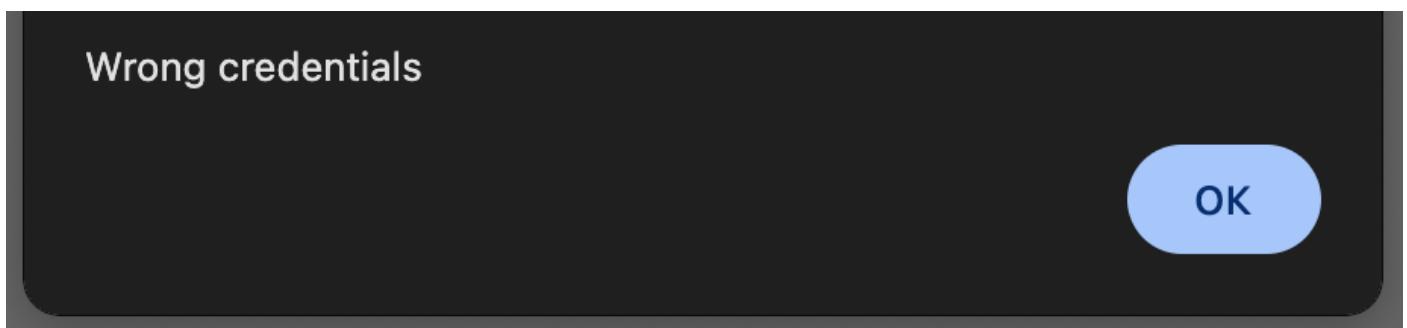


у нас есть красивая страничка с логином, и так как никаких данных у нас нет, по приколу попробуем логин admin:admin



получем wrong credentials, а так как дело идет с полем логина/регистрации сразу тестили SQLi (SQL Injection)

получим просто

ERROR

так как нам не выдало alert() об ошибке неверных кредитов, можно сказать что SQLi прошло, но скорее всего в бд случилась какая то ошибка из за нашего запроса. коротко - SQLi работает, но не совсем

изучая дальше можем обратить внимание на то что название задания - INSERTissue, что намекает на существующую InsertSQLi. и почитав статьи можем найти подобные описания:

пример запроса при регистрации:

```
INSERT INTO accounts (username, password, mysignature)
VALUES ('xxx', 'yyy', 'zzz');
```

InsertSQL инъекция при регистрации пользователя

We can demonstrate the vulnerability by adding a user account using the Username parameter:

```
name', 'pass', 'sign')-- --
```

если примерять её на код запроса будет:

```
INSERT INTO accounts ('name', 'pass', 'sing')--
```

(после -- весь остальной код комментируется, то есть мы смогли подделать запрос и вписать свои данные)

то есть в целом можно попробовать эксплуатировать эту инъекцию. но так как /login не очень подходит для вставки значений (что достаточно логично), попробуем пронести инъекцию в register.

у нас нет точной структуры БД, поэтому стоит только гадать, например она может быть:

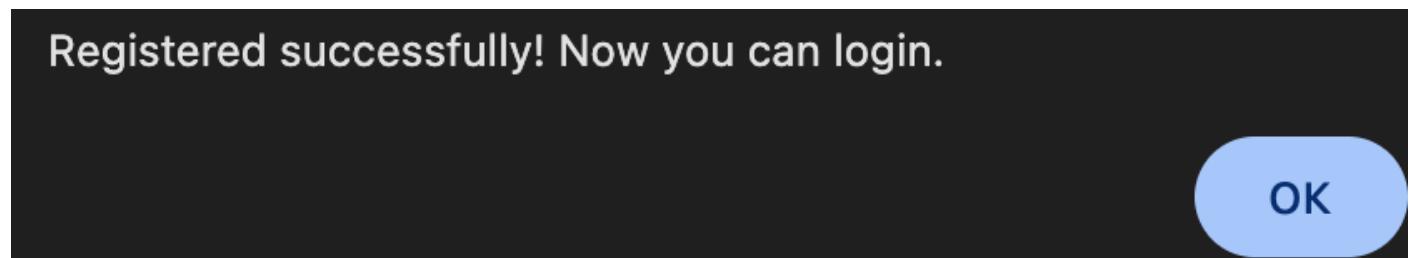
| Username | Password | IsAdmin |
|----------|----------|---------|
|----------|----------|---------|

```
| admin | password | 1 |
| user  | password | 0 |
```

попробуем сделать инъекцию:

`123', '123', 1)--` (то есть мы создаем пользователя 123, с паролем 123 и значением IsAdmin = 1)

получаем:



логинимся и видим флаг, то есть предположение о структуре БД было верным и мой пользователь - админ:

76096,4076121,4076542,4076727,4076931,4076999,4077200,4077219,4077221,4077298,
4077748,**4078175**,4078430,4078455,4078456,4078458,**4078538**,4078552,4078634,407867
4,4079056,4079086,4079155,**4079320**,4079356,4079383,4079387,4079600,4079623,4079
648,4079718,**4079810**,4080204,8300096,8300273,8502184,8503585,8503800,8504110,85
04846,8505150,8505152,8505836,**8506175**,8506175,8506762,8506951,**10200083**,1020195
7,10201990,**1350001**,6750722,1351563,1351727,900107,3300130,3300164,3312771,370
0276,4029815,4031109,4031477,4032677,4036509,**4040527**,4038012,4038214,4038394,4
039268,4041776,4043041,4043492,**4044543**,4045056,4045293,4045841,4046043,4046835
,4046837,**4046904**,4047140,4047454,**4048177**,4048347,4048980,4049063,4050281,**40507**
14,4050750,4051887,**4053233**,4054591,4056126,4056682,4058016,**4059817**,4061155,406
1666,4061980,4062185,4062724,4063881,406468,**4064795**,4064904,4065787,4065959,4
066708,4067185,4068391,4068550,4068560,[406859],4068832,4069148,4069150,4069694
,4069772,4069829,4069838,4069841,[4069847],40704,4070123,4070138,4070327,40716
04,4071842,5071726,507281,507326,507348,407349,507353,507368,4073435,407
3758,4073959,507426,507481,407491,407501,407511,507513,507515,407516,507518,4076121,4
076542,**4076727**,4076931,4076999,4077200,4077219,4077221,4077298,4077748,4078175
,4078430,4078455,4078456,4078458,4078538,4078552,4078634,4078674,**4079056**,40790
86,4079155,4079320,**4079336**,4079383,**4079387**,4079600,4079623,4079648,4079718,407
9810,4080204,8300096,8300273,8502184,8503585,**8503800**,8504110,8504846,8505150,8
505152,**8505836**,8506251,8506255,8506762,8506951,10200083,10201957,10201990 4072
602,4072653,4072690,4072775,4073248,4073405,4073418,4073435,**4073758**,4073959,40
74576.4074683.4074801.4075121.4075966.4075976.4076096.4076121.4076542.4076727.