

Forum:[Hack Forums](#)

Thread: [Very vulnerable website. How can I exploit it?](#)

Smox - August 7, 2017, 11:37 pm

With the information given, how can I exploit it?

New to this

- Nikto v2.1.6

+ Server: Apache/2.4.25 (Amazon) PHP/5.6.30
+ 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
+ Cookie PHPSESSID created without the httponly flag
+ Cookie NEWSLETTER_POP_NEW created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.6.30
+ Server banner has changed from 'Apache/2.4.25 (Amazon) PHP/5.6.30' to 'awselb/2.0' which may suggest a WAF, load balancer or proxy is in place
+ OSVDB-3268: /icons/: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /icons/README, fields: 0x13f40x438c034968a80
+ OSVDB-3233: /icons/README: Apache default file found.

•^v^-[bLacKn3x]-^v^• - August 8, 2017, 12:23 am

How can u see that website is VERY VULNERABLE ?

#can't see any vulnerability on that Nikto report :)

It's better to search manually for exploits on that website .

Regards-

Vana - August 8, 2017, 12:27 am

None of that output indicates a vulnerability exists.

Don't use tools like this if you can't even understand what they output.

arma23hacker - August 8, 2017, 4:09 am

i would recomend downloading a cracked version of acutetix and other tools to help you out, do port scans and find out what other services are on the host

frank3nstien - August 8, 2017, 6:21 am

(Aug 7, 2017 11:37 PM)Smox Wrote: [CITE](#) With the information given, how can I exploit it?

New to this

- Nikto v2.1.6

-
- + Server: Apache/2.4.25 (Amazon) PHP/5.6.30
 - + 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
 - + Cookie PHPSESSID created without the httponly flag
 - + Cookie NEWSLETTER_POP_NEW created without the httponly flag
 - + Retrieved x-powered-by header: PHP/5.6.30
 - + Server banner has changed from 'Apache/2.4.25 (Amazon) PHP/5.6.30' to 'awselb/2.0' which may suggest a WAF, load balancer or proxy is in place
 - + OSVDB-3268: /icons/: Directory indexing found.
 - + Server leaks inodes via ETags, header found with file /icons/README, fields: 0x13f40x438c034968a80
 - + OSVDB-3233: /icons/README: Apache default file found.
- Website is not vulnerable at all as per your Nikto report. There is only information gathering or you can search exploits online for version displayed in report.
- Aside, I think the scan is not completed properly i would suggest use other pro tool such as Acunetix, Netsparkers etc.

BioPhone - August 11, 2017, 10:36 am

the best way to go is searching vulnerablylities manual.