

Forum:[Hack Forums](#)

Thread: [IIS Physical Path?](#)

joni1n3r - May 11, 2020, 8:27 pm

If a IIS 8.5 shows the Physical Path how danger is? Know the path is posible to exploit in some way?

thanks

frank3nstien - May 11, 2020, 11:02 pm

(May 11, 2020 08:27 PM)joni1n3r Wrote: [\[CITE\]](#) If a IIS 8.5 shows the Physical Path how danger is? Know the path is posible to exploit in some way?

thanks

Actually you need to understand the difference between application vs virtual directory in IIS, it is due to "system.webserver" tag sometimes its reveals default credentials you may try those.

You can try to enumerate the path.

Shadow_Cloud - May 11, 2020, 11:04 pm

Typically knowing the actual path is just a quality of life factor for some other checks so you don't need to enumerate to find out what exists and what doesn't. Similar to the difference between SQLi and Blind SQLi

joni1n3r - May 11, 2020, 11:29 pm

(May 11, 2020 11:02 PM)frank3nstien Wrote: [\[CITE\]](#) Actually you need to understand the difference between application vs virtual directory in IIS, it is due to "system.webserver" tag sometimes its reveals default credentials you may try those.

You can try to enumerate the path.

Ok i try to FUZZ the directory, but all errors show Server error 404 only without the physical path and error code. But if i try with some characters with no filter in WAF then show the error 404 dat contains all the information.

Quote:Actually you need to understand the difference between application vs virtual directory in IIS, it is due to "system.webserver" tag sometimes its reveals default credentials you may try those.

How i can do this, im a n00b in IIS. And the Physical Path looks like default in windows C:\inetpub

(May 11, 2020 11:04 PM)Shadow_Cloud Wrote: [\[CITE\]](#) Typically knowing the actual path is just a quality of life factor for some other checks so you don't need to enumerate to find out what exists and what doesn't. Similar to the difference between SQLi and Blind SQLi

Ok, right now if i change in the Request the host, is reflected by Requested URL for example. If i make a request to victim.c0m and intercept the request and change the host like this.

Quote:GET /login HTTP/1.1

Hos: myhost.c0m

in the response i got the same 404 IIS error with physical path, but now in "Request URL" is myhost.c0m/page

Any recomendation?