TEAM 7.6

AI system that verifies user identities based on their online behaviour patterns, adding an extra layer of security.

Team Members

S.NO	NAME	REG NO.	EMAIL ID
1	SALONI GHULE	21BCE1967	saloni.ghule2021@vitstudent.ac.in
2	SHREYA SINGH	21BPS1435	Shreya.singh2021c@vitstudent.ac.in
3	KREET ROUT	21BCE1482	Kreet.rout2021@vitstudent.ac.in
4	NITIN KUMAR	21BCE1792	nitin.kumar2021@vitstudent.ac.in

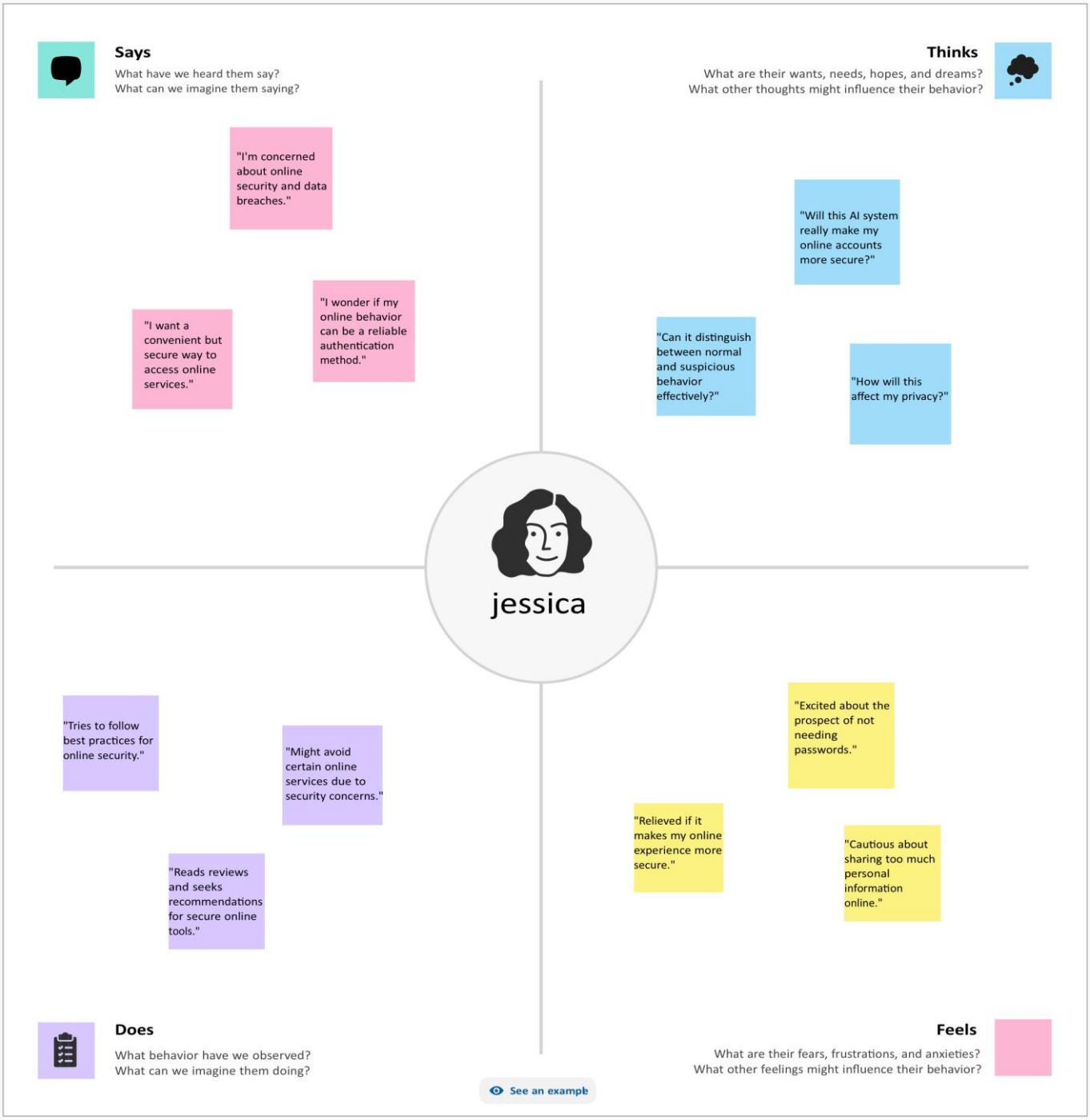
CONTENTS

ABSTRACT

In today's connected digital environment, protecting online platforms and sensitive information is becoming increasingly important. In the face of complex threats, traditional user identification methods are often inadequate and inefficient. Hereby an attempt was made to present a new approach that uses artificial intelligence (AI) to analyze user behavior to improve the security of online systems. This approach adds an extra layer of security by identifying users based on their unique online behavior, such as keystrokes, mouse movements, and browsing habits. This research explores the potential of machine learning algorithms and deep learning to create intelligent machines that can adapt with their users, constantly measuring and evaluating themselves. These artificial intelligence systems can detect unusual or suspicious activities by evaluating various aspects of online behavior and thus detect fraudulent activity and can improve the authentication process against access. We discuss the potential applications of AI-based security approaches in various fields such as banking, e-commerce, healthcare, and social media, as well as nature platforms where the protection of user data is very important. In addition, we highlight the ethical and privacy issues involved in collecting and analyzing online behavioral patterns. The results of this study show that the integration of artificial intelligence-based authentication increases security, reduces dependence on traditional authentication methods, and strengthens online systems against cyber threats. This new approach holds promise against the changing challenges of user authentication as we move to a more secure and reliable digital environment.

IDEATION PHASE

EMPATHY MAP



Shreya Singh

Says

What have we heard them say?
What can we imagine them saying?

"Why do i have again and again proof that I am not a robot by selecting these images? Is password not enough?"

"Can this limit the usage of login credentials for every site?"

"How is it helping in securing my data or preventing my account from getting hacked?"

Thinks

What are their wants, needs, hopes, and dreams?
What other thoughts might influence their behavior?

"I hope I don't have to keep a track of my passwords and change them after every few months."

"I need a convenient way to secure my data without it hampering my day-to-day life."

"I don't want to ever be a victim of hacking or online scams ."

EMPATHY MAP
USER'S POV

"Increased awareness about the recent developments and requirements in cyber security sector."

"Implementing, following and adapting to the new changes in cyber security as well as other IT fields."

"Avoiding the usage of suspicious services."

"It's as if someone invading my privacy by keeping a track of my behavior online."

"Adding an extra layer of security is reassuring."

"Is my online behavior a reliable way of authentication?"

Does

What behavior have we observed?
What can we imagine them doing?

Feels

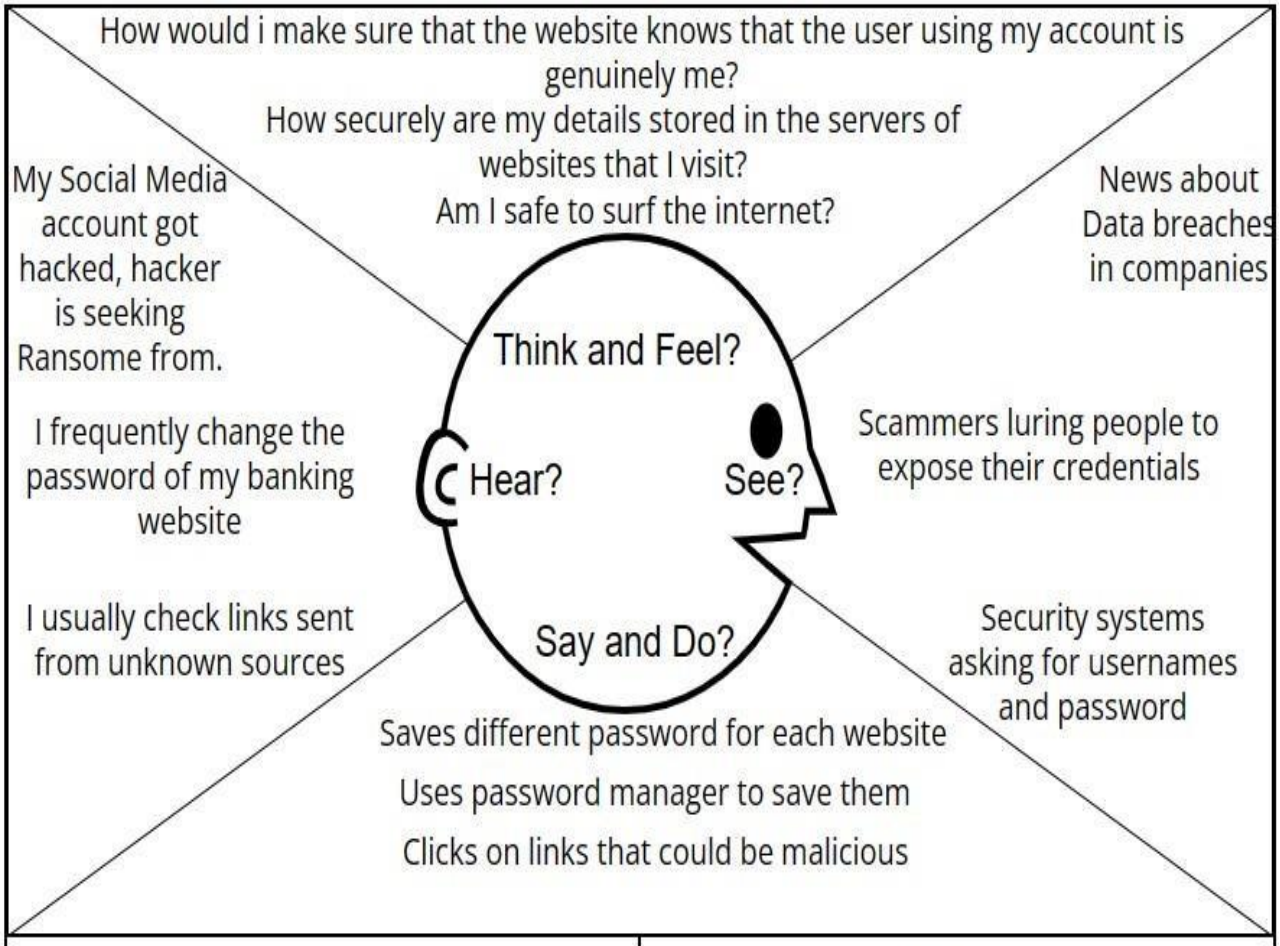
What are their fears, frustrations, and anxieties?
What other feelings might influence their behavior?

Gains

Heightened security
Convenient
Increasing Awareness

Pains

Invasion of Privacy
Complexity and reliability of Identity verification through online behavior.



Pain	Gain
Different Password for each website Needs to remember them LogOut of the website after using Using 2 factor authentication for better security	Gets a safer surfing experience than that of something he used to do. Credentials are safer If one account is hacked, another may not be hacked easily as password is usually different

Empathy Map

Name: Nitin Kumar
21BCE1792

What does he think and feel?

Should I worry more about online security?

How do i protect my family online?

Are consumer antivirus enough?

What to do if i get compromised online?

What does he hear?

Capital loss due to cyber attacks.

Increased attacks on Individuals.

Easy to be secure, just follow simple protocols.

What does he see?

Companies Investing heavily in Cyber Sec.

Govt. spreading more awareness

Better to invest in precaution then spend on repercussions.

What does he say and do?

I'm concerned about online privacy.

I will create stronger passwords.

I will make my family aware about online risks.

Pain

Fear of cyber threats.
Anxiety about personal data exposure.
Difficulty in managing passwords.
Concerns about online scams.
Inconvenience of strong security measures.

Gain

Increased online security.
Greater peace of mind.
Protection against identity theft.
Improved online hygiene practices.
Trust in online platforms.

BRAINSTORMING

Behavioral Biometrics and Authentication:

1. Pattern Analysis for Authentication.
2. Behavioral Biometric Authentication.
3. Multi-Factor Authentication (MFA).
4. Device Fingerprinting.

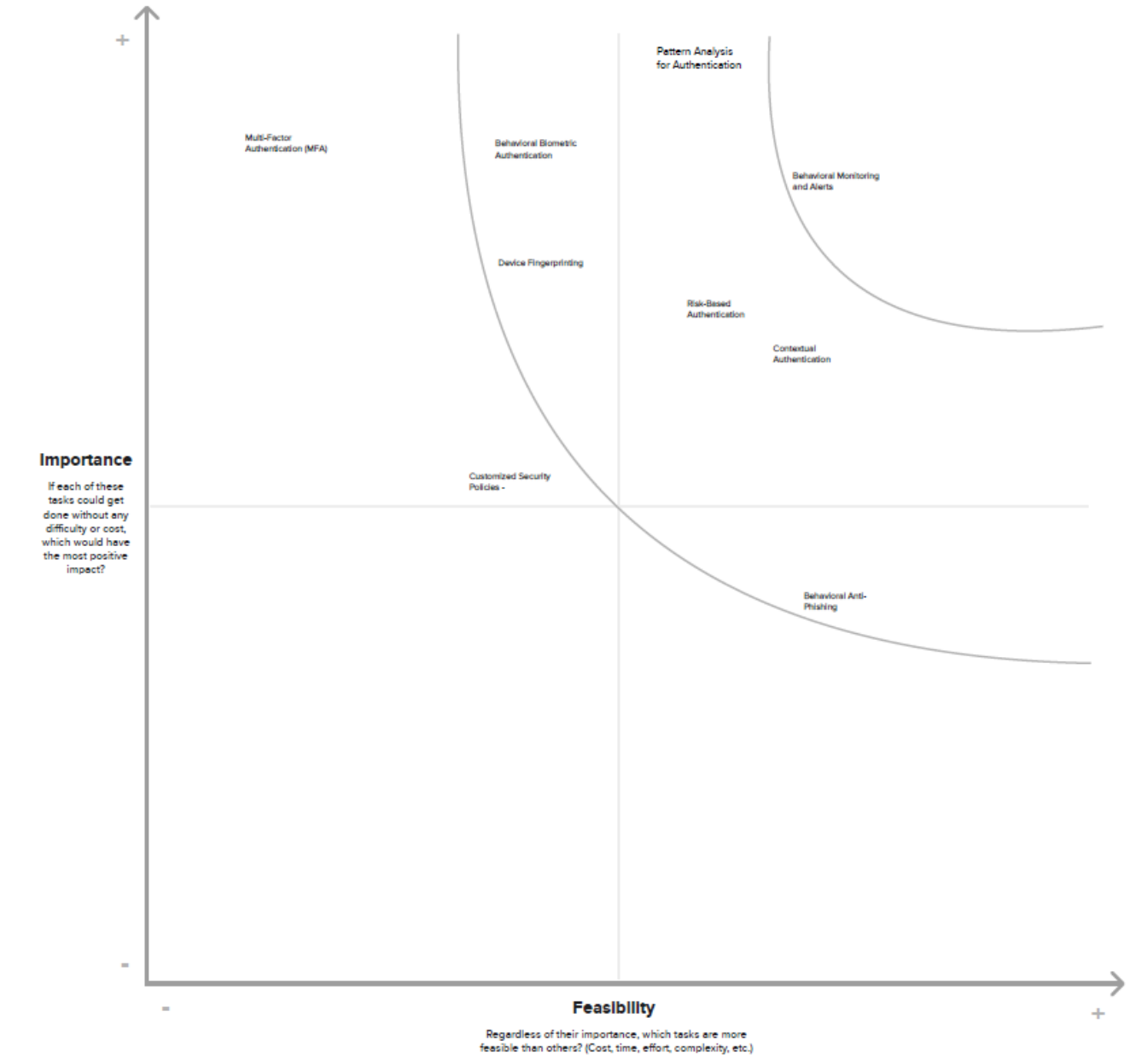
Predictive and Contextual Authentication:

5. Machine Learning Predictive Models.
6. Contextual Authentication.
7. Risk-Based Authentication.
8. Behavioral Monitoring and Alerts.

User Customization and Control:

9. User-Initiated Authentication Challenges.

Customized Security Policies.


+
Pattern Analysis for Authentication
Multi-Factor Authentication (MFA)
Behavioral Biometric Authentication
Behavioral Monitoring and Alerts
Device Fingerprinting
Risk-Based Authentication
Contextual Authentication
Importance
If each of these tasks could get done without any difficulty or cost, which would have the most positive impact?
Customized Security Policies -
Behavioral Anti-Phishing
-
-
Feasibility
+
Regardless of their importance, which tasks are more feasible than others? (Cost, time, effort, complexity, etc.)

PROJECT DESIGN PHASE

PROPOSED SOLUTION

S.NO	PARAMETER	DESCRIPTION
1	Problem Statement (Problem to be solved)	Traditional methods of user identity verification, such as passwords, PINs, and security questions, are vulnerable to various forms of cyberattacks and identity theft. The rise in online security breaches and the increasing sophistication of cybercriminals necessitate the development of a more robust and user-friendly authentication system. The current identity verification methods also inconvenience users and often lead to password fatigue and account lockouts.
2	Idea / Solution description	Our proposed solution is to develop an AI-based system that verifies user identities based on their online behaviour patterns. This system will analyse and recognize unique behavioural biometrics, including typing patterns, mouse movements, touch gestures, and mobile device usage, to verify the user's identity. The core elements of our solution include: • **Behavioural Biometric Data Collection:** The system will collect and analyse user behavioural data over time, creating a unique biometric profile for each user. • **Machine Learning and AI Algorithms:** Machine learning algorithms will process the behavioural data to establish a baseline for

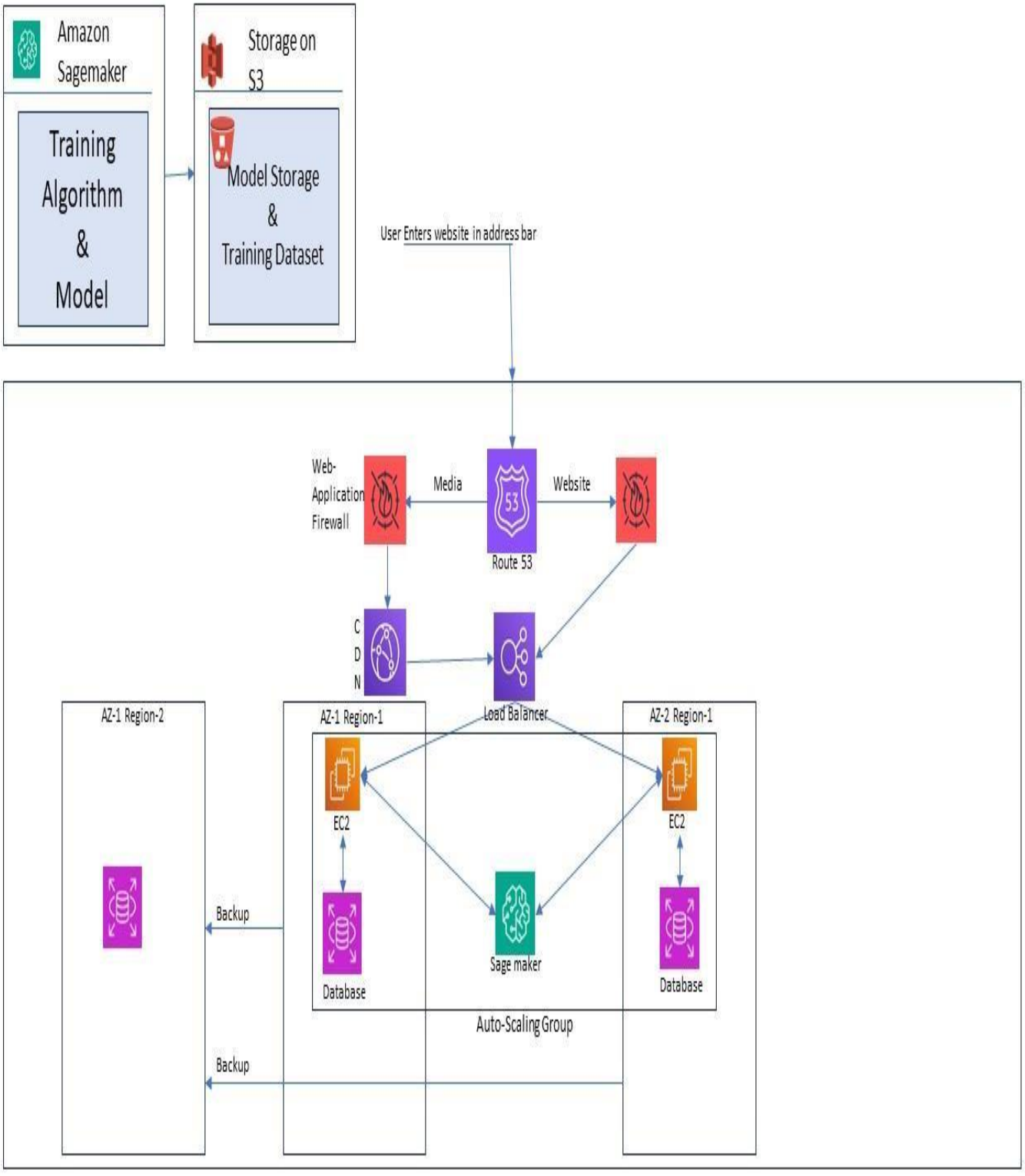
		each user, allowing for real-time verification. • **Multi-Factor Authentication:** Users will have the option to combine behavioural biometrics with other authentication methods, like passwords or facial recognition, for added security. • **Continuous Monitoring:** The system will continuously monitor user behaviour during a session to detect any unusual activities or deviations from the established baseline.
3	Novelty / Uniqueness	Our solution stands out due to the following unique features: • **Passive Authentication:** Unlike traditional methods, users will not need to actively input authentication credentials. This makes the verification process seamless and less prone to phishing attacks. • **Behavioural Adaptability:** The system will adapt to users' changing behaviours and account for variations due to factors like age, health, and device preferences. • **Real-Time Verification:** The system will provide instant verification, reducing user friction and improving security.
4	Social Impact / Customer Satisfaction	Our solution offers several benefits: • **Enhanced Security:** Users will experience higher security levels, reducing the likelihood of identity theft and unauthorized access to their accounts. • **User Convenience:** The system simplifies the verification process, reducing the need for complex passwords and lengthy authentication steps, leading to improved customer satisfaction.

		• **Reduced Account Lockouts:** By continuously monitoring behaviour, the system can prevent account lockouts due to forgotten passwords.
5	Business Model (Revenue Model)	We propose a flexible business model: • **Subscription Model:** Offer monthly or annual subscription plans for businesses, websites, and apps to integrate our identity verification system. • **Pay-Per-Use Model:** Charge businesses on a per-verification basis, making it cost-effective for smaller companies. • **Licensing Model:** License the technology to other security solution providers, generating revenue through licensing fees.
6	Scalability of the Solution	Our solution is highly scalable: • **API Integration:** Can be easily integrated into existing web and mobile applications. • **Cloud-Based Infrastructure:** The system can leverage cloud resources to scale up based on demand. • **Global Reach:** Can be deployed worldwide, catering to a wide range of industries, including finance, healthcare, and e-commerce. • **Continuous Improvement:** Ongoing development and machine learning model updates ensure adaptability and long-term scalability.

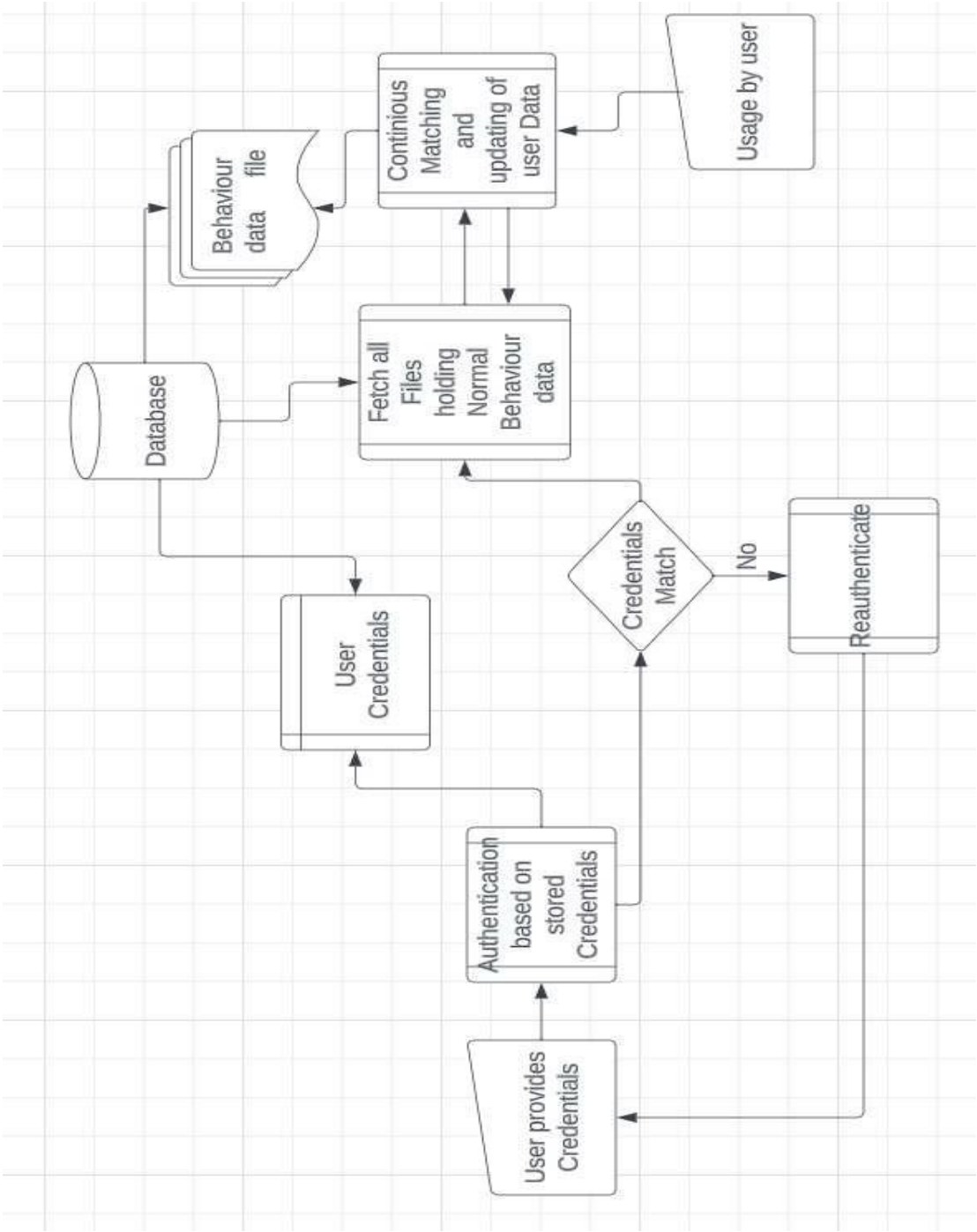
In conclusion, our Behavioral Biometrics-Based User Identity Verification System offers a groundbreaking solution to the growing security challenges in the digital world. It combines advanced technology with user convenience, making it a valuable proposition for businesses and users alike.

SOLUTION ARCHITECTURE

1) User Enters Website in Browser.
2) The request is made to Route 53.
3) Request is passed through Web-Application Firewall.
4) If media is requested the request goes to CDN then Load Balancer, else directly to load balancer.
5) Request is passed to EC2 Instance hosting the server.
6) From where if login is requested the request goes to sage maker, according the user's behaviour, he is a genuine the request will be approved, else denied.
7) Then database is checked for credentials.
8) The Infra works in 2 availability zone for fault tolerance.
9) The Data is backed up in region-2, if needed can be used.


Amazon Sagemaker
Training Algorithm & Model
Storage on S3
Model Storage & Training Dataset
User Enters website in address bar
Web-Application Firewall
Media
Website
Route 53
CDN
Load Balancer
AZ-1 Region-2
AZ-1 Region-1
AZ-2 Region-1
EC2
EC2
Backup
Database
Sage maker
Database
Auto-Scaling Group
Backup

DATA FLOW DIAGRAM



PROJECT PLANNING PHASE

TECHNNOLOGY STACK

S.No	Component	Description	Technologies
1	User Interface	How the user Interacts with the application	HTML, CSS
2	Application Logic	Dynamic verification Logic	Python, Java
3	Application Logic	Data Format	JSON
4	Database and Storage	DataType, Configurations etc	NoSQL
5	ML models	To keep a track of how the user behaves when logged in the website	Linear Regression, Recurrent Nural Networks, Hidden Markov Models
6	External API	For Credential less authentication	Google authenticator, Microsoft Authenticator
7	Internal API	For allowing other organizations to use it	Flask

PROJECT PLANNING DETAILS

Product Backlog, Sprint Schedule, and Estimation

Sprint	Functional Requirement (Epic)	User Story Number	User Story / Task	Story Points	Priority
Sprint-1	User Behavior Verification System	USN-1	As a user, I want to be able to create a profile and set up online behavior verification.	2	High
Sprint-1		USN-2	As a user, I want the system to collect and analyze my online behavior data.	1	High
Sprint-2		USN-3	As a user, I can register for the application through Facebook	2	Low
Sprint-1		USN-4	As a user, I want the system to verify my identity based on my online behavior patterns.	1	High
Sprint-1	Login	USN-5	As a user, I want to receive notifications and alerts for any suspicious activity.	1	High
Sprint-2	Data Collection and Analysis	USN-6	Collect data from various online platforms (e.g., social media, email, browsing history). Implement machine learning models for user behavior analysis.	1	High
Sprint-2	Identity Verification	USN-7	Develop algorithms for identity verification based on behavior patterns. Implement a risk assessment system for verifying identity. Create user-friendly interfaces for users to interact with the verification	2	Medium
Sprint -3	Notification and Alert System	USN-8	Develop a real-time notification system for users. Implement an alert system for the admin to take action on suspicious	3	High
Sprint -4	System Administration and Reporting	USN-9	Develop an admin dashboard for system management.	2	Medium
Sprint-4		USN-10	Create reporting and auditing features for administrators.	3	Low
Sprint-5		USN-11	As a system administrator, I want the ability to generate and export detailed reports on user behavior patterns and identity verification results for compliance and auditing purposes.	2	High

Project Tracker, Velocity & Burndown Chart:

Sprint	Total Story Points	Duration	Sprint Start Date	Sprint End Date (Planned)	Story Points Completed (as on Planned End Date)	Sprint Release Date (Actual)
Sprint-1	5	5 Days	22 Aug 2023	02 Sept 2023	5	02 Sept 2023
Sprint-2	5	5 Days	28 Aug 2023	02 Sept 2023	5	02 Sept 2023
Sprint-3	3	5 Days	05 Sept 2023	10 Sept 2023	3	10 Sept 2023
Sprint-4	5	5 Days	12 Sept 2023	17 Sept 2023	5	17 Sept 2023
Sprint-5	2	5 Days	14 Sept 2023	19 Sept 2023	2	19 Sept 2023

Velocity:

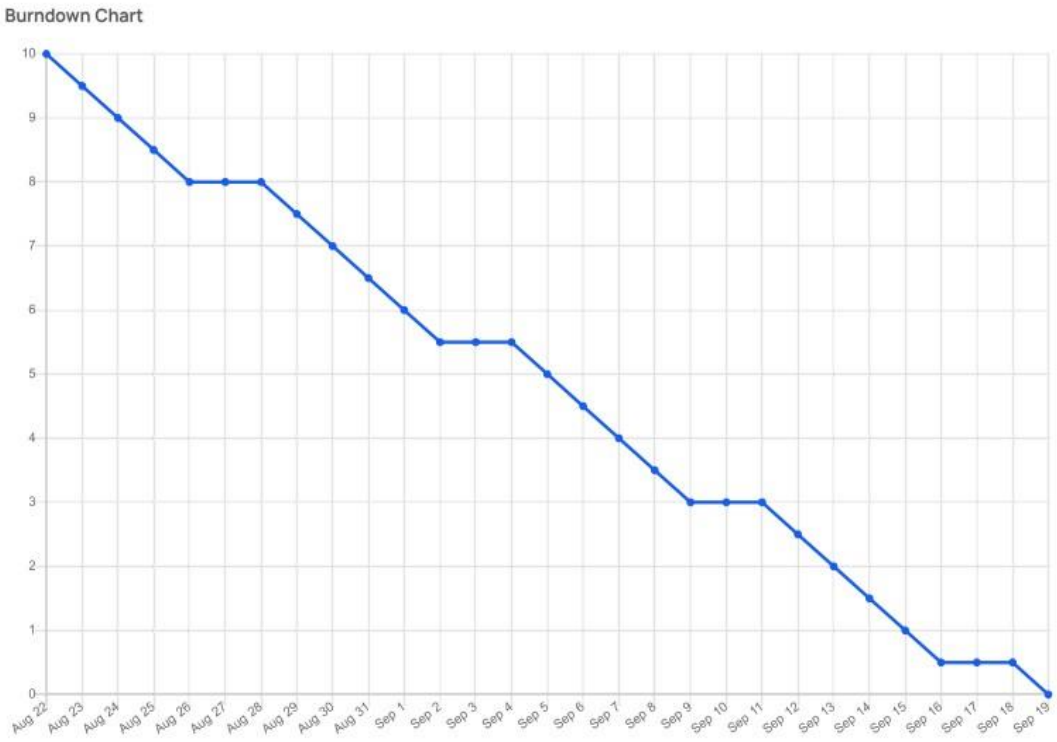
Imagine we have a 10-day sprint duration, and the velocity of the team is 20 (points per sprint). Let's calculate the team's average velocity (AV) per iteration unit (story points per day)

$$AV = \frac{sprint\ duration}{velocity} = \frac{20}{10} = 2$$

AV = (5+5+3+5+2)/5 = 20/5 = **4**

Burndown Chart:

A burn down chart is a graphical representation of work left to do versus time. It is often used in agile software development methodologies such as Scrum. However, burn down charts can be applied to any project containing measurable progress over time.



TESTING PHASE

TEST WEBSITE VULNERABILITIES TESTING REPORT

Sites Used:

1. http://testfire.net/
2. https://juice-shop.herokuapp.com/#/

1) SQL Injection vulnerability allowing login bypass

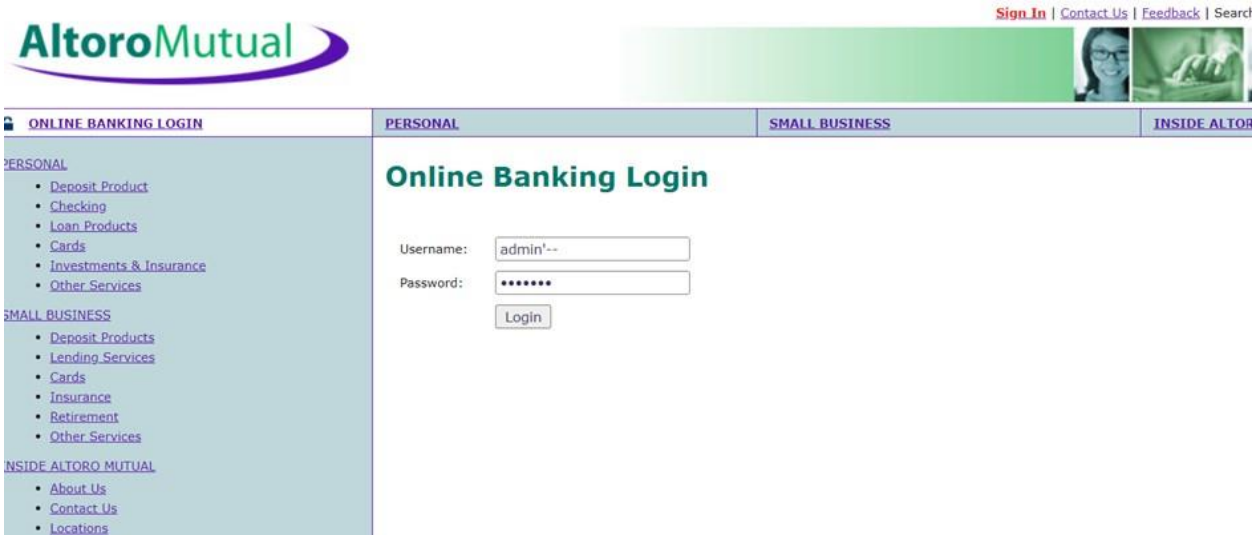
CWE-288: Authentication Bypass Using an Alternate Path or Channel

Description: A product requires authentication, but the product has an alternate path or channel that does not require authentication.

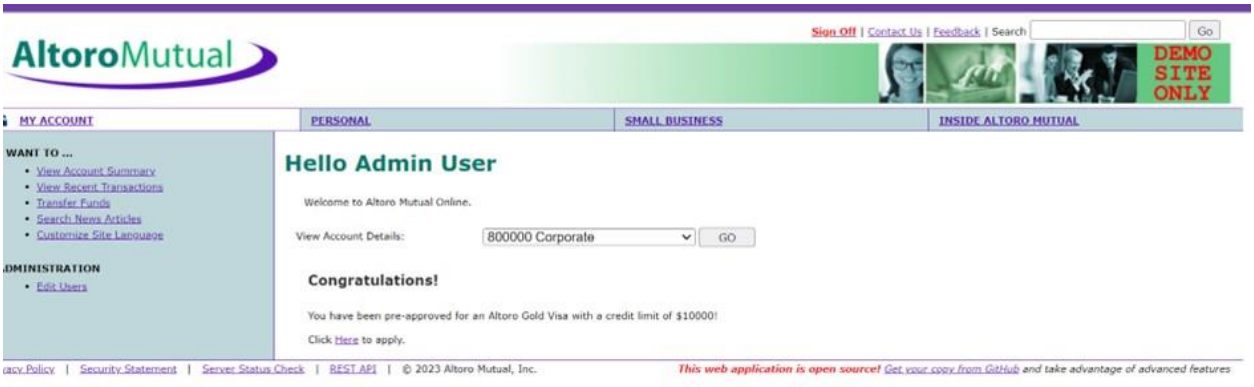
Business Impact:

SQL injection attacks represent an extreme security danger to associations. A successful SQL injection assault can bring about confidential and important information being erased, edited or taken out for malicious uses. Other risks are sites being ruined, defaced or unapproved access to frameworks or accounts and, eventually, compromised machines or whole systems.

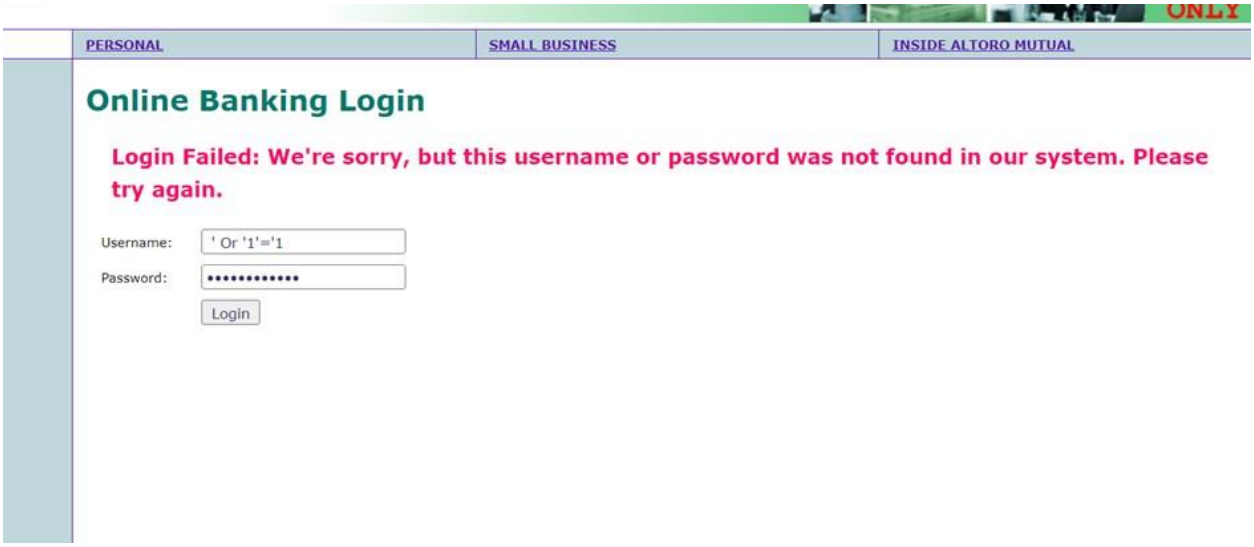
Testing:



We used the command admin'-- as the username what it signifies is that for the username administrator login into the application without checking the password because -- is used which comments out whatever is written ahead of it thus commenting out the password matching SQL query.



Some other SQL Injections that we can use can be the basic ' Or '1'='1.



2.Brute Force Attack

CWE-1391: Use of Weak Credentials

Description: The product uses weak credentials (such as a default key or hard-coded password) that can be calculated, derived, reused, or guessed by an attacker.

CWE-307: Improper Restriction of Excessive Authentication Attempts

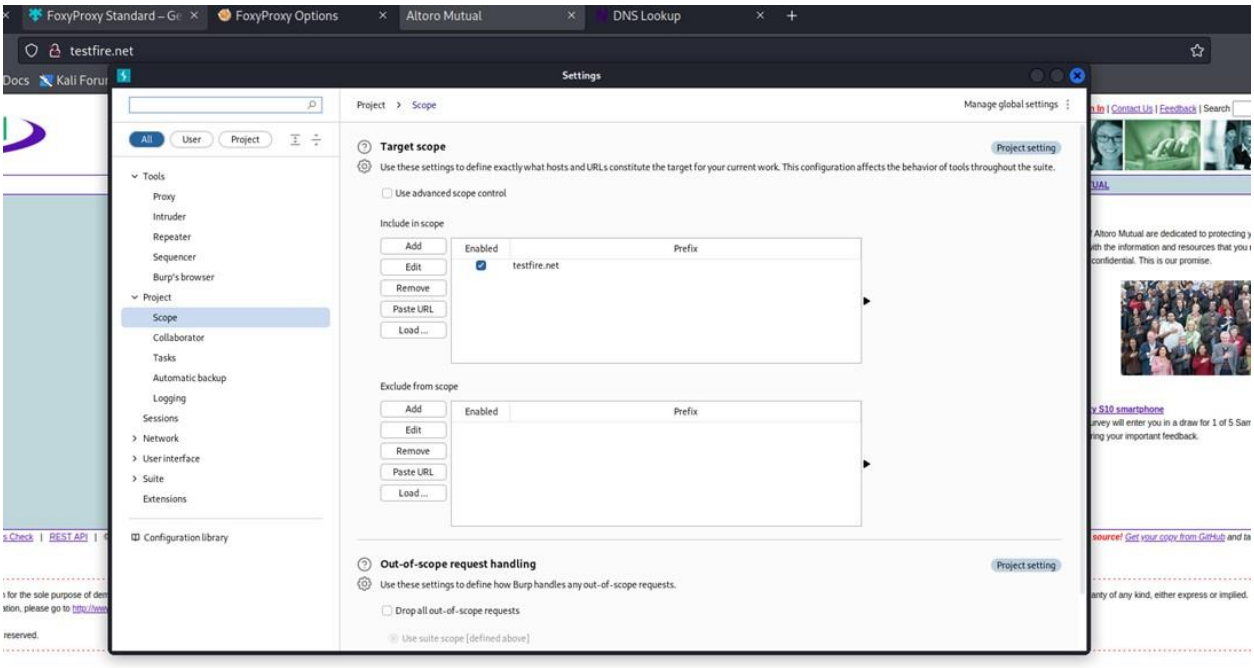
Description: The product does not implement sufficient measures to prevent multiple failed authentication attempts within a short time frame, making it more susceptible to brute force attacks.

Business Impact:

A successful brute force attack on a business can result in unauthorized access, data loss or theft, financial losses, reputational damage, legal consequences, operational disruptions, increased security costs, loss of competitive advantage, damage to trust with customers and partners, and compliance issues, depending on the industry.

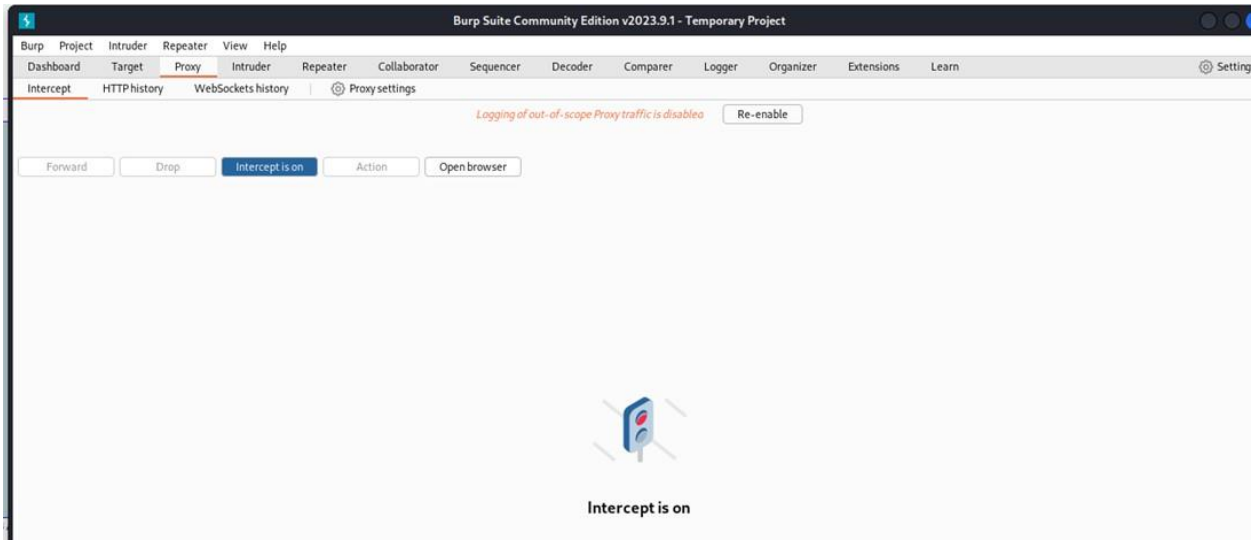
Testing:

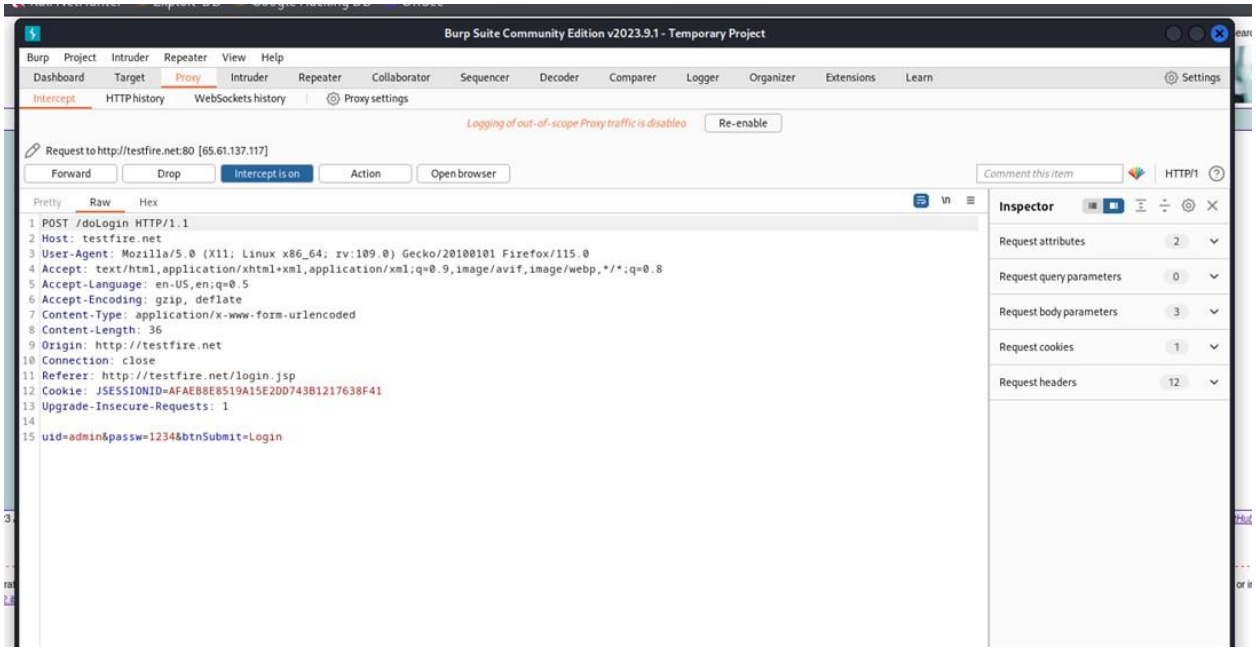
- ·First we add the website by going to target tab -> add



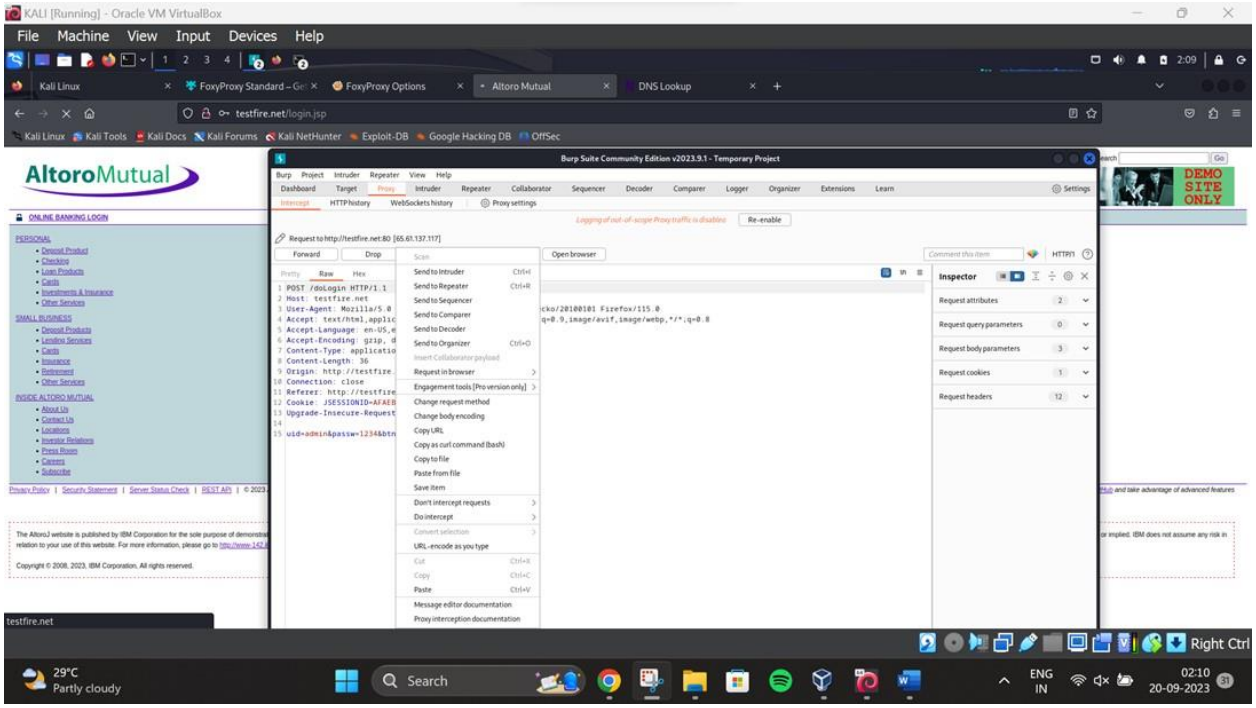
- ·Choose burp as our default proxy on foxyproxy.

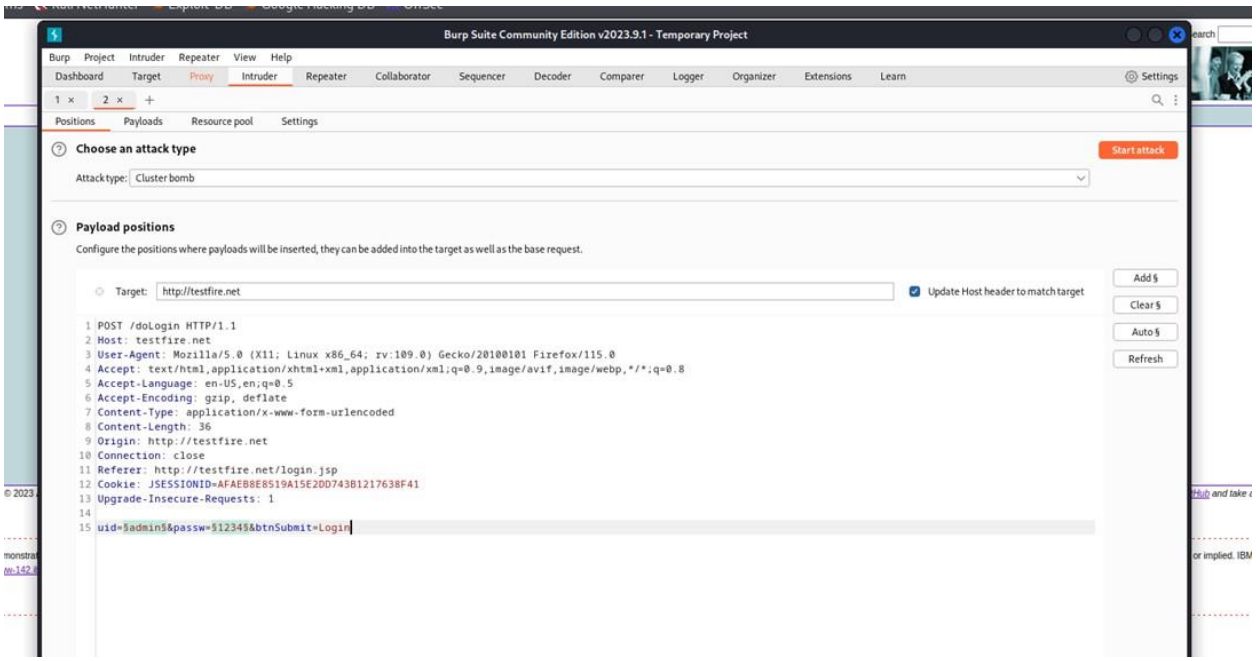
- Go to proxy and turn on the intercept and then click on the login page of the website and give in random username and password.



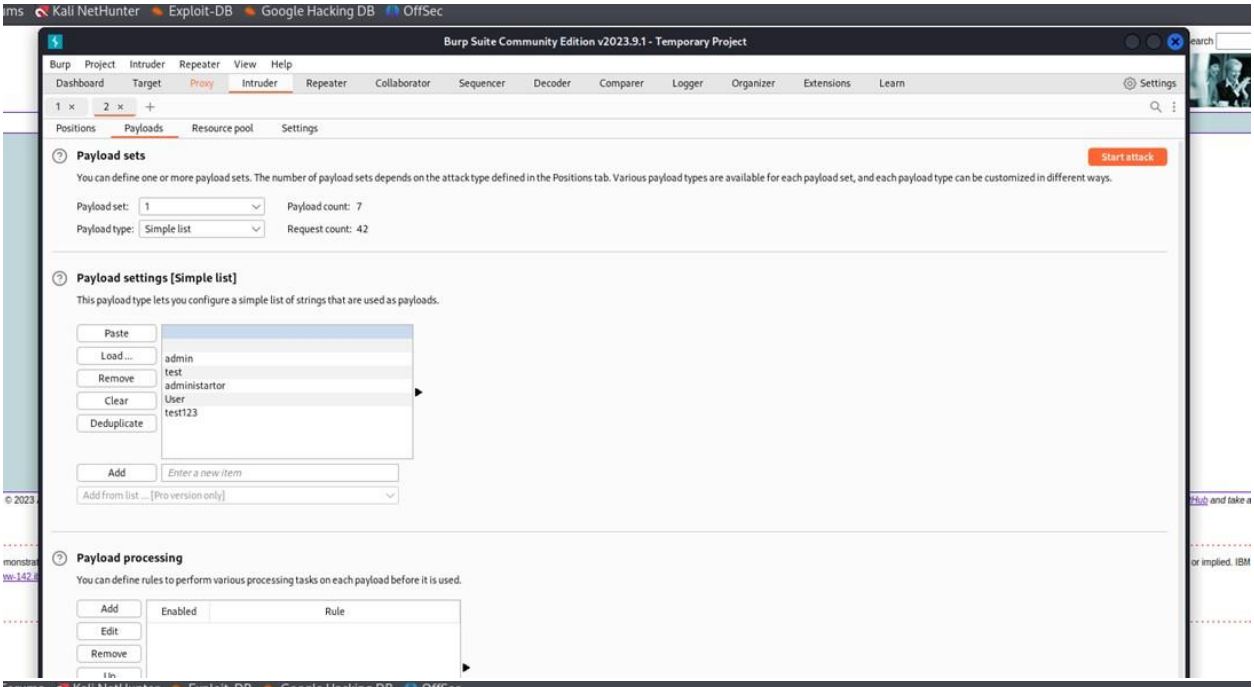


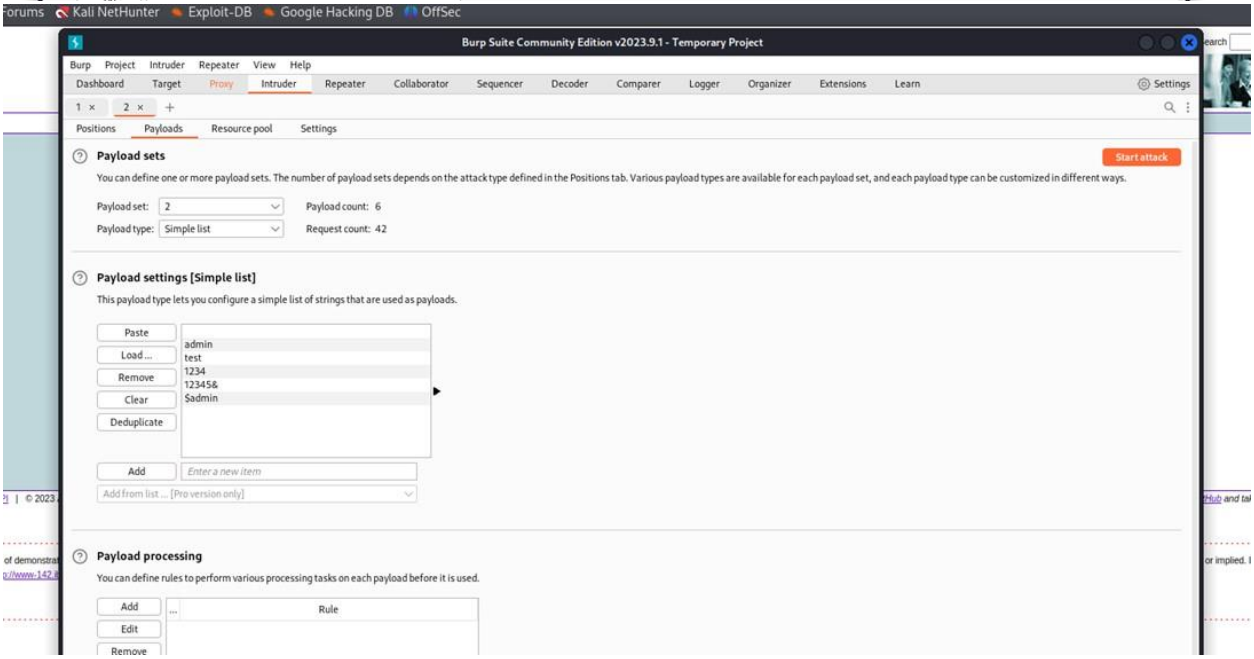
- Then we send it to intruder and go to positions tab choose cluster bomb attack and select the given input of username as payload 1 and given input of password as payload 2 by clicking on add.


KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
FoxyProxy Standard
FoxyProxy Options
Altoro Mutual
DNS Lookup
testfire.net/login.jsp
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
DEMO SITE ONLY
Burp Suite Community Edition v2023.9.1 - Temporary Project
Request to http://testfire.net:80 [65.61.137.117]
Forward
Drop
Open browser
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Send to Intruder
Send to Repeater
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
URL-encode as you type
Cut
Copy
Paste
Message editor documentation
Proxy interception documentation
testfire.net
Right Ctrl
29°C
Partly cloudy
Search
ENG
IN
02:10
20-09-2023

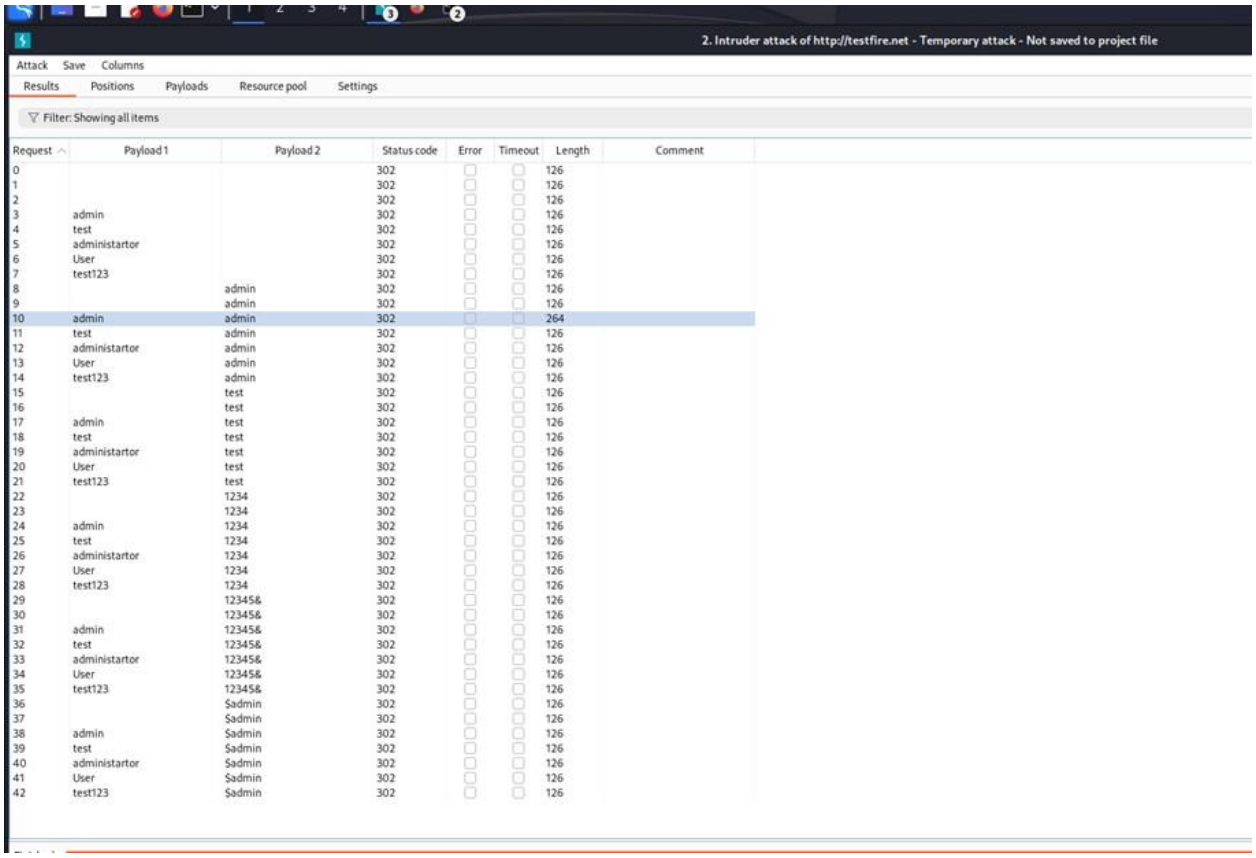

Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
Attack type: Cluster bomb
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://testfire.net
Update Host header to match target
Add §
Clear §
Auto §
Refresh
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=AFAEB8E8S19A15E2DD743B1217638F41
Upgrade-Insecure-Requests: 1
uid=§admin§&passw=§1234§&btnSubmit=Login

- Then we go to the payloads tab and select payload 1 that is our username in this case and choose simple text and below give some random expected usernames. We can also upload a file here but since I do not have one I did it this way. We do the same for payload 2 which is our passwords and then start the attack.

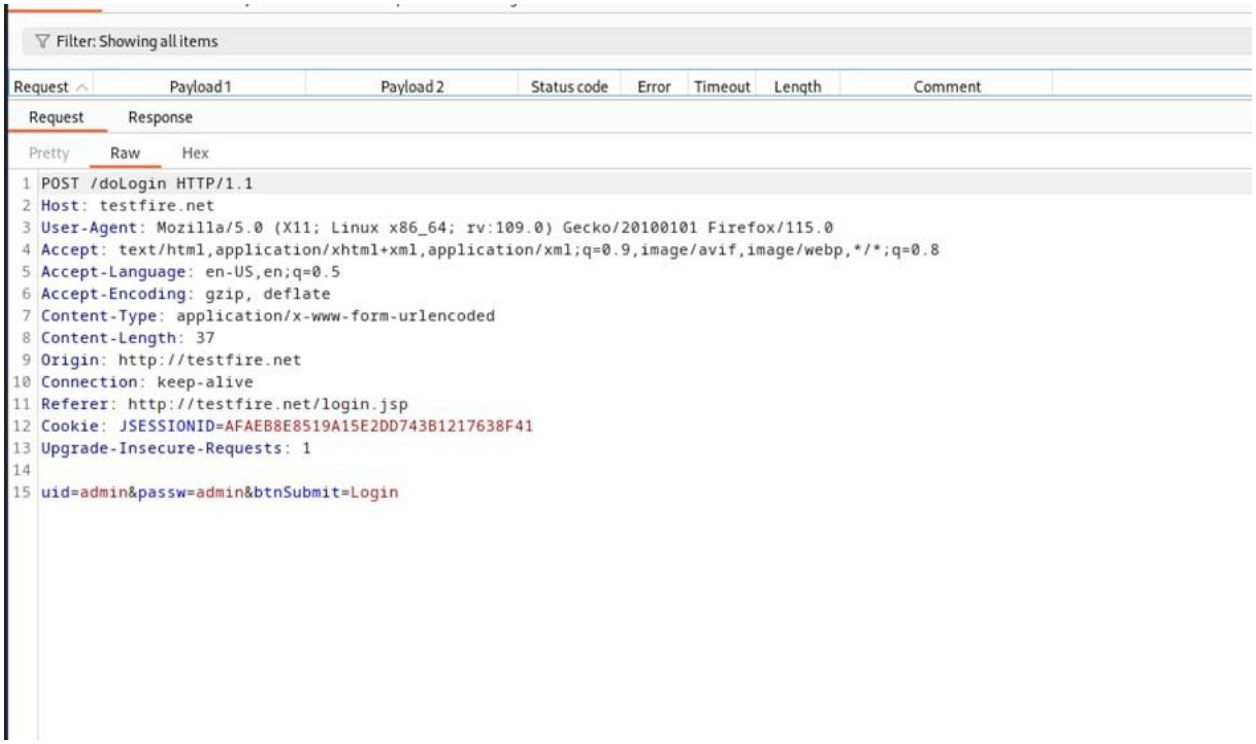




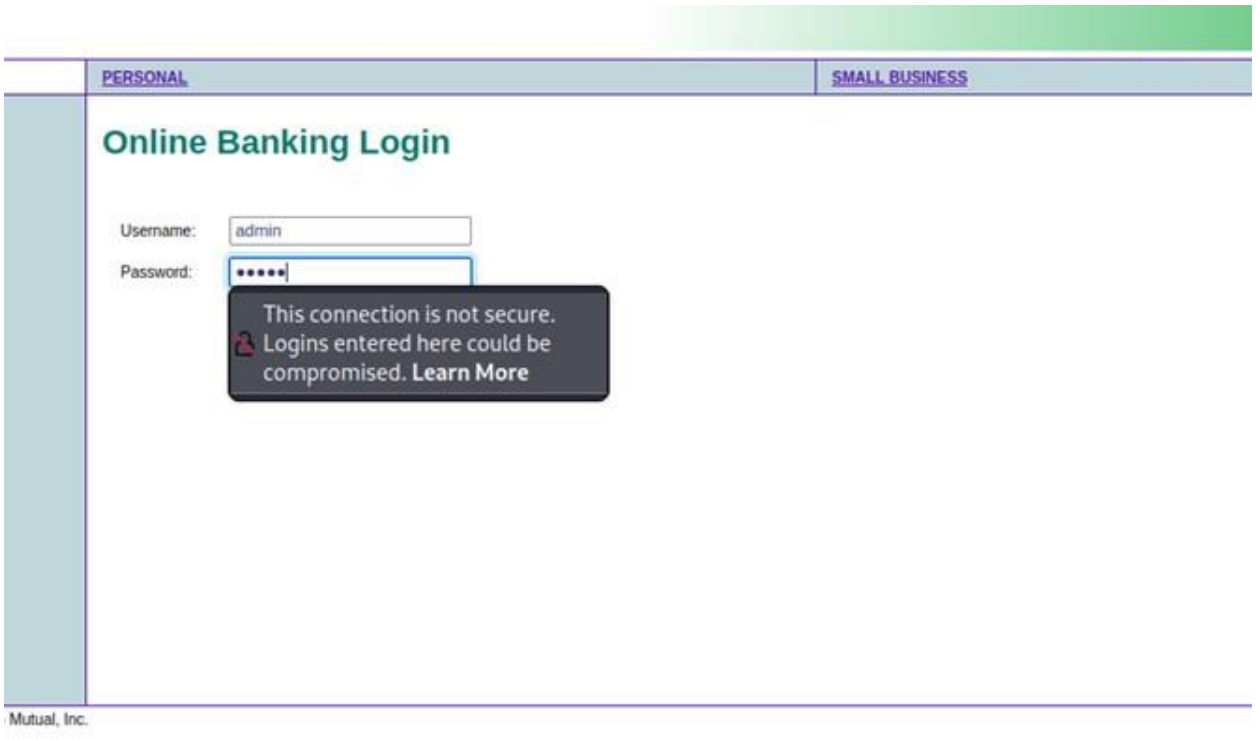
- After the attack is finished we can see that the highlighted admin has different length from the others. Thus it can be a probable solution. Upon checking Request and response we can assure that this is working.

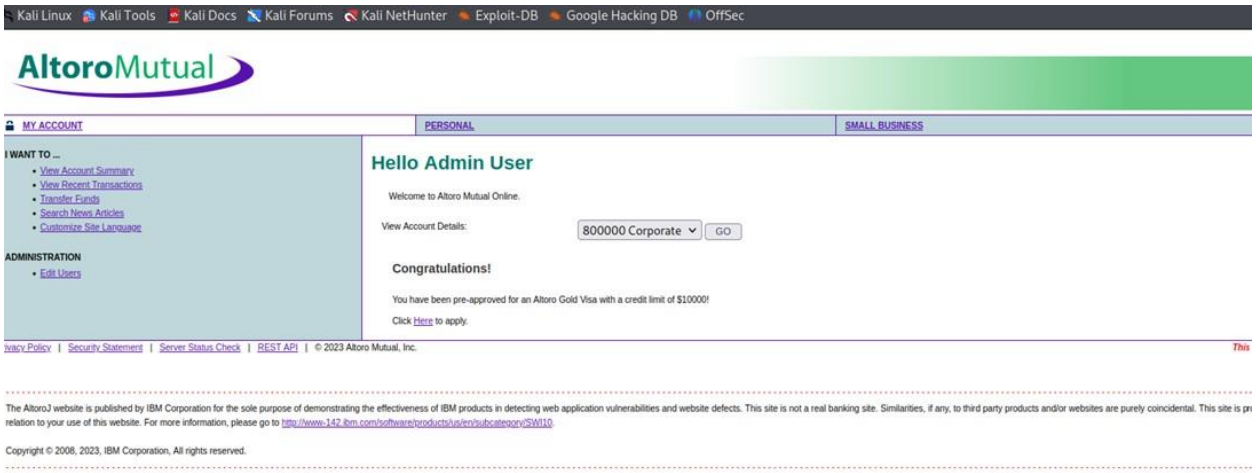


Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			302			126	
1			302			126	
2			302			126	
3	admin		302			126	
4	test		302			126	
5	administartor		302			126	
6	User		302			126	
7	test123		302			126	
8		admin	302			126	
9		admin	302			126	
10	admin	admin	302			264	
11	test	admin	302			126	
12	administartor	admin	302			126	
13	User	admin	302			126	
14	test123	admin	302			126	
15		test	302			126	
16		test	302			126	
17	admin	test	302			126	
18	test	test	302			126	
19	administartor	test	302			126	
20	User	test	302			126	
21	test123	test	302			126	
22		1234	302			126	
23		1234	302			126	
24	admin	1234	302			126	
25	test	1234	302			126	
26	administartor	1234	302			126	
27	User	1234	302			126	
28	test123	1234	302			126	
29		12345&	302			126	
30		12345&	302			126	
31	admin	12345&	302			126	
32	test	12345&	302			126	
33	administartor	12345&	302			126	
34	User	12345&	302			126	
35	test123	12345&	302			126	
36		$admin	302			126	
37		$admin	302			126	
38	admin	$admin	302			126	
39	test	$admin	302			126	
40	administartor	$admin	302			126	
41	User	$admin	302			126	
42	test123	$admin	302			126	



- We then give the inputs in the login page and hence we are logged in.


PERSONAL
SMALL BUSINESS
Online Banking Login
Username:
admin
Password:
This connection is not secure. Logins entered here could be compromised. Learn More
Mutual, Inc.


Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
AltoroMutual
MY ACCOUNT
PERSONAL
SMALL BUSINESS
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
Edit Users
Hello Admin User
Welcome to Altoro Mutual Online.
View Account Details:
800000 Corporate
GO
Congratulations!
You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!
Click Here to apply.
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is pr
relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SW110.
Copyright © 2008, 2023, IBM Corporation, All rights reserved.

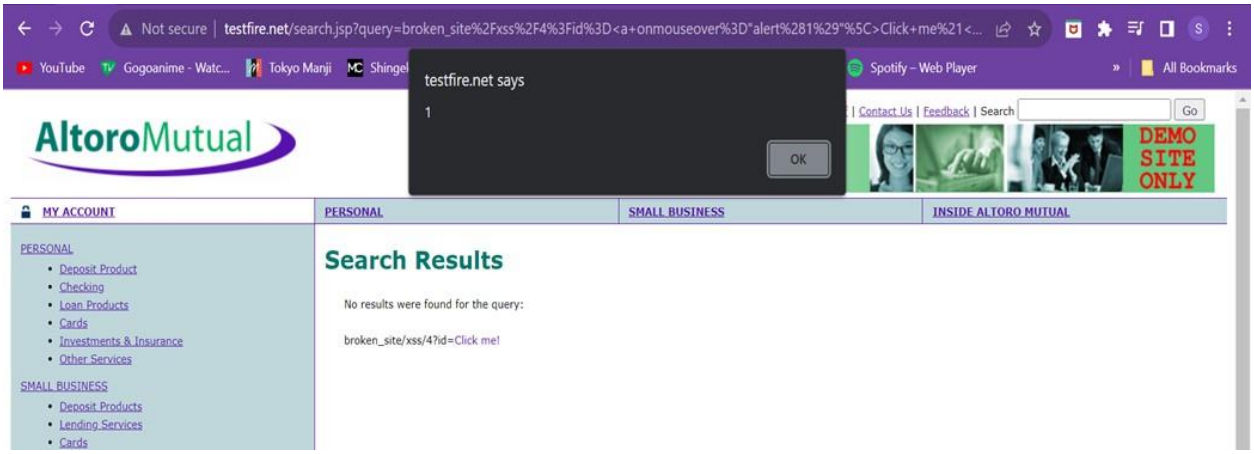
3.Cross Site Scripting (XSS)

CWE-87: Improper Neutralization of Alternate XSS Syntax

Description: The product does not neutralize or incorrectly neutralizes user-controlled input for alternate script syntax.
Business Impact: Cross-Site Scripting (XSS) attacks in business can lead to data theft, user trust erosion, reputation damage, financial losses, legal consequences, operational disruptions, increased security costs, loss of competitive advantage, and customer trust issues.

Testing:

Injecting a basic a tag and seeing how the site reacts to that. Payload is **broken_site/xss/4?id=Click me!**. What we do here is basically create a link that says click me, and when we hover the mouse over it, the alert box should execute.



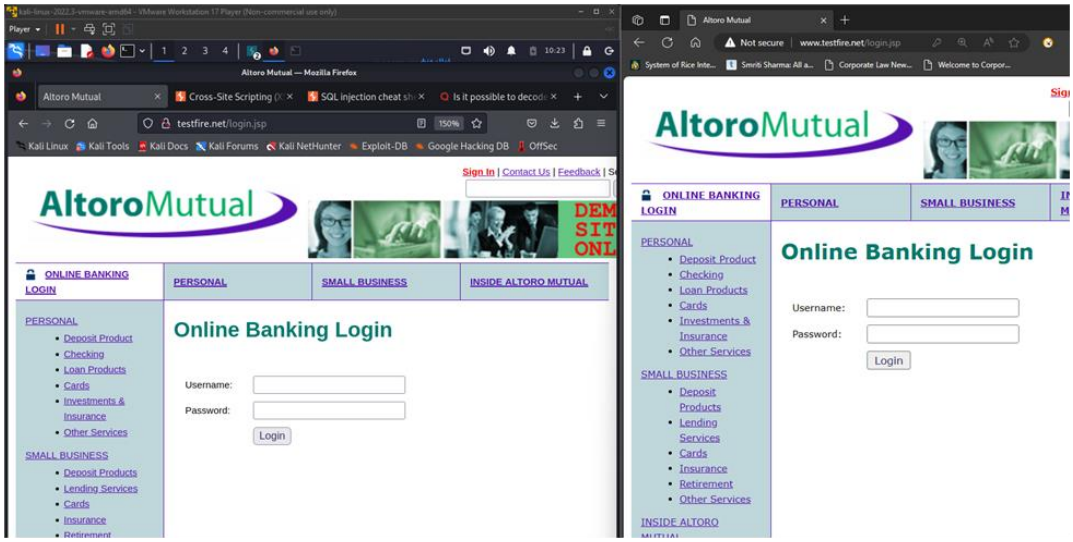
4. Improper Session Management

CWE ID for Session Fixation: CWE-384 (Session Fixation)

Description: Attacker sets or fixes a user's session ID, leading to unauthorized access. This can occur when session management is improperly implemented or lacks adequate security controls.

Business Impact: The business impact of CWE-384 (Session Fixation) can be significant, potentially leading to unauthorized access to user accounts. This can result in data breaches, loss of sensitive information, reputation damage, and financial losses due to legal and remediation costs.

Testing:

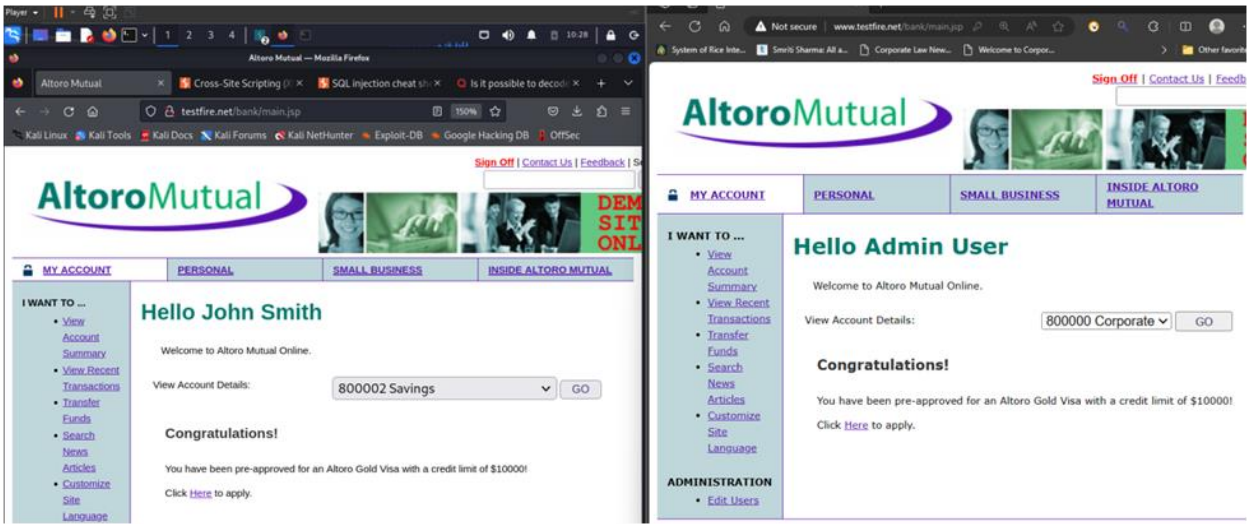


We have accessed the testfire.net website on two different browsers(one on virtual machine and another on main device).

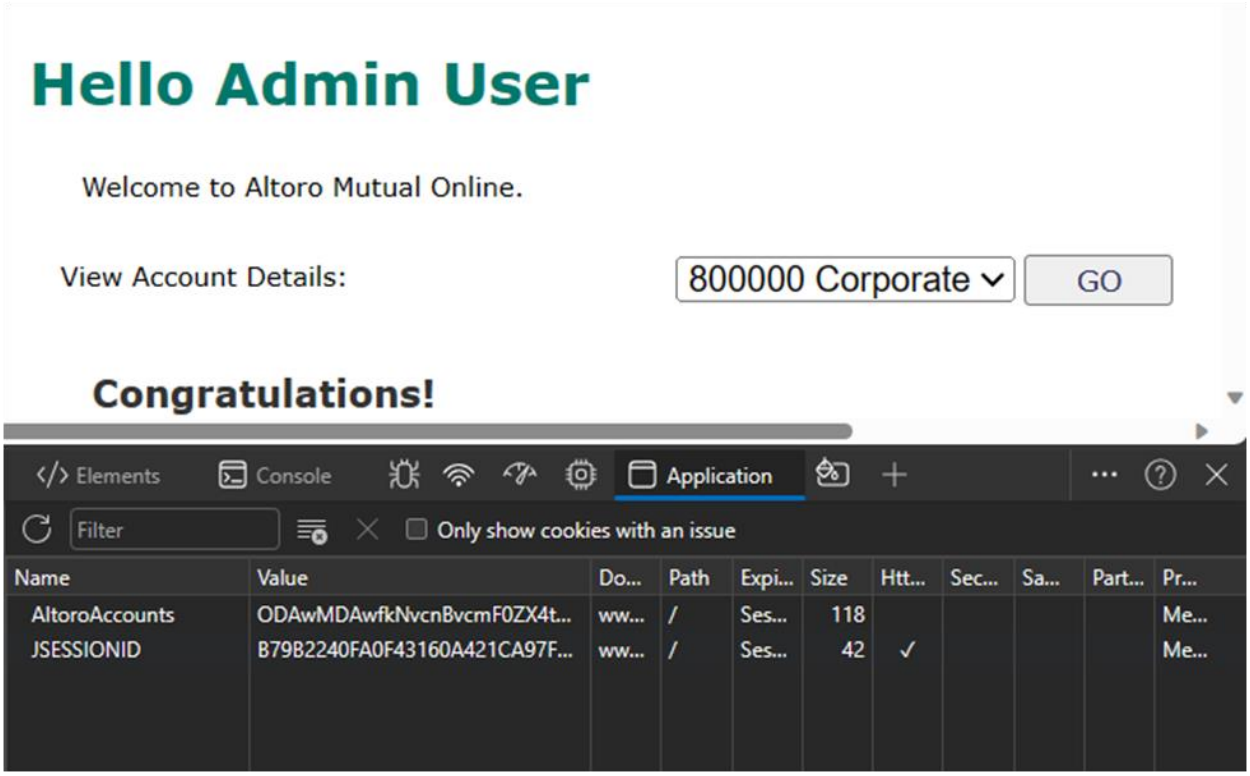
We will login as admin (u_name = admin && pass = admin) in the main machine and as John Smith (u_name = jsmith && pass = Demo1234) in the virtual machine.

Post login, we will fetch the JSESSION_ID of admin logged in account and copy that, intercept a request in the John Smith's account and replace John Smith's Session Id with admin's.

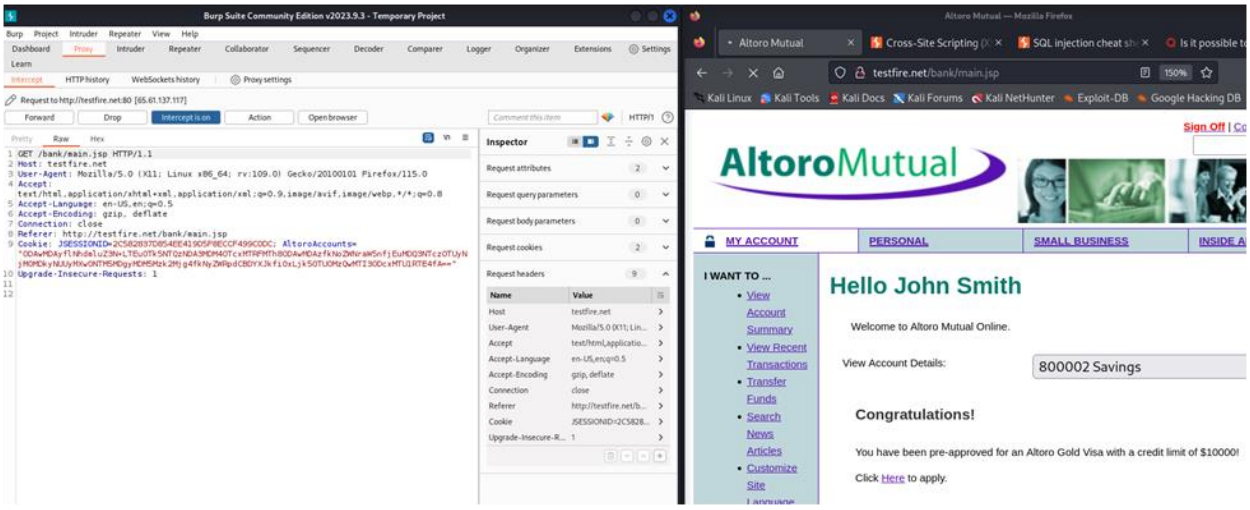
If we are able to access the admins account after this then we could possibly say that theres a security flaw of insecure Session management.



- Logged in to respective accounts.



- Fetched the Admin Session ID value.(B79B2240FA0F43160A421CA97F1343C6)



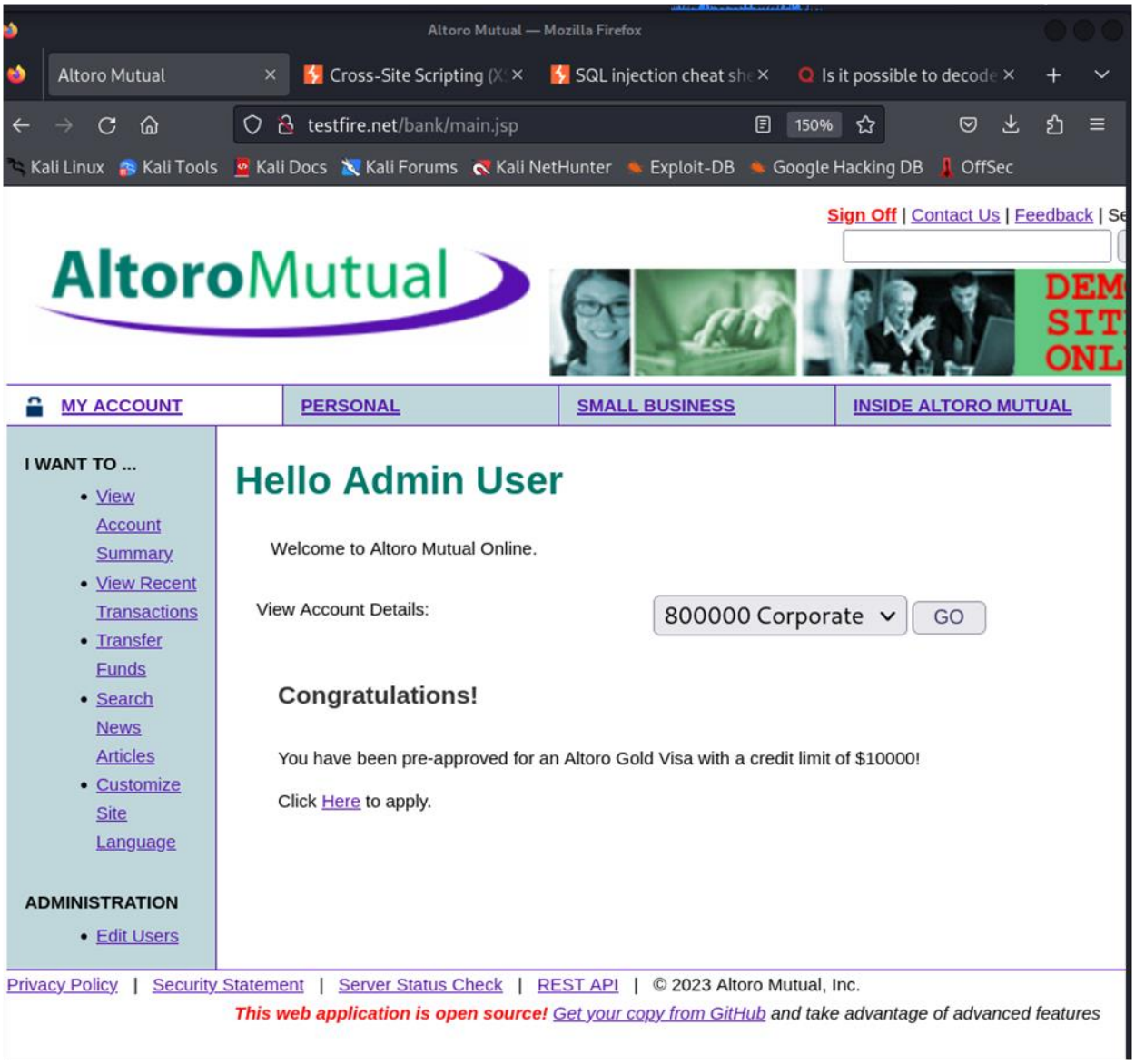
- Intercepted a request from John Smith's account.

```
1  GET /bank/main.jsp HTTP/1.1
2  Host: testfire.net
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://testfire.net/bank/main.jsp
9  Cookie: JSESSIONID=2C582837D854EE419D5F8ECCF499C0DC; AltoroAccounts=
   "ODAwMDAyflNhdmluZ3N+LTEuOTk5NTQzNDA3MDM4OTcxMTRFMTh8ODAwMDAzfkNoZWNraW5nfjEuMDQ3NTczOTUyN
   jM0MDkyNUUyMXw0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI3ODcxMTUlRTE4fA=="
10 Upgrade-Insecure-Requests: 1
11
12
```

- The intercepted request has JSESSIONID value as 2C582837D854EE419D5F8ECCF499C0DC

Pretty Raw Hex \n

```
1  GET /bank/main.jsp HTTP/1.1
2  Host: testfire.net
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://testfire.net/bank/main.jsp
9  Cookie: JSESSIONID=B79B2240FA0F43160A421CA97F1343C6; AltoroAccounts=
   "ODAwMDAyflNhdmluZ3N+LTEuOTk5NTQzNDA3MDM4OTcxMTRFMTh8ODAwMDAzfkNoZWNraW5nfjEuMDQ3NTczOTUyN
   jM0MDkyNUUyMXw0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI3ODcxMTUlRTE4fA=="
10 Upgrade-Insecure-Requests: 1
11
12
```



· Replaced the JSESSIONID with that of admin's

Logged in as admin

5.Broken Access Control:

CWE-284: Improper Access Control.

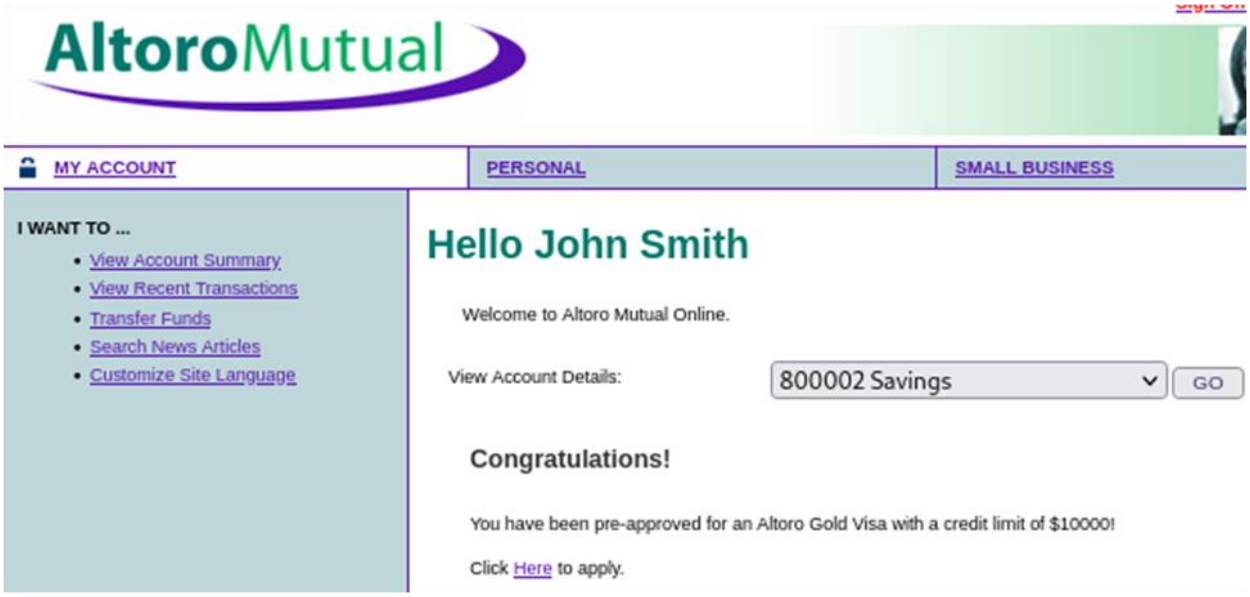
Description: The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

Business Impact:

Data Breaches, Loss of Confidential Information, Financial Loss, Reputation Damage, Regulatory Compliance Issues, Operational Disruption, Lawsuits and Legal Liabilities, Resource Wastage, Loss of Competitive Advantage, Customer Trust Erosion **Testing:**

We will first login as john smith and then try to access a bank account linked to any other user to view their transaction by modifying the url parameter (IDOR attack).

- Logged in as John Smith

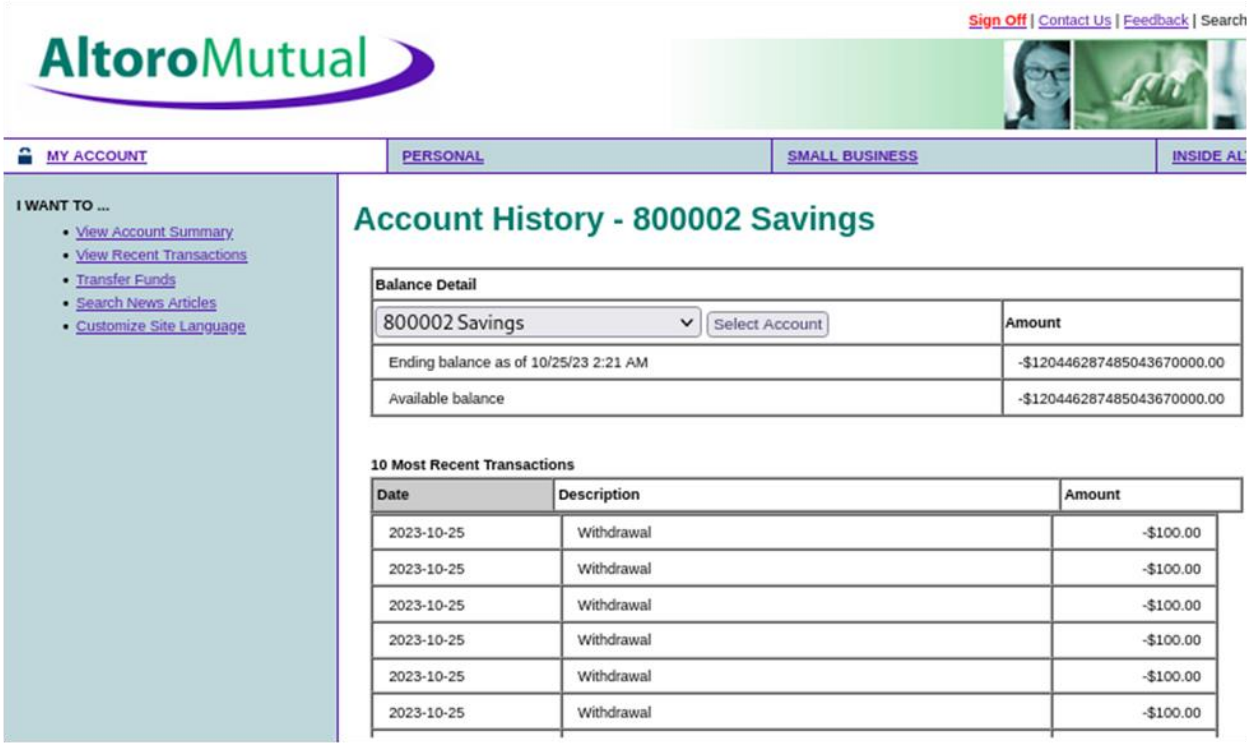


Here if we go to the view account summary section, we will notice an option to search the account history of all the accounts we posses. John Smith has access to the following accounts:

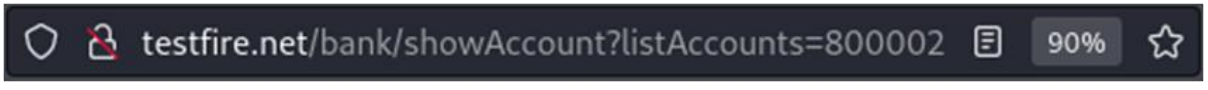
- 800002 – Savings
- 800003 – Checking
- 4539082039396288 – Credit card

If we access his Savings account, we notice account history where the 10 most recent transactions are of $100 each.

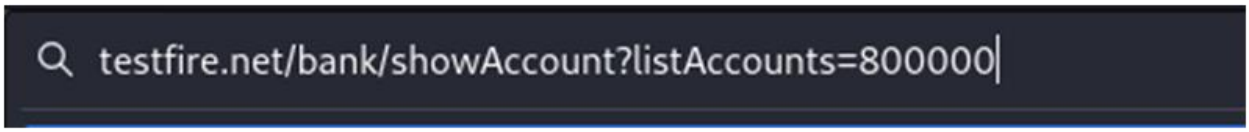
Having a look at the URL we can see the request parameter to be as listAccount=800002.



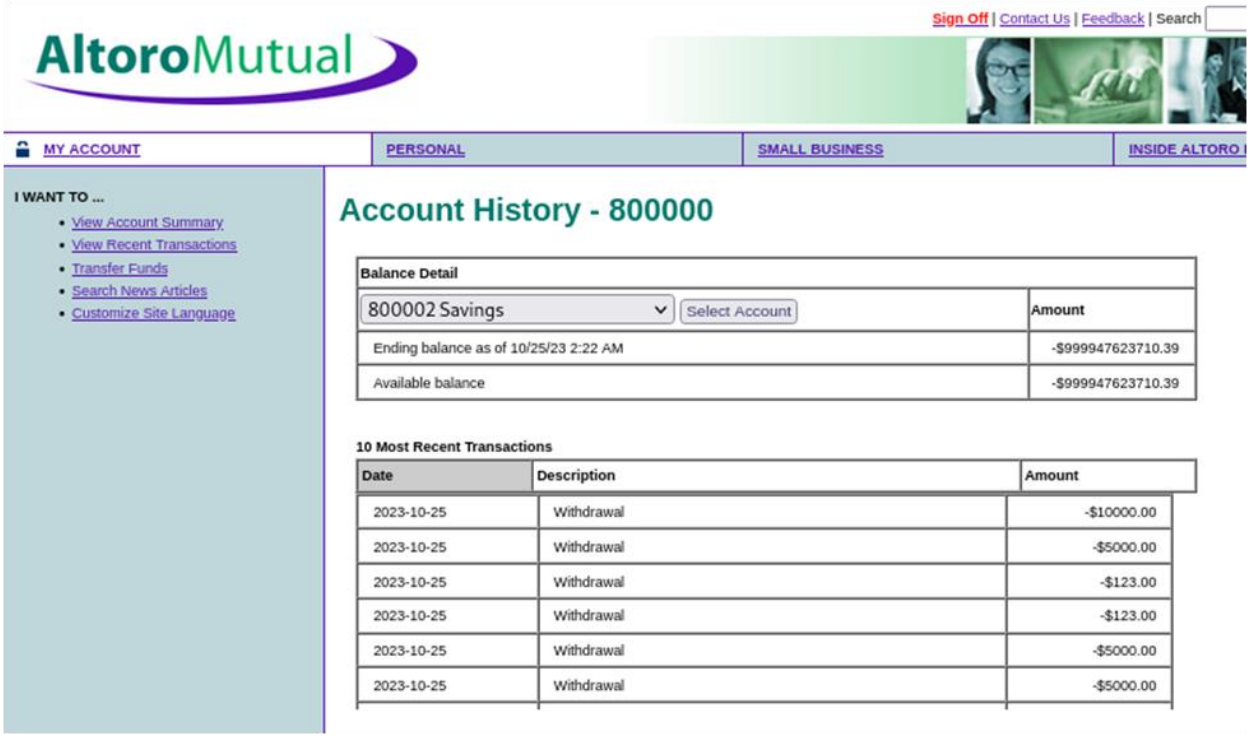
John Smith's Savings account's URL -



From here if we modify the URL to the one shown in the image below with account 800000 which technically doesn't belong to john smith (800000 Belongs to the admin user), we shouldn't be able to access it.



If we send this url request to the server we get a 200 OK response and apparently we are able to view the transaction history of account number 800000 as all the recent transaction values have changed.



Hence we have successfully exploited the IDOR (InDirect Object Reference) vulnerability.

6. HTML injection attack + ClickJacking

CWE=601: URL Redirection to untrusted site('Open Redirect')

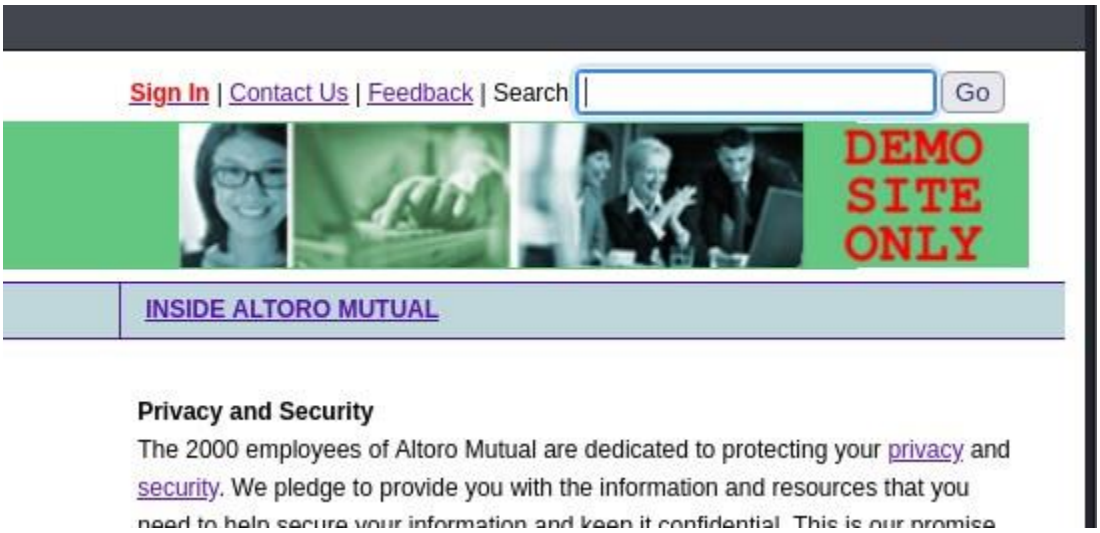
Description: A web application accepts a user-controlled input that specifies a link to an external site, and uses that link in a Redirect. This simplifies phishing attacks.

Business Impact:

The impact of CWE-601 (Open Redirect) includes loss of trust, data breaches, financial loss, legal consequences, brand damage, and operational disruption.

Here a combination of man in the middle attack and html injection can be used to inject an html payload that can return a link to a malicious copy of the login page of the legitimate website seeking the credentials from the user.

The search bar is vulnerable to html injection



HTML payload:

click here to login
This payload's href link can be modified in certain way that it redirects to the malicious login page.

Executing the payload gives the following result.

When the click here to login hyperlink is clicked, we are redirected to the website that is linked to it.

7. Improper Input Validation

The website allows user to transfer amount greater than the user has in their account.

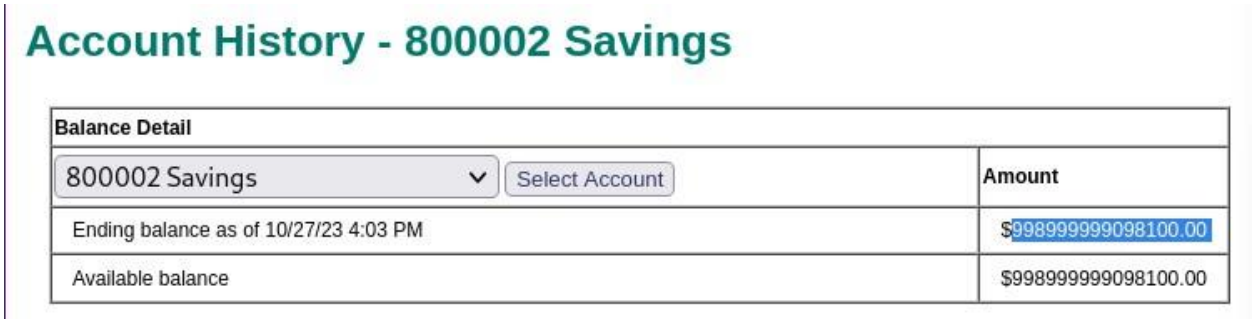
CWE (Common Weakness Enumeration): CWE-132

Business Impact:

- Financial losses: Unauthorized transfers could result in substantial financial losses for both the business and affected users.

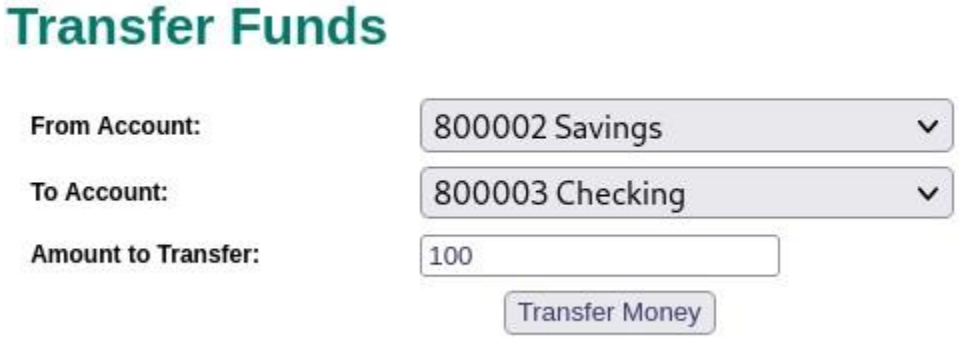
- Reputation damage: Such a security flaw can erode user trust and damage the reputation of the company.
- Legal and regulatory consequences: Violating financial regulations can result in fines and legal actions against the organization.
- Customer churn: Users may leave the platform due to concerns about their financial security.

Wearing off the account 800002.



Amount to be debited to make the account balance empty is 998999999098100

Now trying to transfer amount even after the balance has worn out.



The transfer is successful as shown and the amount is credited in the respective account.

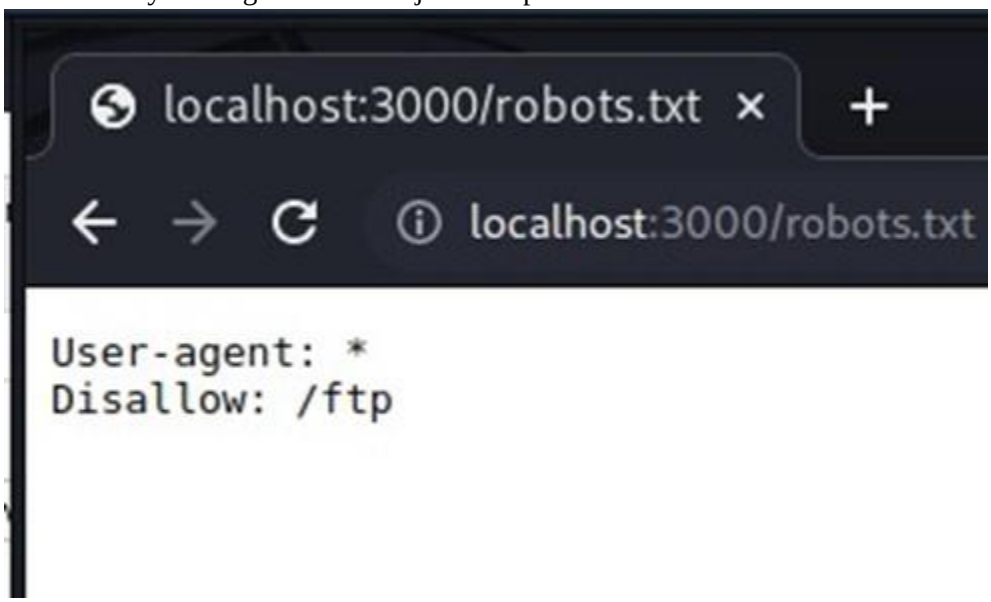
8) CRYPTOGRAPHIC FAILURE / SENSITIVE DATA EXPOSURE

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Description: The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.
Business Impact: Cryptographic failure and the subsequent exposure of sensitive data can have profound business impacts. Financially, it may result in the costs of breach investigations, data recovery, and potential fines, causing significant economic strain. The tarnishing of the company's reputation can lead to the loss of customer trust, hindering revenue generation and making it challenging to acquire new clients. Data theft or exposure can result in identity theft, fraud, and legal consequences, further compounding the overall damage to the business.

Testing:

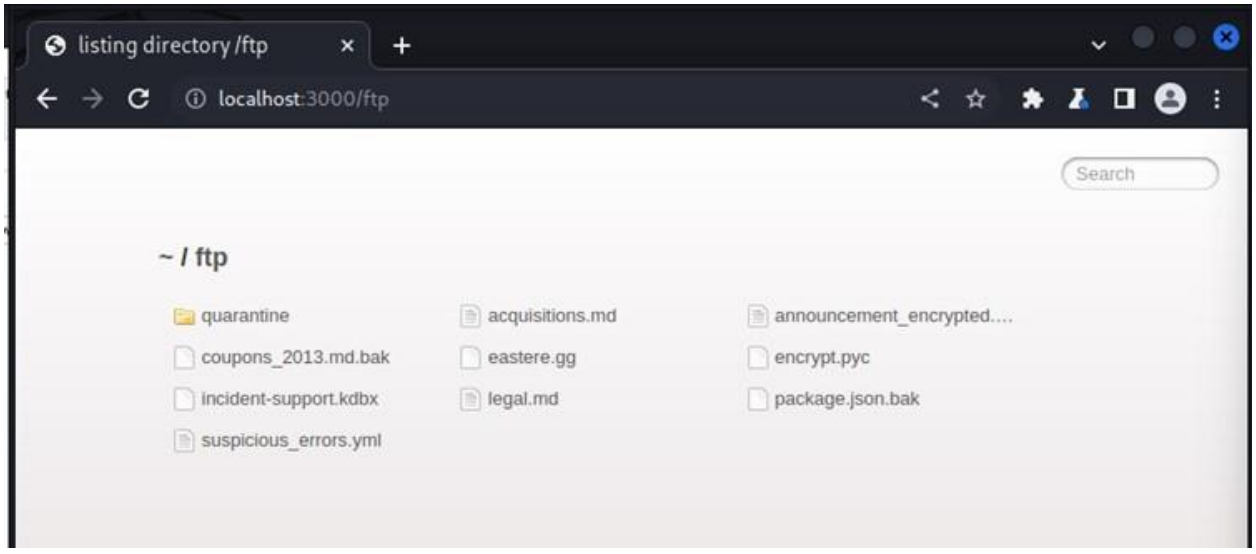
Every website has a reference page called *robots.txt* that declares the names of files/folders that should not be accessed by the browser.

We should try visiting robots.txt of juice-shop

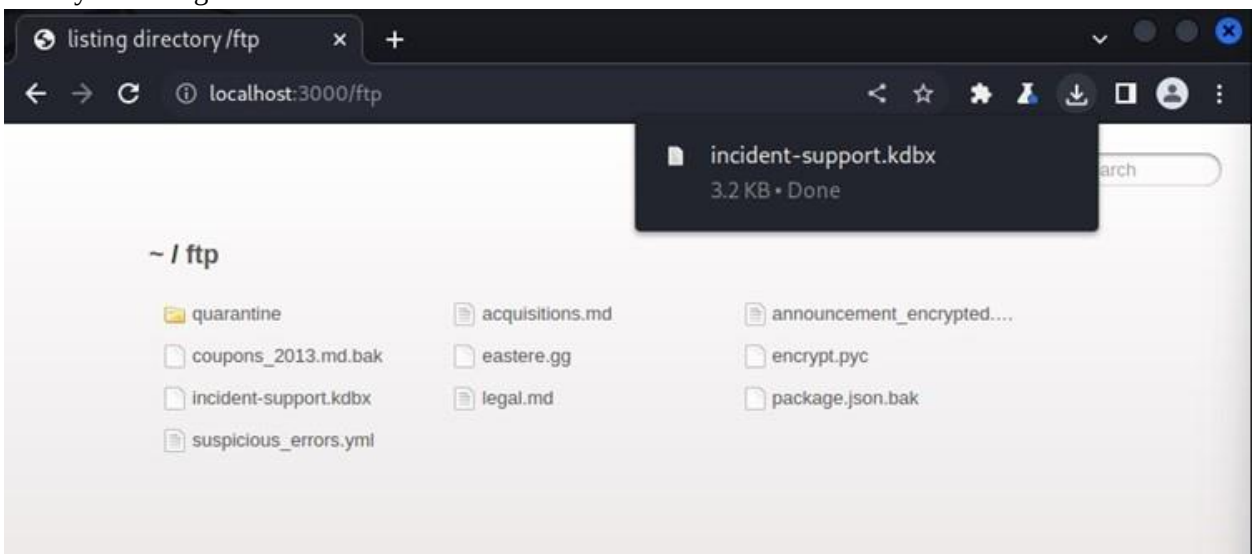


We can see no users are allowed to access the /ftp folder. So lets try accessing it from the browser url bar.

If We Try to access localhost:3000/ftp , we get a list of files and folders.

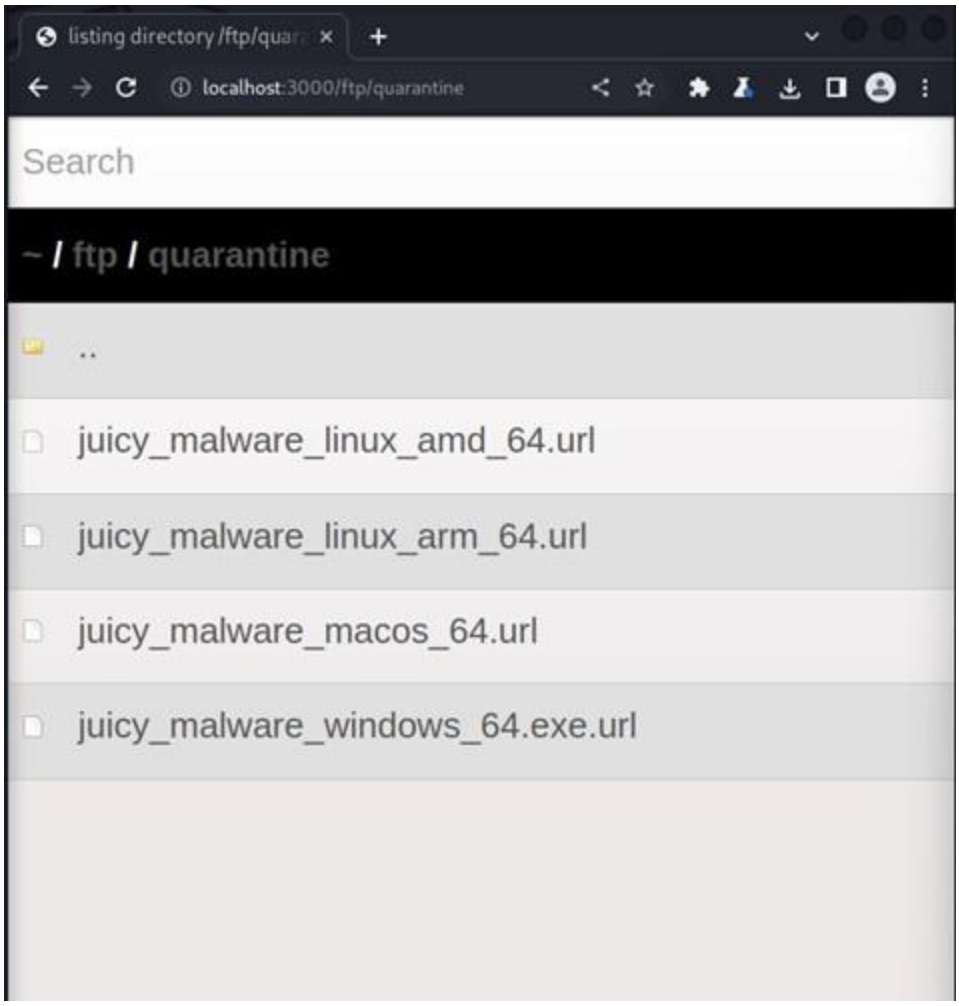


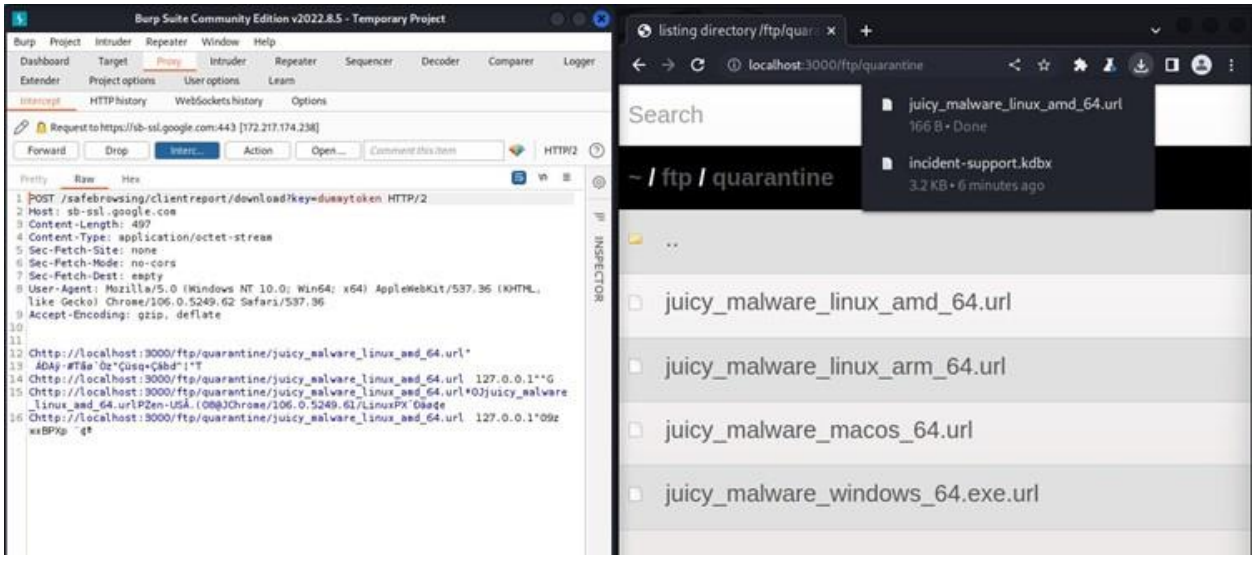
Lets try accessing a random file.



As we can see we can download incident-support.kdbx

If we try to access qurantine folder, using interceptor.


listing directory /ftp/quar
localhost:3000/ftp/quarantine
Search
~ / ftp / quarantine
..
juicy_malware_linux_amd_64.url
juicy_malware_linux_arm_64.url
juicy_malware_macos_64.url
juicy_malware_windows_64.exe.url


Burp Suite Community Edition v2022.8.5 - Temporary Project
POST /safebrowsing/clientreport/download?key=dummytoken HTTP/2
Host: sb-ssl.google.com
Content-Length: 497
Content-Type: application/octet-stream
Sec-Fetch-Site: none
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36
Accept-Encoding: gzip, deflate
Chttp://localhost:3000/ftp/quarantine/juicy_malware_linux_amd_64.url*
Chttp://localhost:3000/ftp/quarantine/juicy_malware_linux_amd_64.url 127.0.0.1**G
Chttp://localhost:3000/ftp/quarantine/juicy_malware_linux_amd_64.url*0Jjuicy_malware_linux_amd_64.url*PZen-USÁ.(08@JChrome/106.0.5249.61/LinuxPX*0aaqe
Chttp://localhost:3000/ftp/quarantine/juicy_malware_linux_amd_64.url 127.0.0.1*09z
listing directory /ftp/quar
localhost:3000/ftp/quarantine
Search
juicy_malware_linux_amd_64.url
166 B • Done
incident-support.kdbx
3.2 KB • 6 minutes ago
~ / ftp / quarantine
..
juicy_malware_linux_amd_64.url
juicy_malware_linux_arm_64.url
juicy_malware_macos_64.url
juicy_malware_windows_64.exe.url

9) Insecure Design

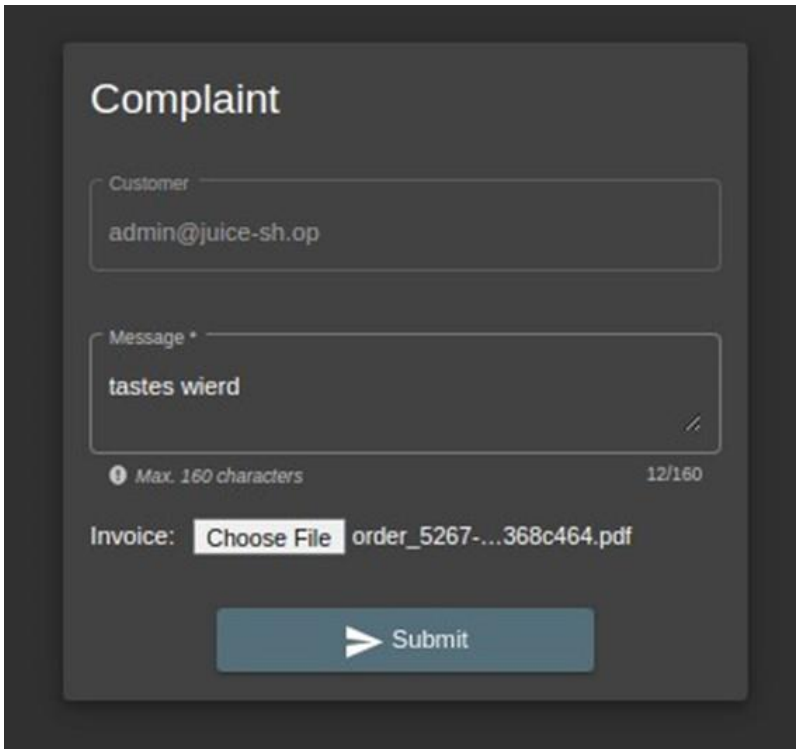
CWE-657: Violation of Secure Design Principles

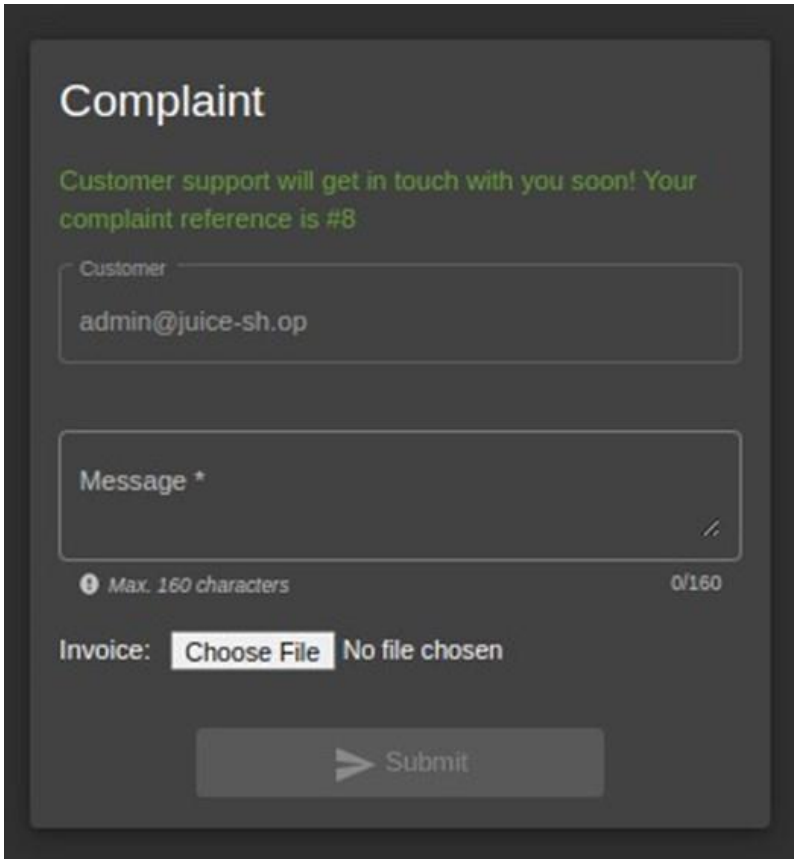
Description: The product violates well-established principles for secure design.

Business Impact: Insecure design within a business's systems and processes can have far-reaching and detrimental impacts. This includes vulnerabilities in software, network architecture, or physical security measures. First and foremost, such flaws can lead to data breaches, exposing sensitive customer information and intellectual property. The financial consequences are substantial, encompassing the costs of breach remediation, regulatory fines, and potential lawsuits. Moreover, the damage to the company's reputation can be severe, eroding customer trust and loyalty. This erosion of trust can result in decreased sales, a loss of existing clients, and difficulty in attracting new ones. Insecure design can also disrupt operations, causing downtime, which translates to lost productivity and revenue. Over time, the cumulative impact of these issues can impair the overall competitiveness and viability of the business in the marketplace. To mitigate these risks, businesses must prioritize robust security measures and adopt a proactive approach to identifying and rectifying vulnerabilities in their design and infrastructure.

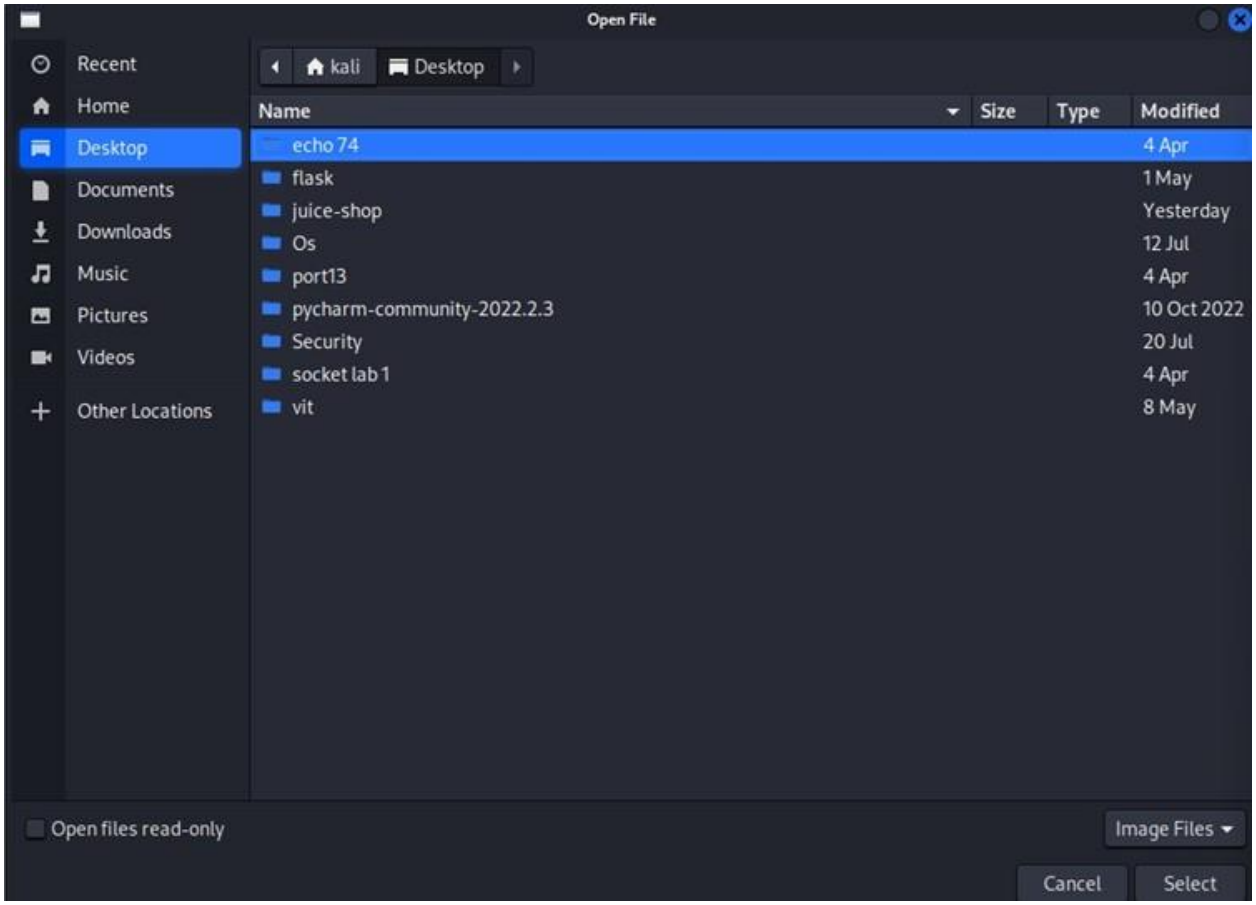
Testing:

Let's consider a situation where we can upload a file with malicious code into the server. We notice that there is a complaint upload portal where we can upload a file. What if we figure out a way to install a backdoor through that upload. Giving the upload section a closer look, we can figure out that the file upload needs to be a pdf/zip file . We can easily figure out that the upload will accept any file with extension .pdf or .zip . Lets first try uploading a .pdf file


Complaint
Customer
admin@juice-sh.op
Message *
tastes wierd
Max. 160 characters
12/160
Invoice:
Choose File
order_5267-...368c464.pdf
Submit

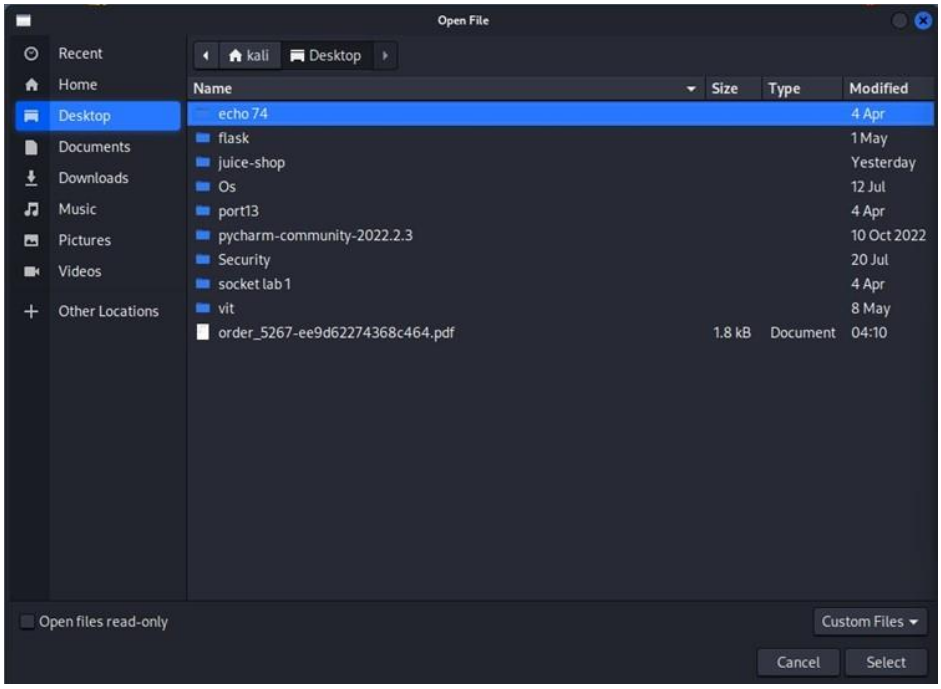

Complaint
Customer support will get in touch with you soon! Your complaint reference is #8
Customer
admin@juice-sh.op
Message *
Max. 160 characters
0/160
Invoice:
Choose File
No file chosen
Submit

The pdf document gets uploaded. Lets try uploading a file with some other extension.



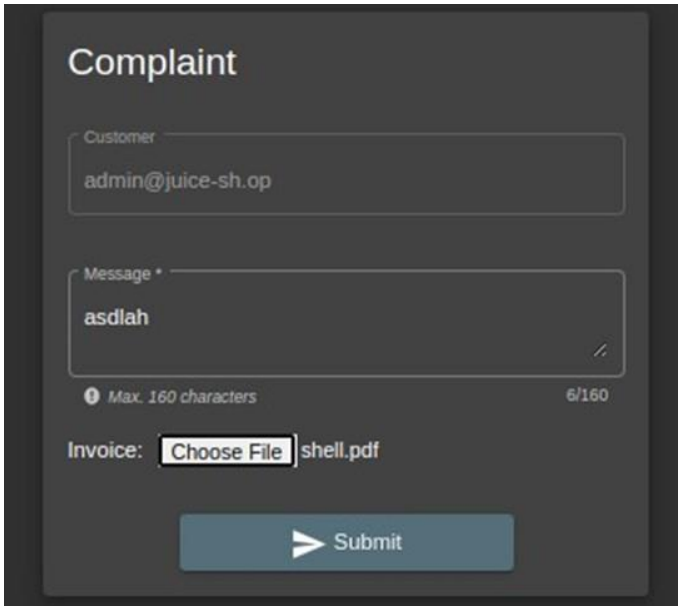
As we can see, files with extensions other than .pdf / .zip are not accessible but we do have other files with different extensions in this particular folder.

In the desktop folder I have two files with .txt extension, but the choose file section is overseeing those files. So we need to find an alternate solution. We can save the malicious file with the .pdf extension and try uploading it.

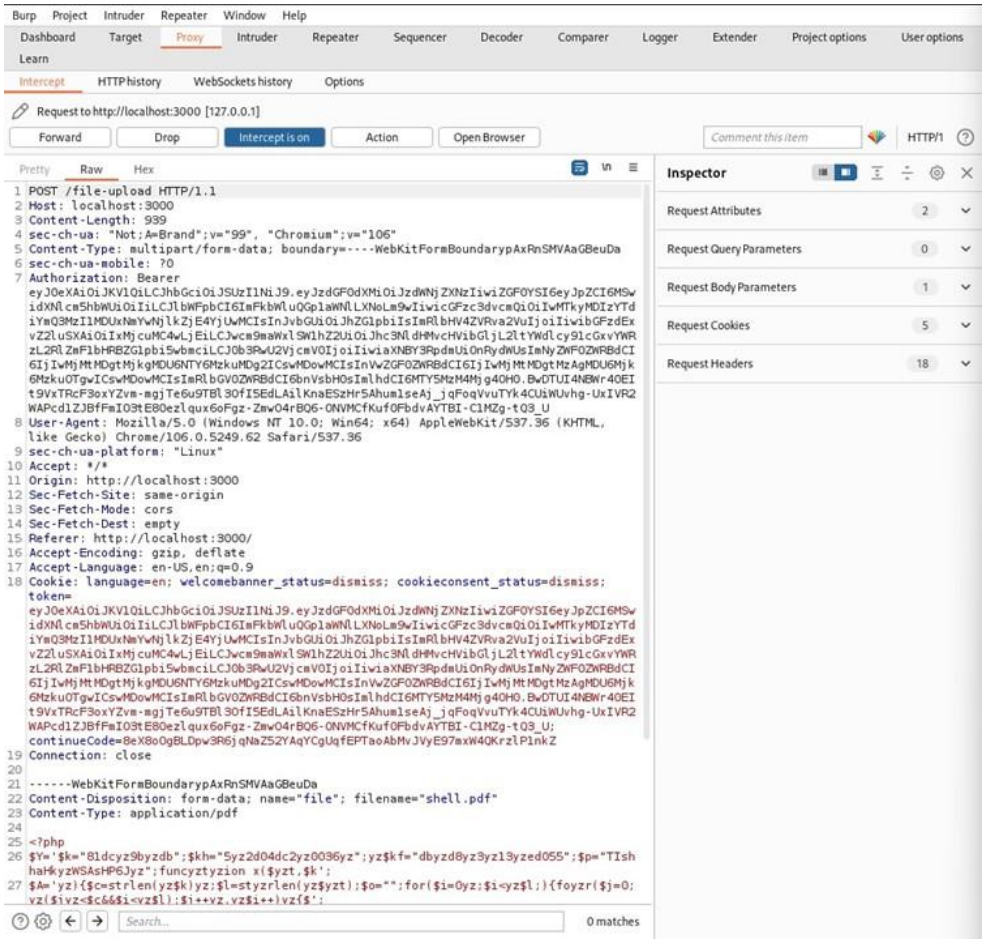


What if we build a malicious file with extension .pdf? Although the content in the pdf file will be malicious, it won't be affecting the server as without the extension it is important to denote the language in which the code should be executed.

Lets try uploading the malicious code as a .pdf extension, intercept it and then change the value to .php later. I used weevely to create a php backdoor and later changed the extension to .pdf later.



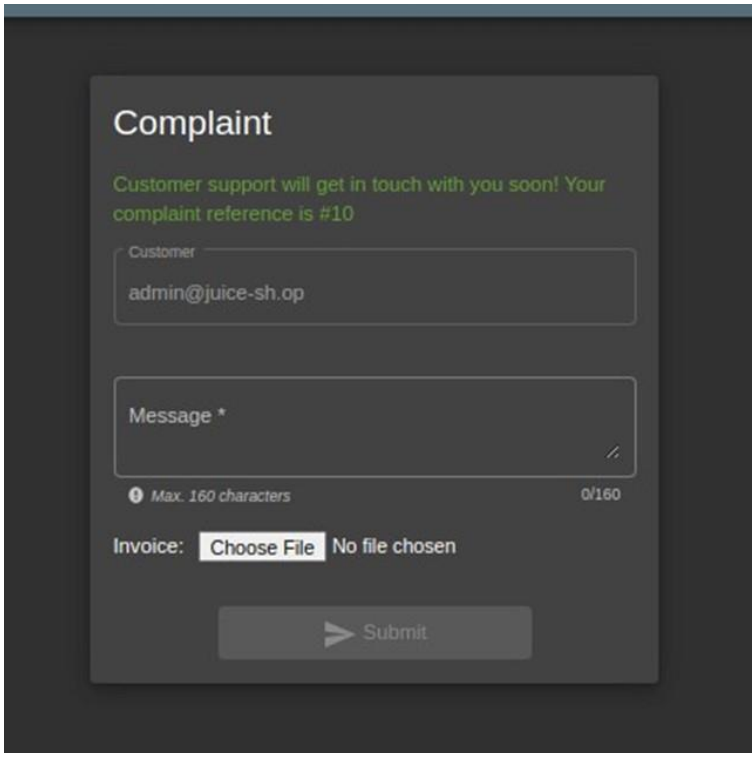
Now I turn the intercept on and press the submit button.



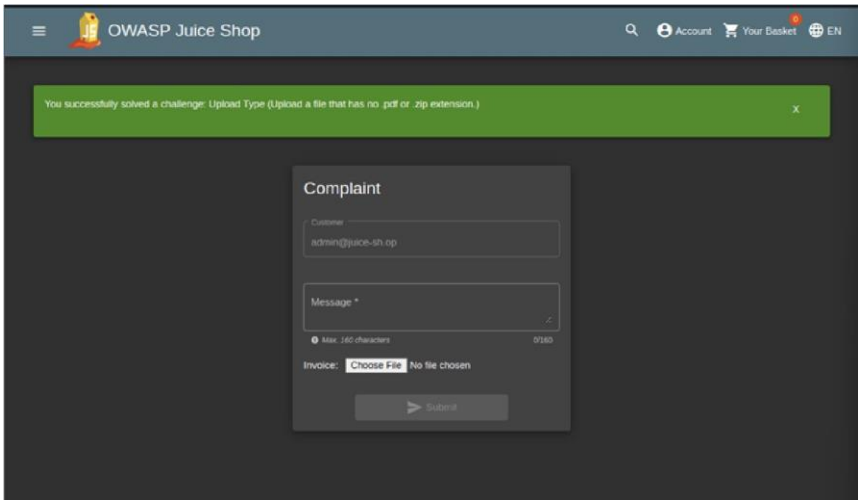
This is the request and we can notice the filename is shell.pdf and file type is application/pdf but to make it executable, we need to change the extension to .php . So now I change the extension to .php .

```
vZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy
zL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZW
6IjIwMjMtMDgtMjkgMDU6NTY6MzkuMDg2ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDgtMz
6MzkuOTgwICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTY5MzM4Mjg4OH0.BwDTUI
t9VxTRcF3oxYZvm-mgjTe6u9TBl30fI5EdLAilKnaESzHr5Ahum1seAj_jqFoqVvuTYk4CUiWUv
WAPcd1ZJBfFmIO3tE80ezlqux6oFgz-Zmw04rBQ6-ONVMCfKuf0FbdvAYTBI-ClMZg-tQ3_U;
continueCode=8eX8oOgBLDpw3R6jqNaZ52YAqYCgUqfEPTaoAbMvJVyE97mxW4QKrzlP1nkZ
Connection: close

------WebKitFormBoundarypAxRnSMVAaGBeuDa
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: application/pdf

<?php
```

Now we forward the request.



As we can see the request has been submitted with extension .php . And hence we've successfully injected a backdoor.



10) BROKEN ACCESS CONTROL (Different method)

CWE-285: Improper Authorization

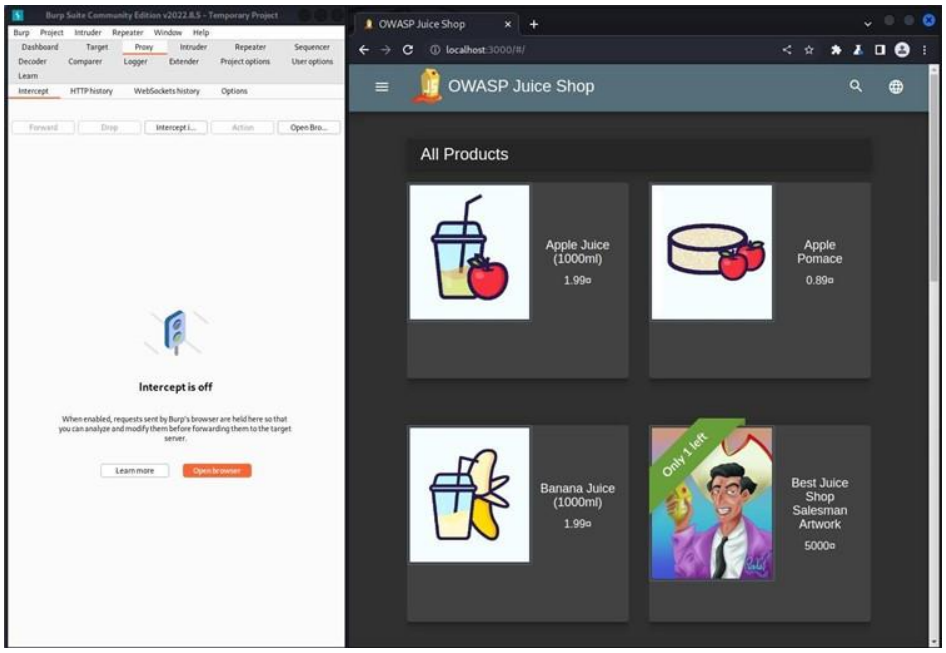
Description: The product does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action.

Business Impact: Broken access control within a business's systems and applications can have significant and detrimental consequences. When users can gain unauthorized access to sensitive data or functions, it can result in data breaches, potentially exposing confidential information, customer records, or intellectual property. This may lead to financial losses, including the costs of breach investigation, regulatory fines, and legal liabilities. Additionally, it can erode customer trust and damage the company's reputation, potentially resulting in lost customers and reduced revenue. Furthermore, such security lapses can disrupt business operations, leading to downtime, lost productivity, and, in some cases, even the complete compromise of critical systems. Businesses should address

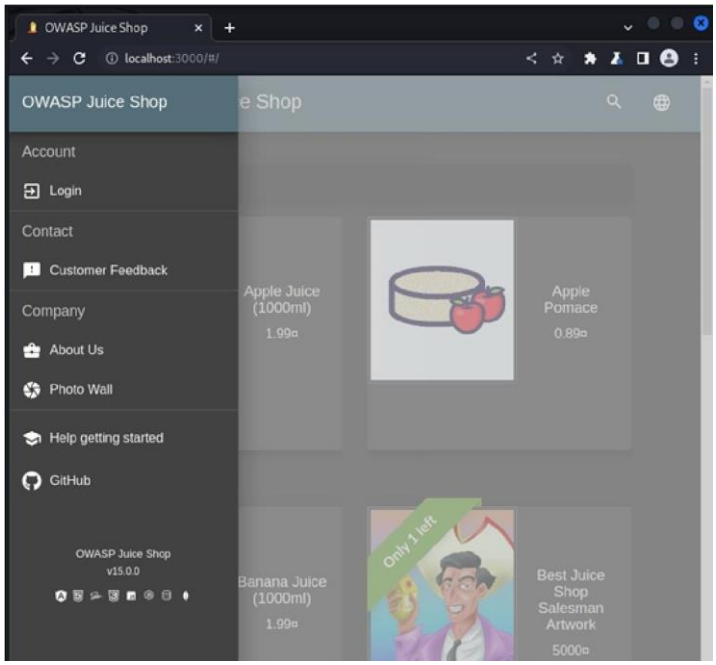
broken access control promptly and implement proper access management to mitigate these risks and protect their data, reputation, and bottom line.

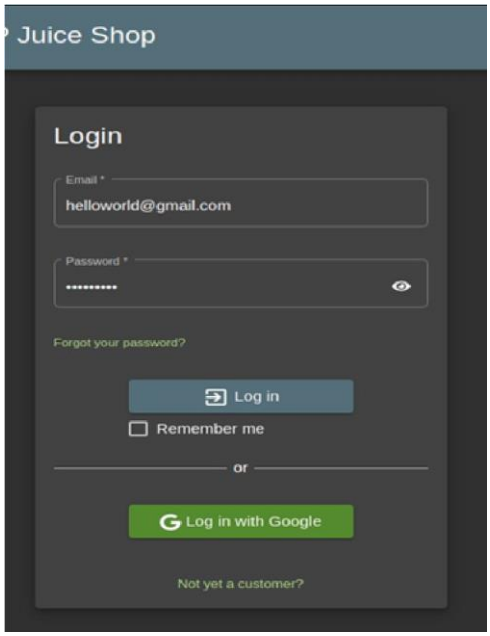
Testing:

Launch the BurpSuit App and go to the proxy tab to launch the burpsuit browser. In the browser access the juice shop website with the localhost:3000 address.



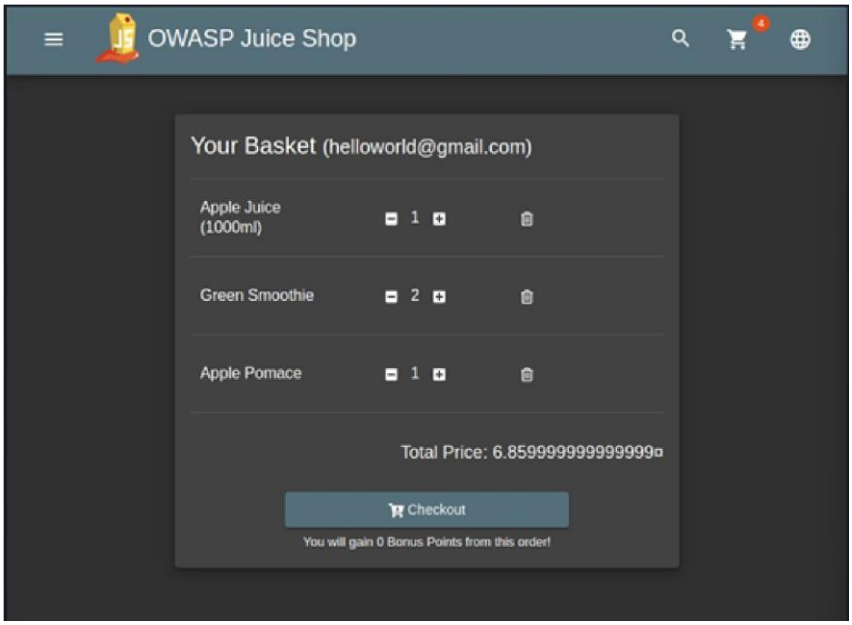
Login to the website with relevant credentials



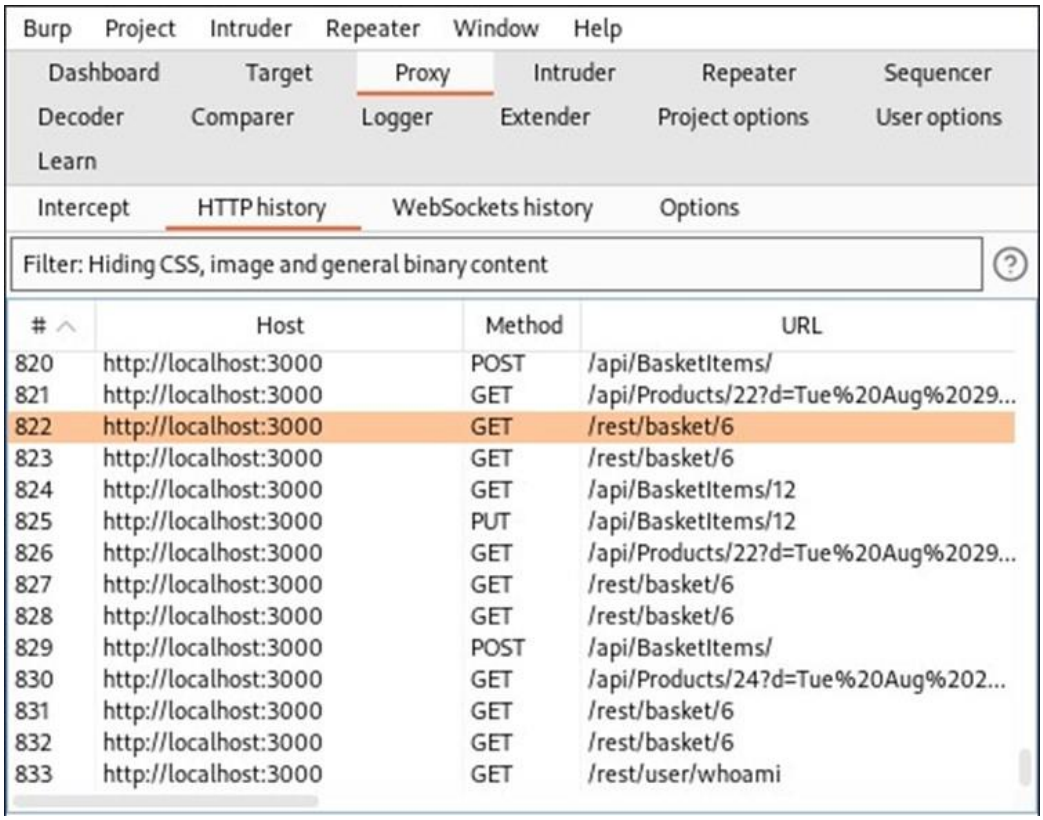


After completing the login process, add drinks of your choice to the cart.

For this particular instance, we will go for -> 1 Apple Juice 2 Green Smoothie 1 Apple Pomace



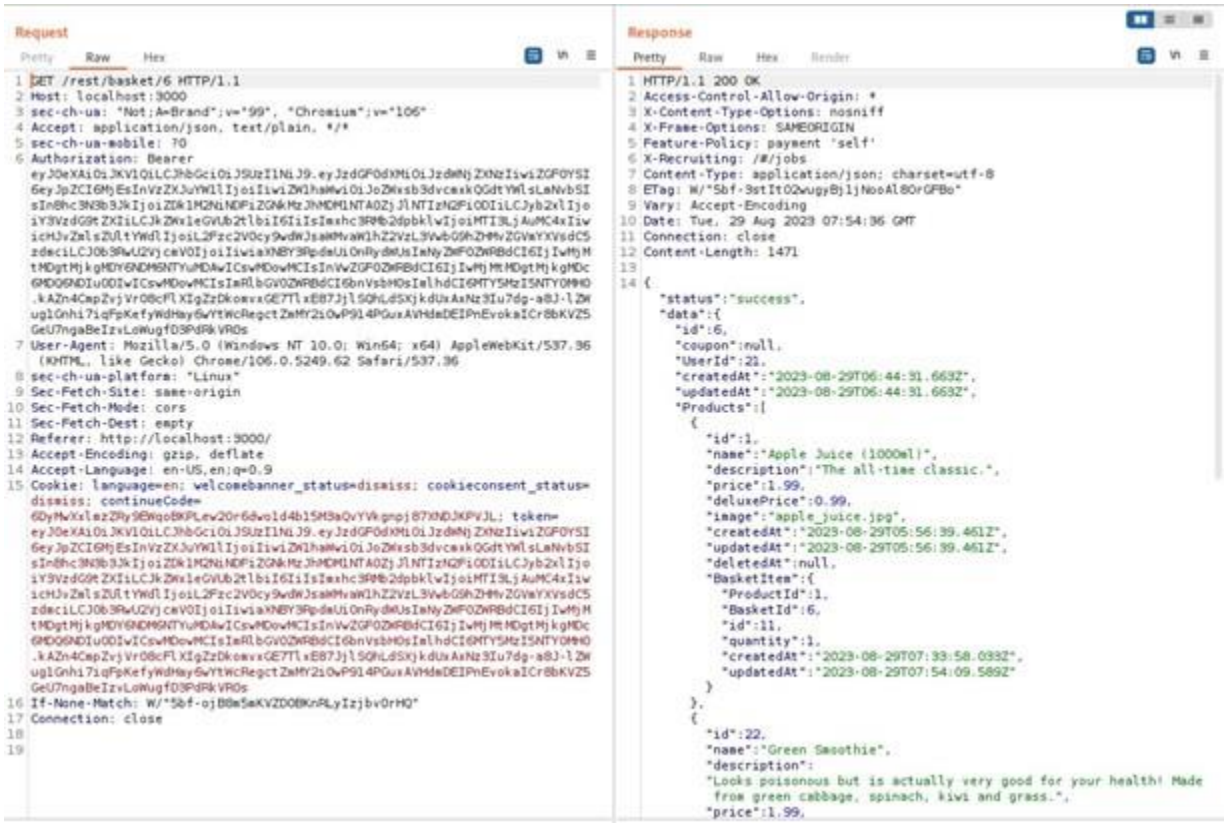
Now go to the http history section in proxy tab and try to find the request that was meant for creation of your basket It would be a get request with basket/<Cart number> URL



We can see that this is the URL linked to our basket.

If we check the Request panel, which must be set in the raw mode, we would find some data related to our basket and items in it

If we select that data and redirect it to the repeater, and click on send, we get some response in JSON format. If we have a closer Look....



These are the data related to the items that we ordered,

Apple Juice


```
"id":1,
"name":"Apple Juice (1000ml)",
"description":"The all-time classic.",
"price":1.99,
"deluxePrice":0.99,
"image":"apple_juice.jpg",
"createdAt":"2023-08-29T05:56:39.461Z",
"updatedAt":"2023-08-29T05:56:39.461Z",
"deletedAt":null,
"BasketItem":{
  "ProductId":1,
  "BasketId":6,
  "id":11,
  "quantity":1,
  "createdAt":"2023-08-29T07:33:58.033Z",
  "updatedAt":"2023-08-29T07:54:09.589Z"
```


Green Smoothie

```
"id":22,
"name":"Green Smoothie",
"description":
"Looks poisonous but is actually very good for your health! Made
 from green cabbage, spinach, kiwi and grass.",
"price":1.99,
"deluxePrice":1.99,
"image":"green_smoothie.jpg",
"createdAt":"2023-08-29T05:56:39.462Z",
"updatedAt":"2023-08-29T05:56:39.462Z",
"deletedAt":null,
"BasketItem":{
  "ProductId":22,
  "BasketId":6,
  "id":12,
  "quantity":2,
  "createdAt":"2023-08-29T07:34:12.176Z",
  "updatedAt":"2023-08-29T07:34:14.177Z"
```

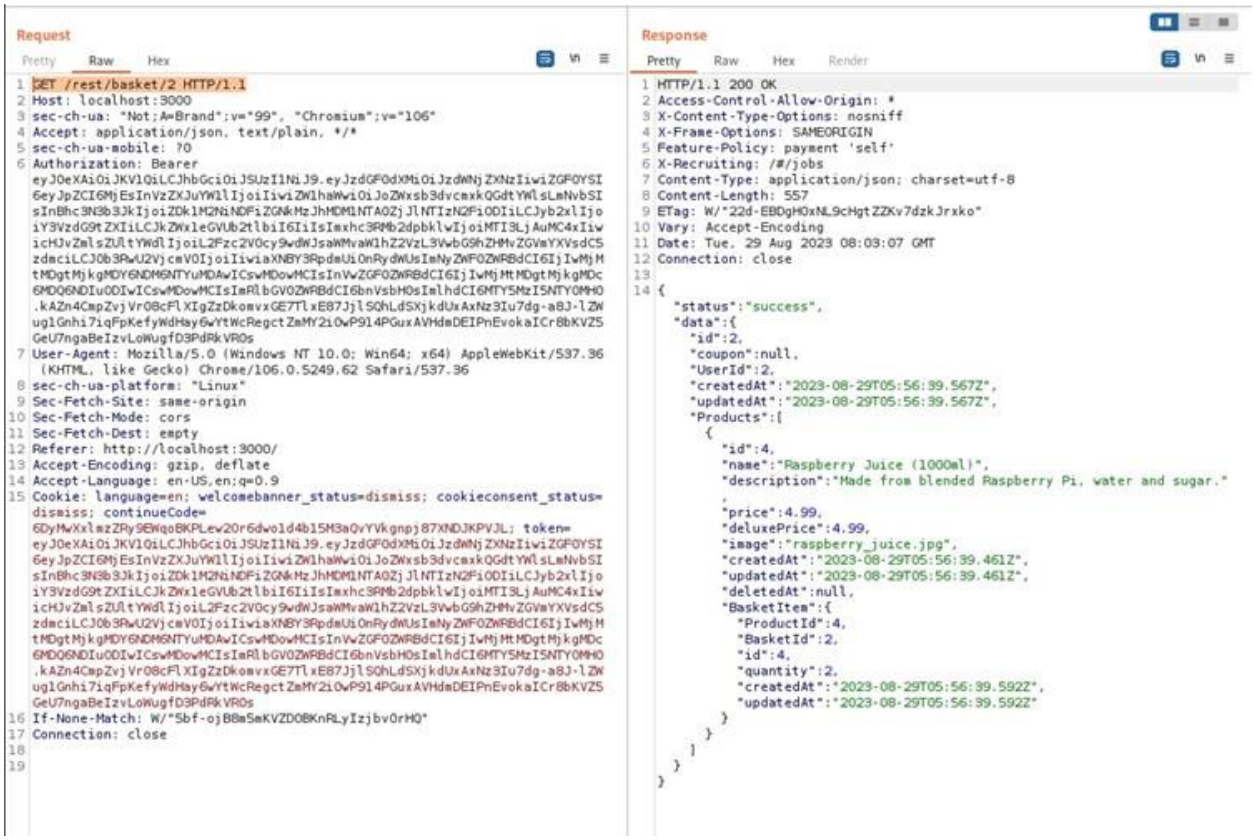

Apple Pomace


```
"id":24,
"name":"Apple Pomace",
"description":
"Finest pressings of apples. Allergy disclaimer: Might contain t
races of worms. Can be <a href=\"/#recycle\">sent back to us</a>
 for recycling.",
"price":0.89,
"deluxePrice":0.89,
"image":"apple_pressings.jpg",
"createdAt":"2023-08-29T05:56:39.462Z",
"updatedAt":"2023-08-29T05:56:39.462Z",
"deletedAt":null,
"BasketItem":{
  "ProductId":24,
  "BasketId":6,
  "id":13,
  "quantity":1,
  "createdAt":"2023-08-29T07:34:22.172Z",
  "updatedAt":"2023-08-29T07:34:22.172Z"
```


GET /rest/basket/6 HTTP/1.1 is somehow linked to our basket and if it is so, most probably the digit 6 is our basket ID.

Now what if I try to change the basket Id to 2 in the request section? This may or may not change the response but it is worth giving a try, if there is a change, we will be able to declare a Broken access control vulnerability.

Now when I changed the request to GET /rest/basket/2 HTTP/1.1 the response has significantly changed.



Request

```
GET /rest/basket/2 HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Not;A=Brand";v="99", "Chromium";v="106"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI
6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJoZWxsb3dvcmxkQGdtYWlsLmNvbSI
sInBhc3N3b3JkIjoiZDk1M2NiNDFiZGNkMzJhMDM1NTA0ZjJlNTIzN2FiODIiLCJyb2xlIjo
iY3VzdG9tZXIiLCJkZWxleGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xIiw
icHJvZmlsZUltYWdlIjoiL2Fzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdC5
zdmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjM
tMDgtMjkgMDY6NDM6NTYuMDAwICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDgtMjkgMDc
6MDQ6NDIuODIwICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbHOsImlhdCI6MTY5MzI5NTY0MHO
.kAZn4CmpZvjVr08cFlXIgZzDkomvxGE7TlxE87JjlSQhLdSXjkdUxAxNz3Iu7dg-a8J-lZW
uglGnhi7iqFpKefyWdHay6wYtWcRegctZaMY2iOwP914PGuxAVHdmDEIPnEvokaICr8bKVZ5
GeU7ngaBeIzvLoWugfD3PdRkVROs
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=
dismiss; continueCode=
6DyMwXxlmzZRy9EWqoBKPLew2Or6dwvold4b15M3aQvYVkgnpj87XNDJKPVJL; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI
6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJoZWxsb3dvcmxkQGdtYWlsLmNvbSI
sInBhc3N3b3JkIjoiZDk1M2NiNDFiZGNkMzJhMDM1NTA0ZjJlNTIzN2FiODIiLCJyb2xlIjo
iY3VzdG9tZXIiLCJkZWxleGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xIiw
icHJvZmlsZUltYWdlIjoiL2Fzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdC5
zdmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjM
tMDgtMjkgMDY6NDM6NTYuMDAwICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDgtMjkgMDc
6MDQ6NDIuODIwICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbHOsImlhdCI6MTY5MzI5NTY0MHO
.kAZn4CmpZvjVr08cFlXIgZzDkomvxGE7TlxE87JjlSQhLdSXjkdUxAxNz3Iu7dg-a8J-lZW
uglGnhi7iqFpKefyWdHay6wYtWcRegctZaMY2iOwP914PGuxAVHdmDEIPnEvokaICr8bKVZ5
GeU7ngaBeIzvLoWugfD3PdRkVROs
If-None-Match: W/"5bf-ojB8m5eKVZDOBKnRLyIzjbvOrHQ"
Connection: close
```

Response

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 557
ETag: W/"22d-EBDgHOxNL9cHgtZZKv7dzkJrxko"
Vary: Accept-Encoding
Date: Tue, 29 Aug 2023 08:03:07 GMT
Connection: close

{
  "status":"success",
  "data":{
    "id":2,
    "coupon":null,
    "UserId":2,
    "createdAt":"2023-08-29T05:56:39.567Z",
    "updatedAt":"2023-08-29T05:56:39.567Z",
    "Products":[
      {
        "id":4,
        "name":"Raspberry Juice (1000ml)",
        "description":"Made from blended Raspberry Pi, water and sugar."
        ,
        "price":4.99,
        "deluxePrice":4.99,
        "image":"raspberry_juice.jpg",
        "createdAt":"2023-08-29T05:56:39.461Z",
        "updatedAt":"2023-08-29T05:56:39.461Z",
        "deletedAt":null,
        "BasketItem":{
          "ProductId":4,
          "BasketId":2,
          "id":4,
          "quantity":2,
          "createdAt":"2023-08-29T05:56:39.592Z",
          "updatedAt":"2023-08-29T05:56:39.592Z"
        }
      }
    ]
  }
}
```

We can notice that the request tab holds basket id 2 and the response tab is giving response 200 OK which means we have successfully accessed the basket with ID 2

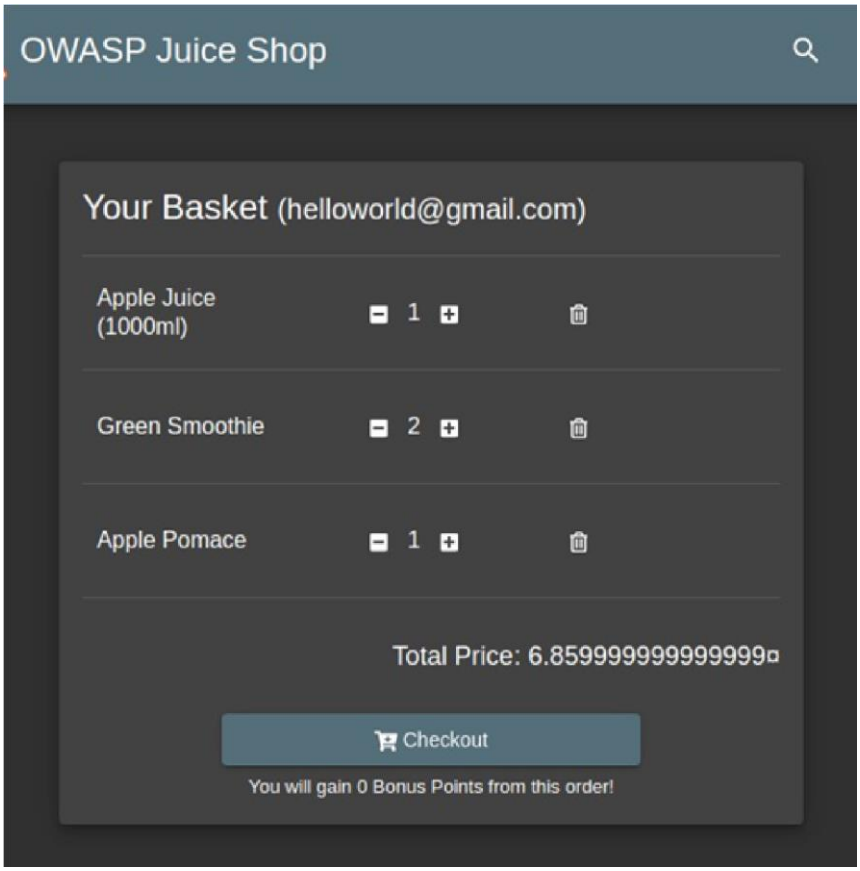
Let's see if that’s actually different from the basket that we built.

```
"id":4,
"name":"Raspberry Juice (1000ml)",
"description":"Made from blended Raspberry Pi, water and sugar."
,
"price":4.99,
"deluxePrice":4.99,
"image":"raspberry_juice.jpg",
"createdAt":"2023-08-29T05:56:39.461Z",
"updatedAt":"2023-08-29T05:56:39.461Z",
"deletedAt":null,
"BasketItem":{
  "ProductId":4,
  "BasketId":2,
  "id":4,
  "quantity":2,
  "createdAt":"2023-08-29T05:56:39.592Z",
  "updatedAt":"2023-08-29T05:56:39.592Z"
```

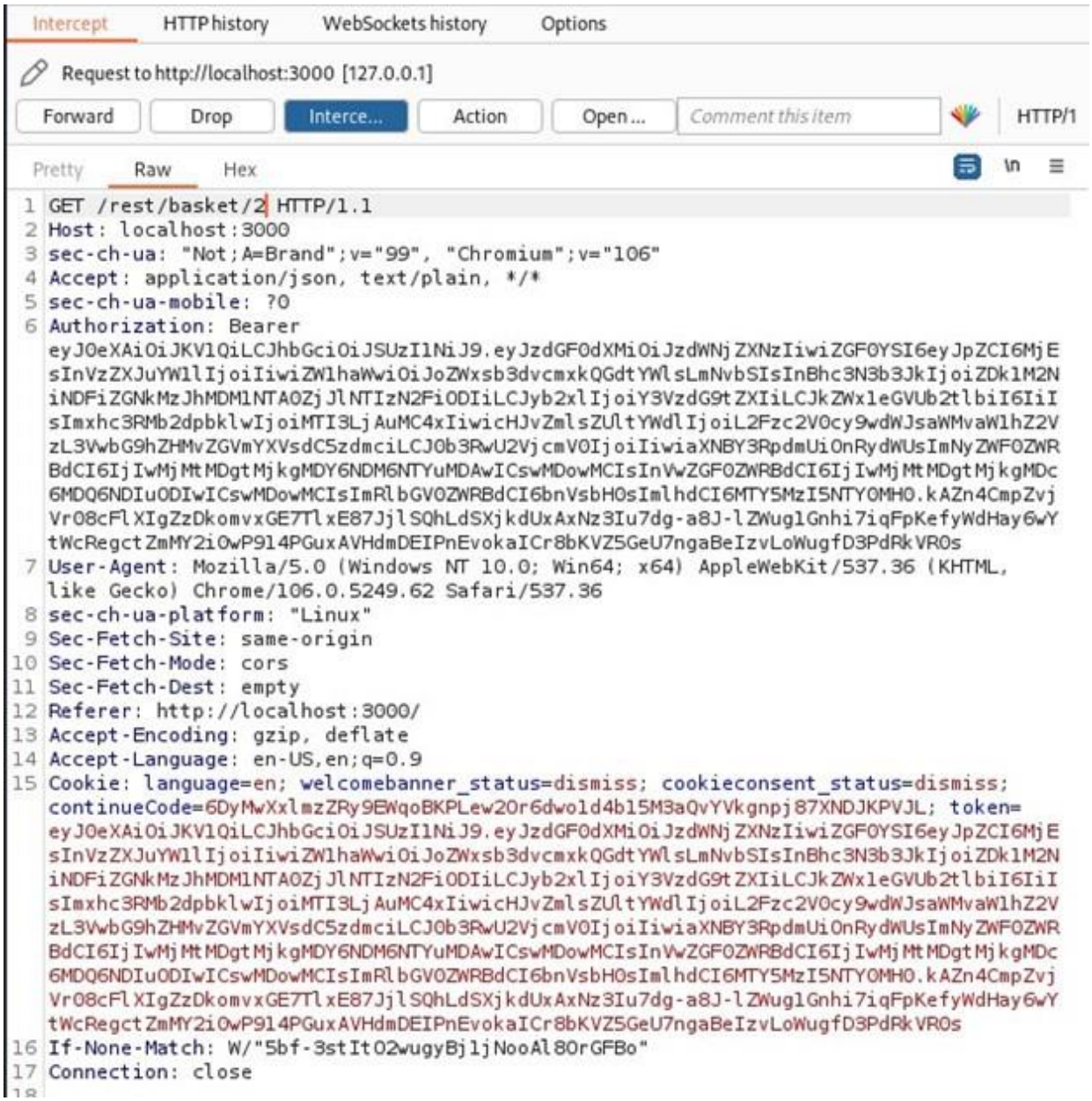
We can see that there is an item named Raspberry Juice which we didn’t order. This proves that we have accessed some other basket.

Now we should try to implement it using the intercept function.

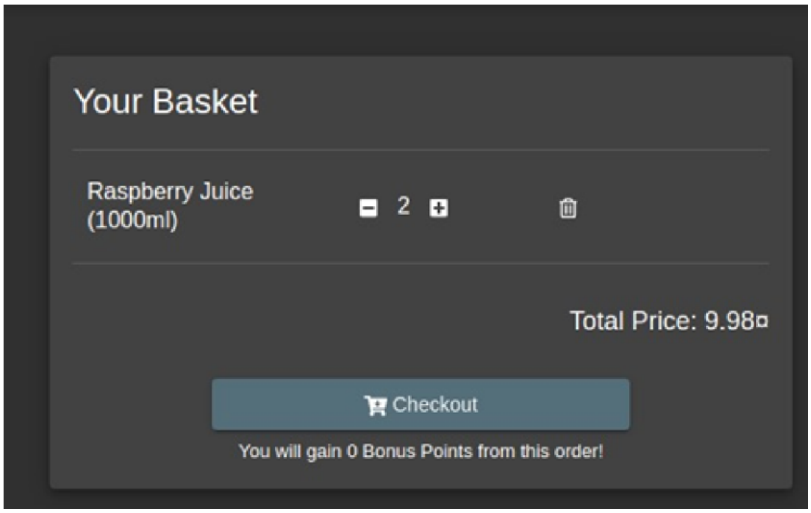
If we go back to the website, we see our very own cart that we built, but now if we turn on the intercept and traverse 1 directory back and then retry to get into our basket by changing the request id from 6 to 2, we must notice a change in our basket.



Basket with order ID 6.


Intercept
HTTP history
WebSockets history
Options
Request to http://localhost:3000 [127.0.0.1]
Forward
Drop
Interce...
Action
Open ...
Comment this item
HTTP/1
Pretty
Raw
Hex
\n
1 GET /rest/basket/2 HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not;A=Brand";v="99", "Chromium";v="106"
4 Accept: application/json, text/plain, */*
5 sec-ch-ua-mobile: ?0
6 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjE
sInVzZXJuYW1lIjoiIiwiZW1haWwiOiJoZWxsb3dvcmxkQGdtYWlsLmNvbSIsInBhc3N3b3JkIjoiZDk1M2N
iNDFiZGNkMzJhMDM1NTA0ZjJlNTIzN2FiODIiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiI
sImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xIiwicHJvZmlsZUltYWdlIjoiL2Fzc2V0cy9wdWJsaWMvaW1hZ2V
zL3VwbG9hZHMvZGVmYXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWR
BdCI6IjIwMjMtMDgtMjkgMDY6NDM6NTYuMDAwICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDgtMjkgMDc
6MDQ6NDIuODIwICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTY5MzI5NTY0MH0.kAZn4CmpZvj
Vr08cFlXIgZzDkomvxGE7TlxE87JjlSQhLdSXjkdUxAxNz3Iu7dg-a8J-lZWuglGnhi7iqFpKefyWdHay6wY
tWcRegctZmMY2iOwP914PGuxAVHdmDEIPnEvokaICr8bKVZ5GeU7ngaBeIzvLoWugfD3PdRkVR0s
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/106.0.5249.62 Safari/537.36
8 sec-ch-ua-platform: "Linux"
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: http://localhost:3000/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=6DyMwXxlmzZRy9EWqoBKPLew2Or6dwo1d4b15M3aQvYVkgnpj87XNDJKPVJL; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjE
sInVzZXJuYW1lIjoiIiwiZW1haWwiOiJoZWxsb3dvcmxkQGdtYWlsLmNvbSIsInBhc3N3b3JkIjoiZDk1M2N
iNDFiZGNkMzJhMDM1NTA0ZjJlNTIzN2FiODIiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiI
sImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xIiwicHJvZmlsZUltYWdlIjoiL2Fzc2V0cy9wdWJsaWMvaW1hZ2V
zL3VwbG9hZHMvZGVmYXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWR
BdCI6IjIwMjMtMDgtMjkgMDY6NDM6NTYuMDAwICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDgtMjkgMDc
6MDQ6NDIuODIwICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTY5MzI5NTY0MH0.kAZn4CmpZvj
Vr08cFlXIgZzDkomvxGE7TlxE87JjlSQhLdSXjkdUxAxNz3Iu7dg-a8J-lZWuglGnhi7iqFpKefyWdHay6wY
tWcRegctZmMY2iOwP914PGuxAVHdmDEIPnEvokaICr8bKVZ5GeU7ngaBeIzvLoWugfD3PdRkVR0s
16 If-None-Match: W/"5bf-3stIt02wugyBj1jNooAl8OrGFBo"
17 Connection: close

Now we forward the request to the browser and see what result we get



We can see Our basket has changed and the order includes Raspberry juice

Hence we can declare a Broken access control Vulnerability as I am able to access Baskets of other clients.

MAIN WEBSITE VULNERABILITIES TESTING REPORT

Main website: https://www.coinhako.com/

Description:

Allowing sign-up with temporary disposable email IDs on coinhako website introduces a significant security risk. Temporary email services tool Tempail, provide users with easily accessible and discardable email addresses, making it difficult for the platform to track and verify the identity of users effectively. This can lead to various malicious activities, including but not limited to fraudulent account creation, money laundering, and unauthorized access to user accounts.

Impact on Business:

1. *Increased Risk of Fraud:* Allowing the use of disposable email addresses significantly increases the risk of fraudulent user registrations. This can lead to an increase in fraudulent transactions, loss of funds, and damage to the platform's reputation.

2. *Reduced KYC Effectiveness:* Crypto trading platforms are often required to perform Know Your Customer (KYC) checks to comply with legal and regulatory requirements. Allowing disposable email sign-ups can undermine the effectiveness of these checks, potentially exposing the platform to legal and compliance issues.

3. *Loss of Trust*: Users may lose trust in the platform if they perceive it as lacking stringent security measures. This loss of trust can lead to a decrease in user engagement and may discourage potential investors from using the platform.

4. *Data Breach Risk:* Disposable email accounts can be used to hide malicious intent, making it easier for attackers to exploit vulnerabilities and gain unauthorized access to user accounts. This increases the risk of data breaches and theft of sensitive user information.

CWE:

This vulnerability can be associated with multiple Common Weakness Enumeration (CWE) identifiers. Some relevant CWEs might include:

- CWE-799: Improper Control of Interaction Frequency: Allowing disposable email sign-ups may result in improper control of user interactions and identity verification.

- CWE-601: URL Redirection to Untrusted Site ('Open Redirect'): Attackers could use disposable email addresses to perform phishing attacks or redirect users to malicious sites.

CVE:

A specific CVE identifier may not be applicable to this issue, as it is more of a general security concern rather than a specific software vulnerability. However, a crypto trading platform's security team should address this issue as part of their security improvements.

Recommended Mitigation:

To mitigate this vulnerability, the crypto trading platform should implement the following measures:

1. Filtering based on known email companies : On the Server Side the developers may include a List of mailing service providers and validate the mail field fed by the user.

2. Enhanced KYC: Implement a robust Know Your Customer (KYC) process to ensure that users are who they claim to be, reducing the risk of fraudulent activities.

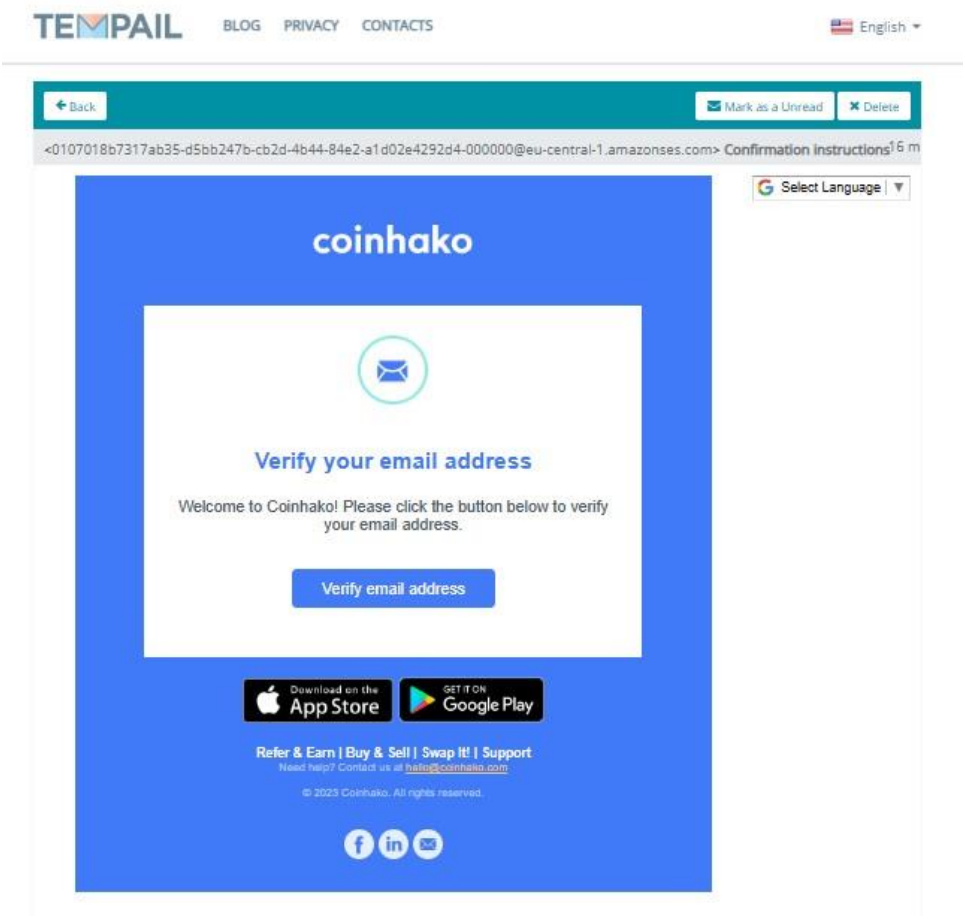
3. Monitoring and Reporting: Implement real-time monitoring for suspicious activities and implement a reporting mechanism for users to report potential fraud or suspicious behavior.

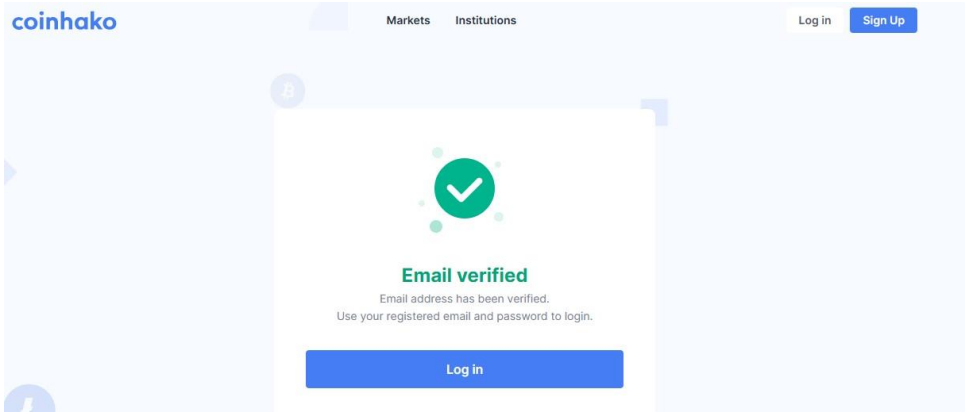
4. Account Lockout: Implement temporary account lockout for users whose activities appear suspicious. This can help prevent unauthorized access and fraud.

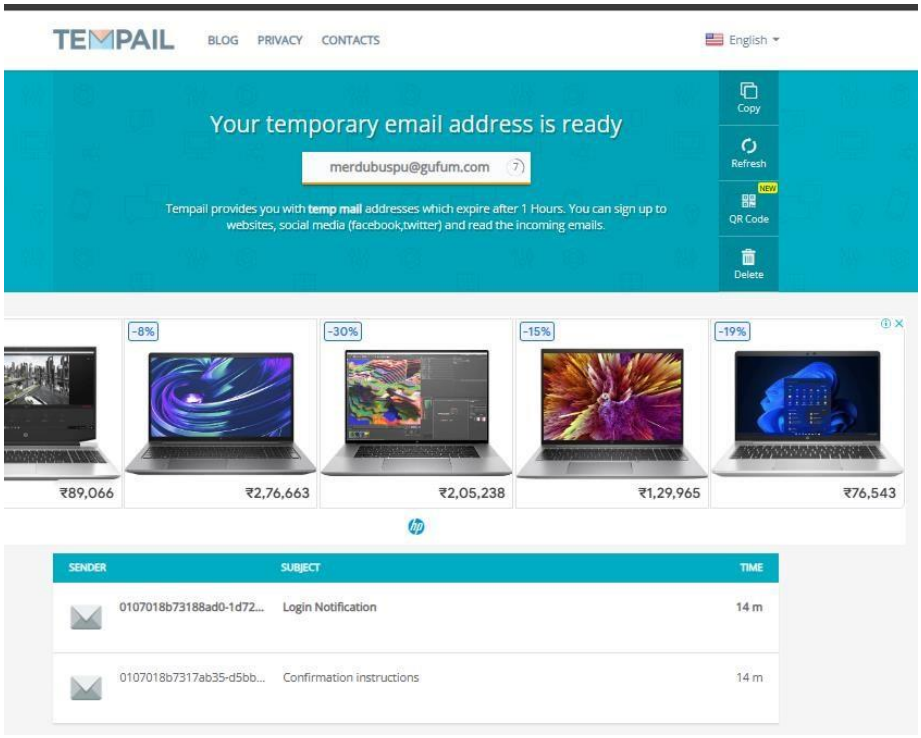
Conclusion:

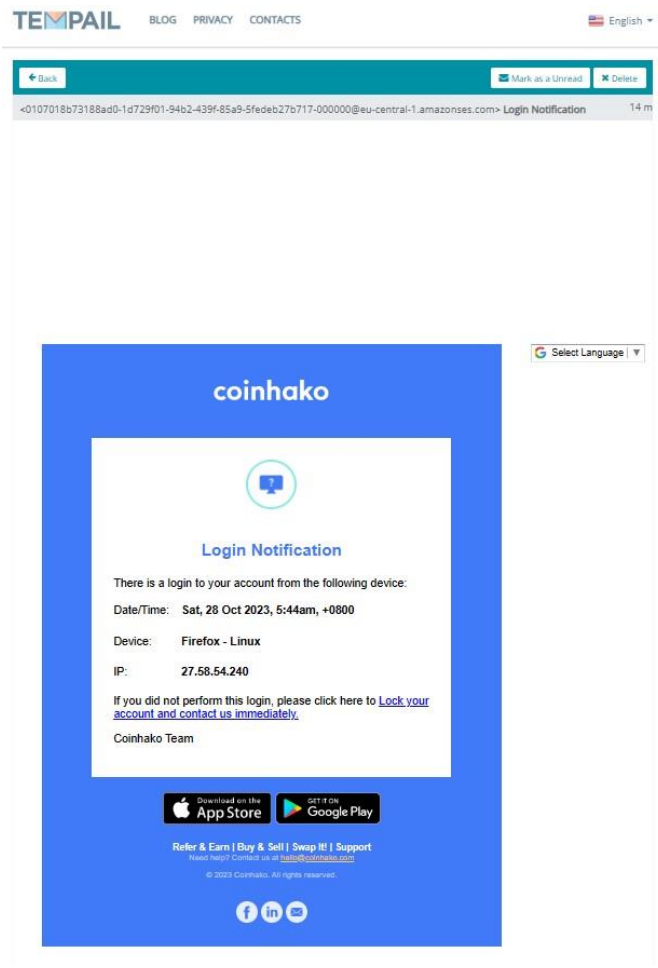
Allowing sign-up with temporary disposable email addresses on a crypto trading website poses a
significant security risk to the platform. Implementing the recommended mitigation measures will help enhance security, protect user accounts, and maintain compliance with regulatory requirements.

Proof of Concept:




coinhako
Markets
Institutions
Log in
Sign Up
Email verified
Email address has been verified.
Use your registered email and password to login.
Log in


TEMPAIL
BLOG
PRIVACY
CONTACTS
English
Your temporary email address is ready
merdubuspu@gufum.com
Tempail provides you with temp mail addresses which expire after 1 Hours. You can sign up to websites, social media (facebook,twitter) and read the incoming emails.
Copy
Refresh
QR Code
NEW
Delete
-8%
-30%
-15%
-19%
₹89,066
₹2,76,663
₹2,05,238
₹1,29,965
₹76,543
SENDER
SUBJECT
TIME
0107018b73188ad0-1d72...
Login Notification
14 m
0107018b7317ab35-d5bb...
Confirmation instructions
14 m


TEMPAIL
BLOG
PRIVACY
CONTACTS
English
Back
Mark as a Unread
Delete
<0107018b73188ad0-1d729f01-94b2-439f-85a9-5fedeb27b717-000000@eu-central-1.amazonses.com> Login Notification
14 m
Select Language
coinhako
Login Notification
There is a login to your account from the following device:
Date/Time: Sat, 28 Oct 2023, 5:44am, +0800
Device: Firefox - Linux
IP: 27.58.54.240
If you did not perform this login, please click here to Lock your account and contact us immediately.
Coinhako Team
Download on the App Store
GET IT ON Google Play
Refer & Earn | Buy & Sell | Swap It! | Support
Need help? Contact us at hello@coinhako.com
© 2023 Coinhako. All rights reserved.

NESSUS SCAN REPORT

TEST WEBSITE

Overview :-

Nessus is a powerful and widely respected vulnerability scanning and assessment tool that plays a pivotal role in enhancing the security of networks, systems, and applications. Its primary mission is to assist organizations in proactively identifying and addressing security vulnerabilities. Nessus achieves this through a comprehensive set of features and capabilities.

One of its standout attributes is its ability to conduct exhaustive scans of networks, systems, and web applications, uncovering a wide spectrum of vulnerabilities, ranging from misconfigurations to missing patches and other common security weaknesses. This breadth of coverage is made possible by Nessus's plugin-based architecture, which supports an extensive library of plugins. This versatility enables users to tailor scans to their specific needs, making it a flexible tool suitable for a diverse array of organizations.

In addition to vulnerability assessment, Nessus offers the capability to evaluate systems and applications for compliance with established security standards and regulations. Its scanning policies can be customized, scan schedules can be configured, and scan parameters can be fine-tuned to match particular requirements. The resulting detailed reports, highlighting vulnerabilities, their severity, and recommended remediation steps, are invaluable resources for IT administrators and security professionals seeking to bolster their defenses.

Nessus's scalability is another distinguishing feature, making it accessible to organizations of varying sizes. Whether deployed in small or large environments, Nessus is equipped to efficiently identify and report on vulnerabilities. Furthermore, its integration capabilities allow it to seamlessly work in conjunction with other security tools and management systems, enabling users to create a holistic security ecosystem.

While Nessus's capabilities are remarkable, it is imperative that users exercise caution and adhere to ethical standards. Unauthorized scanning can disrupt systems and potentially lead to legal and ethical violations. Therefore, Nessus is most effective and responsible when used with proper permissions, making it an indispensable tool for security professionals in safeguarding digital assets and fortifying the defenses of modern organizations.

Target website : Testfire.net

Target ip address: 65.61.137.117

List of vulnerability

s.no	Vulnerability name	Severity	plugins
1.	- CGI Generic XSS (comprehensive test)	MEDIUM	47831
2.	Web Application Potentially Vulnerable to Clickjacking	MEDIUM	85582
3.	Web Server Allows Password Auto-Completion Web Server Transmits	LOW	42057

	Cleartext Credentials		
4.	Apache Tomcat Detection	LOW	26194
5.	CGI Generic Injectable Parameter	INFO	39446
6.	CGI Generic Tests HTTP Errors	INFO	47830
7.	CGI Generic Tests Load Estimation (all tests)	INFO	40406
8.	CGI Generic Tests Timeout		
9.	External URLs	INFO	33817 –
10.	HSTS Missing From HTTPS Server	INFO	39470
11.	HTTP Cookie 'secure' Property Transport Mismatch	INFO	49704
12.	HTTP Methods Allowed (per directory)	INFO	84502
13.	HTTP Server Type and Version	INFO	69826 –

14.	HyperText Transfer Protocol (HTTP) Information	INFO	43111
15.	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	INFO	10107 –
16.	Missing or Permissive X-Frame-Options HTTP Response Header	INFO	24260
17.	Nessus SYN scanner Nessus Scan Information	INFO	50344
18.	Web Application Cookies Not Marked Secure Web Application Sitemap Web mirroring	INFO	50345

19.		INFO	11219
20.		INFO	19506
21.			85602
22.			91815
23.			10662

MAIN WEBSITE

Nessus is a powerful and widely-used vulnerability scanning tool that plays a pivotal role in cybersecurity and network management. Developed by Tenable Network Security, it empowers organizations to proactively identify and address security weaknesses in their systems. Nessus conducts comprehensive scans of networks, operating systems, applications, and hardware, identifying vulnerabilities and potential threats. Its extensive database of known vulnerabilities, coupled with constant updates, ensures that it remains at the forefront of cybersecurity defense. Beyond its vulnerability assessment capabilities, Nessus provides valuable insights into compliance monitoring, enabling businesses to adhere to industry standards and regulatory requirements. Whether utilized by security professionals, network administrators, or IT managers, Nessus is a critical asset for securing digital infrastructure, minimizing the risk of breaches, and maintaining the integrity of data and systems. Its versatility, user-friendly interface, and reporting features make it an indispensable tool in the ongoing battle against cyber threats and data breaches. Nessus boasts a wide array of features that make it a go-to solution for security professionals. It offers various scanning options, including credentialed scans for in-depth analysis, and agent-based scanning for offline and disconnected devices. Nessus not only identifies vulnerabilities but also provides detailed information on their severity, potential impact, and remediation steps, aiding IT teams in prioritizing and addressing the most critical issues first. Its integration capabilities with other security tools and platforms make it a cornerstone of a comprehensive cybersecurity strategy. Moreover, Nessus has adapted to the evolving threat landscape, addressing emerging vulnerabilities and aiding in the protection of cloud environments and containerized applications. With its history of reliability and effectiveness, Nessus has earned the trust of organizations across the globe, making it an indispensable asset for bolstering security, maintaining compliance, and safeguarding against an ever-expanding range of cyber threats. In a digital age where

security is paramount, Nessus stands as a stalwart guardian of networks and systems.

Target website: coinhako.com

Target IP: 104.18.2.84

List of Vulnerability:

S.No	Vulnerability	Severity	Plugins
1	HTTP server type and version	INFO	10107
2	HTTP info	INFO	24260

FUTURE SCOPE

User authentication is a critical aspect of digital security. While traditional methods such as passwords, PINs, and biometrics have their place, behavior-based user authenticity verification has emerged as a promising field. This innovative approach leverages user behavior patterns to enhance security and user experience. Here is a future scope for advancing this feature:

1. Continuous Learning and Adaptation: - Implement a dynamic system that continuously learns and adapts to a user's changing behavior. The feature should be able to distinguish between genuine changes in behavior and unauthorized access attempts, ensuring user convenience and security.

2. Advanced Behavioral Biometrics: - Integrate advanced behavioral biometric features like keystroke dynamics (typing speed, rhythm), mouse movement, touchscreen gestures, voice recognition, and facial expressions analysis to create a more comprehensive and accurate user profile.

3. Multi-Modal Authentication: - Incorporate multi-modal authentication by combining various behavioral biometrics to increase accuracy and reduce false positives. For instance, combining keystroke dynamics with voice recognition for a more robust verification process.

4. AI and Machine Learning: - Leverage AI and machine learning algorithms to analyze and model user behavior more accurately. These algorithms can identify even subtle variations in behavior, making it harder for impostors to mimic a legitimate user.

5. Anomaly Detection: - Develop an anomaly detection system that can identify unusual behavior patterns, such as accessing an account from a different location or at an unusual time. These anomalies should trigger additional verification steps or alerts to the user.

6. User-Controlled Customization: - Give users the ability to customize their behavior-based authentication settings. This could include allowing users to

adjust sensitivity levels or add specific behaviors they want to use for verification.
7. Accessibility and Inclusivity: - Ensure that the feature is designed with accessibility and inclusivity in mind. Consider users with disabilities and create options for different types of behavioral biometrics that are inclusive and user-friendly.
8. Behavioral Authentication API: - Develop a secure API for third-party applications to integrate behavior-based user authentication. This will enable a broader adoption of the technology across various industries and applications.
9. Behavioral Risk Scoring: - Implement a risk-scoring system that assesses the overall user behavior and provides risk scores for each session. The system should be able to automatically escalate authentication requirements for high-risk sessions.
10. Privacy and Ethical Considerations: - Pay special attention to privacy and ethical considerations, including obtaining user consent for collecting and analyzing behavioral data. Implement robust data protection measures to safeguard user information.
11. User Education and Awareness: - Develop educational materials and campaigns to inform users about the benefits and proper usage of behavior-based authentication. This will increase user acceptance and trust in the feature.
12. Continuous Security Improvements: - Stay up to date with the latest security threats and regularly update the feature to address new challenges. This may involve collaborating with cybersecurity experts and conducting security audits.

CONCLUSION

The future scope for behavior-based user authenticity verification is promising, as it has the potential to enhance security and user experience. By focusing on continuous learning, advanced biometrics, multi-modal authentication, AI, user customization, accessibility, and ethical considerations, this feature can become an integral part of digital security in various industries.

THANK YOU