What is SQL?

- Most websites use a database to store data
- Most data stored in it (usernames, passwords, products, news articles, etc.)
- Web application reads, updates, and inserts data in the database
- Interaction with database usually done with SQL

Show a Database

- Metasploitable
- cmd: mysql -u root -h <ip address>

mysql commands

- show databases
    - shows all databases that exist on the target server
- information_schema
    - gets installed by default
    - contains information about all of the other databases
- all other databases are for metasploitable
- each web application has a database that holds the info used by that web app
- use owasp10
- show tables
    - shows the tables (data types) in the database
- shopping websites actually would have credit card information stored in the database
- select * from accounts
    - each row is a different
-

Takeaways

- usually, you would not have this access. only the admin would have this kind of access
- the goal of exploitatation is to gain access to this database so you can access information stored there, read from, alter, or write to it
- Why SQL is dangerous?
    - They are everywhere. Easy to make a mistake, even on a big site, that gives access
    - Give access to the database
    - No need to gain further access. Do not need to open a reverse shell. If you can find a SQL injection vulnerability, you can already see everything

    - can be used to read local files outside of www root (other websites hosted on the same server)
    - can be used to upload files

Exploitation of SQL

- try to break the page
- using ‘and’, ‘order by’, or ‘ (quote characters)
- test text boxes and url parameters of the form
    - http://target.com/page.php?something=something

Mutillidae Login Hacking

- sign up for an account
- login with the account to show that it works
- “Name” and “password” text boxes
- put a single quote into the password
    - error displayed (database)
    - normally the error won’t be as informative as this
    - sometimes the page just doesn’t look as it should
    - if it’s a news page, maybe there’s an article missing, etc.
    - point out the statement that the system is trying to run
        - SELECT * FROM accounts WHERE username=’zaid’ AND password=’’’
    - Select * from accounts where username=’zaid’ and password=’$PASSWORD’
    - by inserting our own quotation mark, it closes the password field
- SELECT * FROM accounts WHERE username=’zaid’ AND password=’123456’ and 1=1 #‘
    - system will complain about the open quote
        - therefore, we must add a comment, the hash (#) sign
    - able to login
- try to add a false statement
    - SELECT * FROM accounts WHERE username=’zaid’ AND password=’123456’ and 1=2 #‘
- SELECT * FROM accounts WHERE username=’zaid’ AND password=’123456’ and 1=1 <your code here> #‘
- Login to admin without knowing the password
    - select * from accounts where username = ‘admin’’ and password=’aaa’ or 1=1 #’
    - if you have an OR (logical or) everything is true
    - notice the changing search bar
- Select * from accounts where username= ‘admin’ #’ <everything here is not executed>

Examples/Exercises

- https://www.hacksplaining.com/exercises/sql-injection#