

Forum:[Hack Forums](#)

Thread: [CGI Hacks](#)

ironchin21 - October 16, 2017, 12:17 pm

Anyone Really good with hacking CGI, all Im looking for is a CGI script to get the get ROOT access to the server.

Nikto:

/cgi-sys/cgiwrap/ allows arbitrary uses to access remote command execution.

On the webbrowser:

This is what I have so far....

[http://BLAH.com/cgi-sys/cgiwrap?user=\(USERNAME\)](http://BLAH.com/cgi-sys/cgiwrap?user=(USERNAME))

[http://www.BLAH.com/cgi-sys/cgiwrap?user=\(USERNAME\)&scriptname=\(ANY_DEFAULT_SCRIPTS?\)](http://www.BLAH.com/cgi-sys/cgiwrap?user=(USERNAME)&scriptname=(ANY_DEFAULT_SCRIPTS?))

Any Default scripts I can you in order to access it?

k245nx - October 18, 2017, 3:36 am

maybe it is vulnerable to shellshock. u can have internal function declaration in its environment variable. U can run arbitrary command by declaring an empty function and add a command after this declaration. Most web servers like Apache uses environment variables to pass headers to the CGI.

ironchin21 - November 8, 2017, 6:31 pm

ok , thanks for replying, and can you dumb that down a tad bit lol . pretty much now I have enumerate the user but still need to find the query string in order to access anything on the server, what can I do now!