

Forum:[Hack Forums](#)

Thread: [403 Forbidden Bypass](#)

hex-r - April 16, 2022, 3:06 pm

Hallo!

i'm new here and i hope can someone here help me!

this website dir jtl5 .shoptemplate .net/shop3/includes/ return 403 Forbidden and in this directory contain a file 'config.JTL-Shop.ini.php' and this file contain database credentials!

Can someone hack it? or access to the file content and extract the values?

more dirs

jtl5 .shoptemplate .net/shop3/plugins/
jtl5 .shoptemplate .net/shop3/templates/

i am sure they have wrong htaccess configuration and site is hackable!

and server is also not secure, nmap output/log

```
21/tcp open  ftp      ProFTPD (requires SSL)
22/tcp open  ssh       (protocol 2.0)
25/tcp open  smtp
80/tcp open  http      Apache httpd
110/tcp open pop3      Courier pop3d
143/tcp open  imap      Dovecot imapd
222/tcp open  ssh       OpenSSH 7.9p1 (protocol 2.0)
443/tcp open  ssl/http  Apache httpd
465/tcp open  ssl/smtp
587/tcp open  smtp
993/tcp open  ssl/imap  Dovecot imapd
995/tcp open  ssl/pop3  Courier pop3d
5432/tcp open postgresql PostgreSQL DB 9.6.0 or later
8080/tcp open  http      nginx 1.19.8
```

ist there a service that's i can exploit it?

pllllllllllz help

SIM-2501407 - April 17, 2022, 7:00 am

A 403 is a 403, so there's nothing to be done there...

That nginx they are running seems interesting.

<https://x41-dsec.de/lab/advisories/x41-2021-002-nginx-resolver-copy/>

Quote:Confirmed Affected Versions:

0.6.18 - 1.20.0

There's a proof of concept included in there too.

<https://access.redhat.com/security/cve/cve-2021-23017>

Quote: A flaw was found in nginx. An off-by-one error while processing DNS responses allows a network attacker to write a dot character out of bounds in a heap allocated buffer which can allow overwriting the least significant byte of next heap chunk metadata likely leading to a remote code execution in certain circumstances. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

Good luck finding someone to do your dirty work.

Also, can poke at that OpenSSH too probably.

https://nvd.nist.gov/vuln/search/results?form_type=Advanced&cves=on&cpe_version=cpe:/a:openbsd:openssh:7.9

hex-r - April 17, 2022, 8:14 am

Thanks for your reply Educational Purposes! do you think can i exploit server? when yes, how? do you have some references? plllz help

SIM-5172123 - April 17, 2022, 9:06 am

(Apr 17, 2022 08:14 AM)hex-r Wrote: [\[CITE\]](#) Thanks for your reply Educational Purposes! do you think can i exploit server? when yes, how? do you have some references? plllz help
after what he mentioned if you have basic knowladge about hacking you should know now what exactly to do , but seems you don't know about this topic so i recommend you to hire someone to do the job for you , best of luck