

Forum:[Hack Forums](#)

Thread: [File Inclusion](#)

Pizza_Rollz - February 21, 2019, 6:23 am

I was using sqlmap on a bunch of different sites and one i found said it had a File Inclusion vulnerability.Can someone help me on What can I do from here?

valetta - February 21, 2019, 6:38 am

First you need to understand what File Inclusion is. In short term: You should be able to include local files from the webapp (or url bar) and the content would be displayed. From here, you can do further enumeration of the system.

In shorter term: Google "Local file inclusion" -> Check OWASP top 10 and they usually have PoCs for you to try (Basic ones)

Pizza_Rollz - February 21, 2019, 6:47 am

(Feb 21, 2019 07:38 AM)valetta Wrote: [\[CITE\]](#) First you need to understand what File Inclusion is. In short term: You should be able to include local files from the webapp (or url bar) and the content would be displayed. From here, you can do further enumeration of the system.

In shorter term: Google "Local file inclusion" -> Check OWASP top 10 and they usually have PoCs for you to try (Basic ones)

Thanks

Daxer - February 21, 2019, 6:48 am

Read database connection files and dump whole website

Pizza_Rollz - February 21, 2019, 6:58 am

(Feb 21, 2019 07:48 AM)Daxer Wrote: [\[CITE\]](#) Read database connection files and dump whole website

I don't how do that, can you tell how?

Daxer - February 21, 2019, 7:00 am

(Feb 21, 2019 07:58 AM)Pizza_Rollz Wrote: [\[CITE\]](#) I don't how do that, can you tell how?

Read a file that you know connects to the database. there will usually be database username and password or file that includes the config. Then read the config through the vulnerability

LegendBegins - February 21, 2019, 12:58 pm

Practice with OWASP's vulnerable web app project; it has some great examples on how these vulnerabilities work and how to utilize them. Just be aware that the less you know, the more dangerous it is to be messing with production systems.

shelled - February 22, 2019, 9:41 pm

You can try and see if it's vulnerable to directory traversal.

So with that, you're able to read sensitive files and directories that might be of use to you. /etc/passwd and/or where to upload a file etc. System version, what the website is running on, on and on.

Once you're authenticated you'll probably be able to then include a shell if you can find a place to upload it so it'll parse your shell allowing you to gain an initial foothold into the environment.

Sitrep - *February 28, 2019, 4:36 am*

You seem to have pretty low knowledge to be playing around on live targets like that. You should set up an virtual test environment to attack instead, it's better for you in the long run since you might get arrested if you don't know what you're doing. Just a kind advice.

It's good that you're practicing but it's better to be safe than sorry :)