

Forum:[Hack Forums](#)

Thread: [webserver vulnerability](#)

imsodumb - February 5, 2020, 1:41 pm

Hey , im new i need to get if possible some details and help about exploiting a vulnerability in webserver i use kali and nikto btw im bad i just started ! tanks for help me ?[

BigJoe7413 - February 5, 2020, 1:49 pm

can you provide more info?

imsodumb - February 5, 2020, 2:16 pm

yup , i use nikto to scan a webserver and i found that :Retrieved x-powered-by header: PHP/7.1.17
+ Retrieved access-control-allow-origin header: *
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ RFC-1918 IP address found in the 'location' header. The IP is "172.31.46.56".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "172.31.46.56".
+ Uncommon header 'x-amz-request-id' found, with contents: 9902EBE6B4877F3D
+ Uncommon header 'x-amz-id-2' found, with contents:
IXJdyve686S40jPHuNDNcNVwEnlqXEWM0MWnkwcojmHEv1YVjcVEOy/Wyt5WgtUKNs0yc9yPIEs
=
+ /help/: Help directory should not be accessible
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3093: /.htaccess: Contains configuration and/or authorization information
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 1 error(s) and 12 item(s) reported on remote host

I try to understand MIMS sniffing but i still dont get it.
after i see something intersting : "/config : PHP config file may contain database lds passwords.
i try to catch the file with adding the file in the web bar and nothing return back i dont get any web error juste nothing happend..
so you can give my some way to exploit those vulnerability that be great i wanna learn after all !

thewolf21 - February 7, 2020, 8:46 pm

send me information bro i help

imsodumb - February 9, 2020, 10:23 am

Hey thewolf21 cannot pm you i don't have the lvl sorry ..

compalabee - February 9, 2020, 11:43 am

(Feb 5, 2020 03:16 PM)imsodumb Wrote: [CITE](#) yup , i use nikto to scan a webserver and i found that :Retrieved x-powered-by header: PHP/7.1.17

Try to read up on the terms in the report. You won't get very far without research.

Header best practice problems

PHP Code

<?php

access-control-allow-origin

X-Frame-Options

X-XSS-Protection

X-Content-Type-Options

Vulnerabilities

PHP Code

<?php

OSVDB-630

OSVDB-3093

Predictable resource location

PHP Code

<?php

/help

/config.php

Also, note that scanners are very noisy. I wouldn't be surprised if the sysadmin already knows that someone was taking a peek. Hopefully you masked your IP address too.