Assessment 3: Practical Lab

INSTRUCTIONS

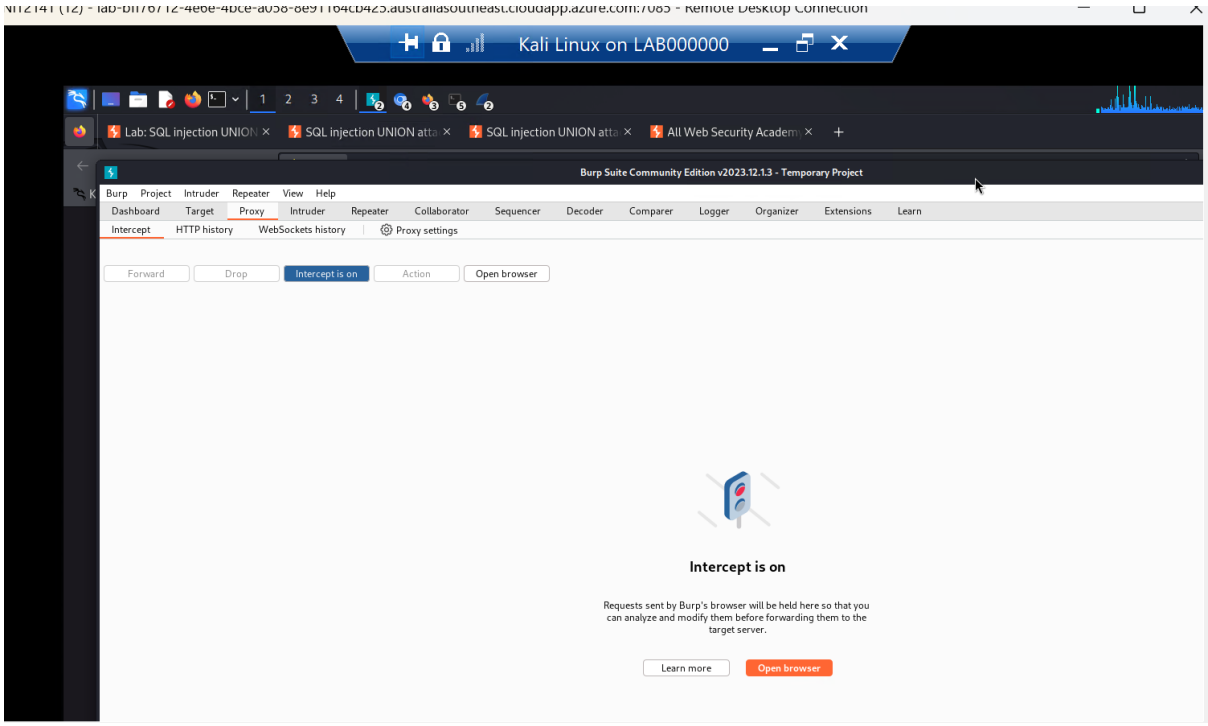
- You will have 120 minutes to complete this Practical laboratory
- At the end of the practical lab, please submit your screenshots to the dropbox provided.
- Please sign up to this website (it is a free sign-up process): Create your account - PortSwigger

1. SQL injection attack (10 Marks)

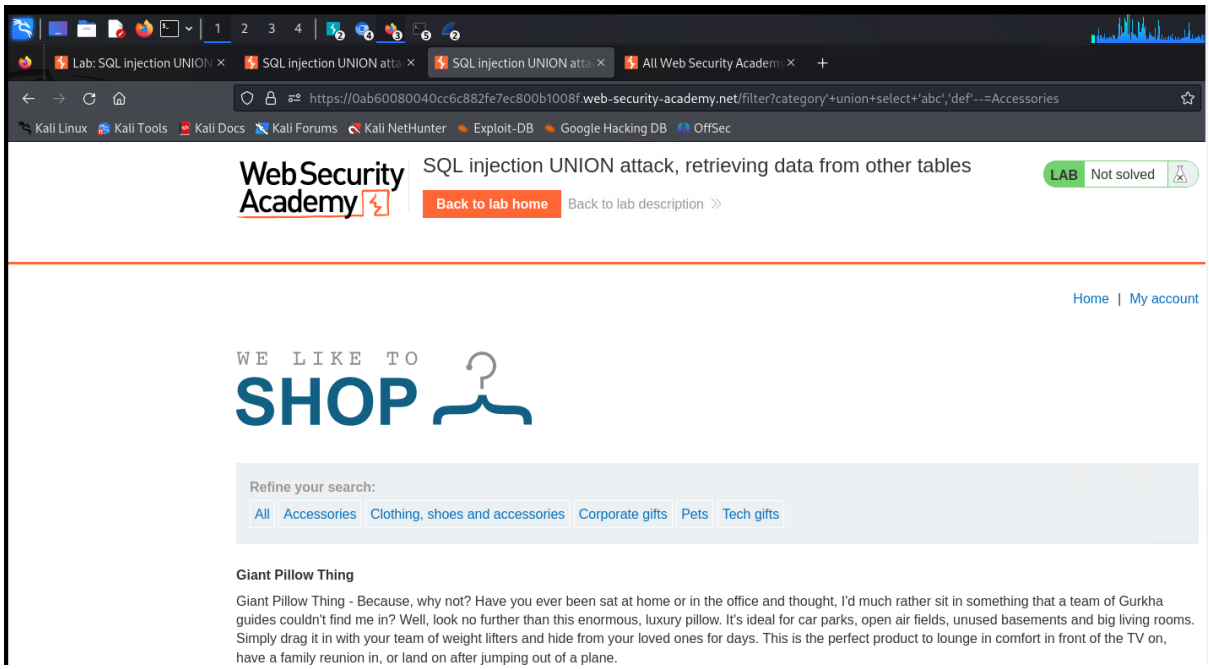
Complete this lab Lab: SQL injection UNION attack, retrieving data from other tables | Web Security Academy (portswigger.net) (10 Marks)

You need to figure out the website admin username and password and write in your report. Moreover, add screen shots for the steps you followed to solve this lab.

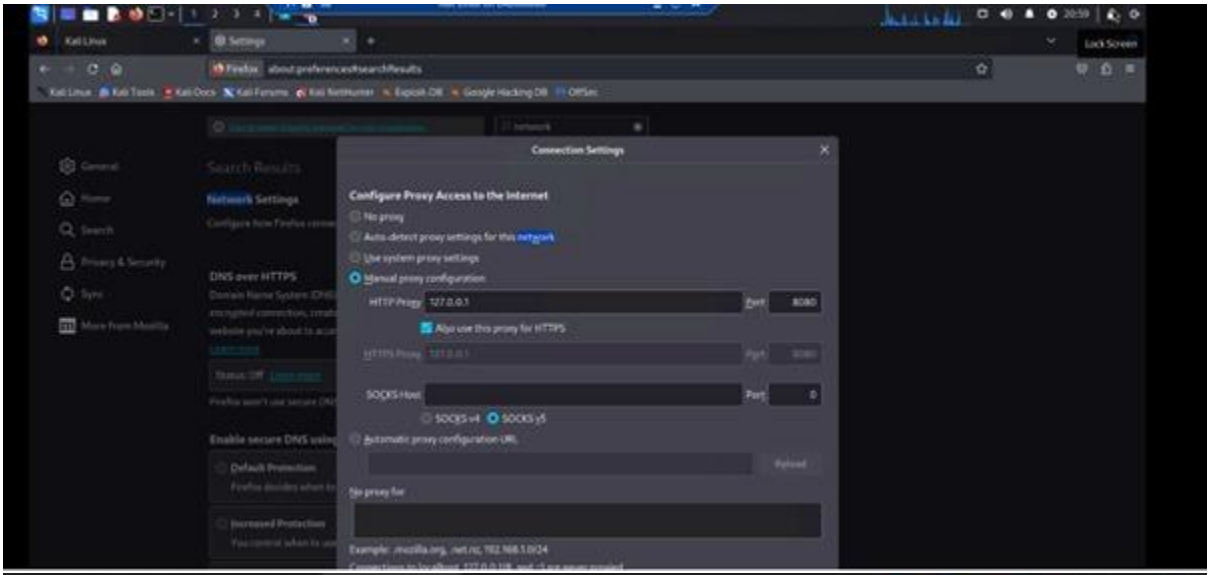
In this lab, I performed a SQL injection UNION-based attack to retrieve the administrator's username and password hash from a different table in the database. By identifying a vulnerable input field, determining the number of columns, and using the UNION SELECT statement, I was able to extract hidden data from the backend. This exercise demonstrated how attackers can use SQL injection to access sensitive information stored in other database tables, highlighting the importance of input validation and secure coding practices.

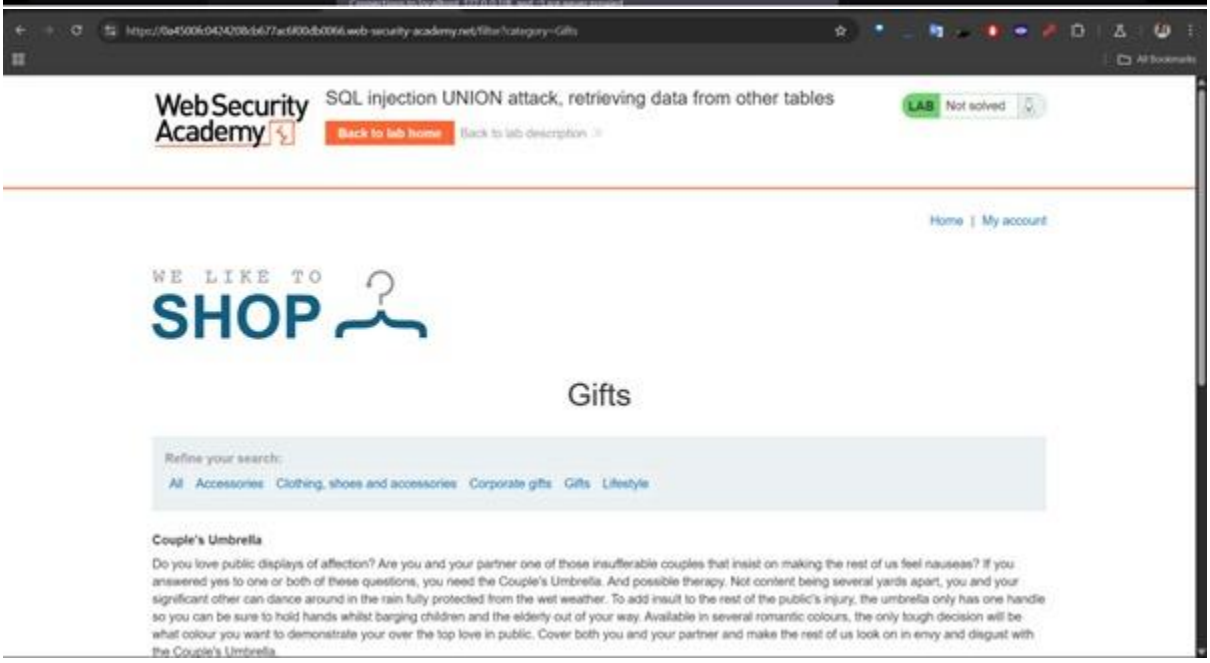


1. opening burpsuit



Union+select+abc+def


Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy 127.0.0.1
Port 8080
Also use this proxy for HTTPS
SOCKS Host
Port 0
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
No proxy for


Web Security Academy
SQL injection UNION attack, retrieving data from other tables
Back to lab home
Back to lab description
LAB Not solved
Home | My account
WE LIKE TO SHOP
Gifts
Refine your search:
All Accessories Clothing, shoes and accessories Corporate gifts Gifts Lifestyle
Couple's Umbrella
Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy. Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public. Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple's Umbrella.

Web Security Academy

SQL injection UNION attack, retrieving data from other tables

Back to lab home | Back to lab description

LAB Not solved

Home | My account

WE LIKE TO SHOP

Gifts' UNION SELECT 'abc', NULL--

Refine your search:

All | Accessories | Clothing, shoes and accessories | Corporate gifts | Gifts | Lifestyle

Conversation Controlling Lemon

Are you one of those people who opens their mouth only to discover you say the wrong thing? If this is you then the Conversation Controlling Lemon will change the way you socialize forever! When you feel a comment coming on pop it in your mouth and wait for the acidity to kick in. Not only does the lemon render you speechless by being inserted into your mouth, but the juice will also keep you silent for at least another five minutes. This action will ensure the thought will have passed and you no longer feel the need to interject. The lemon can be cut into pieces - make sure they are large enough to fill your mouth - on average you will have four single uses for the price shown, that's nothing an evening. If you're a real chatterbox you will save that money in drink and snacks, as you will be

WE LIKE TO SHOP

Gifts' UNION SELECT table_name, NULL FROM information_schema.tables--

Refine your search:

All | Accessories | Clothing, shoes and accessories | Corporate gifts | Gifts | Lifestyle

pg_partitioned_table
pg_available_extension_versions
pg_shdescription
user_defined_types
udt_privileges
sql_packages
pg_event_trigger
pg_amop
schemata
routines

2. Performing brute force password guess (10 Marks)

Follow the instructions in this lab and add screenshots for your solution.

[Lab: Username enumeration via different responses | Web Security Academy (portswigger.net)]

3. Performing Passive Reconnaissance (10 Marks)

The best way to learn passive information gathering is to use the tools. In this exercise, you perform reconnaissance on several organizations. Acquire only the information requested.

Step 1. Review Table 1 to determine the target of your passive information gathering.

Table 1 Passive Information Gathering

Domain Name	IP Address	Location	Contact Person	Address and Phone Number
Tryhackme.com	172.67.27.10	United States	abuse@namecheap.com	+1.6613102107
example.com	23.192.228.80	United states	Not provided	Not provided
www.hackthebox.eu	104.18.9.132	United kingdom	Hackthebox.eu	+30-2106475600

Step 2. Start by resolving the IP address. This can be done by pinging the site.

Step 3. Next, use a tool such as https://www.whois.net or any of the other tools mentioned throughout the lecture. Some of these include

http://www.betterwhois.com (http://www.betterwhois.com)

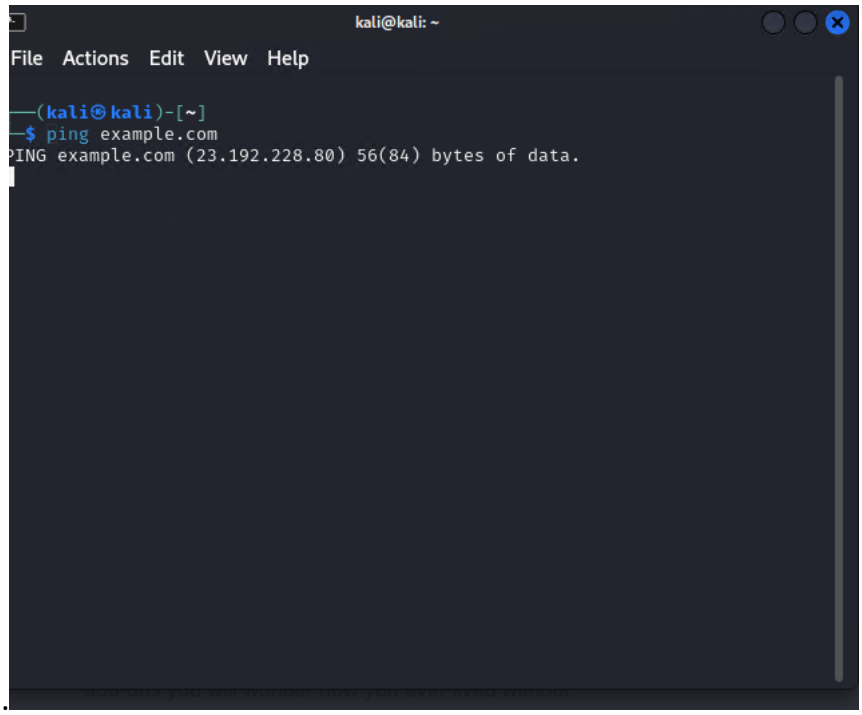
www.allwhois.com (http://www.allwhois.com)

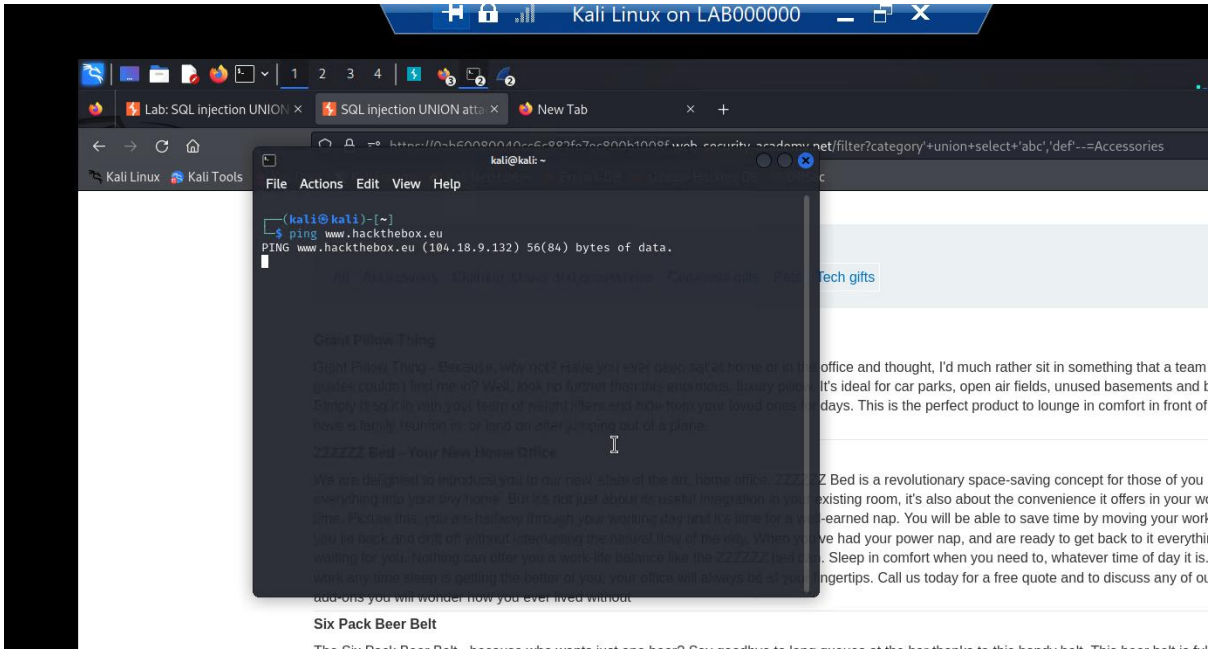
http://geektools.com (http://geektools.com)

www.centralops.net (http://www.centralops.net)

www.dnsstuff.com (http://www.dnsstuff.com)

Step 4. To verify the location of the organization, perform a traceroute or a ping with the -r option.





Step 5. Use the ARIN, RIPE, and IANA to fill in any information you have yet to acquire.

tryhackme.com

Updated 21 minutes ago

Domain Information

Domain:	tryhackme.com
Registered On:	2018-07-05
Expires On:	2027-07-05
Updated On:	2021-05-01
Status:	client transfer prohibited
Name Servers:	kip.ns.cloudflare.com uma.ns.cloudflare.com

Registrar Information

Registrar:	NameCheap, Inc.
IANA ID:	1068
Abuse Email:	abuse@namecheap.com
Abuse Phone:	+1.6613102107

Note that all these labs include the general solution steps you just need to follow them and install any tools you need to follow the steps to solve these challenges.