

Forum:[Hack Forums](#)

Thread: [Stealing Sensitive data with access-control-allow-origin header: *](#)

MikeGolfRomeo - June 25, 2020, 9:14 am

So I NiktoScanned a website and found that

+ Retrieved access-control-allow-origin header:

I navigated to the robots.txt and found this

User-agent: Disallow: /admin/ Disallow: /cache/ Disallow: /calendarjotter/ Disallow: /app/file/download/* Disallow: /downloadfile/* Disallow: /asset/* Sitemap: <http://www.hawkedon.wokingham.sch.uk/sitemap.xml>

It disallows /admin/.

How could I use a GET request to see all the data in the /admin and all the other forbidden directories?

printf - June 25, 2020, 10:40 am

Hello, I need a web penetration service, and I have several goals that require a database inside. I hope you can contact me, we can talk, I can pay bitcoin. My telegram: @li520

christo - June 25, 2020, 10:44 am

(Jun 25, 2020 10:40 AM)printf Wrote: [\[CITE\]](#) Hello, I need a web penetration service, and I have several goals that require a database inside. I hope you can contact me, we can talk, I can pay bitcoin. My telegram: @li520
check my convo

linkinpork - June 26, 2020, 10:22 pm

(Jun 25, 2020 09:14 AM)MikeGolfRomeo Wrote: [\[CITE\]](#) So I NiktoScanned a website and found that

+ Retrieved access-control-allow-origin header: *

Hey, mate.

You got what's called a CORS vulnerability. Cross Origin Resource Sharing allows data to pass between websites. In your case, your target can interact with anyone, which means any website could leak the data from the target.

Wordpress used to have this bug, like, more than a year ago, until they fixed it by default.

I'm not going to go into the specifics, but this was the exploit page I made:

<https://pastebin.com/vmtEFF59>

(Jun 25, 2020 09:14 AM)MikeGolfRomeo Wrote: [\[CITE\]](#) How could I use a GET request to see all the data in the /admin and all the other forbidden directories?

This one -- If I recall correctly I saw a bug report about someone editing the web.config and htaccess file to allow access to them. If you could put a RAT into the website, you can find the files to edit here:

Code `www.website.com/.htaccess`

www.website.com/web.config
I hope it goes well, mate

MikeGolfRomeo - June 28, 2020, 8:54 am

(Jun 26, 2020 10:22 PM)linkinpork Wrote: [\[CITE\]](#) Hey, mate.

You got what's called a CORS vulnerability. Cross Origin Resource Sharing allows data to pass between websites. In your case, your target can interact with anyone, which means any website could leak the data from the target.

Wordpress used to have this bug, like, more than a year ago, until they fixed it by default.

I'm not going to go into the specifics, but this was the exploit page I made:

<https://pastebin.com/vmtEFF59>

This one -- If I recall correctly I saw a bug report about someone editing the web.config and htaccess file to allow access to them. If you could put a RAT into the website, you can find the files to edit here:

Code www.website.com/.htaccess

www.website.com/web.config

I hope it goes well, mate

Hey bro thanks for helping!

I was trying to use your exploit but it didn't seem to work....

This might be a bit much and a bit???but could you teach me how to do it for that website specifically?

I can't currently afford to pay but Ill try to repay you somehow ?

Edit:

These are some other things i found..

X-Frame-Options Not set

X-XSS-Protection Not set

Strict-Transport-Security Not set

X-Content-Type-Options Not Set

Ubuntu	Operating Systems
Apache 2.4.43	Web Servers
PDF.js	Miscellaneous
SWFObject	Miscellaneous
Varnish	Cache Tools
Google Font API	Font Scripts
MediaElement.js	Video Players
New Relic	Analytics
jQuery	JavaScript Frameworks

Thanks anyway
matt

linkinpork - June 28, 2020, 9:17 am

(Jun 28, 2020 08:54 AM)MikeGolfRomeo Wrote: [\[CITE\]](#) Hey bro thanks for helping!

I was trying to use your exploit but it didn't seem to work....

This might be a bit much and a bit???but could you teach me how to do it for that website specifically?

Sure, I'll try. Hmu over convo.