Exploitation

#Search Exploit with google;

site:exploit-db.com "October CMS"

site:github.com "October CMS"

#Search Exploit with searchsploit;

searchsploit OpenSSL

searchsploit OpenSSL | grep --invert-match 'PHP\|Heartbleed\|dos\|windows'

searchsploit -p 41936.txt

cp /usr/share/exploitdb/exploits/php/webapps/41936.txt .

- ----------

#Compiler the exploit

##for Linux;

which gcc

gcc -o kernel-exploit 44298.c

./kernel-exploit

or

dos2unix exploit.sh (very useful ;))

For more; https://tools.kali.org/reporting-tools/dos2unix

##for Windows;

i686-w64-mingw32-gcc 40564.c -o exploit.exe -lws2_32

- ----------

#Running the Exploit

##Firstly;

chmod +x asd.sh

or

chmod 755 asd.sh

##Later;

./asd.sh

python asd.py

perl asd.pl

ruby asd.rb

php asd.php (php-curl is installed: apt install php-curl)

- ----------