Arkham,luks[解碼]、JSF反彈shell

```
—# nmap -sCV -p80,135,139,445,8080,49666,49667 -A 10.10.10.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 16:11 EDT
Nmap scan report for 10.10.10.130
Host is up (0.21s latency).

PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
8080/tcp  open  http          Apache Tomcat 8.5.37
|_http-open-proxy: Proxy might be redirecting requests
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-title: Mask Inc.
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
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: 2024-09-05T20:12:17
|_  start_date: N/A

TRACEROUTE (using port 80/tcp)
```

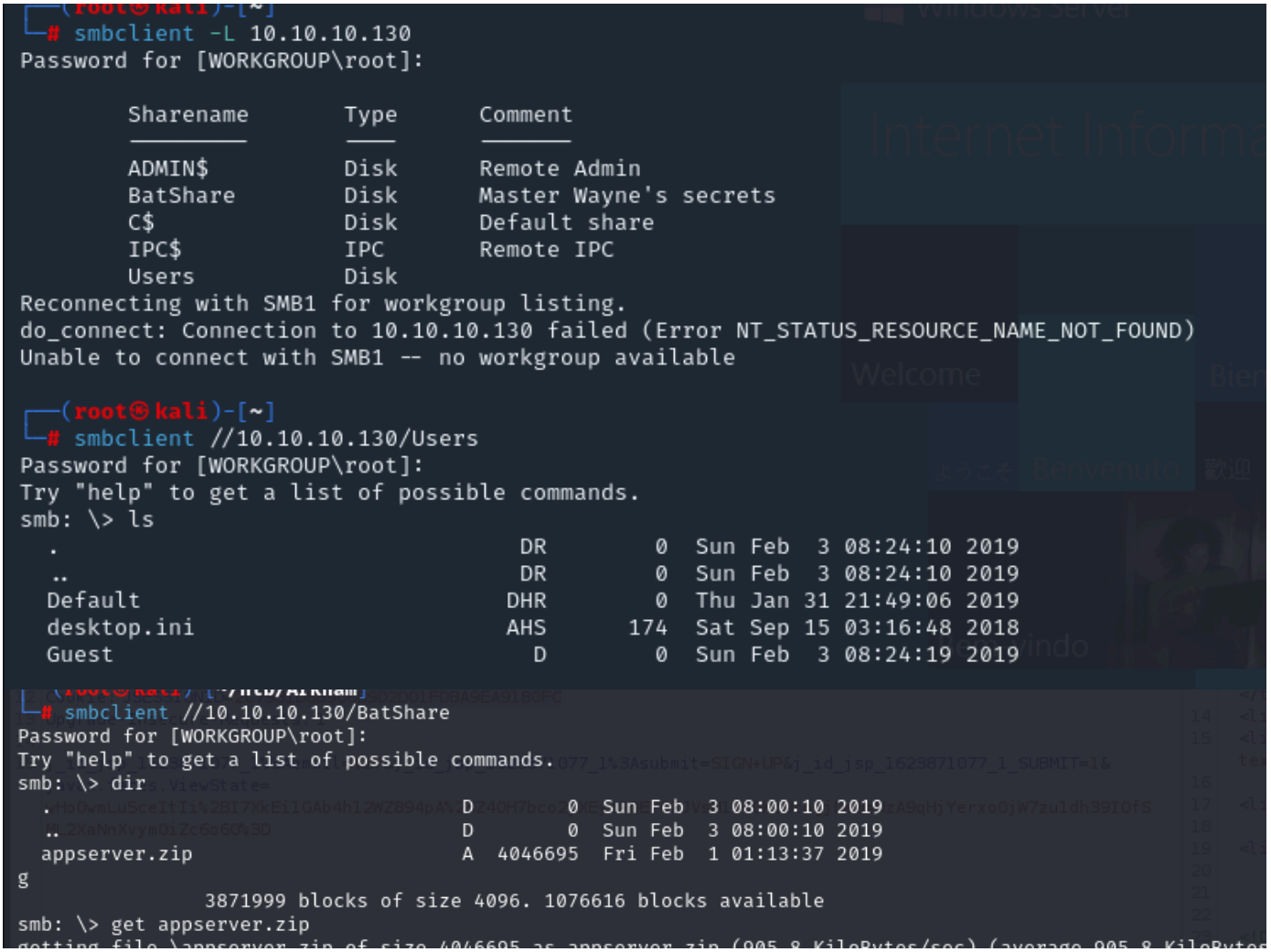
```
HOP RTT       ADDRESS
1   217.13 ms 10.10.14.1
2   217.56 ms 10.10.10.130

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 104.05 seconds
```

80Port

單純IIS Server，目前爆破無發現任何睦路

139、445Port SMB

可匿名登入



將所有檔案下載出來...

指令：

```
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
```

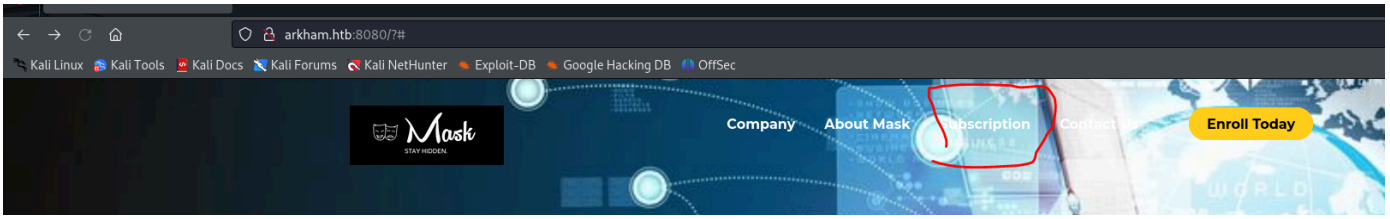
因檔案大，先給它下載。我先看8080Port

8080Port

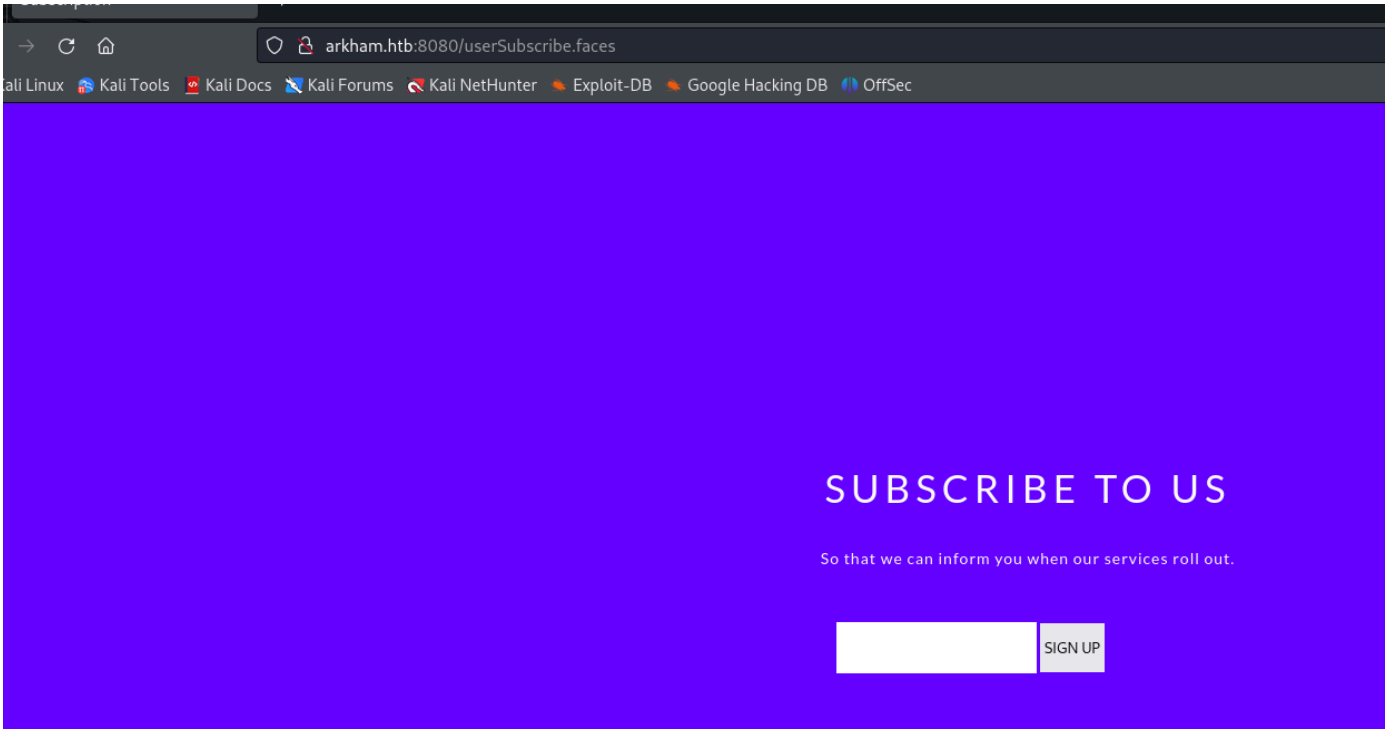
目錄爆破

```
gobuster dir -u http://arkham.htb:8080 -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -k
===============================================================
/images               (Status: 302) [Size: 0] [--> /images/]
/css                  (Status: 302) [Size: 0] [--> /css/]
/js                   (Status: 302) [Size: 0] [--> /js/]
/fonts                (Status: 302) [Size: 0] [--> /fonts/]
```

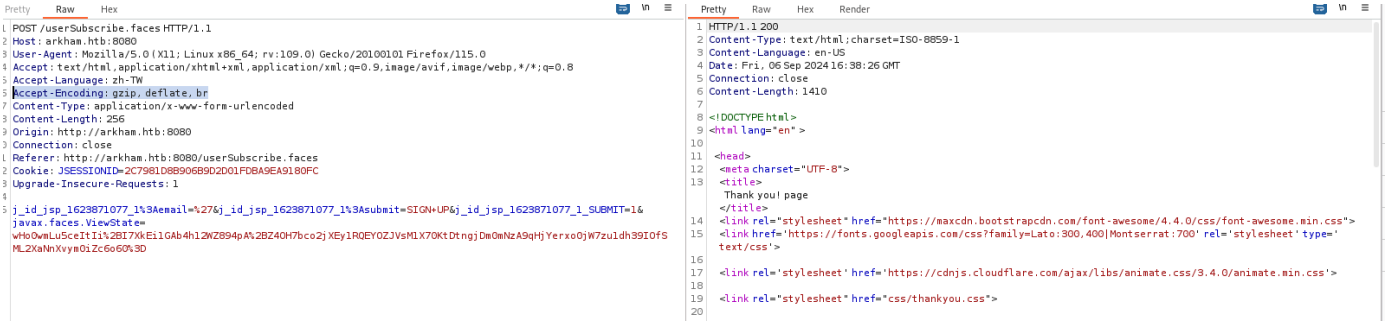
進去都404。唯一按訂閱才有用



轉到`http://arkham.htb:8080/userSubscribe.faces`

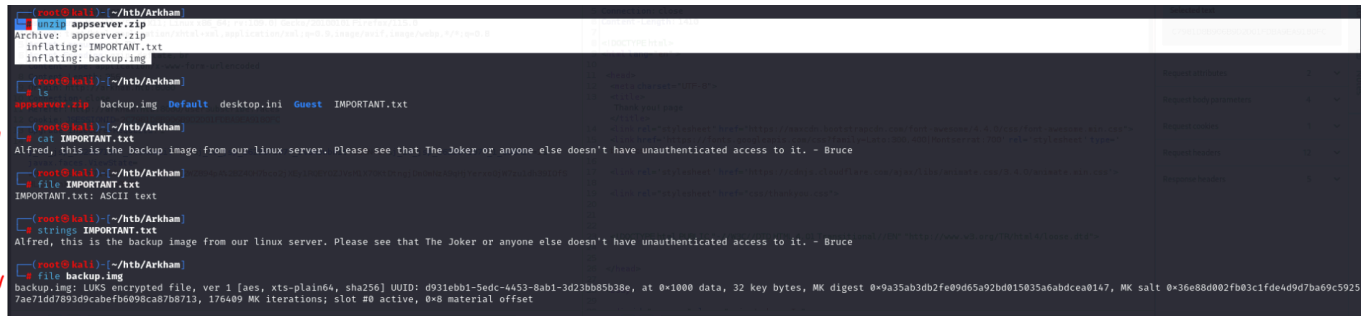


提交內容，會被編碼：`gzip, deflate, br`



回到前面SMB，先前有找到zip檔。

解壓後會取一個txt、一個圖片



txt內容：

```
Alfred, this is the backup image from our linux server. Please see that The Joker or anyone else doesn't have unauthenticated access to it. - Bruce
```

img內容：

```
backup.img: LUKS encrypted file, ver 1 [aes, xts-plain64, sha256] UUID: d931ebb1-5edc-4453-8ab1-3d23bb85b38e, at 0x1000 data, 32 key bytes, MK digest 0x9a35ab3db2fe09d65a92bd015035a6abdcea0147, MK salt 0x36e88d002fb03c1fde4d9d7ba69c59257ae71dd7893d9cabefb6098ca87b8713, 176409 MK iterations; slot #0 active, 0x8 material offset
```

LUKS加密參考：

- https://book.hacktricks.xyz/v/cn/generic-methodologies-and-resources/brute-force#fang-fa-1
- https://github.com/glv2/bruteforce-luks

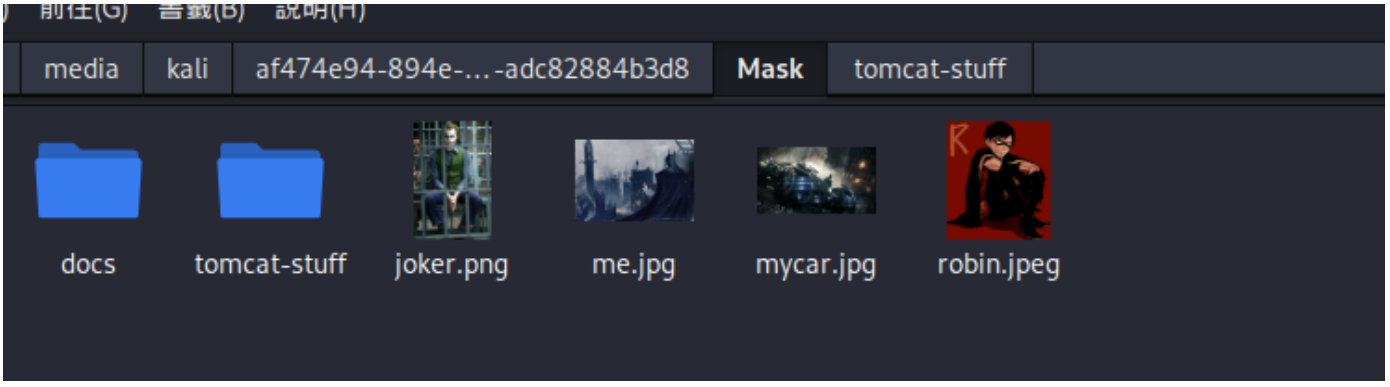
很吃電腦效能・・・跑超久

指令：

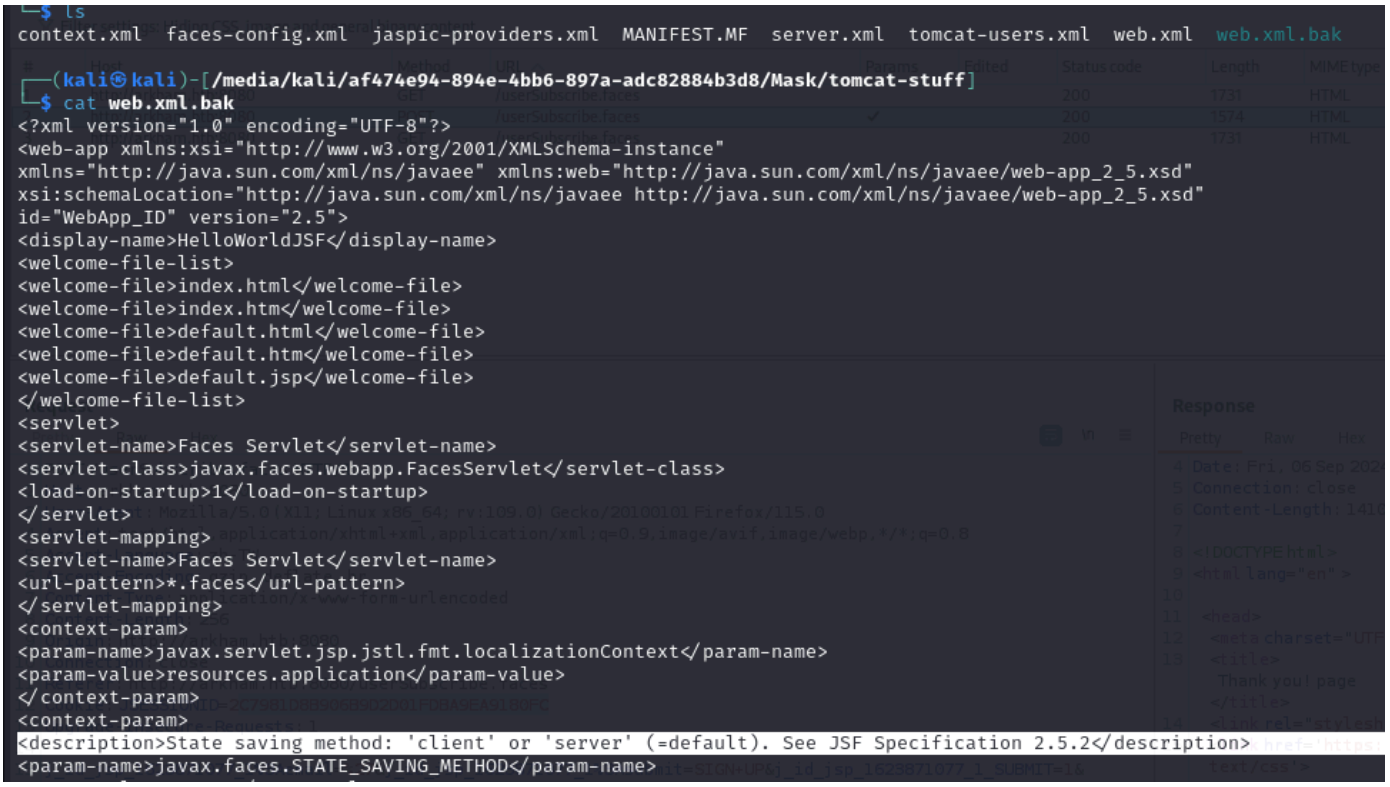
```
bruteforce-luks -t 10 -f /usr/share/wordlists/rockyou.txt -w passwd.txt -v 30 ../backup.img
```

獲取：Password found: batmanforever

解碼後，發現很多文件



在`/tomcat-stuff`發現`web.xml.bak`有顯示版本資訊`JSF Specification 2.5.2`



還有一些加密、演算法、金鑰[使用chatGTP]

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://java.sun.com/xml/ns/javaee"
xmlns:web="http://java.sun.com/xml/ns/javaee/web-app_2_5.xsd"
xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
http://java.sun.com/xml/ns/javaee/web-app_2_5.xsd"
id="WebApp_ID" version="2.5">

    <!-- Web 應用的顯示名稱 -->
    <display-name>HelloWorldJSF</display-name>

    <!-- 設置默認的歡迎文件 -->
    <welcome-file-list>
        <welcome-file>index.html</welcome-file>
        <welcome-file>index.htm</welcome-file>
        <welcome-file>default.html</welcome-file>
        <welcome-file>default.htm</welcome-file>
        <welcome-file>default.jsp</welcome-file>
    </welcome-file-list>

    <!-- 定義 FacesServlet -->
    <servlet>
        <servlet-name>Faces Servlet</servlet-name>
        <servlet-class>javax.faces.webapp.FacesServlet</servlet-class>
        <load-on-startup>1</load-on-startup>
```

```
    </servlet>

    <!-- 定義 FacesServlet 的 URL 映射 -->
    <servlet-mapping>
        <servlet-name>Faces Servlet</servlet-name>
        <url-pattern>*.faces</url-pattern>
    </servlet-mapping>

    <!-- 設置 JSTL 的本地化上下文 -->
    <context-param>
        <param-name>javax.servlet.jsp.jstl.fmt.localizationContext</param-name>
        <param-value>resources.application</param-value>
    </context-param>

    <!-- 設置狀態保存方法：'client' 或 'server'（默認） -->
    <context-param>
        <description>State saving method: 'client' or 'server' (=default). See JSF
Specification 2.5.2</description> <= 版本
        <param-name>javax.faces.STATE_SAVING_METHOD</param-name>
        <param-value>server</param-value>
    </context-param>

    <!-- 設置 MyFaces 的加密秘鑰 -->
    <context-param>
        <param-name>org.apache.myfaces.SECRET</param-name>
        <param-value>SnNGOTg3Ni0=</param-value>
    </context-param>

    <!-- 設置 MAC 算法 -->
    <context-param>
        <param-name>org.apache.myfaces.MAC_ALGORITHM</param-name>
        <param-value>HmacSHA1</param-value>
    </context-param>

    <!-- 設置 MAC 算法的加密秘鑰 -->
    <context-param>
        <param-name>org.apache.myfaces.MAC_SECRET</param-name>
        <param-value>SnNGOTg3Ni0=</param-value>
    </context-param>

    <!-- 設置是否允許 Javascript -->
    <context-param>
        <description>
```

```
    This parameter tells MyFaces if javascript code should be allowed in
    the rendered HTML output.
    If javascript is allowed, command_link anchors will have javascript code
    that submits the corresponding form.
    If javascript is not allowed, the state saving info and nested parameters
    will be added as url parameters.
    Default is 'true'
    </description>
    <param-name>org.apache.myfaces.ALLOW_JAVASCRIPT</param-name>
    <param-value>true</param-value>
</context-param>

<!-- 設置是否格式化 HTML 代碼 -->
<context-param>
    <description>
    If true, rendered HTML code will be formatted, so that it is 'human-readable'
    i.e. additional line separators and whitespace will be written, that do not
    influence the HTML code.
    Default is 'true'
    </description>
    <param-name>org.apache.myfaces.PRETTY_HTML</param-name>
    <param-value>true</param-value>
</context-param>

<!-- 設置是否檢測 Javascript -->
<context-param>
    <param-name>org.apache.myfaces.DETECT_JAVASCRIPT</param-name>
    <param-value>false</param-value>
</context-param>

<!-- 設置是否自動滾動到之前的垂直位置 -->
<context-param>
    <description>
    If true, a javascript function will be rendered that is able to restore the
    former vertical scroll on every request. Convenient feature if you have pages
    with long lists and you do not want the browser page to always jump to the top
    if you trigger a link or button action that stays on the same page.
    Default is 'false'
    </description>
    <param-name>org.apache.myfaces.AUTO_SCROLL</param-name>
    <param-value>true</param-value>
</context-param>
```

```
    <!-- 設置會話中視圖的最大數量 -->
    <context-param>
        <param-name>com.sun.faces.numberOfViewsInSession</param-name>
        <param-value>500</param-value>
    </context-param>

    <!-- 設置邏輯視圖的最大數量 -->
    <context-param>
        <param-name>com.sun.faces.numberOfLogicalViews</param-name>
        <param-value>500</param-value>
    </context-param>

    <!-- 定義啟動時加載的監聽器 -->
    <listener>
        <listener-
class>org.apache.myfaces.webapp.StartupServletContextListener</listener-class>
    </listener>

</web-app>
```

找JSF漏洞參考文件：

- https://book.hacktricks.xyz/v/cn/pentesting-web/deserialization/java-jsf-viewstate-.faces-deserialization
- https://www.alphabot.com/security/blog/2017/java/Misconfigured-JSF-ViewStates-can-lead-to-severe-RCE-vulnerabilities.html
- https://0xrick.github.io/hack-the-box/arkham/ [hacktrick也有答案せ~]
- https://github.com/frohoff/ysoserial

好難...