تمرین عملی چهارم

هدف: آشنایی با نفوذگری در برنامه‌های کاربردی وب

تمرین ۱. نفوذ به سایت‌های PHP با تزریق sql

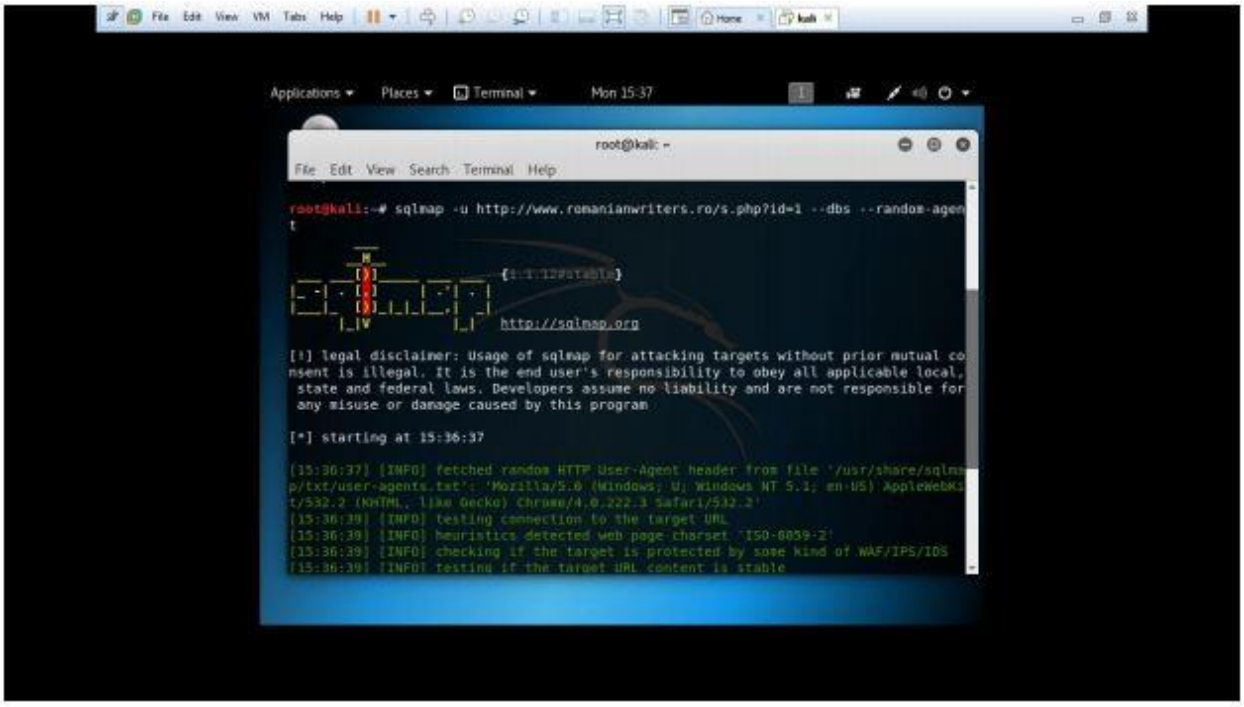
- در سیستم‌عامل کالی لینوکس، اقدام به شناسایی یک سایت PHP کنید.
- برای این کار دستور inurl:php?id=1 را در مرورگر کالی لینوکس وارد کنید. توضیحات مرتبط با گوگل دورک و روش عملکرد آن در کلاس توضیح داده شده است.
- بر روی یکی از این وب سایت‌ها کلیک کنید و آن را باز کنید.
- پس از باز شدن سایت مورد نظر علامت اپستروف (') را در انتهای urlوب سایت مربوطه وارد کنید.
- در این جا اگر پیامی همانند پیام زیر را مشاهده کردید، احتمالا این سایت آسیب‌پذیر است.

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

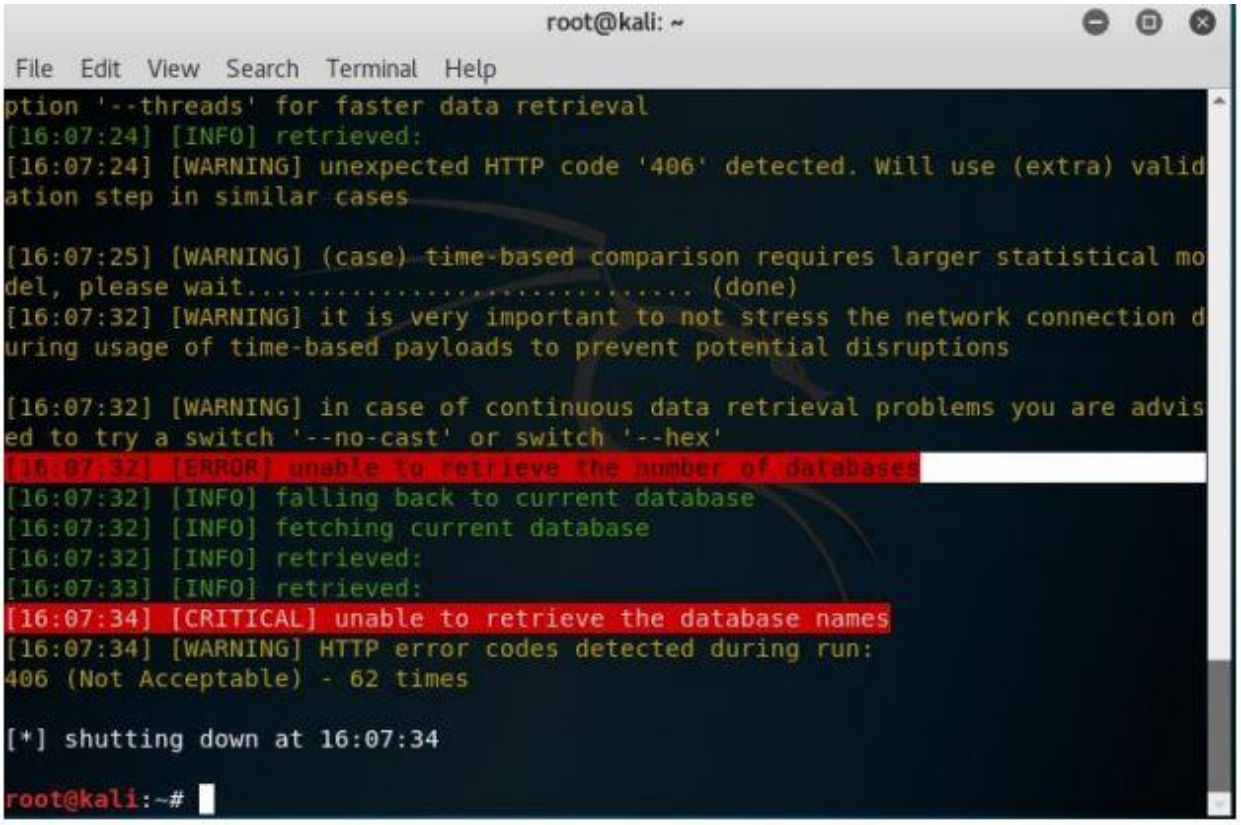
- پس از آن با باز کردن ترمینال kali linux دستور Sqlmap را در آن جا وارد کنید؛ با اجرای این دستور شما optionهای این برنامه را مشاهده میکنید.
- مراحل زیر را دنبال کنید:

sqlmap -u URL --dbs --random-agent

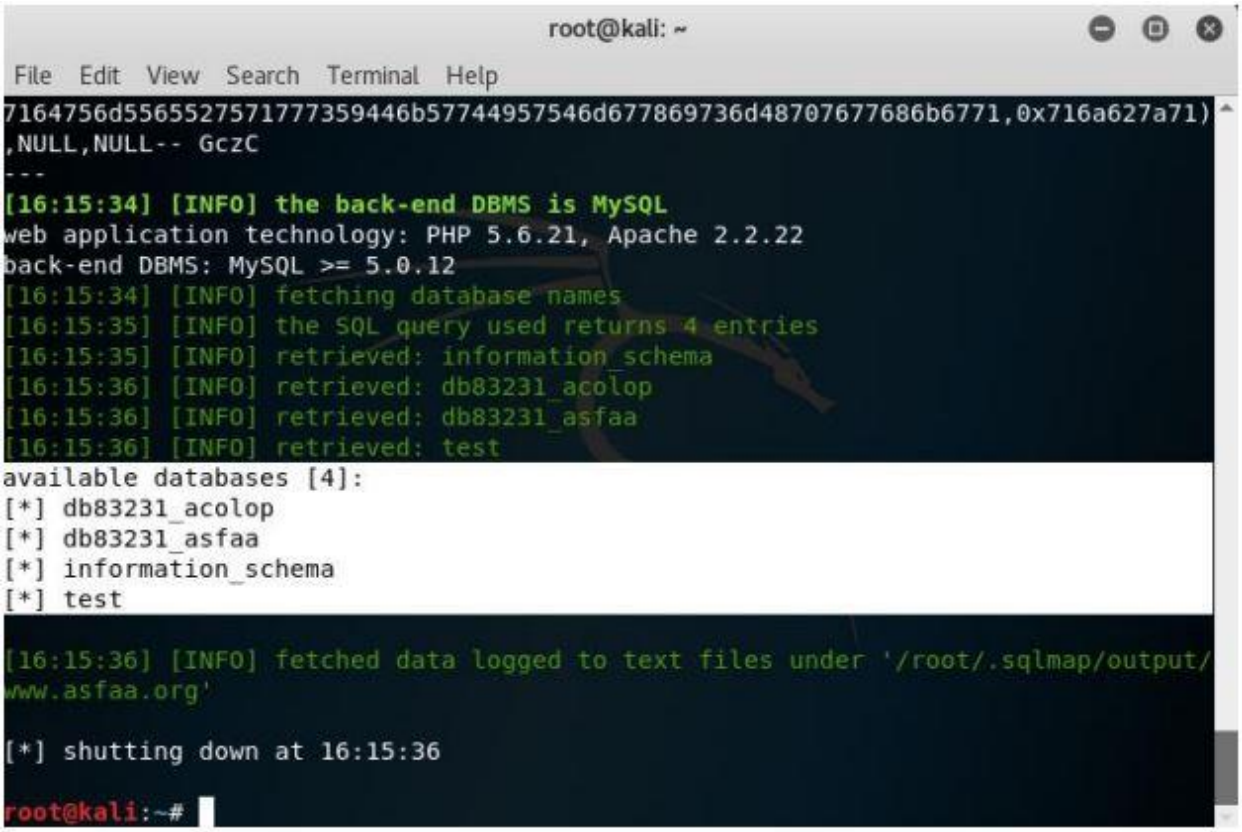
- در این دستور به جای url آدرس را کپی کنید،توجه داشته باشید که قبل از آن آپستروف را پاک کرده باشید .همچنین سوئیچ agent-randomبرای استفاده از پروکسی میباشد.



- مراحل را دنبال کنید؛در قسمتی از متون نمایش داده شده ،میتوانید این نکته را ببینید که به عنوان مثال این ابزار به شما میگوید این سایت آسیب پذیر است و میتوان به آنsql تزریق کرد،و یا سایر آسیب پذیری ها .در انتهای پردازش این دستور،در صورتی که مشاهده کردید نام پایگاه های داده ی این وب سرور به شما نمایش داده میشود؛میتوانید عملیات زیر را دنبال کنید.توجه فرمایید برخی از وب سرور ها در مقابل این حمله مقاوم هستند،مانند تصویر زیر:



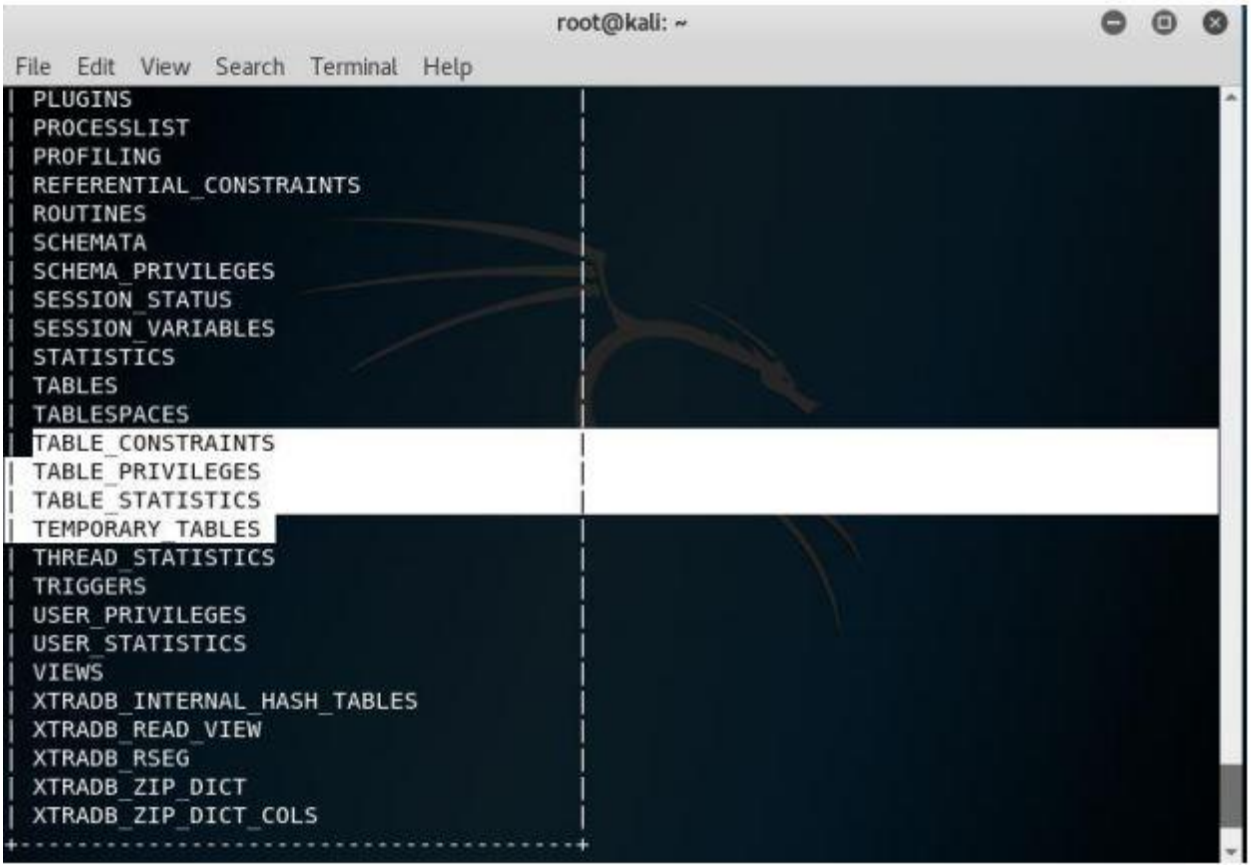
- در تصویر زیر،همانطور که مشاهده میکنید ،این ابزار توانسته است نام پایگاه داده این وب سرویس را بازگرداند.



- همانطور که مشاهده میکنید ،۴ دیتا بیس در تصویر فوق مشاهده میشود .دستور زیر را اجرا کنید :

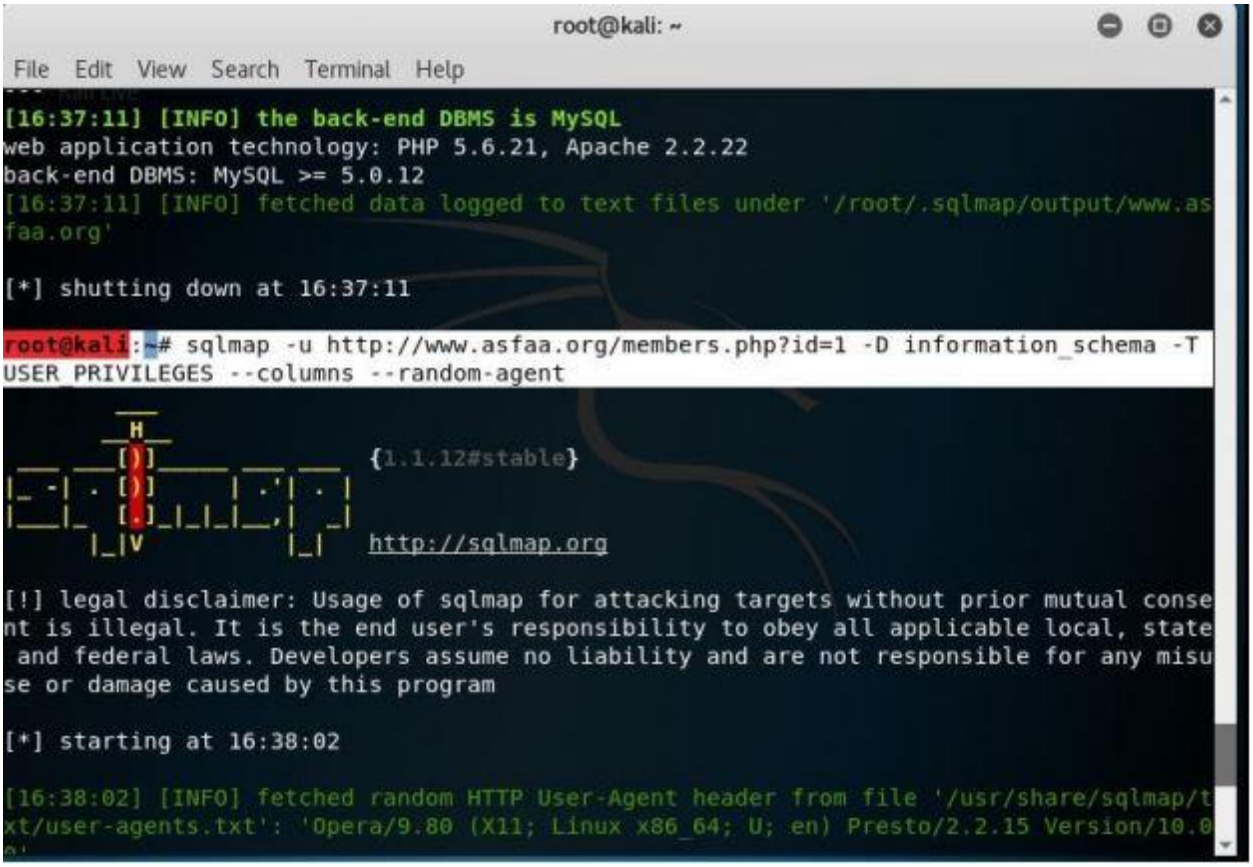
Sqlmap –u URL –D dbname –tables –random-agent

با اجرای دستور فوق جداول پایگاه داده‌ی مربوطه نمایش داده میشود:

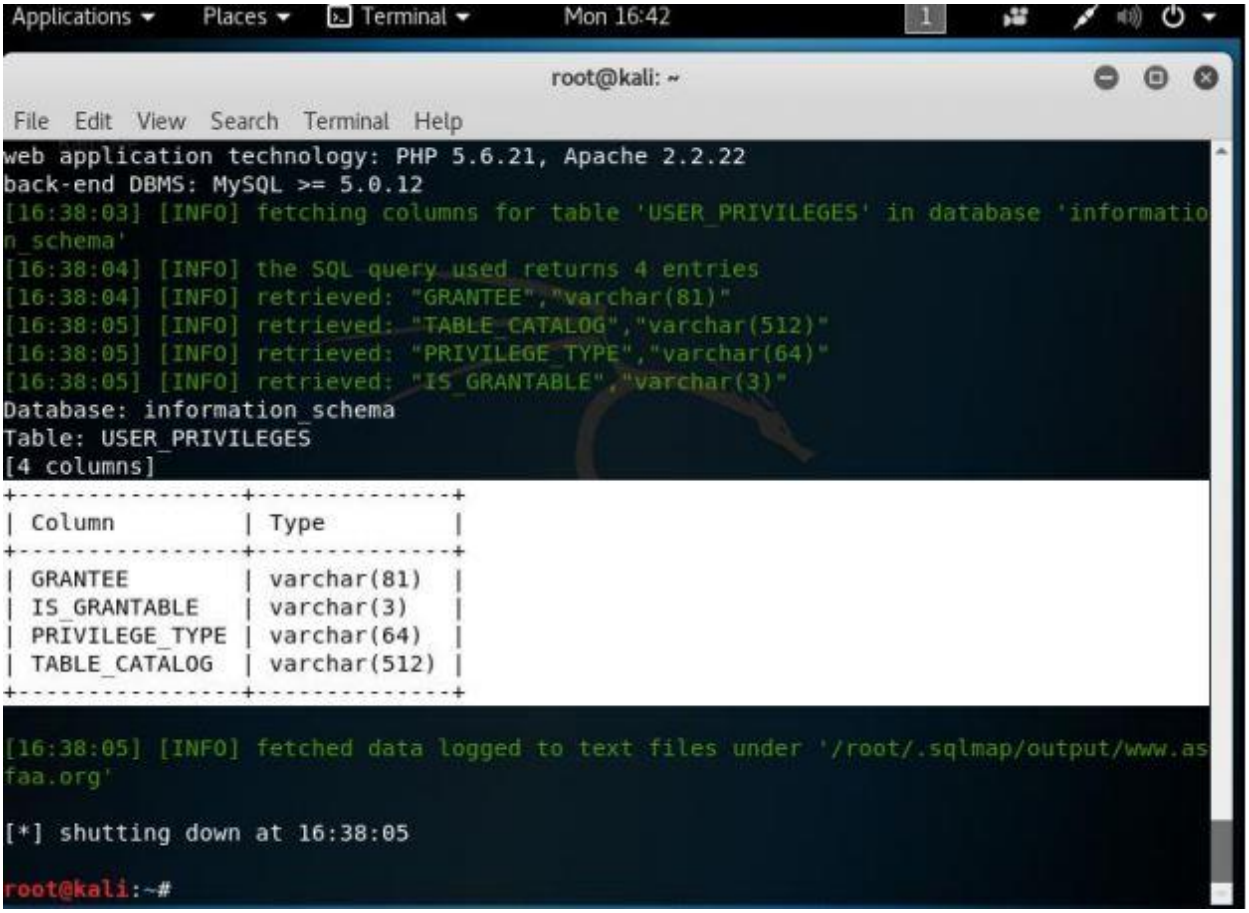


- همان طور که مشاهده میکنید، بنده توانستم با اجرای این دستور بر روی یکی از دیتابیس های وب سایت،جداول آن را مشاهده کنم، در مرحله بعد تلاش میکنیم تا یکی از این جداول را به صورت دقیق تر بررسی کنیم.در مرحله بعد تلاش میکنیم تا یکی از این جداول را به صورت دقیق تر بررسی کنیم. در اینجا لازم است بگویم، شما میتوانید با پیدا کردن جداول مربوط به username و password، دسترسی کامل به این وب سایت را اخذ نمایید.

Sqlmap –u URL –D DBNAME –T TABLENAME –columns—random-agent



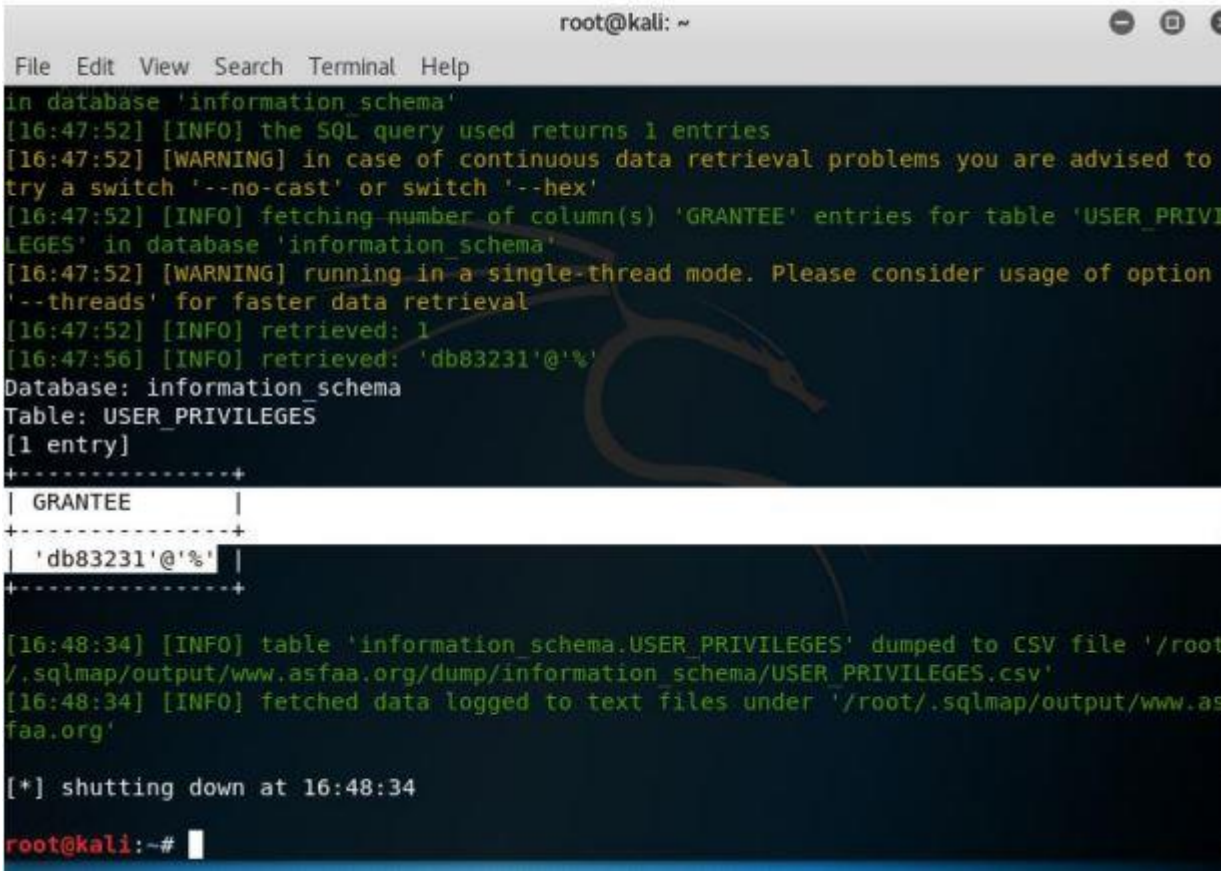
- در تصویر فوق وارد کردن کامند توضیح داده شده را مشاهده میکنید؛ در ادامه میتوانید ستون های این جدول را مشاهده کنید.



- در انتها اقدام به دریافت یکی از این ستون ها میکنیم. دستور زیر را اجرا کنید.

Sqlmap –u URL –D DBNAME –T TABLENAME –C COLUMNNAME –dump –random-agent

در ادامه بنده اقدام به اجرای این دستور برای ستون grantee کردم که خروجی آن مطابق تصویر زیر است.



- این تمرین را بر روی یک سایت "خارجی" دلخواه اجرا کنید و از مراحل کار عکس برداری کرده و در داکیومنت خود به طور کامل بیاورید.
- در صورتی که در جدول مربوط به اطلاعات نام کاربردی و رمز عبور؛ رمزعبور به صورت خروجی فایل درهمساز ذخیره شده باشد، چگونه میتوان به رمزعبور دست یافت؟

تمرین دوم. آشنایی با آسیب‌پذیری XSS

حملات Cross-site Scripting (XSS) یکی از جدی‌ترین آسیب پذیری‌های برنامه‌های کاربردی تحت وب است. به جرات میتوان گفت امروزه هیچ برنامه کاربری تحت وب وجود ندارد که در مقابل این آسیب‌پذیری کاملا ایمن باشد. در واقع آشنایی شما با این نوع حمله و صرف زمان مقتضی برای کشف این آسیب پذیری در یک برنامه‌ی کاربردی تحت وب خاص، میتواند منجر به دسترسی شما به هر هدف شود.

حملات XSS به چند دسته تقسیم میشوند، مشهورترین این حملات در دوسته‌ی ذخیره شده(stored) و بازتابی (reflected) هستند. بهترین منبع برای یادگیری انواع متدولوژی‌های این حملات مستندات گروه پژوهشی OWASP میباشد.

در این قسمت ابتدا تحقیقی در خصوص نحوه انجام این حملات انجام دهید؛ سپس ابزار DVWA را بر روی سیستم خود نصب کنید. این ابزار یک وب اپلیکیشن آسیب پذیر است که شما میتوانید حملات مختلف را توسط آن شبیه‌سازی کنید. در این ابزار دو روش مطرح شده برای حملات XSS شامل بازتابی و ذخیره‌شده شده شبیه‌سازی کنید.

گزارش کاملی از حملات XSS و نحوه عملکردآن، روش‌های کشف این آسیب‌پذیری در برنامه‌های مختلف و همچنین گزارش انجام این حملات در برنامه معرفی شده را در گزارش خود بیاورید.