the time

```
<!--#exec cmd="ls -a" --></pre><!--#exec cmd="ls -a" --></pre>
```

 succeed but when i try to inject my shell i fails.

Do you know what i am doing wrong ?How would anyone know what's you're doing wrong without knowing what are you doing? :\

Syntax?

P3rF3cT - June 23, 2012, 8:51 am

can we wget our shell.txt from dropbox also??

Because i am not able to download my shell.txt on any of these websites.

DirgofCeberus - August 8, 2012, 5:02 am

Thanks a lot Đan! I learned from your tutorial

TheNeutron - August 8, 2012, 8:02 am

Thanks man! Just what I was searching for! :D

WTF just happened when I tried to inject this site??? O_o

<http://iloveimages.com/user/login.shtml>

lolollolz. :p

whattehp406 - August 31, 2012, 5:18 am

<http://www.getstock.com/user/login.shtml> sends you to the nsa.gov site when you try to do this lol

Desmolicious - August 31, 2012, 5:55 am

(Aug 8, 2012 08:02 AM)-=Hack0pz=- Wrote: [\[CITE\]](#) Thanks man! Just what I was searching for! :D

WTF just happened when I tried to inject this site??? O_o

<http://iloveimages.com/user/login.shtml>

lolollolz. :pl laugh whenever I see that happen, Just because this means they have a 'Anti-SSI EXEC' XD