

NAME-MILAN RATH

OWASP TOP 5 APPLICATION SECURITY RISKS 2023

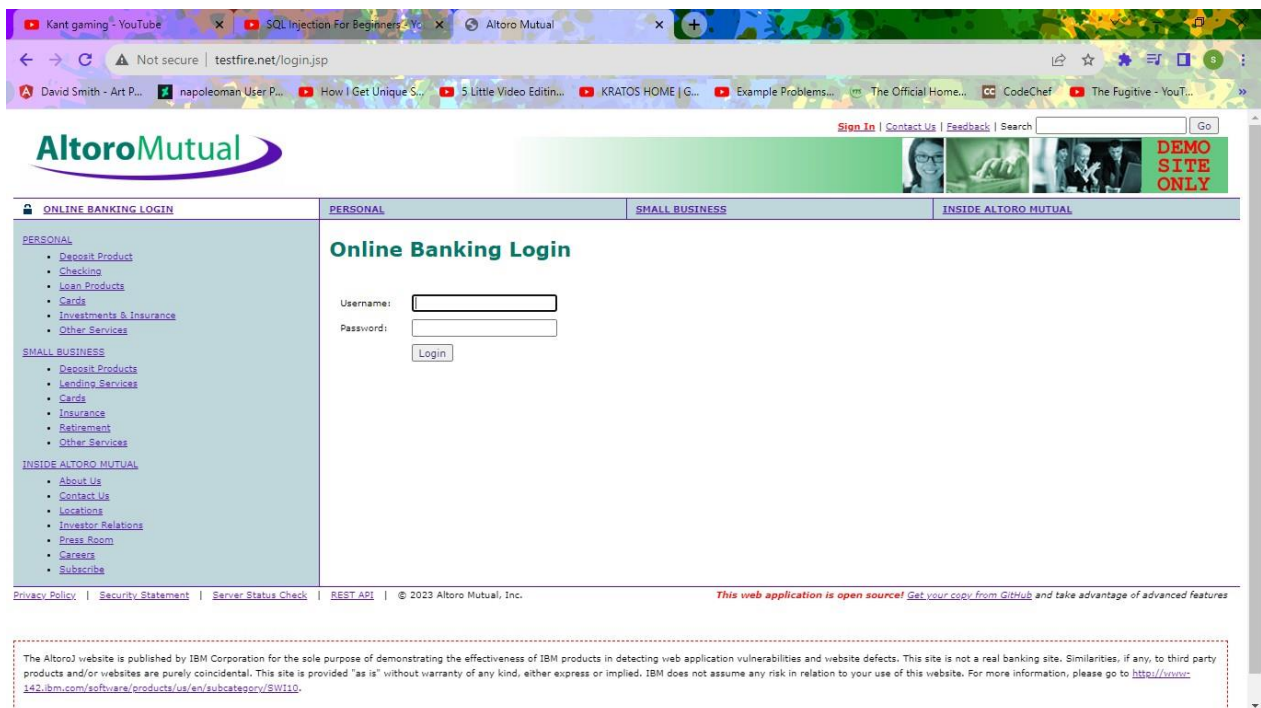
WE TALK ABOUT THE TOP 5 WEB SECURITY THREATS OR WE CAN SAY VULNERABILITIES OF WEB APPLICATIONS.SO HACKERS FIND A WAY TO HACK THE WEB APPLICATION AND ACCESS THEIR DATABASE.SO HERE WE DISCUSS SOME WAYS TO HACK A WEB APPLICATION.

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.

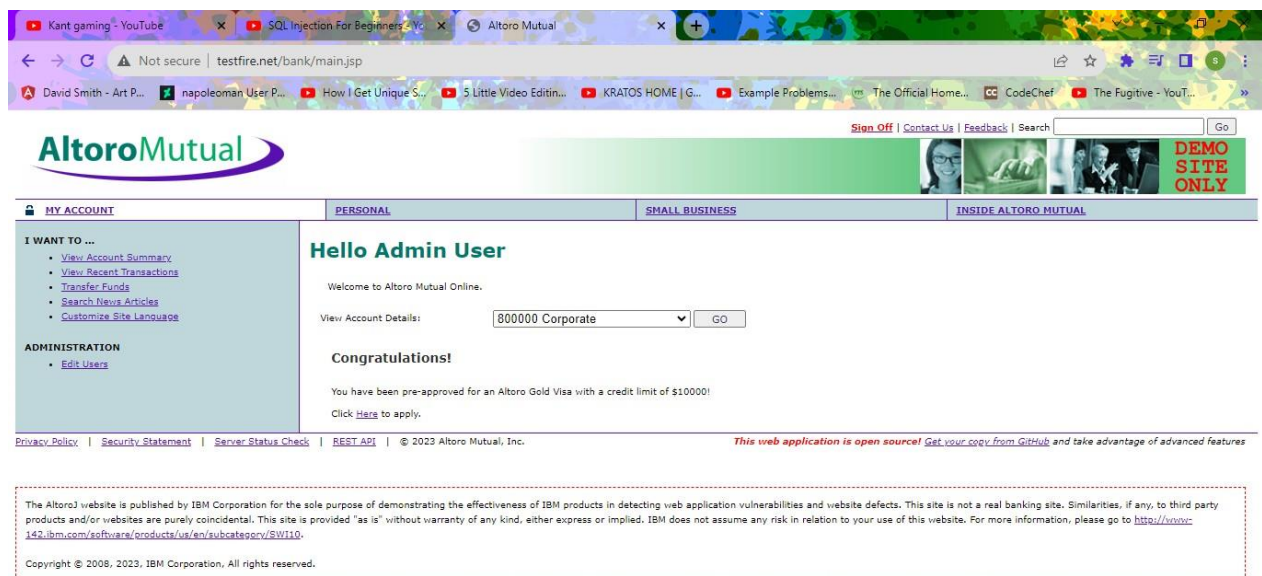
BEFORE INJECTION.....



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 WANT 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 DATABASE.

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

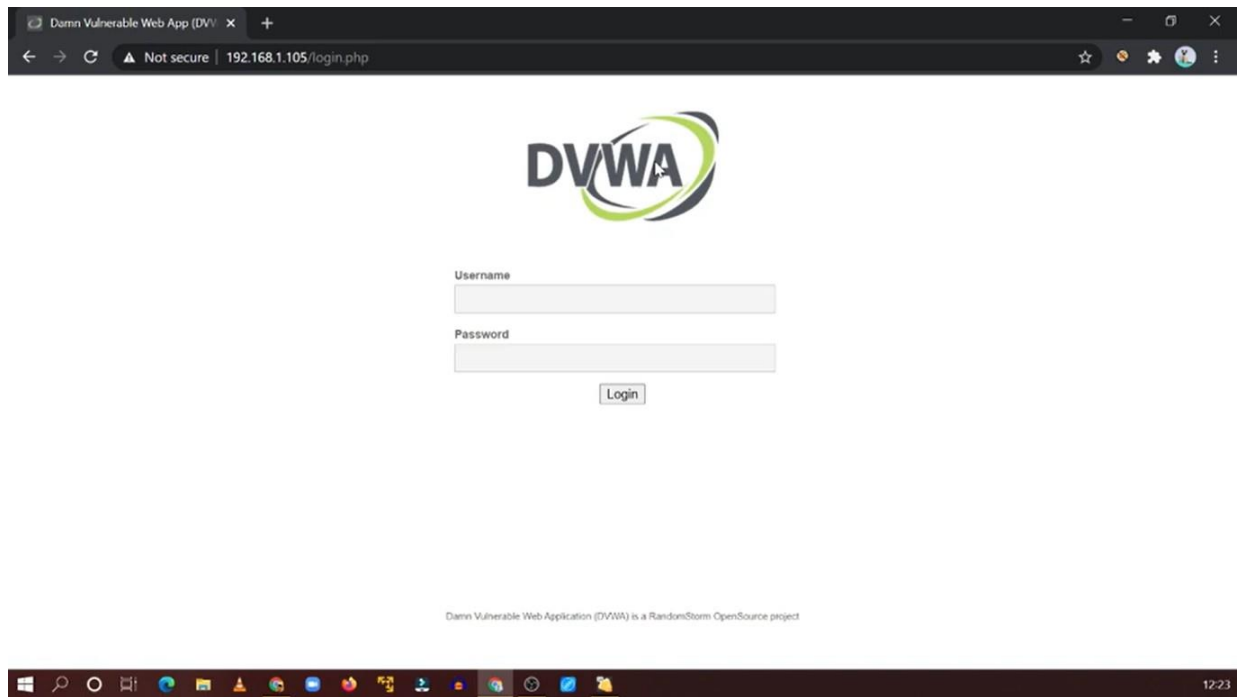
SO NOW WE TALK ABOUT SECURITY MISCONFIGURATION IN THIS VULNERABILITY SUPPOSE WE USE A DVWA THAT IS BASICALLY A TOOL IN KALI LINUX TO PRACTICE THE MOST COMMON WEB VULNERABILITIES.

WE CHECK FIRST CASE,

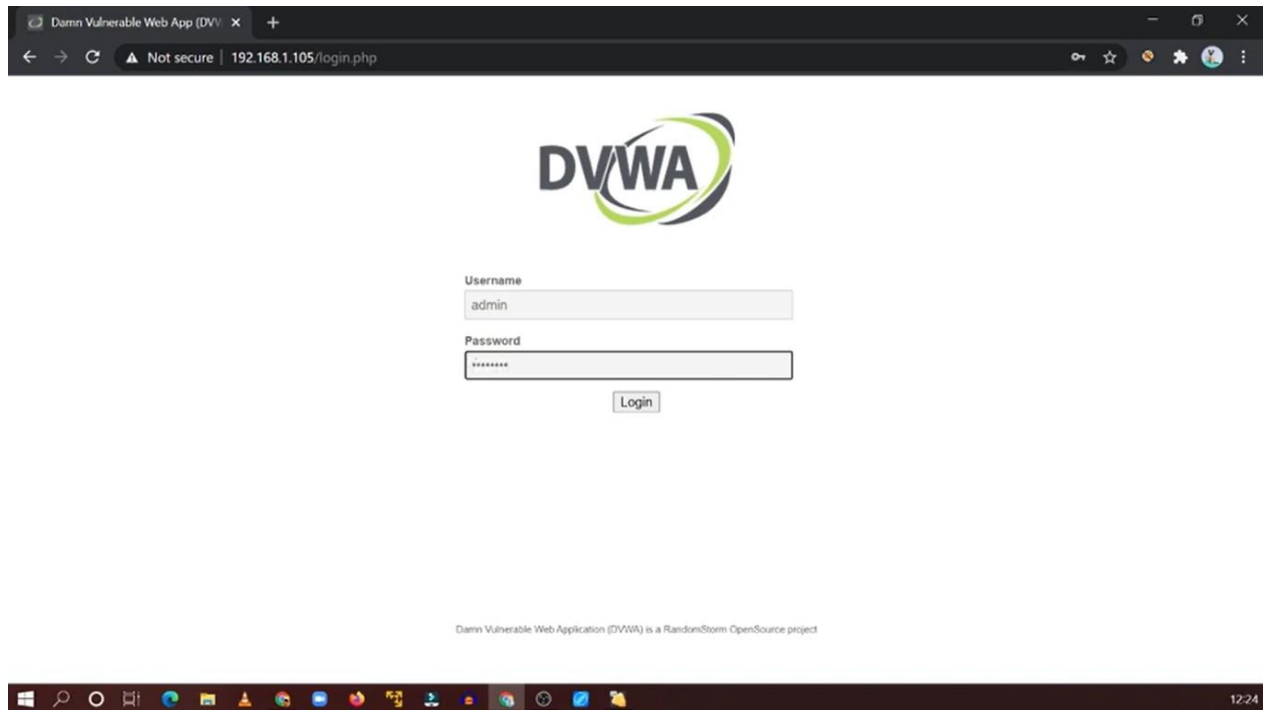
THE FIRST VULNERABILITY WE SAW WAS WHEN WE WENT TO THE LOGIN PAGE OF ANY WEB APPLICATION, FOR EXAMPLE, DVWA WE TRIED TO LOG IN USING A USERNAME AND PASSWORD SO JUST WE TRIED THE USERNAME AS ADMIN AND PASSWORD AS PASSWORD AND IT WORKED. SO THIS IS THE FIRST SECURITY VULNERABILITY WE SEE IF SOMEONE DOES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

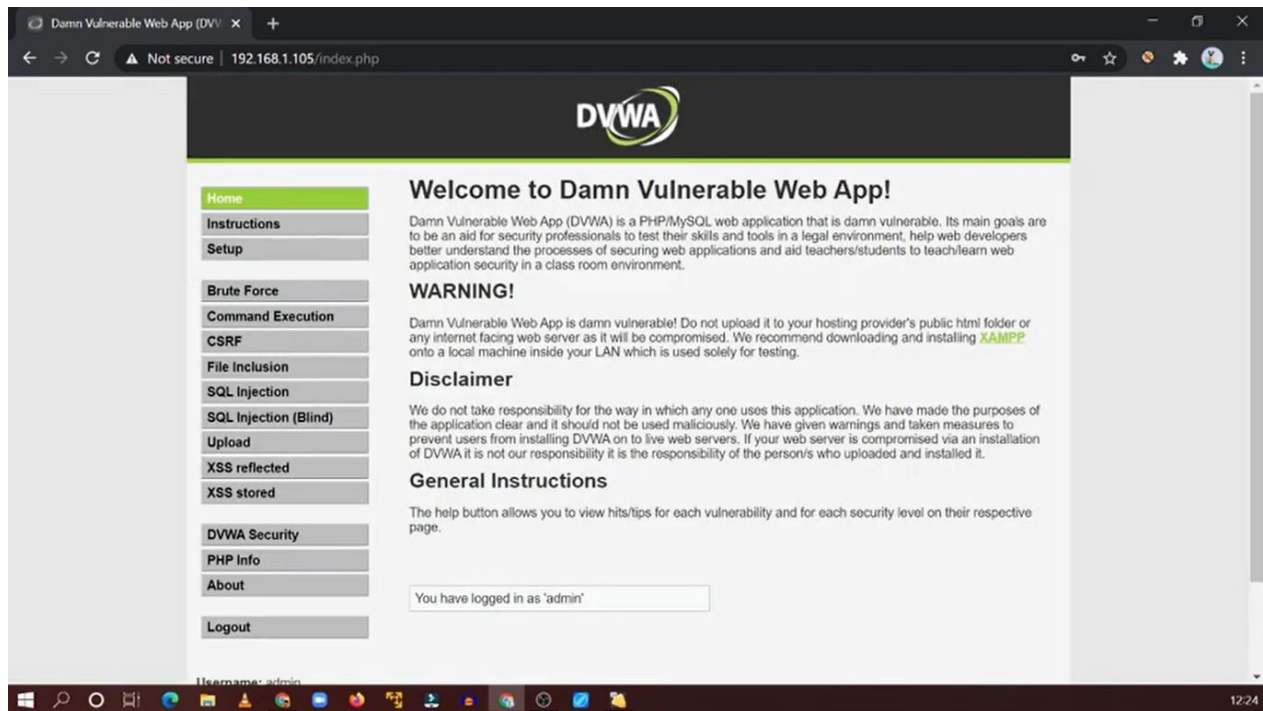
1) WE GO TO LOGIN PAGE OF A WEB APPLICATION.



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



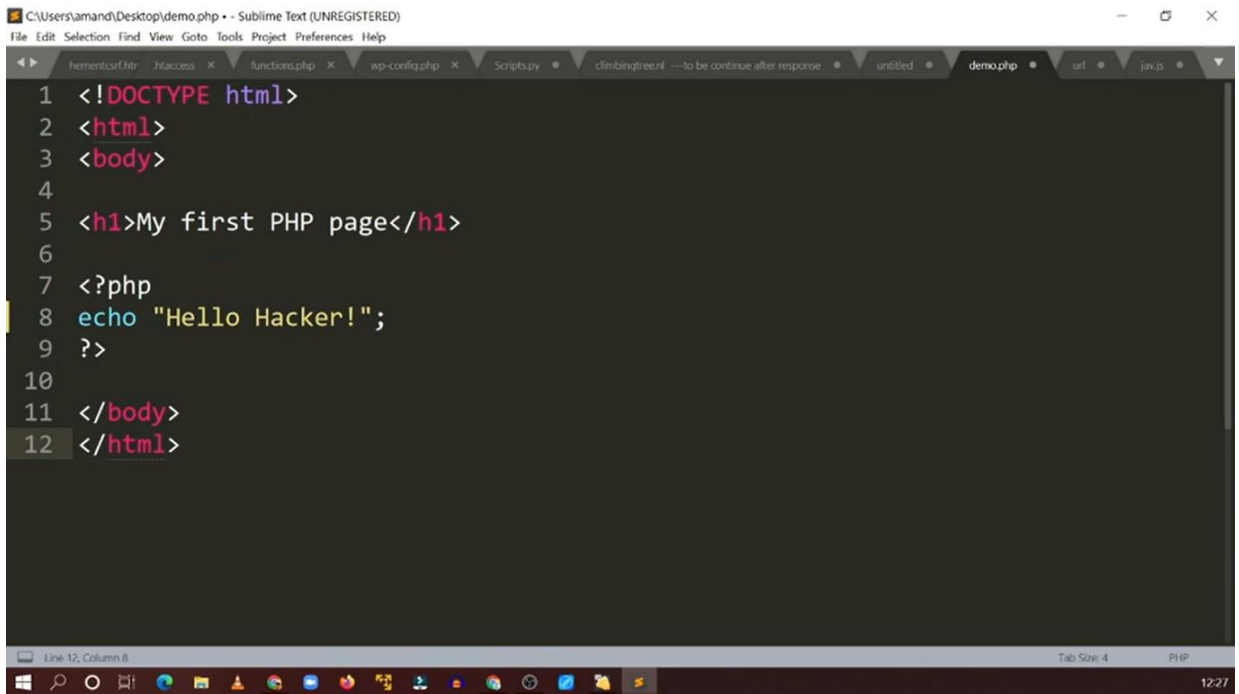
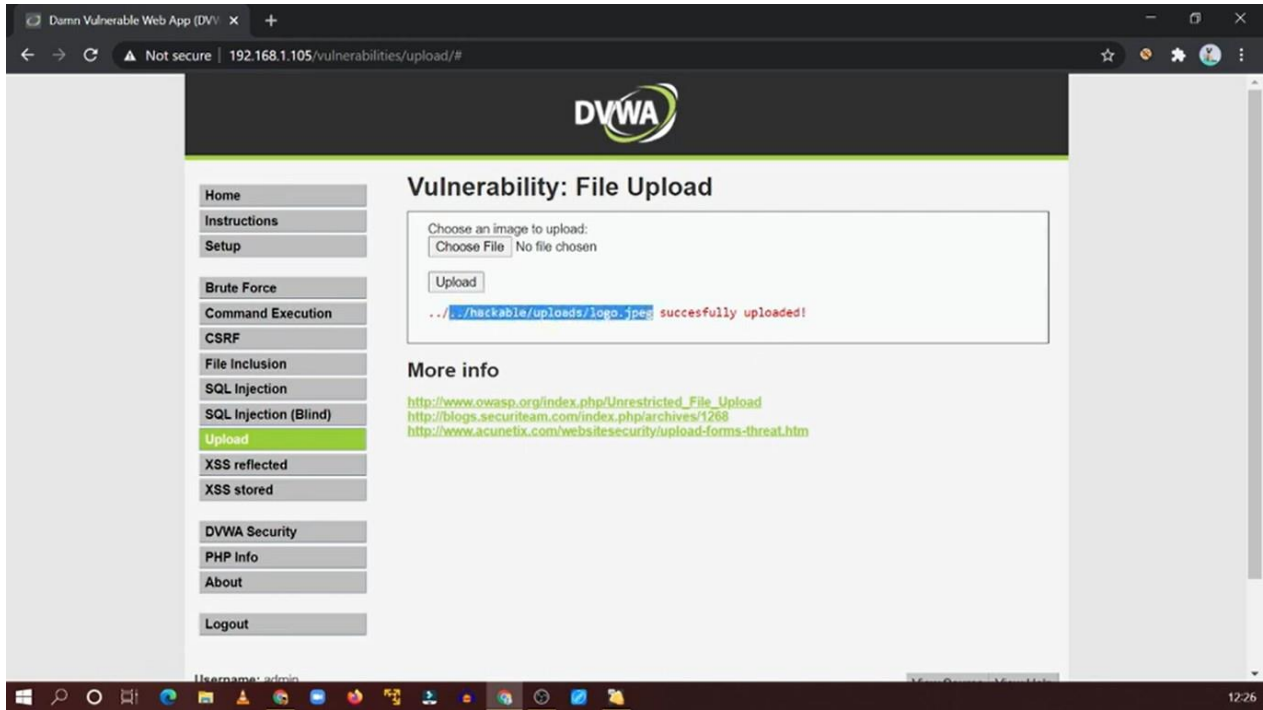
3)WE FINLAY LOGIN INTO A WEB APPLICATION WHICH IS A MISCONFIGURATION OF SECURITY BECAUSE IF ANYONE GOES TO THAT WEBSITE IT MIGHT BE EASIER TO CRACK THE PASSWORD AND USER NAME.

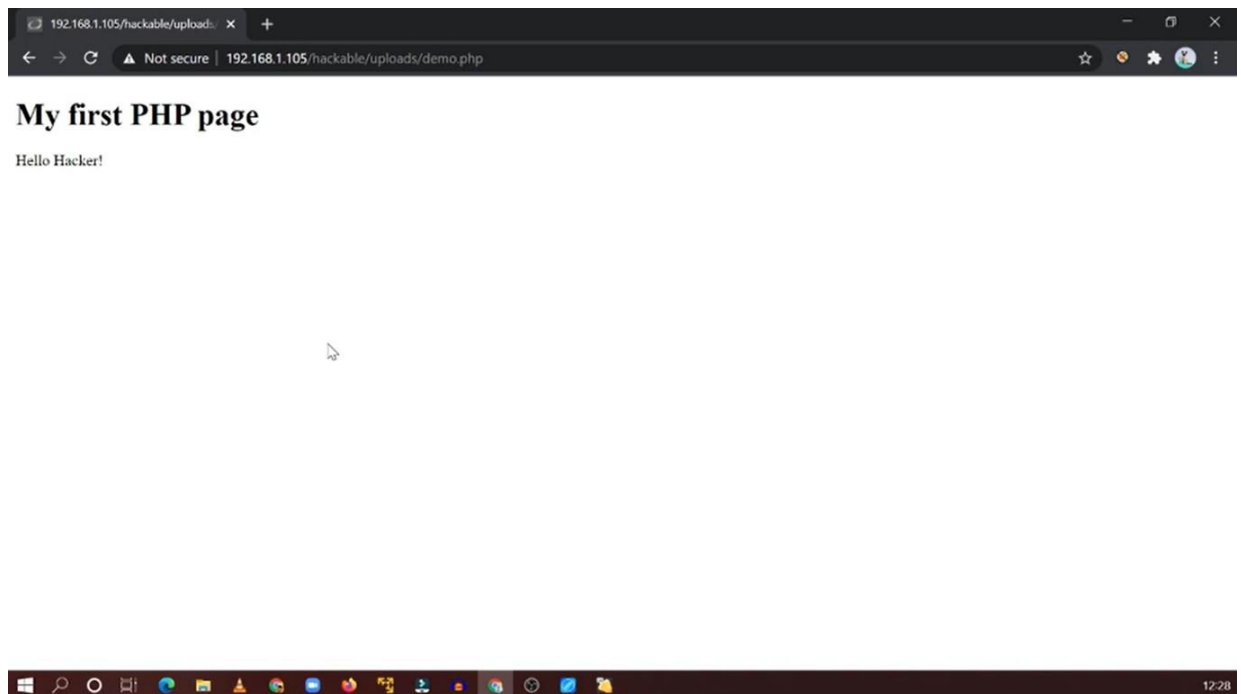
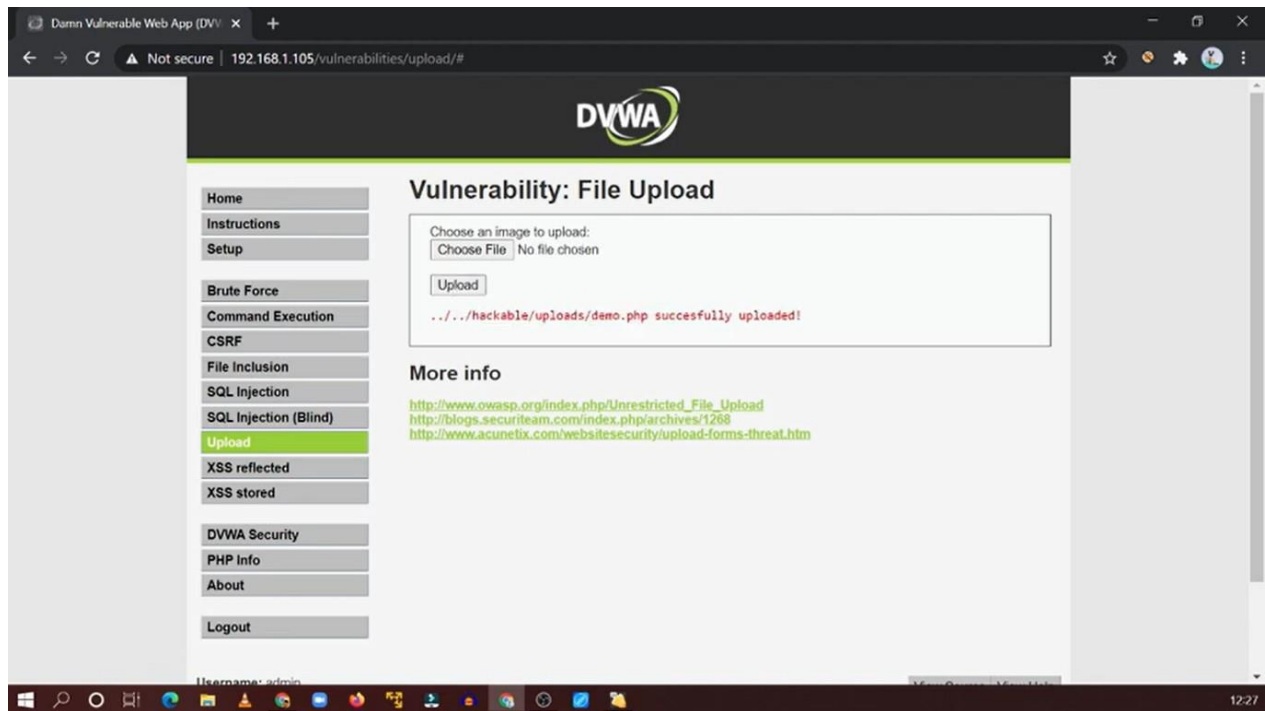


2)SECOND CASE OF MISCONFIGURATION,

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,





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?

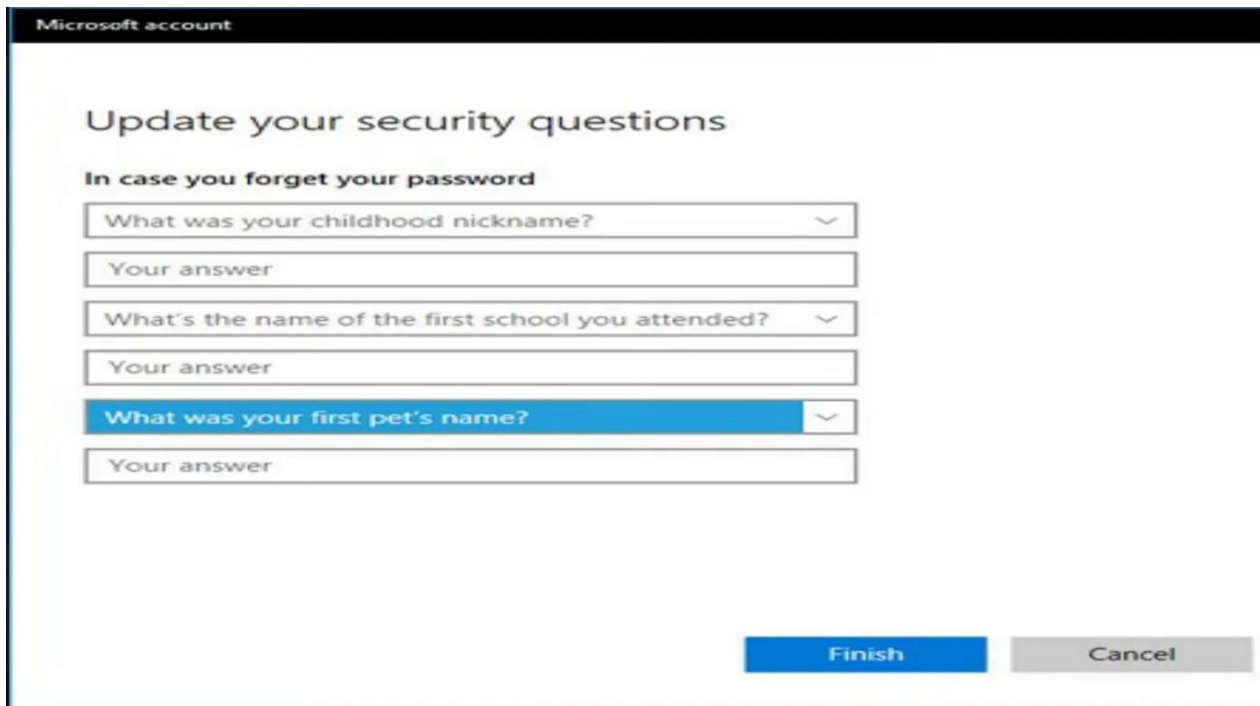
SO NOW WE SEE SOME BUGS THAT HAPPEN BECAUSE OF INSECURE DESIGN OR PEOPLE FIND THOSE BUGS AND REPORT TO WEB APPLICATION ADMIN.

- 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) SUPPOSE FOR RESETTING PASSWORD THEY USE A SECURITY QUESTION THEN THIS IS ALSO A VULNERABILITY.



The screenshot shows a web interface for updating security questions on a Microsoft account. The title is "Update your security questions". Below it, a subtitle reads "In case you forget your password". There are three sets of questions, each with a dropdown menu for the question and a text input for the answer. The third question, "What was your first pet's name?", is highlighted with a blue background. At the bottom right, there are two buttons: "Finish" (blue) and "Cancel" (grey).

Microsoft account

Update your security questions

In case you forget your password

What was your childhood nickname?

Your answer

What's the name of the first school you attended?

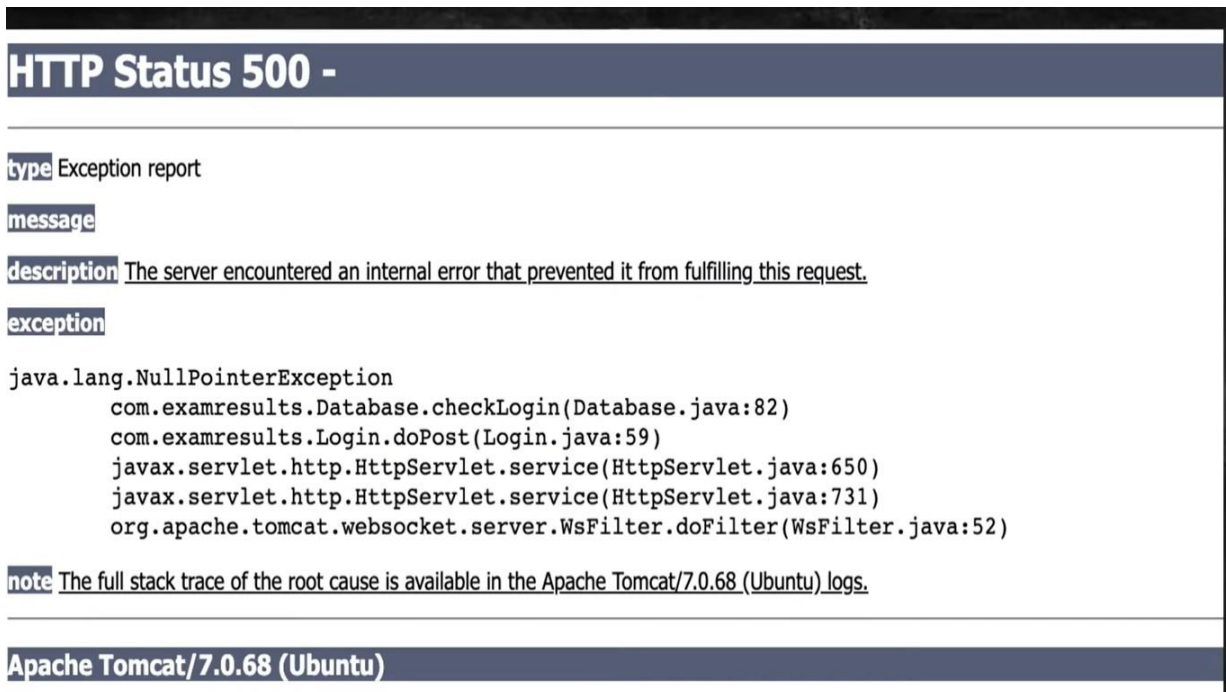
Your answer

What was your first pet's name?

Your answer

Finish Cancel

2) NO PROPER ERROR HANDLING.



The screenshot shows an HTTP Status 500 error page. The title is "HTTP Status 500 -". Below the title, there is a section for "Exception report" with fields for "message", "description", and "exception". The "description" field contains the text "The server encountered an internal error that prevented it from fulfilling this request." The "exception" field shows a stack trace starting with "java.lang.NullPointerException" and listing several method calls. At the bottom, there is a "note" field stating "The full stack trace of the root cause is available in the Apache Tomcat/7.0.68 (Ubuntu) logs." The footer of the page reads "Apache Tomcat/7.0.68 (Ubuntu)".

HTTP Status 500 -

type Exception report

message

description The server encountered an internal error that prevented it from fulfilling this request.

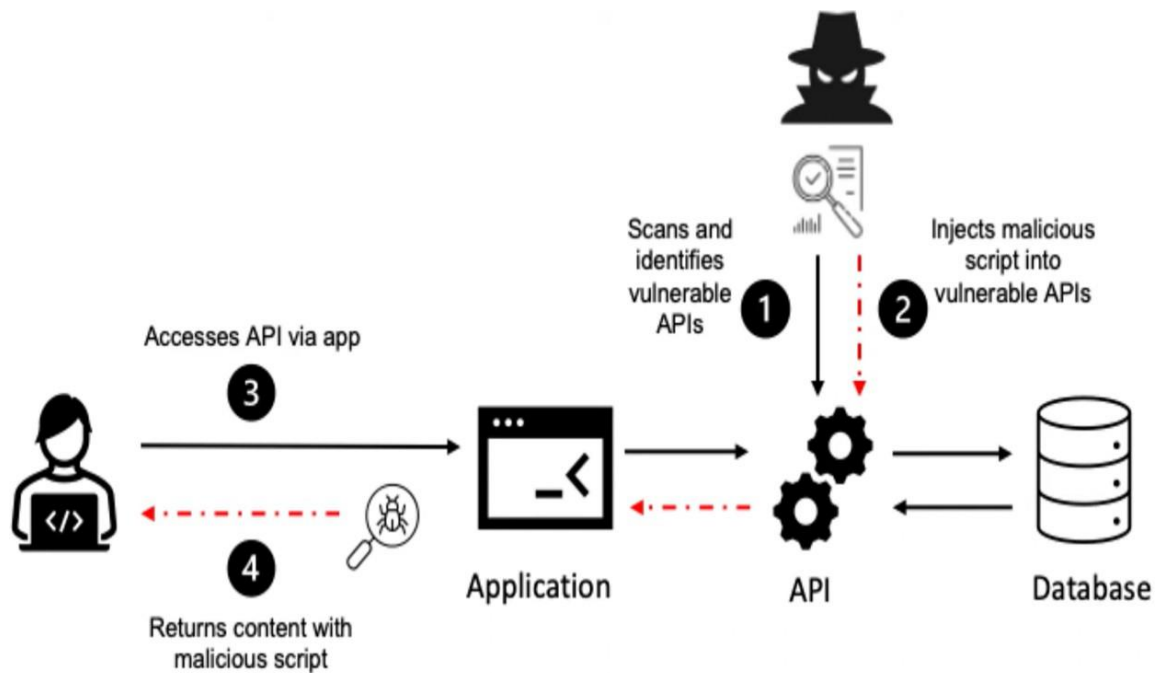
exception

```
java.lang.NullPointerException
    com.examresults.Database.checkLogin(Database.java:82)
    com.examresults.Login.doPost(Login.java:59)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:650)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
    org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
```

note The full stack trace of the root cause is available in the Apache Tomcat/7.0.68 (Ubuntu) logs.

Apache Tomcat/7.0.68 (Ubuntu)

DESIGN OF INSURE VULNERABILITY.



4) Broken Access Control

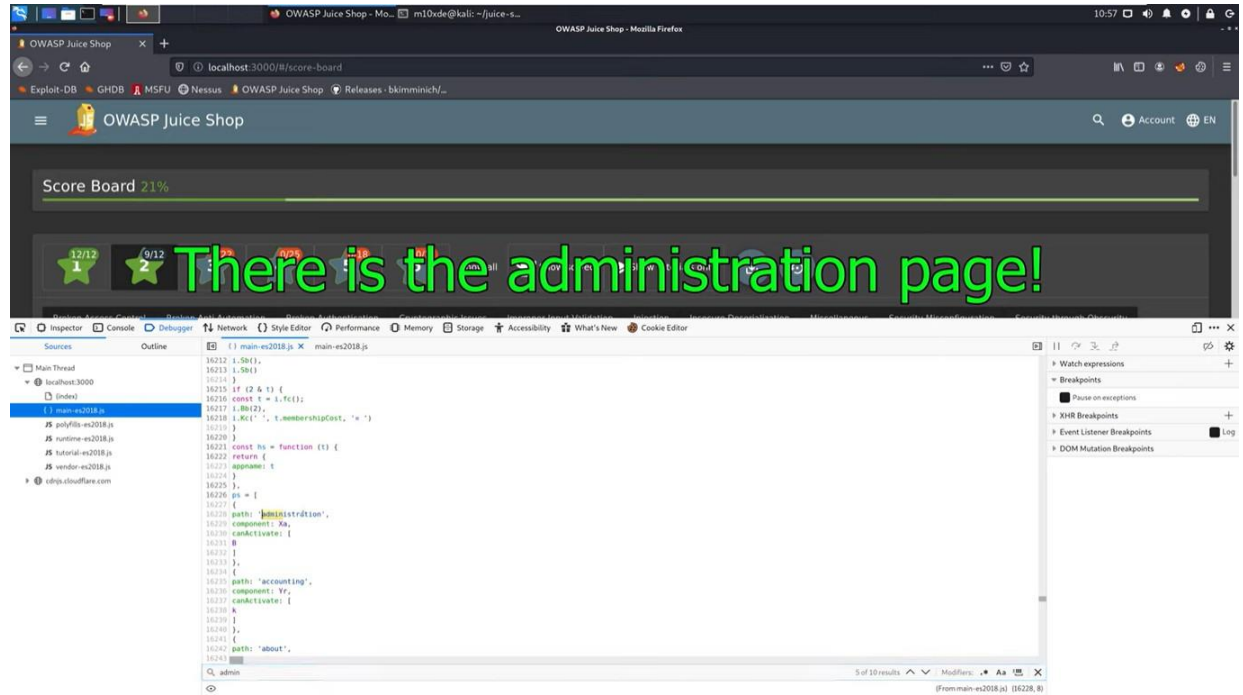
IT IS BASICALLY A VULNERABILITY WHERE AN ATTACKER GAINS UNAUTHORIZED ACCESS TO A RESTRICTED OR MANIPULATED SYSTEM OR INFORMATION.

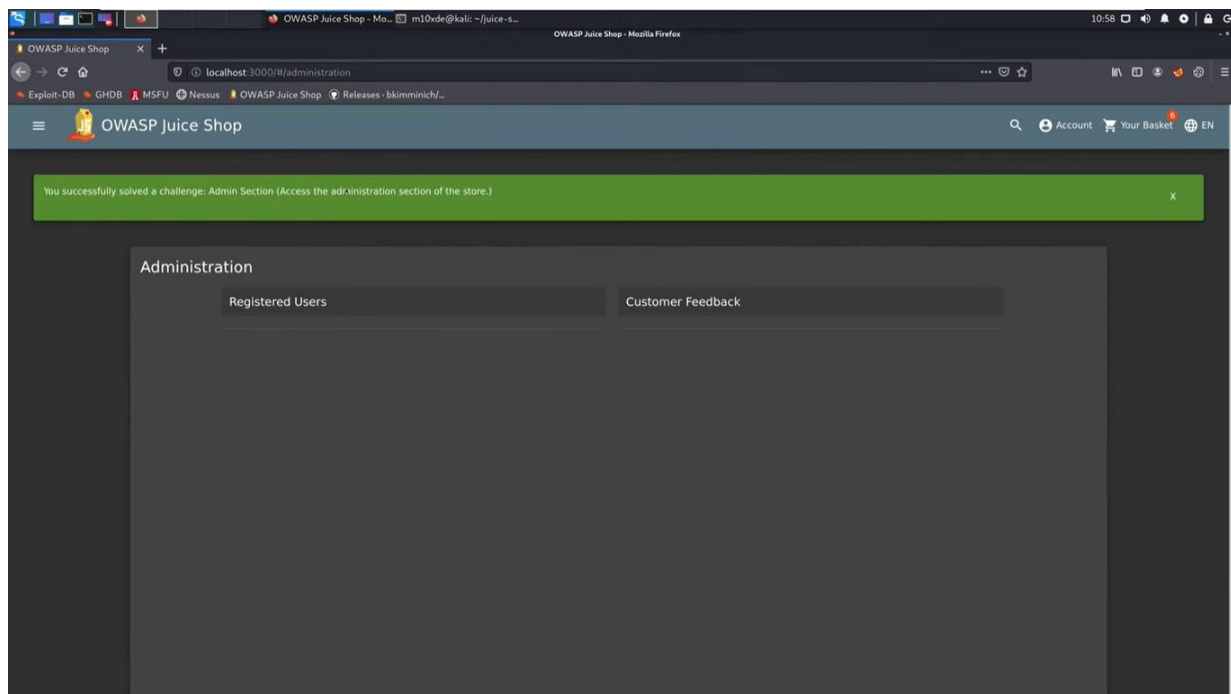
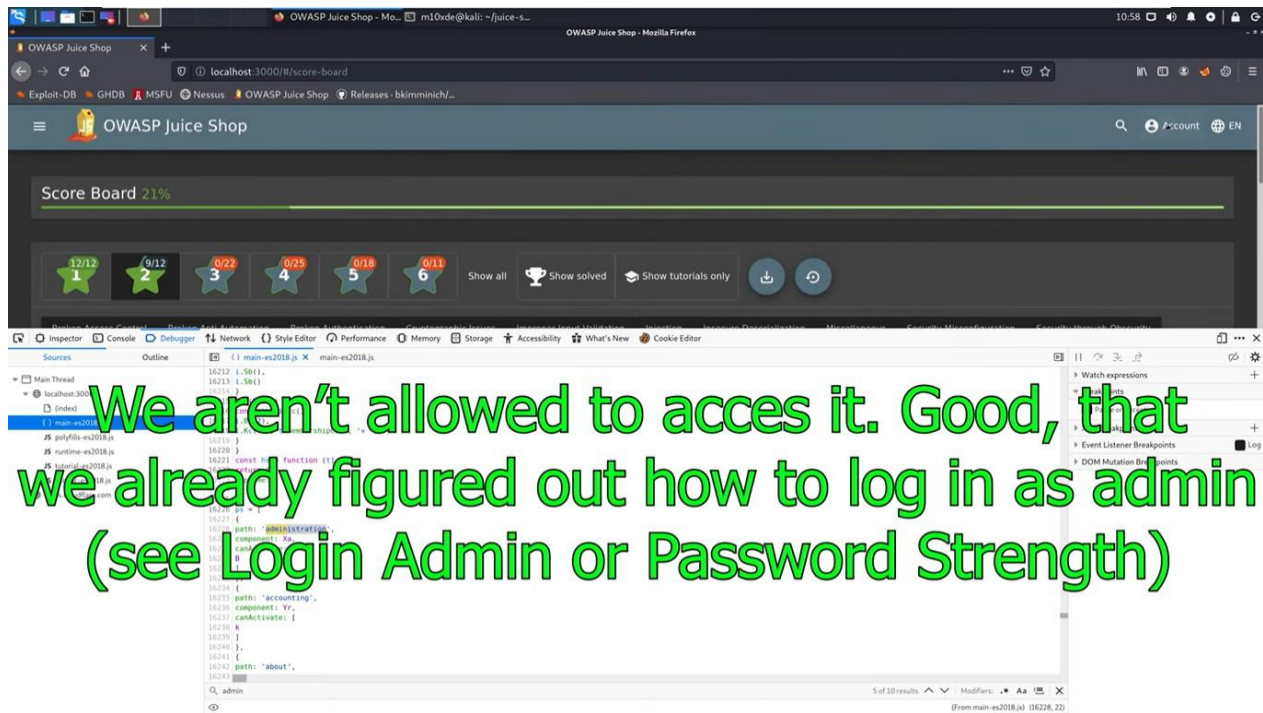
OR WE CAN SAY WHEN HACKERS ENTER AN UNAUTHORIZED AREA AND TRY TO RESTRICT THE INFORMATION FROM OTHERS IT IS BASICALLY CALLED BROKEN ACCESS CONTROL.

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.





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 CREDENTIALS USING MAN IN A MIDDLE ATTACK OR SNIFFING ATTACK WHICH COMES UNDER CRYPTOGRAPHIC FAILURE.

