

Forum:[Hack Forums](#)

Thread: [Found Website Vulnerabilities](#)

beltona - July 30, 2023, 9:42 am

Hello , I'm pentesting on my friend's website and I found some vulnerabilities and admin page (protected with user and pass and code) but still don't know what to do with it , I even have the full source code of the website but don't know (which is a shame XD)
this the scan report here

Code Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
+ /: Cookie PHPSESSID created without the httponly flag.
+ /: Retrieved x-powered-by header: PHP/5.6.30.
+ /: The anti-clickjacking X-Frame-Options header is not present.
+ /: 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
+ OpenSSL/1.0.2j appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ PHP/5.6.30 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ Apache/2.4.25 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST.
+ /admin/config.php: PHP Config file may contain database IDs and passwords.
+ /sips/sipssys/users/a/admin/user: SIPS v0.2.2 allows user account info (including password) to be retrieved remotely.
+ /_mem_bin/remind.asp: Page will give the password reminder for any user requested (username must be known).
+ /admin/cplogfile.log: DevBB 1.0 final log file is readable remotely. Upgrade to the latest version.
+ /admin/system_footer.php: myphpnuke version 1.8.8_final_7 reveals detailed system information.
+ /admin/admin_phpinfo.php4: Mon Album version 0.6.2d allows remote admin access. This should be protected.
+ /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper authentication. Attempt to log in with user 'test' password 'test' to verify.
+ /admin/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin. S
+ //admin/admin.shtml: Axis network camera may allow admin bypass by using double-slashes before URLs.
+ /admin/database/wwForum.mdb: Web Wiz Forums pre 7.5 is vulnerable to Cross-Site Scripting attacks. Default login/pass is Administrator/letmein.
+ //admin/aindex.htm: FlexWATCH firmware 2.2 is vulnerable to authentication bypass by prepending an extra /'s.
+ /admin/wg_user-info.ml
+ /admin/: This might be interesting.
+ /news: This might be interesting.
+ /admin/auth.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/cfg/configscreen.inc.php+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/cfg/configsite.inc.php+: This might be interesting: has been seen in web logs from an

unknown scanner.

+ /admin/cfg/configsql.inc.php+: This might be interesting: has been seen in web logs from an unknown scanner.

+ /admin/cfg/configtache.inc.php+: This might be interesting: has been seen in web logs from an unknown scanner.

+ /admin/cms/htmltags.php: This might be interesting: has been seen in web logs from an unknown scanner.

+ /admin/credit_card_info.php: This might be interesting: has been seen in web logs from an unknown scanner.

+ /admin/exec.php3: This might be interesting: has been seen in web logs from an unknown scanner.

+ /admin/index.php: This might be interesting: has been seen in web logs from an unknown scanner.

+ /admin/modules/cache.php+: This might be interesting: has been seen in web logs from an unknown scanner.

+ /admin/objects.inc.php4: This might be interesting: has been seen in web logs from an unknown scanner.

+ /admin/script.php: This might be interesting: has been seen in web logs from an unknown scanner.

+ /admin/settings.inc.php+: This might be interesting: has been seen in web logs from an unknown scanner.

+ /admin/templates/header.php: This might be interesting: has been seen in web logs from an unknown scanner.

+ /admin/upload.php: This might be interesting: has been seen in web logs from an unknown scanner.

+ /icons/: Directory indexing found.

+ /admin/adminproc.asp: Xpede administration page may be available. The /admin directory should be protected.

+ /admin/datasource.asp: Xpede page reveals SQL account name. The /admin directory should be protected.

+ /admin/admin.php?adminpy=1: PY-Membres 4.2 may allow administrator access. See

+ /icons/README: Apache default file found.

+ /Admin/: This might be interesting.

+ /patch/: Directory indexing found.

+ /admin/account.asp: Admin login page/section found.

+ /admin/account.html: Admin login page/section found.

+ /admin/account.php: Admin login page/section found.

+ /admin/controlpanel.asp: Admin login page/section found.

+ /admin/controlpanel.html: Admin login page/section found.

+ /admin/controlpanel.php: Admin login page/section found.

+ /admin/cp.asp: Admin login page/section found.

+ /admin/cp.html: Admin login page/section found.

+ /admin/cp.php: Admin login page/section found.

+ /admin/home.asp: Admin login page/section found.

+ /admin/home.php: Admin login page/section found.

+ /admin/index.asp: Admin login page/section found.

+ /admin/index.html: Admin login page/section found.

+ /admin/login.asp: Admin login page/section found.

+ /admin/login.html: Admin login page/section found.

+ /admin/login.php: Admin login page/section found.

+ /admin/html: Tomcat Manager / Host Manager interface found (pass protected).

+ /admin/status: Tomcat Server Status interface found (pass protected).

+ /admin/sites/new: ComfortableMexicanSofa CMS Engine Admin Backend (pass protected).

- + /.idea/modules.xml: JetBrains project IDE reveals application information.
- + /.idea/vcs.xml: JetBrains project IDE reveals application information.
- + /.idea/workspace.xml: JetBrains project IDE reveals application information.
- + /.gitignore: .gitignore file found. It is possible to grasp the directory structure.
- + /README.md: Readme Found.

Appreciate any help thank youu in advance

Sentry Guard - July 30, 2023, 10:03 am

Look through the code for vulnerabilities? What is your goal? Just to show you can access his server? If you can see his database structure and the connection info couldn't you remotely inject?

Skorp - July 30, 2023, 2:25 pm

Judging by the report OP, it is best you don't post his website here. Whatever friend's website you did the report on is highly exploitable and would just get dumped on or just be a shell in this case. Btw, you do know his PHP is six years old... did he not update it?

' Wrote:but still don't know what to do with it
What are your intentions fella? ?

beltona - July 30, 2023, 8:51 pm

(Jul 30, 2023 02:25 PM)Skorp Wrote: [\[CITE\]](#) Judging by the report OP, it is best you don't post his website here. Whatever friend's website you did the report on is highly exploitable and would just get dumped on or just be a shell in this case. Btw, you do know his PHP is six years old... did he not update it?

that's how we started this hacking conversation about the php version , but still couldn't prove anything hahaha

(Jul 30, 2023 02:25 PM)Skorp Wrote: [\[CITE\]](#) What are your intentions fella? ?

Exploit any vulnerability like upload a shell or edit a page to prove that I gained access

seriouserial - July 30, 2023, 10:18 pm

What do you use to scan this? nikto? You can pretty much do a lot of things knowing these stuff.

beltona - July 31, 2023, 6:52 am

(Jul 30, 2023 10:18 PM)seriouserial Wrote: [\[CITE\]](#) What do you use to scan this? nikto? You can pretty much do a lot of things knowing these stuff.

Yes nikto , tried php cgi arg injection but didn't work