NAME-**ANMOL KANT**

OWASP TOP 5 APPLICATION SECURITY RISKS 2023

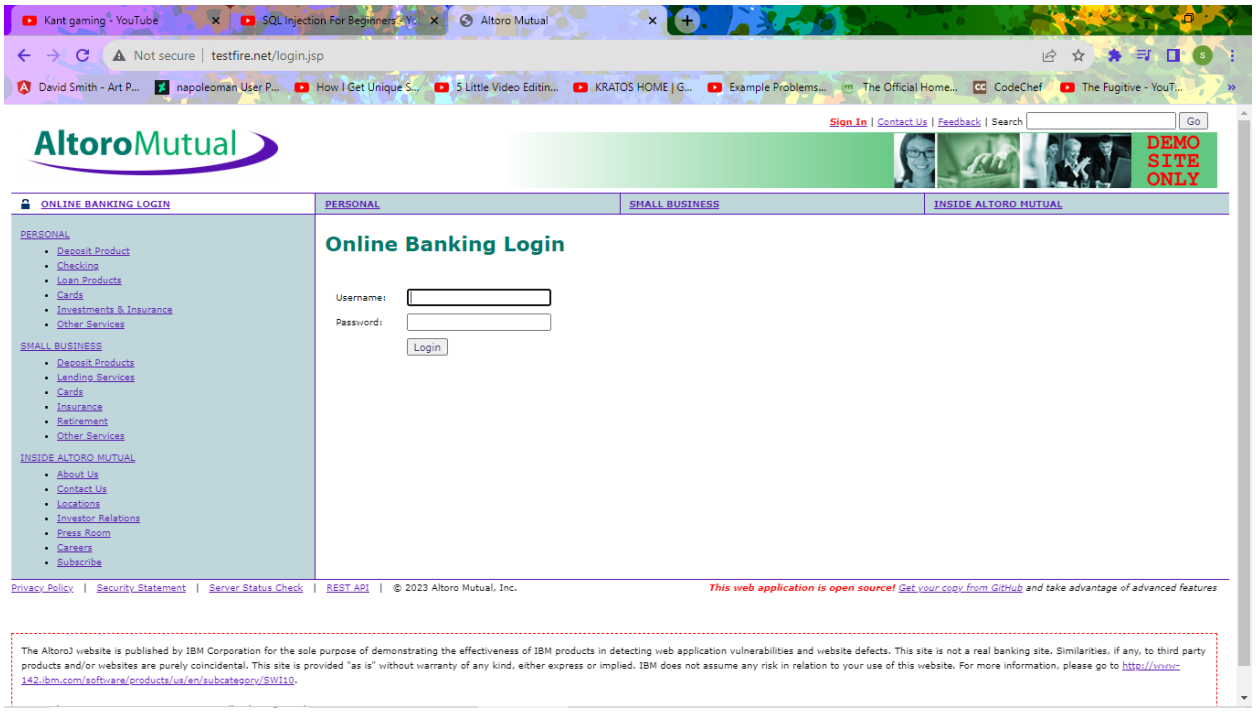
WE TALK ABOUT THE TOP 5 WEB SECURITY THREATS OR WE CAN SAY VULNERABILITIES OF WEB APPLICATIONS.SO HACKERS FIND A WAY TO HACK THE WEB APPLICATION AND ACCESS THEIR DATABASE.SO HERE WE DISCUSS SOME WAYS TO HACK A WEB APPLICATION.

1)Injection

WE TAKE A WEBSITE WHICH ARE VERY VULNERABLE AND TRY TO ACCESS THRIE LOGIN PAGES THROUGH SQL INJECTOR. WE ALSO TRY AS A USER OR ADMIN.BASICALLY, IT INJECTS THE SQL QURIES IN THE WEB APPLICATION TO ACCESS THAT WEB APPLICATION SO THAT WE CAN MAKE CHANGES IN THE DATABASE.

HERE I PERFORM THE INJECTION ATTACK I SHOW SCREENSHOTS OF LOGIN PAGES BEFORE INJECTION AND AFTER INJECTION.

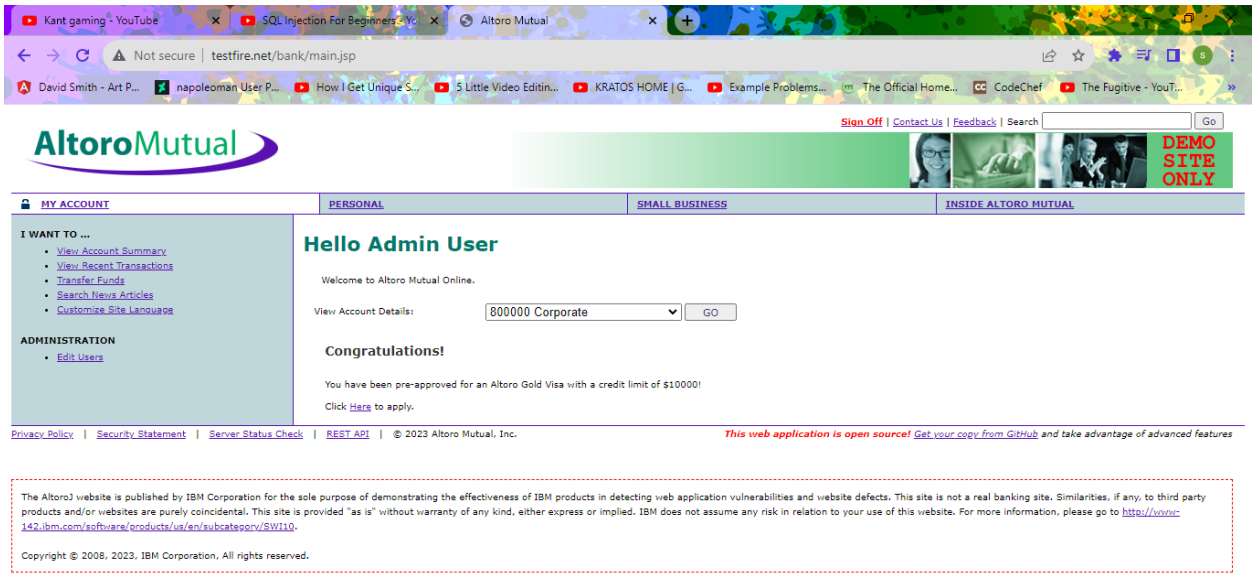
BEFORE INJECTION…….



HERE WE SEE AN ALTORO MANUAL WEBSITE WHICH IS A VERY VULNERABLE OR WEAKER WEBSITE SO WE TRY TO BYPASS THE LOGIN USING INJECTION.

SO WE STUDIED IN THE DATABASE SYSTEM IF WE ANT TO CHANGE SOMETHING WE USE “OR” OPERATOR AND USE THIS “select * FROM USERS WHERE NAME='TOM' AND PASSWORD="1234".SO HERE WE CAN SEE DATABASE WHICH WE STUDIED IN COLLEGE TIME. NOW WE USE “OR” INSTEAD OF AND AND MANIPULATE LIKE THIS “' or 1=1–” AND USE ANY PASSWORD BECAUSE AFTER USING O FDASH(-) WE DONT CARE WHAT WE WRITE IN PASSWORD SECTION JUST CONFIRM WE WRITE SOMETHING AFTER THAT WE ENTER IN THE WEB APPLICATION AS A ADMIN AND ACCESS THE DATABSE.

HERE IS ANOTHER SCREENSHOT AFTER WE USED INJECTION ON THIS APPLICATION.



SO THIS IS ALL ABOUT INJECTION BUT IF YOU WANT TO KNOW MORE ABOUT SQL INJECTION THEN YOU GO TO KALI LINUX OPEN TERMINAL TYPE cd Injections/ls and headSQL.txt.After that you get more SQL injectors you can also use them for your purpose.

2)Security Misconfiguration

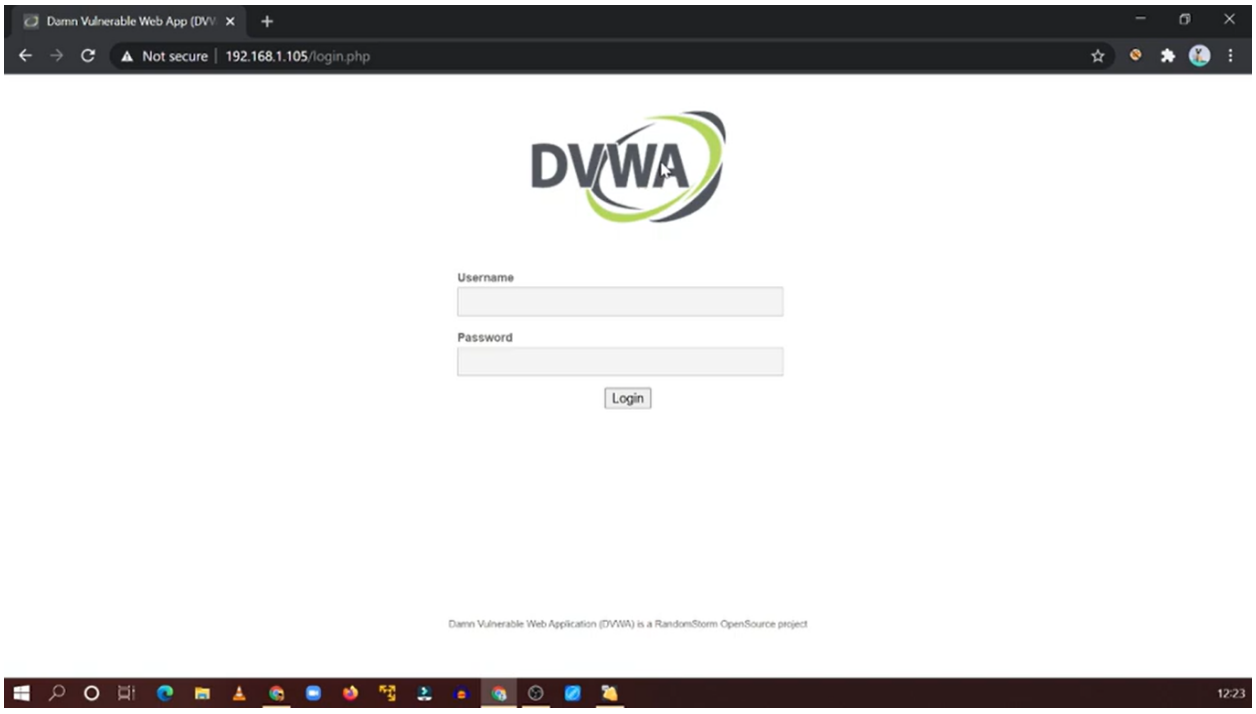
SO NOW WE TALK ABOUT SECURITY MISCONFIGURATION IN THIS VULNERABILITY SUPPOSE WE USE A DVWA THAT IS BASICALLY A TOOL IN KALI LINUX TO PRACTICE THE MOST COMMON WEB VULNERABILITIES.

WE CHECK FIRST CASE,

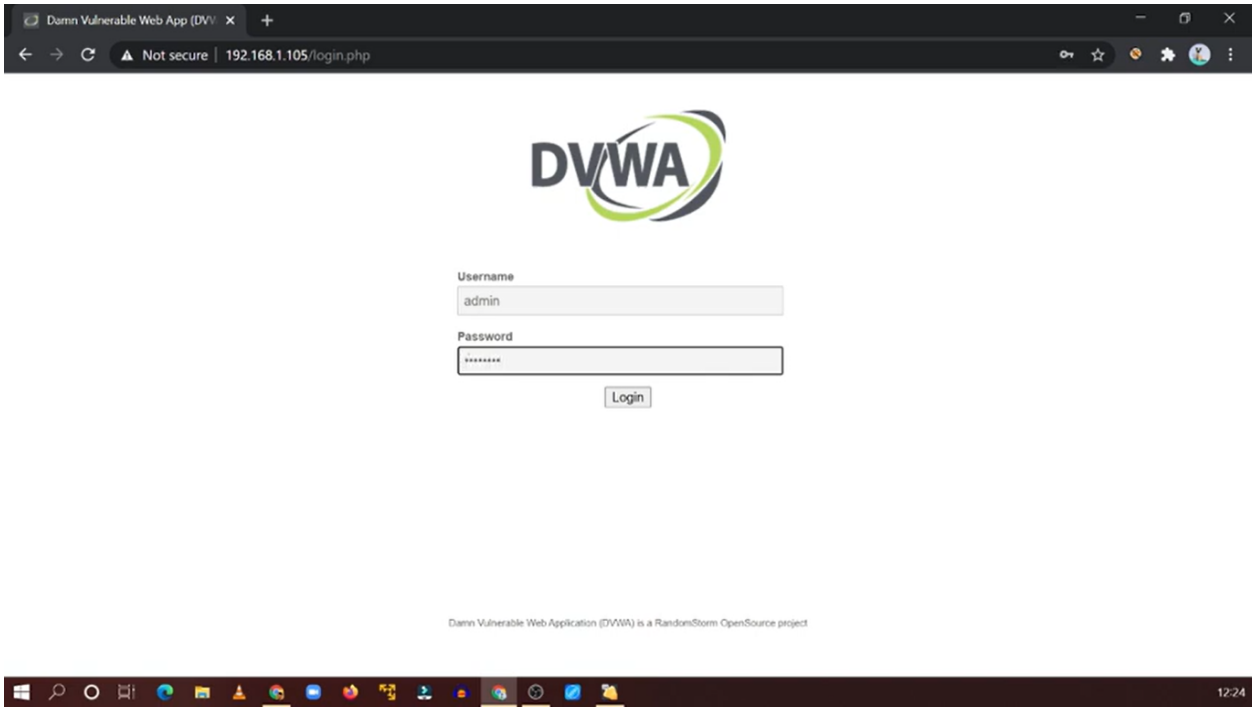
THE FIRST VULNERABILITY WE SAW WAS WHEN WE WENT TO THE LOGIN PAGE OF ANY WEB APPLICATION, FOR EXAMPLE, DVWA WE TRIED TO LOG IN USING A USERNAME AND PASSWORD SO JUST WE TRIED THE USERNAME AS ADMIN AND PASSWORD AS PASSWORD AND IT WORKED.SO THIS IS THE FIRST SECURITY VULENARBILTES WE SEE IF SOMEONE DOES NOT KNOW THE PASSWORD THEN HE/SHE MIGHT ALSO TRY BRUTE FROCE'S METHOD TO CRACK THE PASSWORD AND USERNAME SO THIS IS DEFINITELY A MISCONFIGURATION OF A WEB APPLICATION IF ANYONE VISITS THIS APPLICATION. THIS IS THE FIRST SECURITY MISCONFIGURATION.

WE ALSO SHOW SCREENSHOTS SO THAT IT MIGHT BE EASY FOR YOU TO UNDERSTAND.

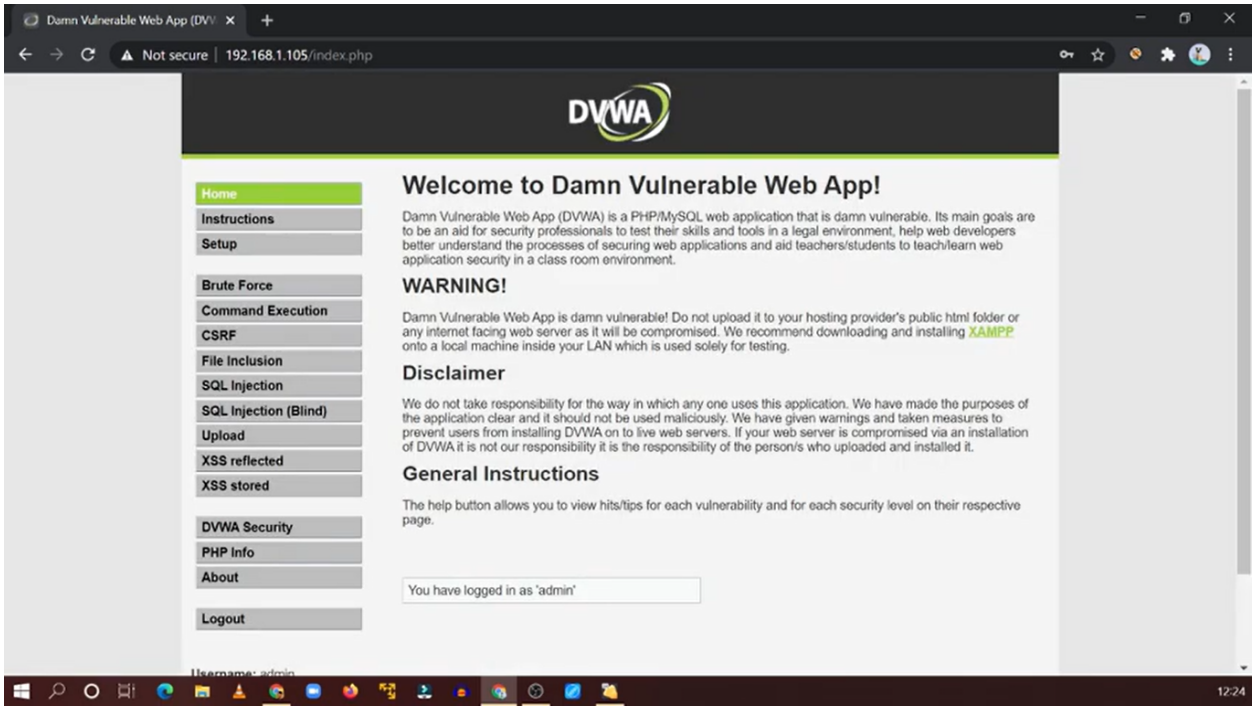
1)WE GO TO LOGIN PAGE OF A WEB APPLICATION.



2)WE TRY BRUTE FORCE OR RANDOM TYPE ADMIN AND PASSWORD INSTEAD OF USERNAME AND PASSWORD.



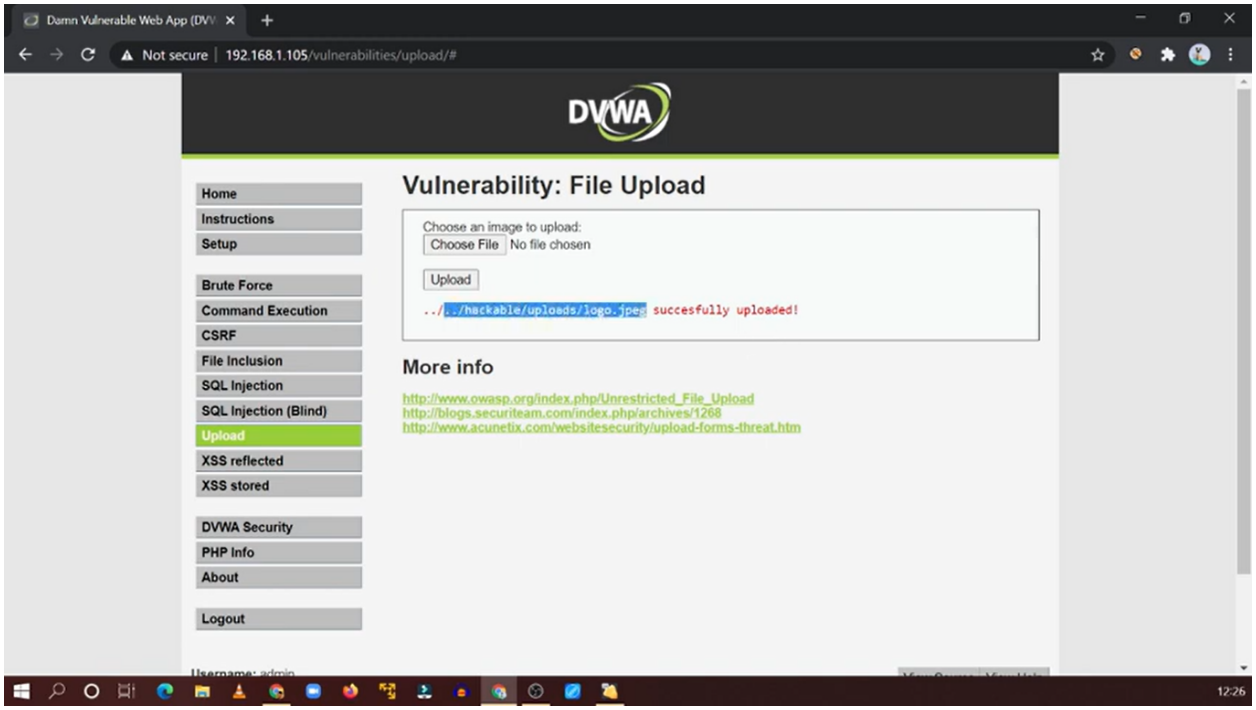
3)WE FINLAY LOGIN INTO A WEB APPLICATION WHICH IS A MISCONFIGURATION OF SECURITY BECAUSE IF ANYONE GOES TO THAT WEBSITE IT MIGHT BE EASIER TO CRACK THE PASSWORD AND USER NAME.

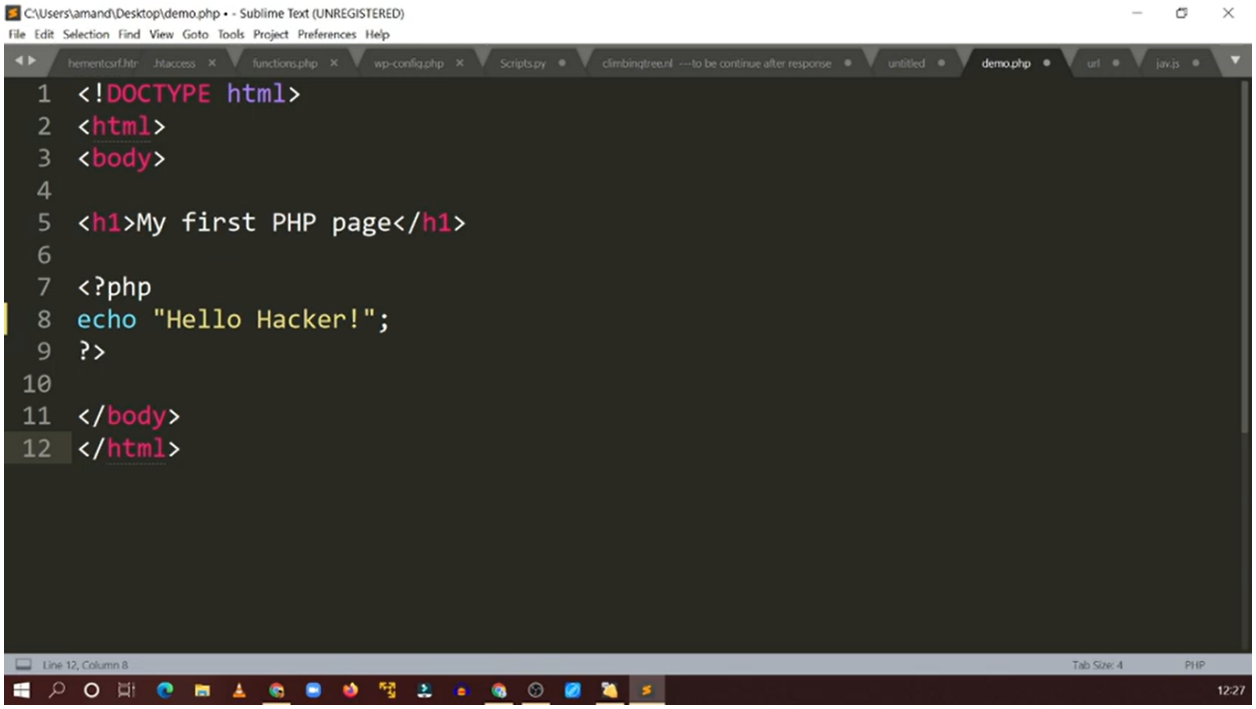


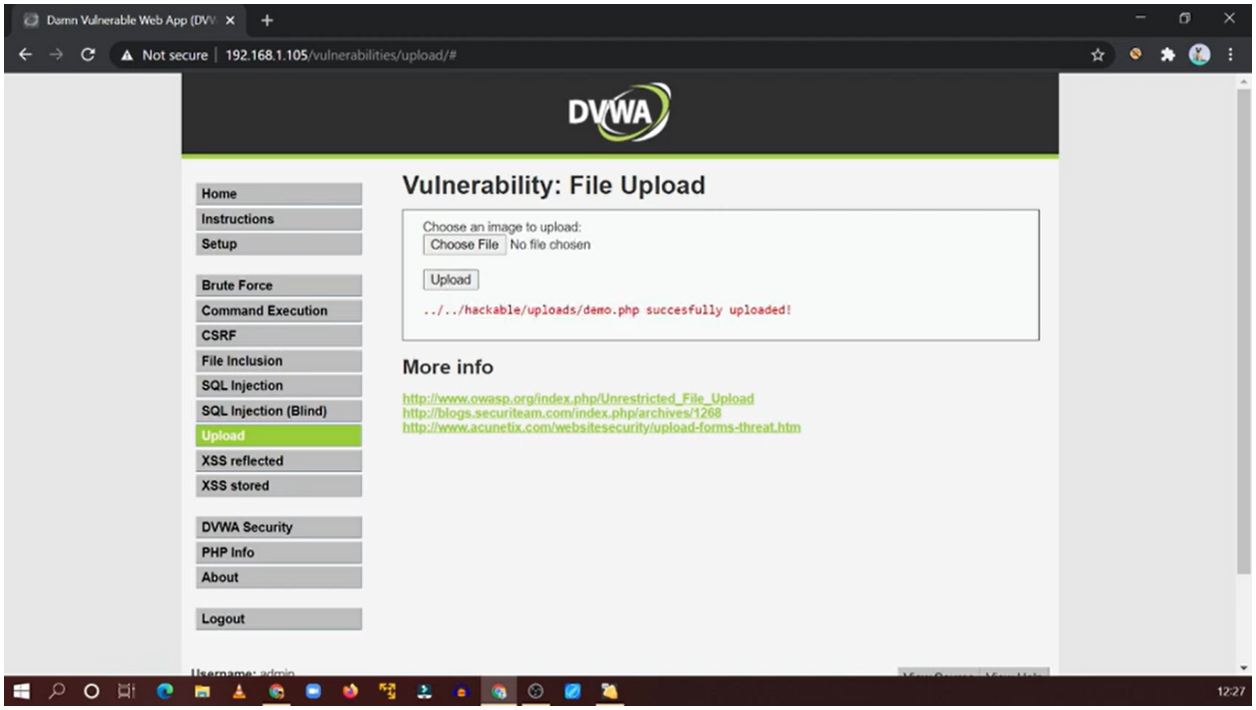
2)SECOND CASE OF MISCONFIGURATION,

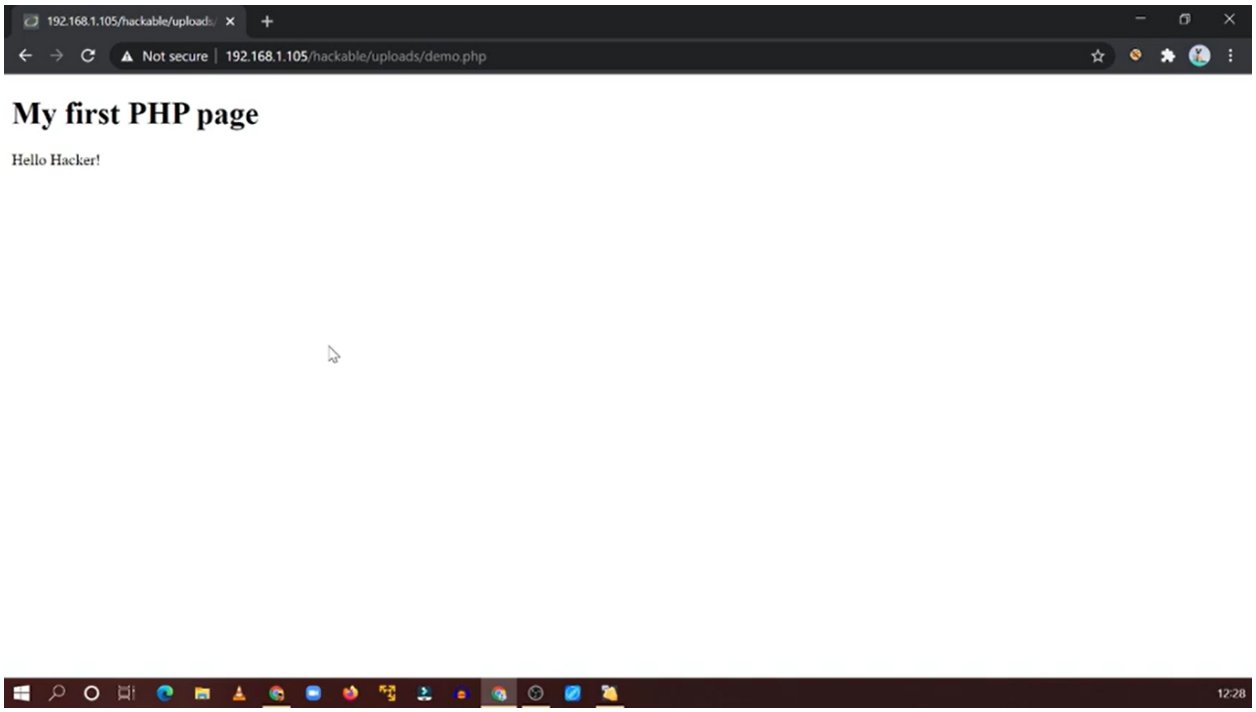
THE SECOND THING WE TALK ABOUT IS FILE UPLOAD WEB SECURITY THREAT. SUPPOSE WE UPLOAD SOME FILE LIKE AN IMAGE AND WE TRY TO COPY THE LINK OF THE UPLOADED FILE AND PASTE IT INTO THE SEARCH BAR WE SAW THE IMAGE OF WILL COME THERE IS NO BASELINE OR MINIMAL SECURITY SO THAT ANYONE CAN HACK THAT EASILY WHEN A HACKER UPLOAD ANY THING LIKE KEYLOGGER FILE. HACKERS CAN ALSO SEND SHELL SCRIPT FILES AND WHEN WE OPEN THAT FILE WITHOUT ANY SECURITY OUR SYSTEM IS HACKED AND THEN ENTERED IN OUR SERVERS.SO THIS IS A SECURITY MISCONFIGURATION.

WE ALSO SHOW THEM WITH SCREENSHOTS FOR BETTER UNDERSTANDING,


Damn Vulnerable Web App (DV
Not secure | 192.168.1.105/vulnerabilities/upload/#
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: File Upload
Choose an image to upload:
Choose File No file chosen
Upload
../hackable/uploads/logo.jpeg succesfully uploaded!
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm
12:26


C:\Users\amand\Desktop\demo.php • - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
demo.php
1 <!DOCTYPE html>
2 <html>
3 <body>
4
5 <h1>My first PHP page</h1>
6
7 <?php
8 echo "Hello Hacker!";
9 ?>
10
11 </body>
12 </html>
Line 12, Column 8
Tab Size: 4
PHP
12:27


Damn Vulnerable Web App (DVW
Not secure | 192.168.1.105/vulnerabilities/upload/#
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: File Upload
Choose an image to upload:
Choose File No file chosen
Upload
../../hackable/uploads/demo.php succesfully uploaded!
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm
12:27


192.168.1.105/hackable/uploads/
Not secure | 192.168.1.105/hackable/uploads/demo.php
My first PHP page
Hello Hacker!
12:28

3) **INSECURE DESIGN**

IT IS BASICALLY A VULNERABILITY IT IS A BROAD CATEGORY RELATED TO DESIGN AND ARCHITECTURAL FLAWS IN WEB APPLICATIONS THAT ARE EXPLOITED BY HACKERS. SUPPOSE A WEB DEVELOPER BUILDS A WEB APPLICATION OR SOFTWARE BUT HE/SHE DOES NOT MUCH FOCUS ON DESIGN OR WE CAN SAY AN ARCHITECTURAL VIEW THAT CAN CREATE A VULNERABILITY IN THE APPLICATION THAT IS AN INSECURE DESIGN. MANY TIMES WE SEE PEOPLE FIND BUGS ON MANY WEB APPLICATIONS AND COMPANIES LIKE GOOGLE REWARD WHOEVER FINDS THAT BUG. HOW DOES A BUG HAPPEN BECAUSE OF INSECURE DESIGN?

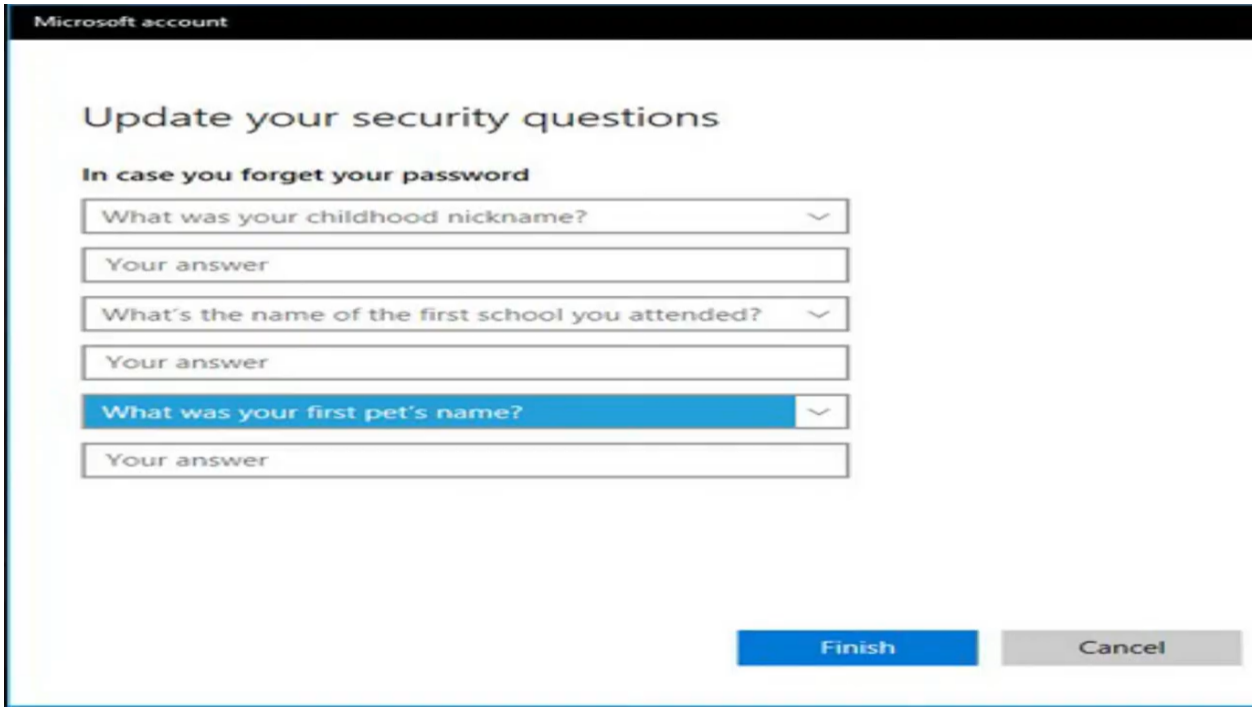
SO NOW WE SEE SOME BUGS THAT HAPPEN BECAUSE OF INSECURE DESIGN OR PEOPLE FIND THOSE BUGS AND REPORT TO WEB APPLICATION ADMIN.

1)OTP BYPASS
2)BRUTE FORCE ATTACK
3)SUPPOSE FOR RESETTING PASSWORD THEY USE A SECURITY QUESTION THEN THIS IS ALSO A VULNERABILITY.
4)NO PROPER HANDLING OF ERRORS.
5)HE ALSO DID NOT INCLUDE A FIREWALL TO PREVENT THE WANTED ATTACK.
6)ACCOUNT TAKEOVER.

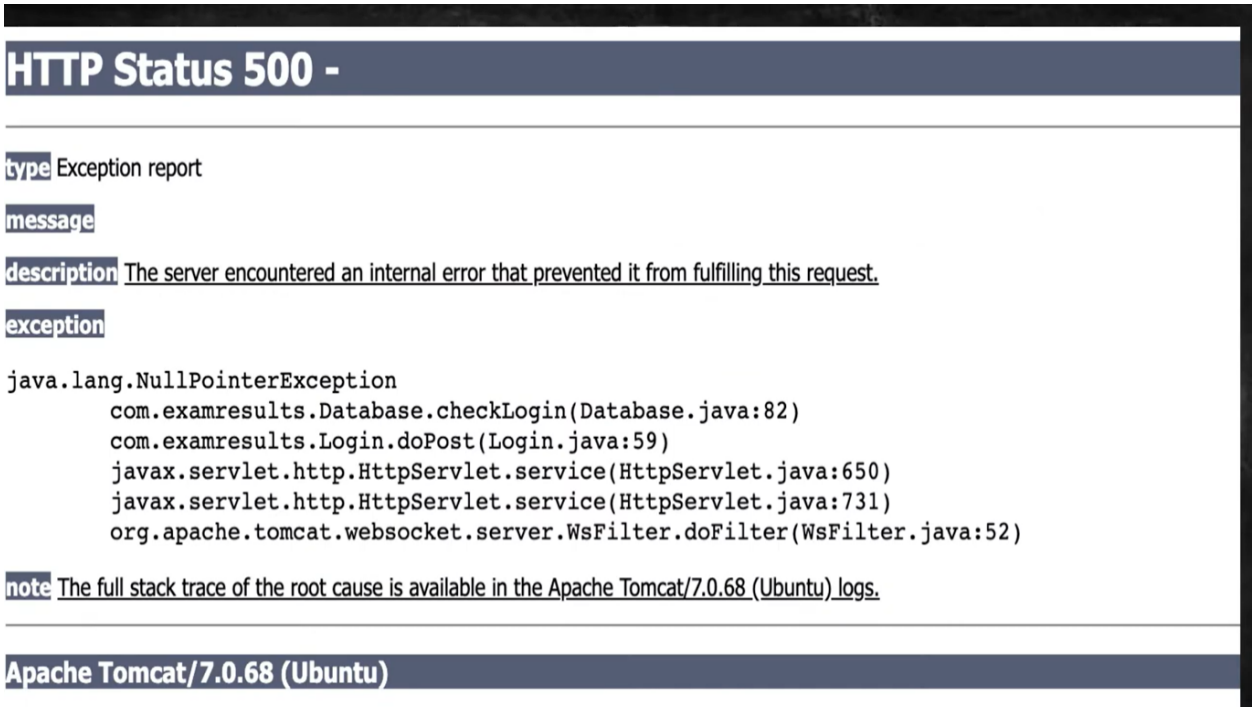
SO THESE ARE THE BUGS WE GENERALLY FIND IN ANY VULNERABLE WEB APPLICATION. WHEN YOU FIND SOMETHING SPECIFIC ABOUT INSECURE DESIGN YOU CAN NOT FIND ANYTHING YOU JUST FIND THESE BUGS BECAUSE THESE ALL COME UNDER INSECURE DESIGN.

SO HERE WE SHOW SOME SCREENSHOTS OF SOME BUGS FOR A BETTER UNDERSTANDING.

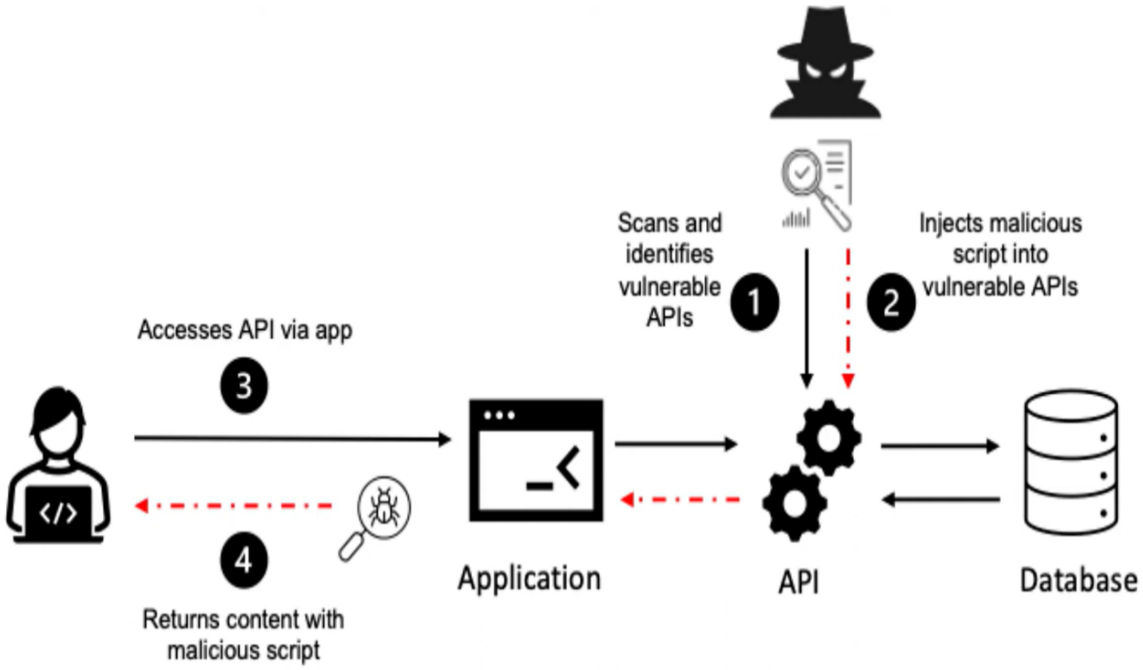
1)S**UPPOSE FOR RESETTING PASSWORD THEY USE A SECURITY QUESTION THEN THIS IS ALSO A VULNERABILITY.**



2)NO PROPER ERROR HANDLING.



DESIGN OF INSURE VULNERABILITY.



4)Broken Access Control

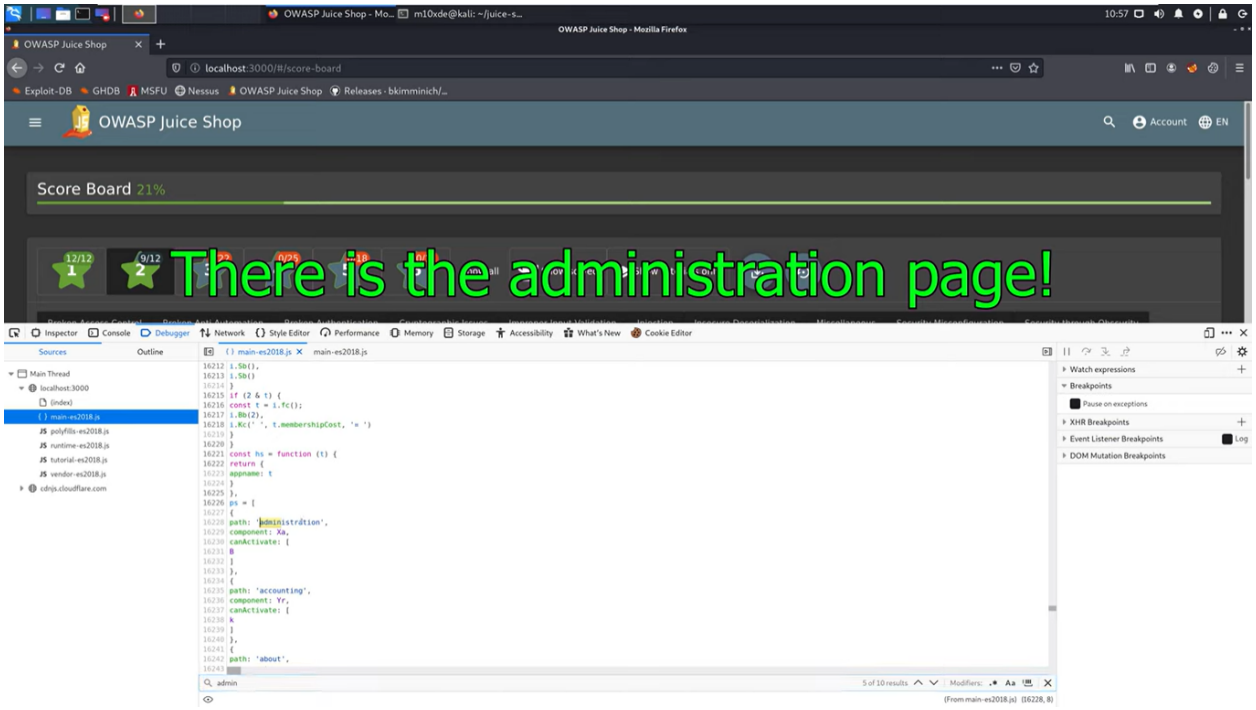
IT IS BASICALLY A VULNERABILITY WHERE AN ATTACKER GAINS UNAUTHORIZED ACCESS TO A RESTRICTED OR MANIPULATED SYSTEM OR INFORMATION.

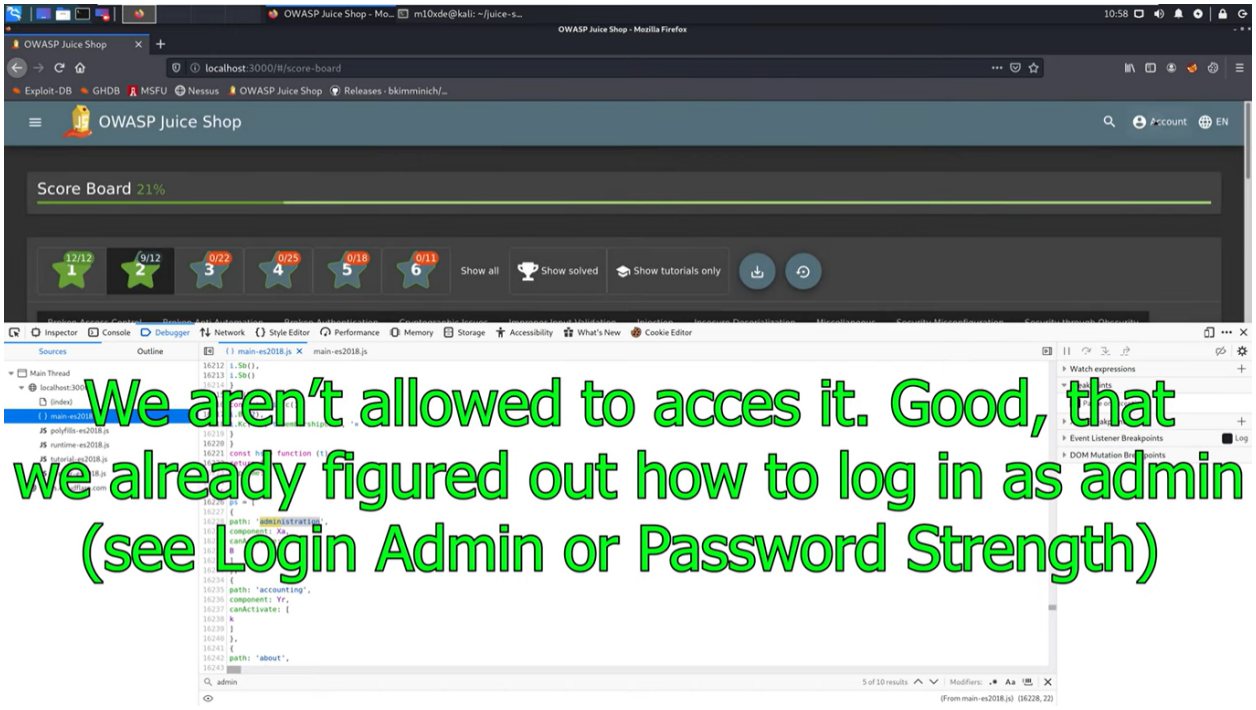
OR WE CAN SAY WHEN HACKERS ENTER AN UNAUTHORIZED AREA AND TRY TO RESTRICT THR INFORMATION FROM OTHERS IT IS BASICALLY CALLED BROKEN ACCESS CONTROL.

WE ALSO ELABORATE ON THAT WAY SUPPOSE THERE ARE TWO USER WITH ID1 AND ID2 ONE WITH ID1 ACCESS ALL INFORMATION OF THE ID2 USER

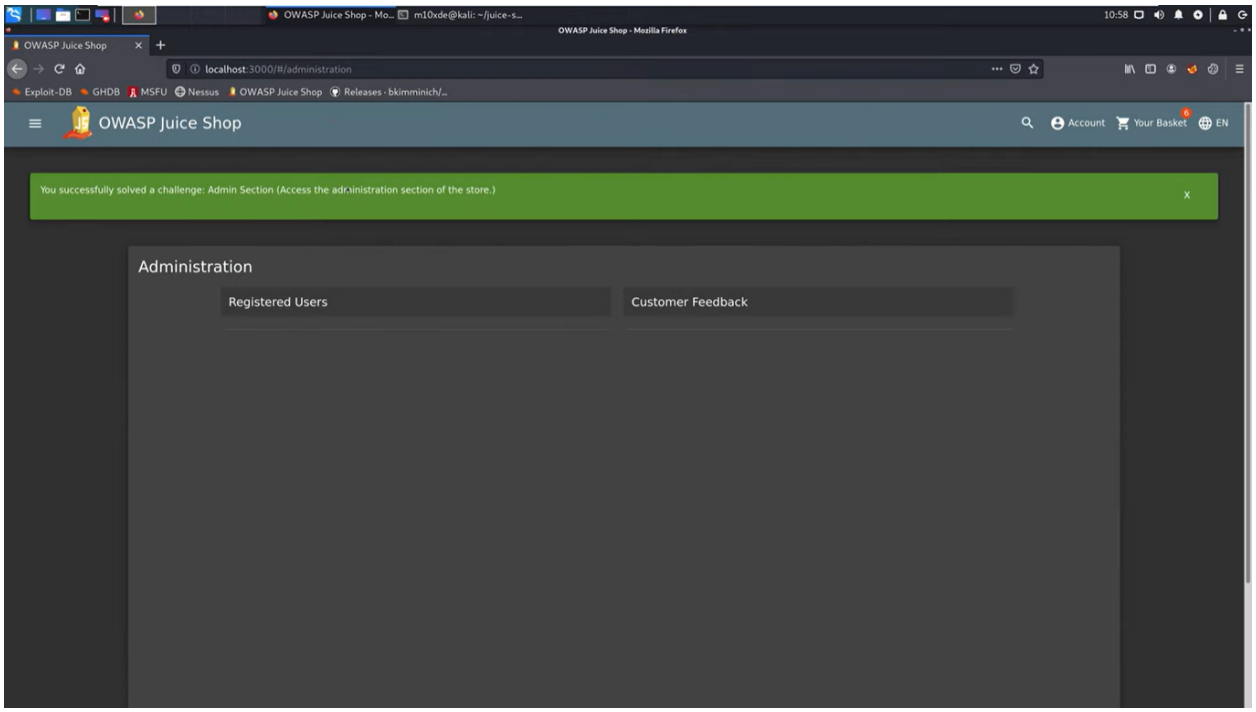
WITHOUT PERMISSION IN A WEB APPLICATION THEN IT IS A BROKEN ACCESS CONTROL.

NOW WE TRY TO UNDERSTAND BY FOLLOWING EXAMPLE.





We aren't allowed to acces it. Good, that we already figured out how to log in as admin (see Login Admin or Password Strength)

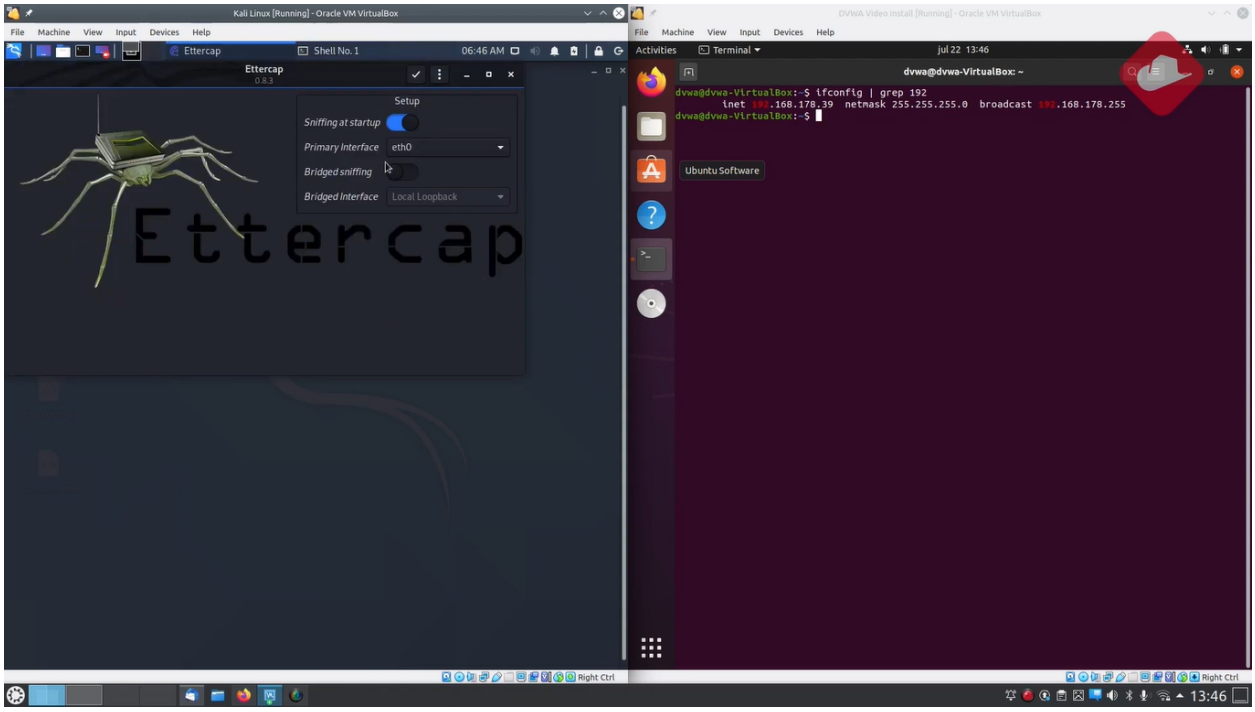


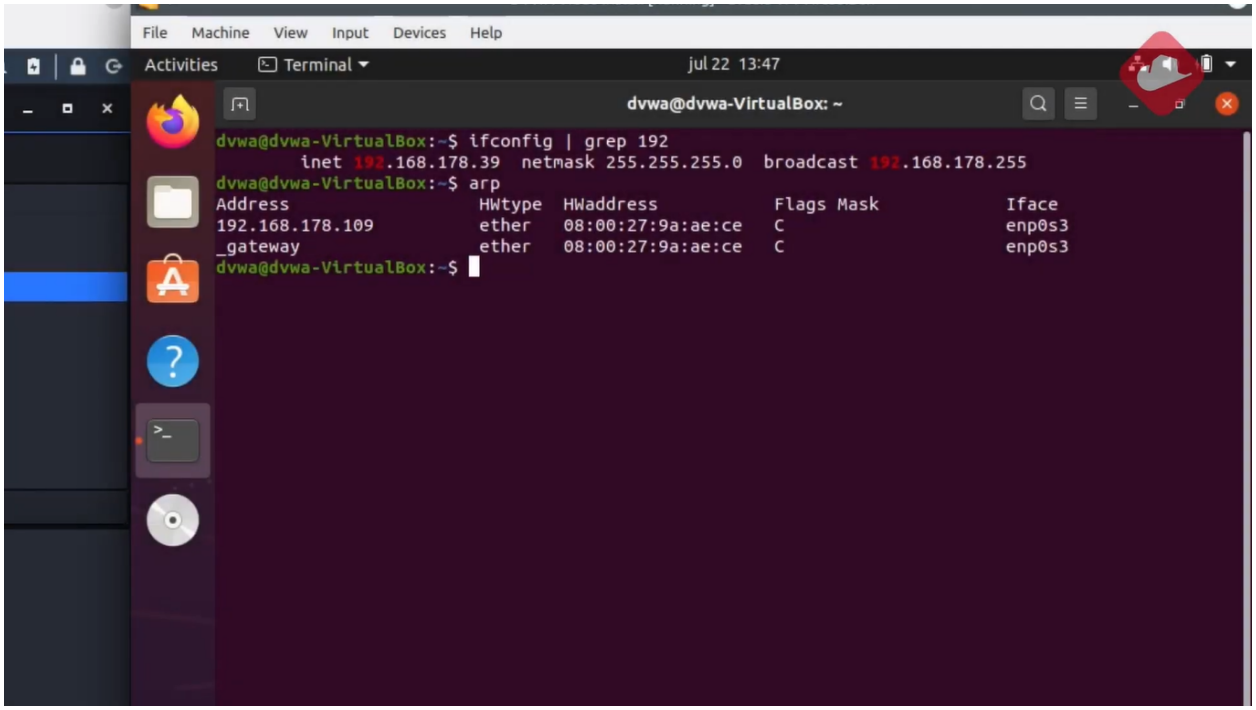
5)Cryptographic Failures

where attackers often target sensitive data, such as passwords, credit card numbers, and personal information, when you do not properly protect them.

Cryptographic failures can lead to serious security breaches, as attackers may be able to bypass encryption or decrypt sensitive data

SO WE JUST SHOW SOME DEMO OF HOW SOMEONE STEALS OUR CRENDITIALS USING MAN IN A MIDDLE ATTACK OR SNIFFING ATTACK WHICH COMES UNDER CRYPTOGRAPHIC FAILURE.




File Machine View Input Devices Help
Activities
Terminal
jul 22 13:47
dvwa@dvwa-VirtualBox: ~
dvwa@dvwa-VirtualBox:~$ ifconfig | grep 192
inet 192.168.178.39 netmask 255.255.255.0 broadcast 192.168.178.255
dvwa@dvwa-VirtualBox:~$ arp
Address HWtype HWaddress Flags Mask Iface
192.168.178.109 ether 08:00:27:9a:ae:ce C enp0s3
_gateway ether 08:00:27:9a:ae:ce C enp0s3
dvwa@dvwa-VirtualBox:~$