Team 2.5
CyberSpectrum

—

Overview :-

In today's interconnected and digital world, cybersecurity is a paramount concern for organizations of all sizes and industries. The project, "Enhancing Organizational Cybersecurity Resilience," aims to establish a robust cybersecurity framework to protect an organization's digital assets, data, and infrastructure from a wide range of cyber threats. The project's primary objective is to create a comprehensive and proactive approach to cybersecurity, aligning with the organization's business objectives and risk tolerance.

Key Project Steps and Objectives:-

- Cybersecurity Policy and Strategy Development: The project will begin by crafting a clear and well-defined cybersecurity policy and strategy. This strategic framework will serve as a guide for all cybersecurity initiatives, aligning them with the organization's overarching goals and risk management strategies.

- Risk Assessment and Mitigation: A thorough risk assessment will be conducted to identify potential cybersecurity threats and vulnerabilities specific to the organization. Risks will be prioritized based on their potential impact and likelihood of occurrence. Risk mitigation measures will be implemented, and a risk management plan will be created to address identified vulnerabilities.

- Access Control and Authentication: Strong access control measures will be put in place to ensure that only authorized personnel can access sensitive data and critical systems. Multi-factor authentication (MFA) will be implemented for an additional layer of security.

- Network Security: The project will deploy firewalls, intrusion detection/prevention systems (IDS/IPS), and secure gateways to monitor and control network traffic, ensuring that unauthorized access and malicious activities are promptly identified and blocked.

- Endpoint Security: Antivirus software, endpoint protection tools, and host-based firewalls will be installed on all devices to defend against malware and other threats at the device level, enhancing the security of endpoints.

- Data Encryption: Sensitive data will be encrypted both at rest and in transit to prevent unauthorized access and ensure data confidentiality, even in the event of a breach.

- Patch Management: A systematic process will be established to apply security patches and updates promptly to all software, operating systems, and firmware to address known vulnerabilities and reduce the organization's exposure to threats.

- Incident Response Planning: The project will develop a well-defined incident response plan (IRP) to effectively handle cybersecurity incidents. This IRP will include guidelines for identifying, reporting, containing, eradicating, and recovering from security incidents, minimizing potential damage and downtime.

- Security Audits and Assessments: Regular internal and external security audits and assessments will be conducted to evaluate the organization's security posture and identify potential weaknesses or gaps. These evaluations will ensure that the cybersecurity framework remains effective and up-to-date.

- Monitoring and Logging: The project will implement centralized logging and real-time monitoring of network and system activities to detect and respond to suspicious activities promptly, minimizing the impact of potential security incidents.

List of teammates–

S.no	Name	College	Contact
1	Anondita Dutta	VIT Bhopal	Anondita.dutta2021@vitbhopal.ac.in
2	Hardik Kanane	VIT Bhopal	Hardik.kankane2021@vitbhopal.ac.in
3	Elisabeth Varghese	VIT Bhopal	Elisabeth.varghese2021@vitbhopal.ac.in

List of Vulnerability Table ▬

S.no	VulnerabilityName	CWE - No
1	SQL injection	89: Improper Neutralization of Special Elements used in an SQL Command
2	Brute Force Attack	1391: Use of Weak Credentials
3	Broken authentication	285: Improper Authorization
4	Improper Input Validation	132: Miscalculated Null Termination
5	Web server allows password auto-completion	CWE-310: Cryptographic Issues
6	Clickjacking	CWE-1021: Improper Restriction of Rendered UI Layers or Frames
7	HTML injection attack	CWE - 601: URL Redirection to Untrusted Site ('Open Redirect')
8	Cross site scripting (stored)	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
9	Cleartext Transmission of Sensitive Information	CWE-319: Cleartext Transmission of Sensitive Information
10	Insecure Direct object Reference	CWE-639: Authorization Bypass Through User-Controlled Key

<p style="text-align:center"># REPORT:-</p>

1. **Vulnerability name**: SQL injection
   CWE: 89

   Description: The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. Business Impact: In summary, it is crucial to underscore that CWE-89, known as SQL Injection, can exert a profound and diverse business impact. This encompasses critical facets such as data breaches, financial setbacks, harm to reputation, legal ramifications, and operational turmoil. Hence, the imperative of preventing and remedying SQL injection vulnerabilities cannot be overstated, as it is indispensable for fortifying the security and continuity of an organization's applications and data.

   Vulnerability path: http://testfire.net/

   Steps to Reproduce:

   Access the URL
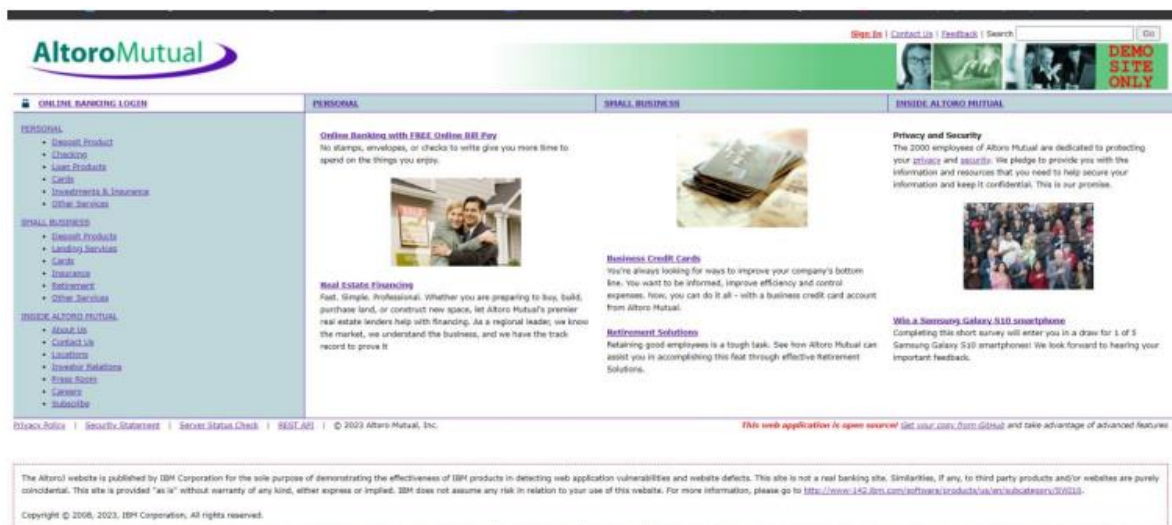
   Now we will try to sign in to this website with admin privileges but using SQL injection
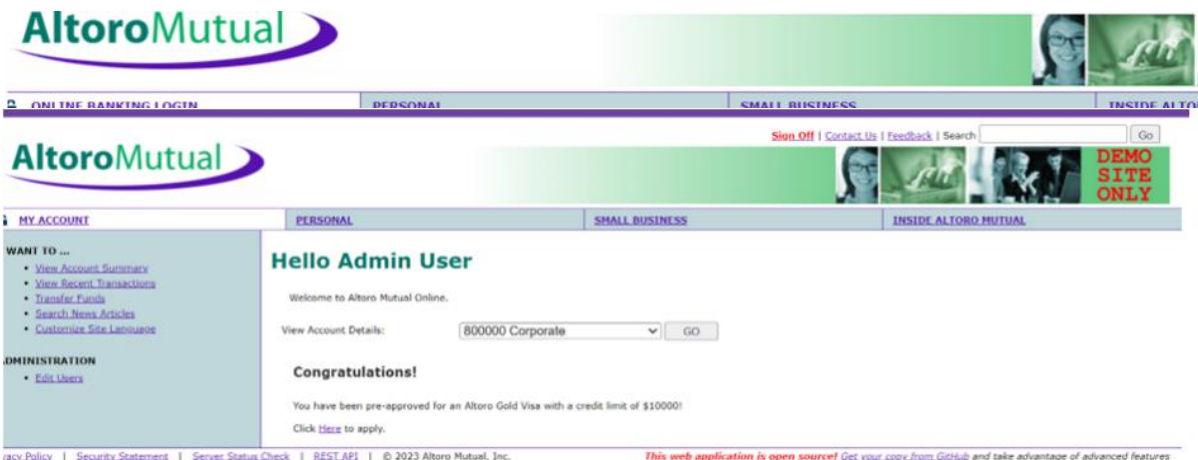
With this we can know that sql injection worked and we got the admin privileges

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.

2. **Vulnerability name**: 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.

Steps to reproduce

Add the website by going to target tab -> add
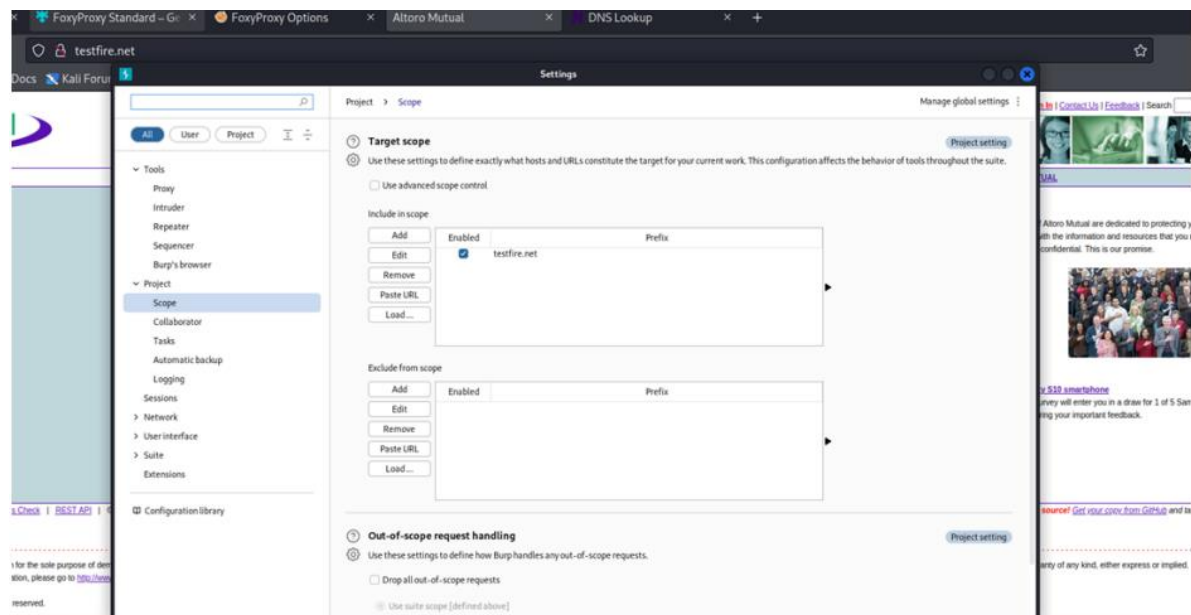
Choose burp as our default proxy on foxyproxy
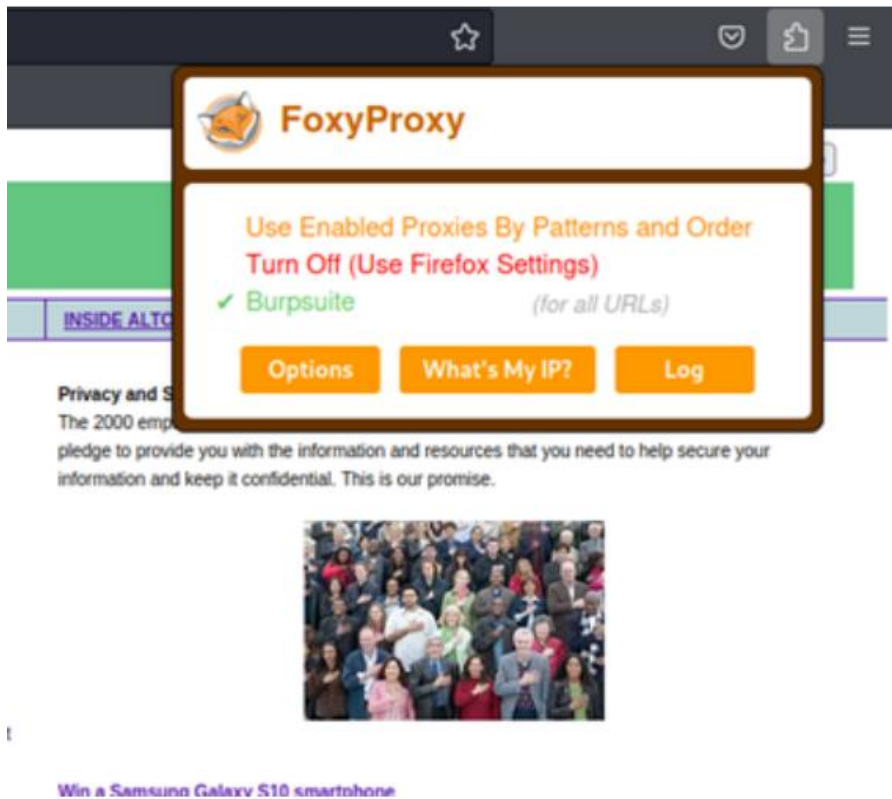
Go to proxy and turn on the intercept and then click on the login page of the website and give in random username and password.
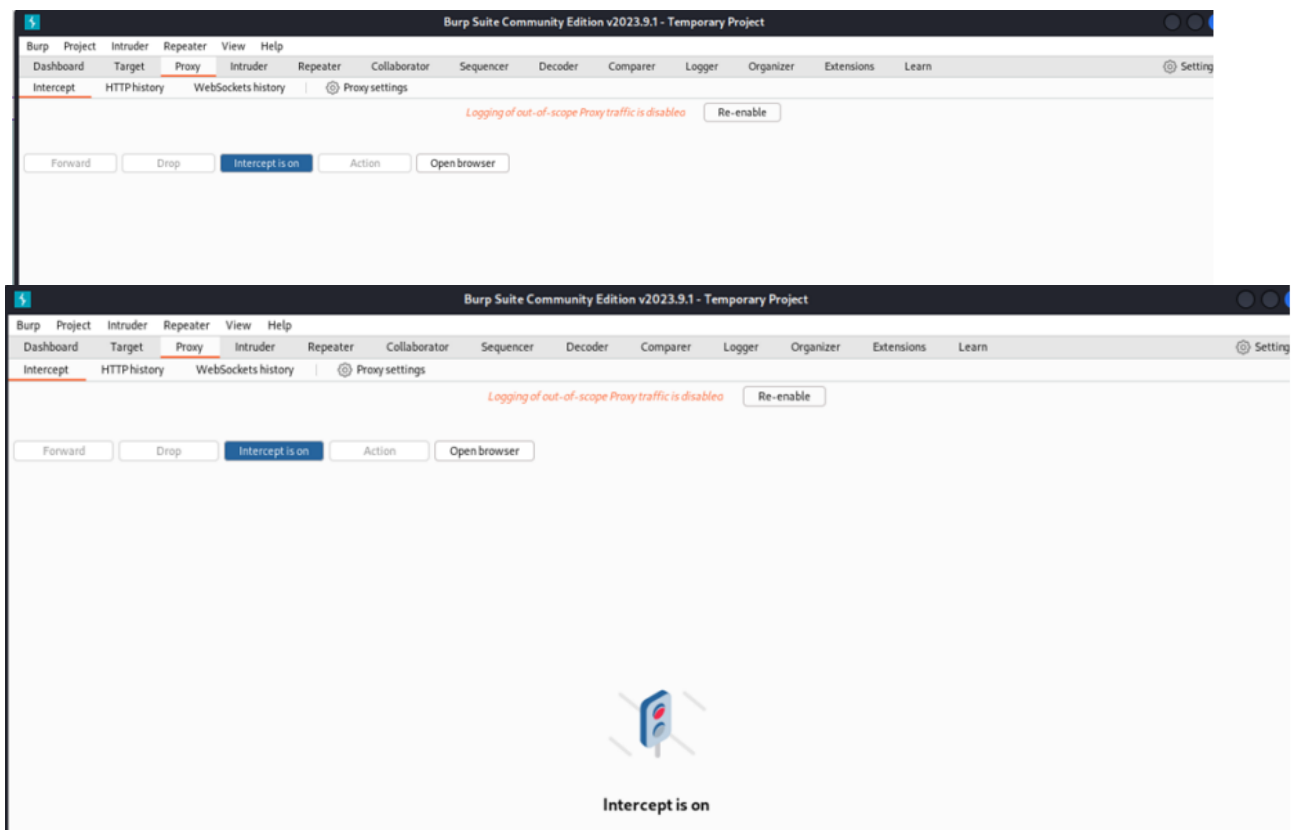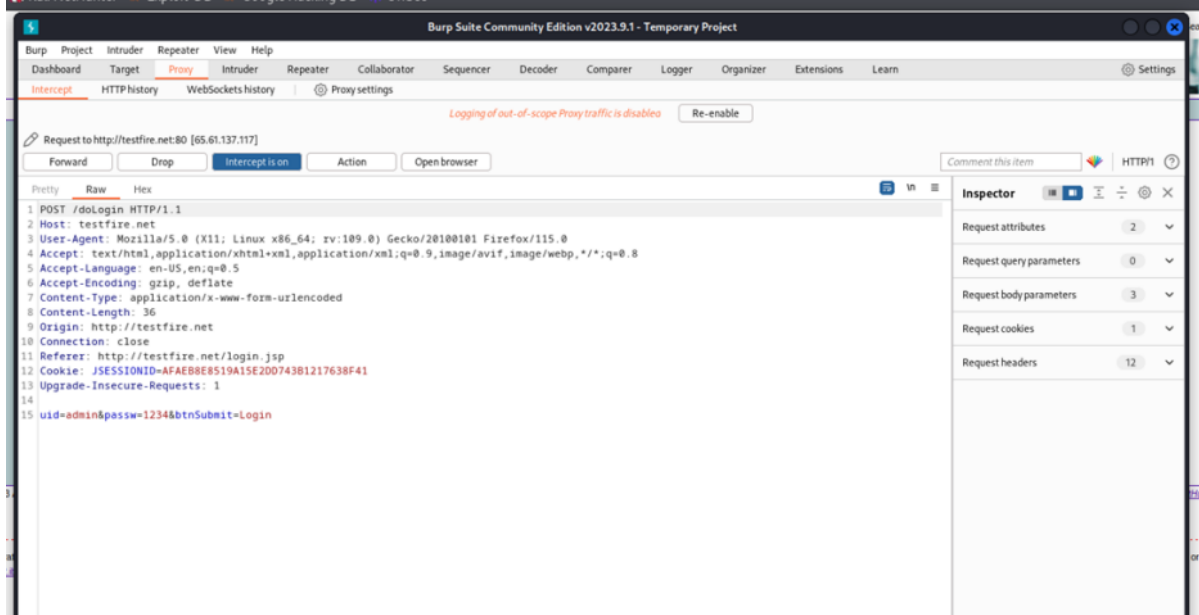
Then we sent it to intruder and go to positions tab choose cluster bomb attack and select the given input of username as payload 1 and given input of password as payload 2 by clicking on add.
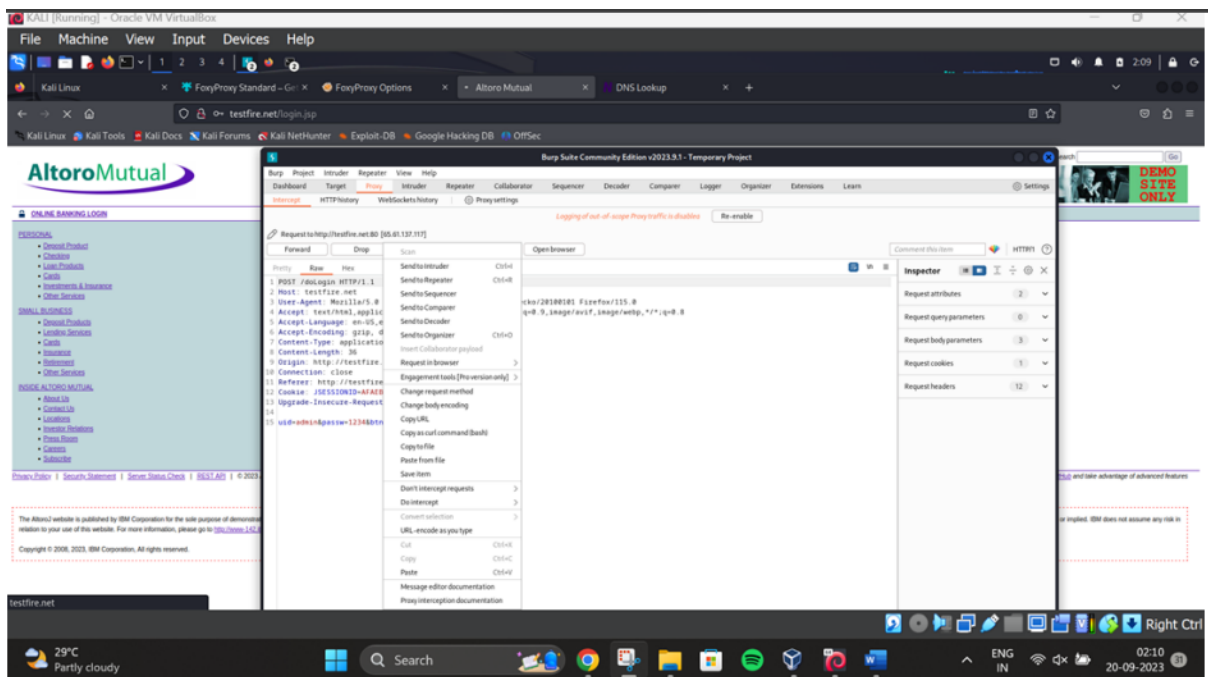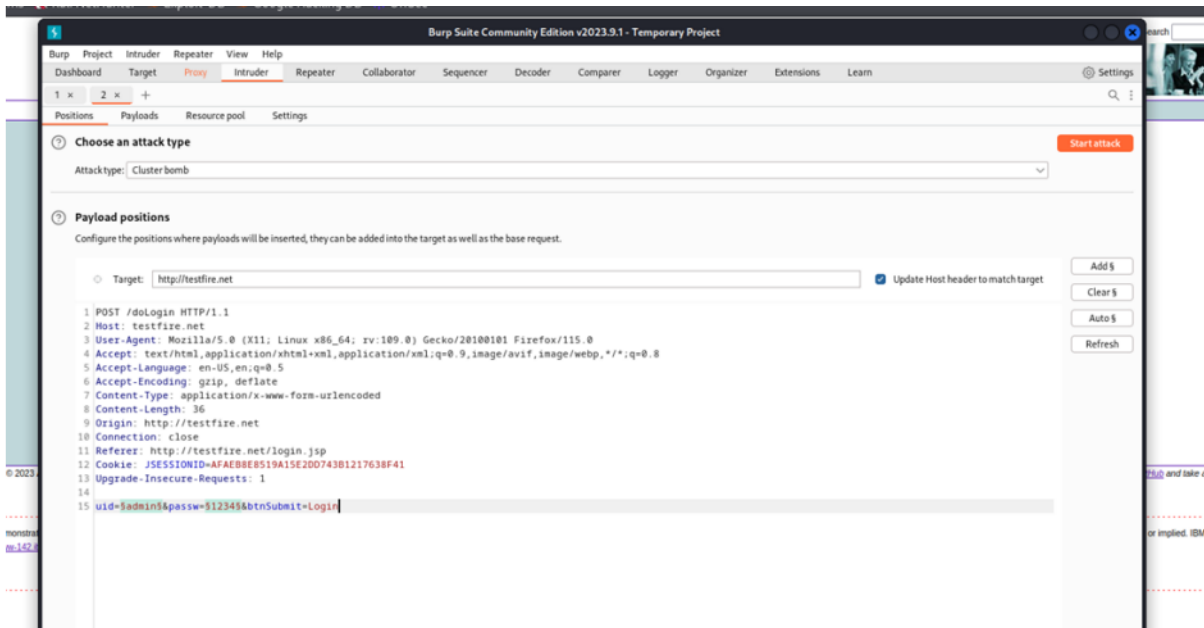
Then we go to the payloads tab and select payload 1 that is our username in this case and choose simple text and below give some random expected usernames. We can also upload a file here but since I do not have one I did it this way. We do the same for payload 2 which is our passwords and then start the attack.
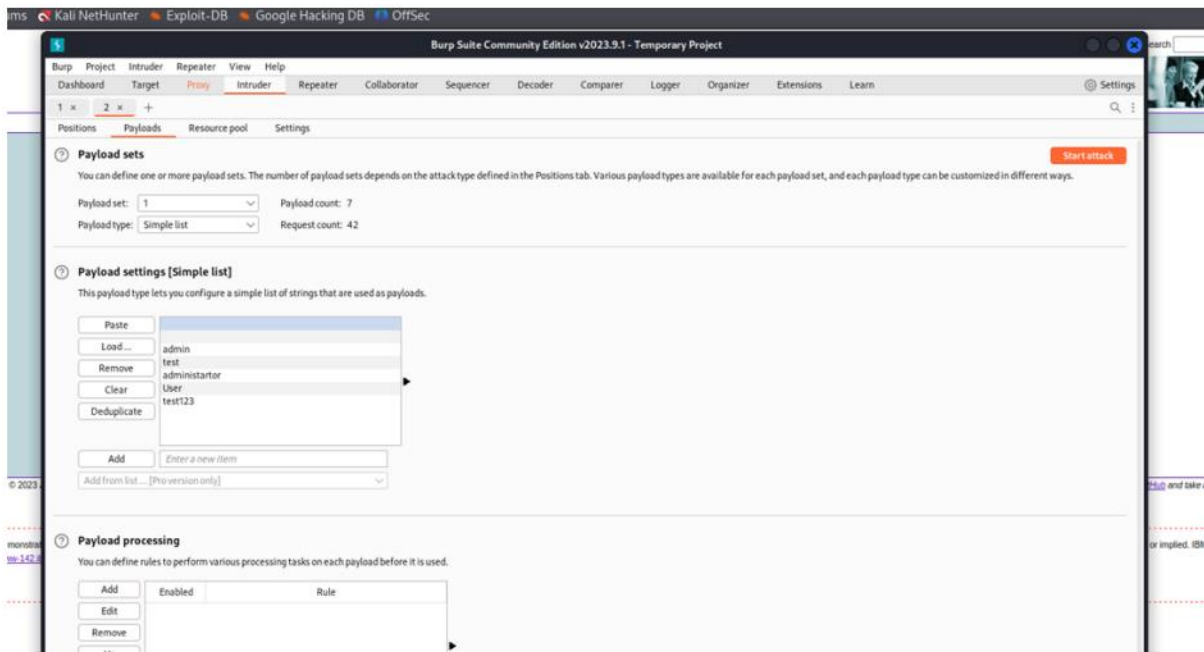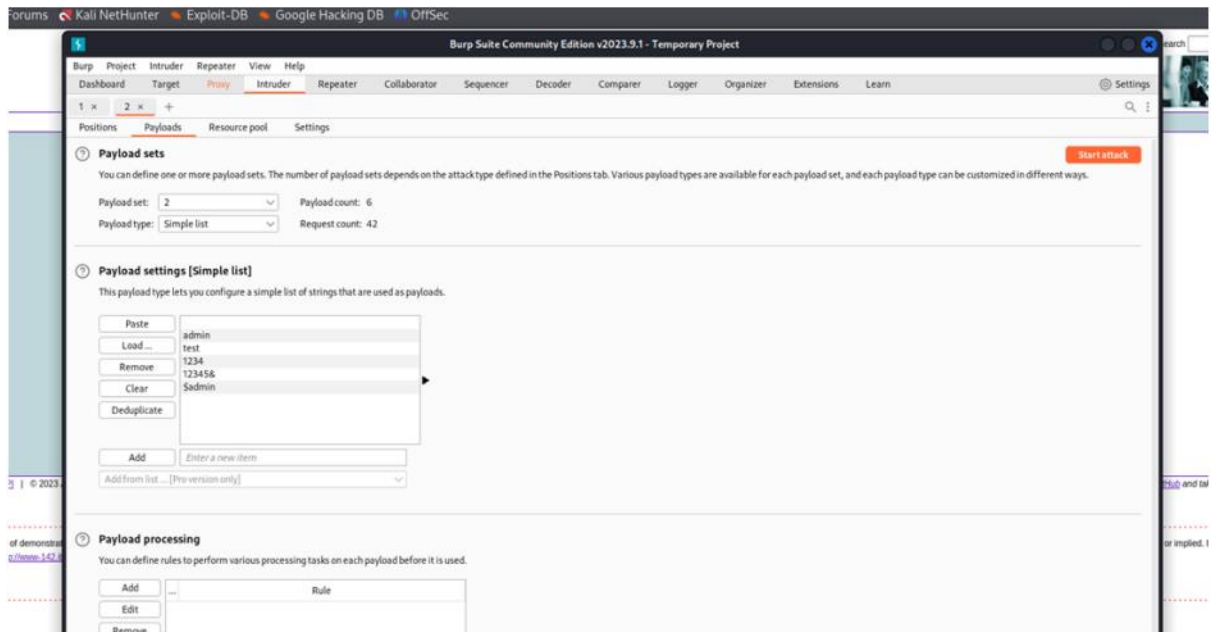
After the attack is finished we can see that the highlighted admin admin has different length from the others. Thus it can be a probable solution. Upon checking Request and response we can assure that this is working.

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	

```
   ▽ Filter: Showing all items

Request ∧        Payload 1              Payload 2         Status code   Error   Timeout   Length        Comment

   Request      Response

   Pretty     Raw     Hex

 1 POST /doLogin 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 Content-Type: application/x-www-form-urlencoded
 8 Content-Length: 37
 9 Origin: http://testfire.net
10 Connection: keep-alive
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=AFAEB8E8519A15E2DD743B1217638F41
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=admin&btnSubmit=Login
```

We then give the inputs in the login page and hence we are logged in
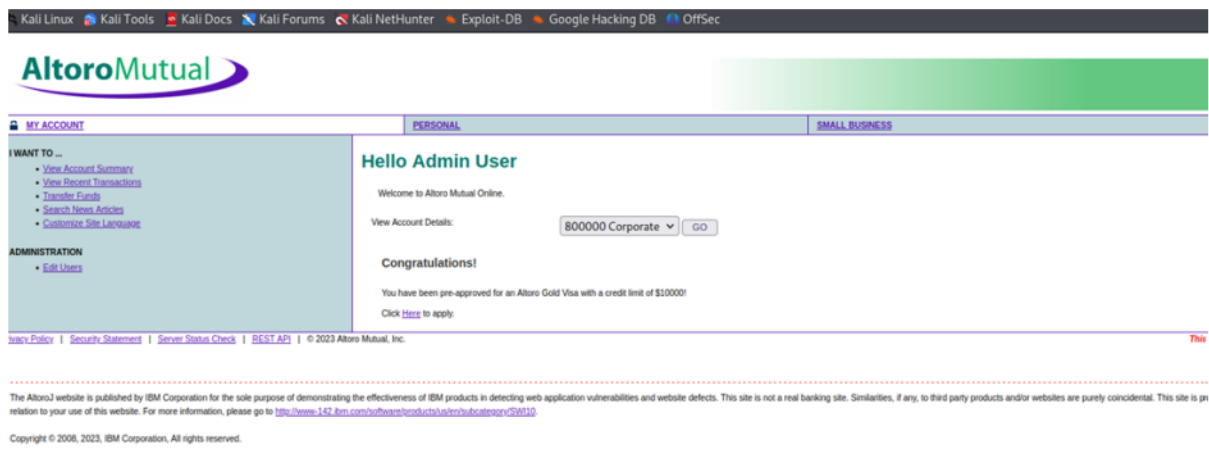
Business Impact:

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.

3. **Vulnerability name**: Broken authentication
   CWE: 285
   Description: The system's authorization functionality does not prevent one user from gaining access to another user's data or record by modifying the key value identifying the data.

Steps to reproduce:

Access the URL
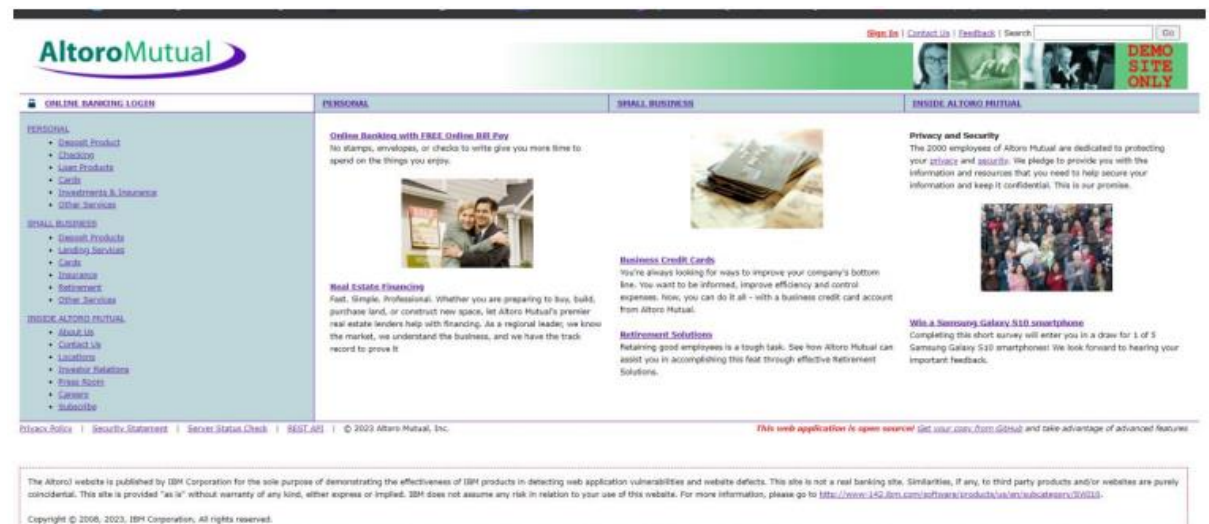
Now we will try to login using some different approach.

As we know which users are present in the database of this website by using the admin privileges. We can directly access a particular user by simply knowing their username; we will add some characters after his user name as a sql injection to simply bypass the password.

This leads us to the details of this person's account.

Business Impact:
 To effectively mitigate the business impact of CWE-285, it is imperative that organizations place a strong emphasis on bolstering their authentication and session management practices. This should encompass the adoption of multi-factor authentication, the secure storage of credentials, meticulous session handling, and a commitment to conducting routine security assessments and testing. The rectification of these vulnerabilities stands as a critical imperative, safeguarding sensitive data, user identities, and the organization's overarching security stature and reputation.

4. **Vulnerability Name**: Improper Input Validation (The website allows user to transfer amount greater than the user has in their account)

CWE (Common Weakness Enumeration): CWE-132

Description: The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.

Steps to reproduce:
Wearing off the account 800002.

Account History - 800002 Savings

Balance Detail		Amount
800002 Savings ⌄ Select Account		
Ending balance as of 10/27/23 4:03 PM		$998899999098100.00
Available balance		$998899999098100.00

Amount to be debited to make the account balance empty is 998899999098100

Account History - 800002 Savings

Balance Detail		Amount
800002 Savings ⌄ Select Account		
Ending balance as of 10/27/23 5:34 PM		$0.00
Available balance		$0.00

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

Transfer Funds

From Account:	800002 Savings ⌄
To Account:	800003 Checking ⌄
Amount to Transfer:	100

Transfer Money

Transfer Funds

From Account:	800002 Savings ⌄
To Account:	800002 Savings ⌄
Amount to Transfer:	

Transfer Money

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

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

5. **Vulnerability name:** Web server allows password auto-completion
   CWE: 310

   Description: Weaknesses in this category are related to the design and implementation of data confidentiality and integrity. Frequently these deal with the use of encoding techniques, encryption libraries, and hashing algorithms. The weaknesses in this category could lead to a degradation of the quality data if they are not addressed.

   Steps to reproduce:

   Access the URL
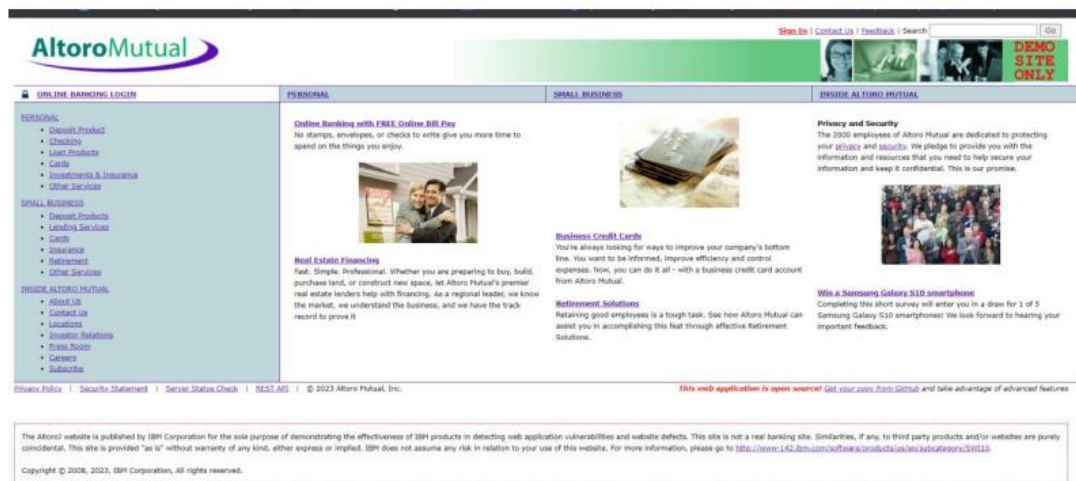
Online Banking Login

Username: [|]

Password: [   ]

[Login]

' or 1=1--

admin

Jsmith'--

Jdoe'--

— —

Username: [   ]

Password:

This connection is not secure.
Logins entered here could be
compromised. **Learn More**

⊕ admin
From this website

View Saved Logins

From this image we can see the usernames and the passwords getting auto filled. This is a potential vulnerability as this can be a doorway for attackers.

Business impact:

To effectively lessen the business consequences associated with CWE-310, organizations must prioritize the adoption of secure cryptographic practices. This entails ensuring proper password storage and robust encryption key management. Simultaneously, conducting routine security assessments and testing is pivotal in detecting and mitigating vulnerabilities related to cryptographic issues. Striving for compliance with pertinent data protection regulations and industry standards is equally essential. These actions are of paramount importance in the protection of sensitive data, the upholding of user trust, and the preservation of the organization's esteemed reputation.

6. **Vulnerability name**: Clickjacking
   CWE: 1021
   Description: The web application does not restrict or incorrectly restricts frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with
   Steps to reproduce:
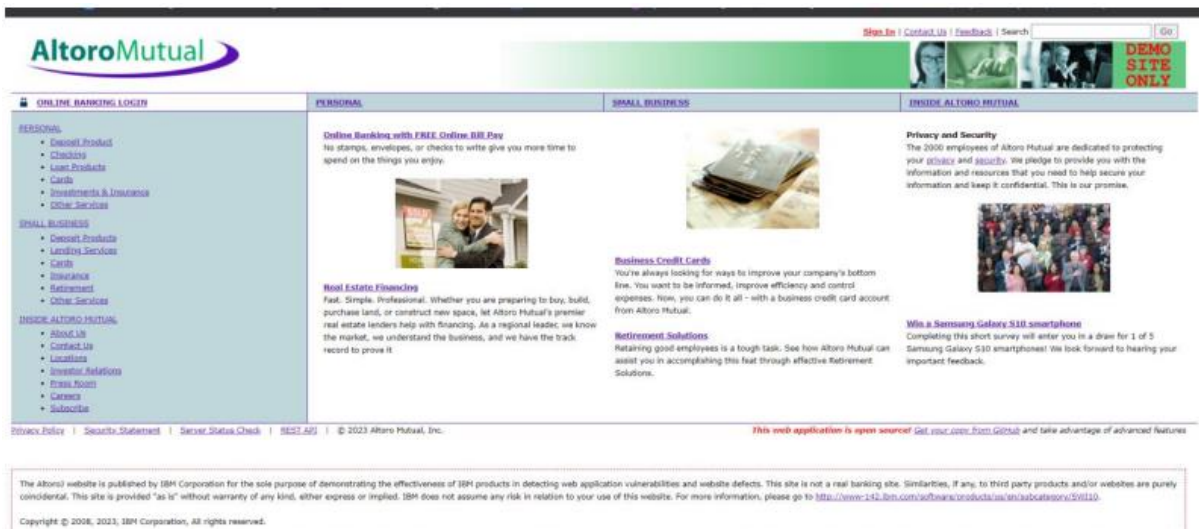
Then take the URL and use it for the html code we will be writing some html code to perform this vulnerability. We will be writing the code in vs code for better flexibility and functionality

```html
<html>
<body>
<title>Click jacking vulnerability</title>
<h2>This website is vulnerable to clickjacking</h2>
<iframe  src="http://testfire.net/"></iframe>
</body>
</html>
```

Executing the code in the browser

From this image we can see that the vulnerability has been found.

Business Impact:
To effectively reduce the business consequences resulting from CWE-1021, organizations must prioritize the implementation of protective measures, such as frame-busting code. Simultaneously, educating users on safe browsing practices plays a crucial role in preventing clickjacking incidents. Additionally, routine security assessments and testing are pivotal for identifying and mitigating

vulnerabilities associated with clickjacking. These actions are of paramount importance in upholding user trust, ensuring data protection, and safeguarding the organization's reputation.

7. **Vulnerability Name:** HTML injection attack

   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.

   Steps to reproduce:
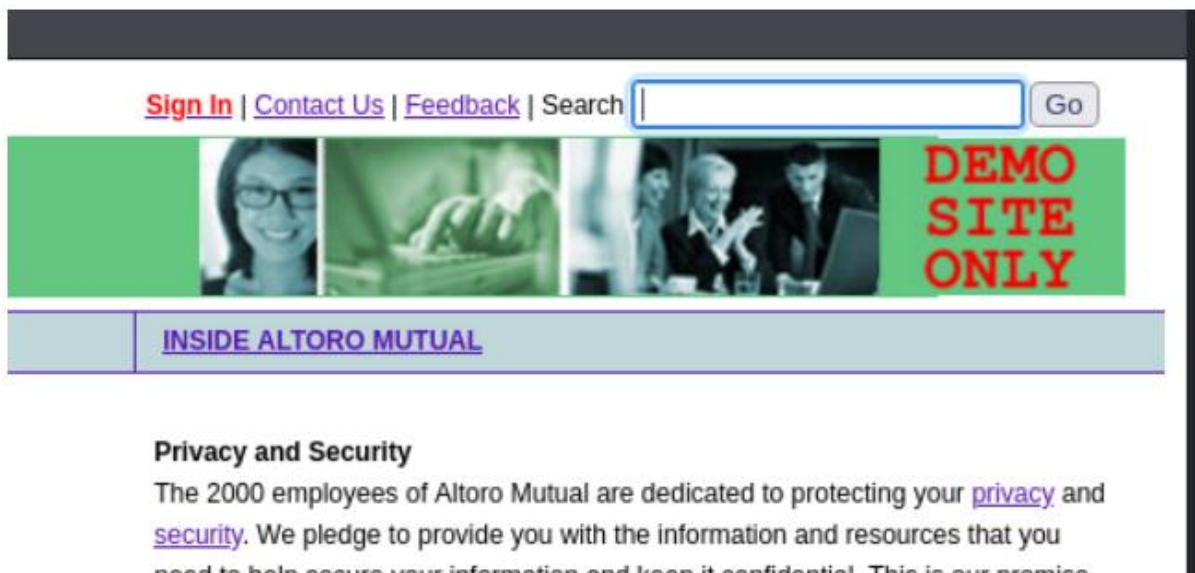
HTML payload: Click her to login
This payload's href link can be modified in certain way that it redirects to the malicious login page
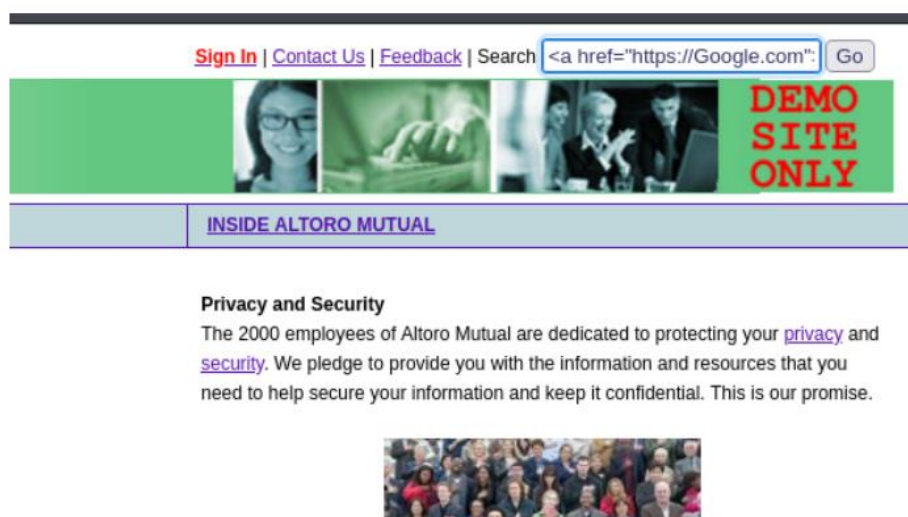
Executing the payload gives the following result.

Search Results

No results were found for the query:

click here to login

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

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.

8. **Vulnerability name**: Cross site scripting (stored)

   CWE: 79

   OWASP category: A03:2021 -Injections

   Description: It occurs when a malicious script is injected directly into a vulnerable web application. Reflected XSS involves the reflection of a malicious script of a web application, onto a user's browser.

   Steps to reproduce:

In the search box we will input some code to perform the vulnerabilit

The Script we will be inputting is <script> alert('hacked)</script>. This displays a harmless pop up alert box with the text saying 'hacked'

Business Impact:

The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. Later, the dangerous data is subsequently read back into the application and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user.

9. **Vulnerability name**: Cleartext Transmission of Sensitive Information

CWE: 319

Description: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors. Many communication channels can be "sniffed" (monitored) by adversaries during data transmission. For example, in networking, packets can traverse many intermediary nodes from the source to the destination, whether across the internet, an internal network, the cloud, etc. Some actors might have privileged access to a network interface or any link along the channel, such as a router, but they might not be authorized to collect the underlying data. As a result, network traffic could be sniffed by adversaries, spilling security-critical data.

Steps to reproduce:

Access the URL

Now we will try to sign in to this website with admin privileges

Also, we will be using burp suite to get requests from the website and know additional information. We use 'admin' for the username and password.

This request has been received in the burp suite with the username and password as well in clear text.

Now we click on forward request in the burp suite and then we will be redirected to the admin user details. Here in the burp suite, we can clearly see the login details in clear text. this is the clear indication of the vulnerability which can lead to data breach, monitored, and manipulated as well.

Business Impact:

To effectively reduce the business consequences associated with CWE-319, organizations must prioritize the adoption of secure data transmission practices. This includes the utilization of encryption and robust, secure protocols. The routine conduct of security assessments and testing is pivotal in pinpointing and remedying vulnerabilities linked to data transmission. Furthermore, the education of users on secure data handling practices plays a vital role in proactively preventing data exposure incidents. These actions are of paramount importance in the protection of sensitive data and in preserving the trust of both customers and partners.

10. **Vulnerability Name:** Insecure Direct object Reference
    CWE: 639
    OWASP Category: A01: Broken Access Control
    Description: Insecure Direct Object Reference (IDOR) is a vulnerability that arises when attackers can access or modify objects by manipulating identifiers used in a web application's URLs or parameters. It occurs due to missing access control checks, which fail to verify whether a user should be allowed to access specific data.
    Steps to reproduce:
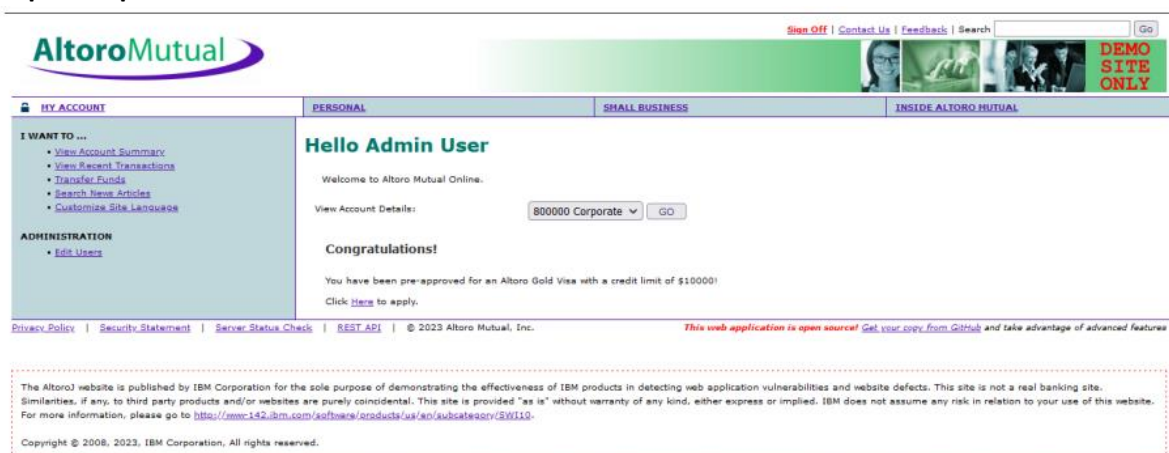
Open "Transfer Money" on the left side and fill in the details. On the intercept and click transfer

Open burp and notice the change

In the 15th line change the amount from 100 to 1000 and click forward

Look at the site, we can notice the msg that shows the transfer of 1000

Off the Intercept and open "View Recent Transactions".

I WANT TO ...
- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION
- Edit Users

Recent Transactions

After [ ] *yyyy-mm-dd*   Before [ ] *yyyy-mm-dd*   [Submit]

Transaction ID	Transaction Time	Account ID	Action	Amount
9016	2023-10-16 06:28	800001	Deposit	$1000.00
9015	2023-10-16 06:28	800000	Withdrawal	-$1000.00
8920	2023-10-16 04:46	800001	Deposit	$23345.00
8919	2023-10-16 04:46	800000	Withdrawal	-$23345.00
8916	2023-10-16 04:44	800001	Deposit	$23345.00
8915	2023-10-16 04:44	800000	Withdrawal	-$23345.00
8894	2023-10-16 04:40	800001	Deposit	$23345.00
8893	2023-10-16 04:40	800000	Withdrawal	-$23345.00
8892	2023-10-16 04:40	800001	Deposit	$23345.00
8891	2023-10-16 04:40	800000	Withdrawal	-$23345.00
7565	2023-10-16 04:17	800000	Withdrawal	-$10.00
7228	2023-10-16 04:14	800000	Deposit	$1000.00
6802	2023-10-16 04:09	800001	Deposit	$100000000000000.00
6801	2023-10-16 04:09	800000	Withdrawal	-$100000000000000.00
5388	2023-10-16 03:58	800000	Deposit	$10000000000.00
4628	2023-10-16 03:36	800001	Deposit	$20190.00
4627	2023-10-16 03:36	800000	Withdrawal	-$20190.00
4626	2023-10-16 03:35	800001	Deposit	$20190.00
4625	2023-10-16 03:35	800000	Withdrawal	-$20190.00
4624	2023-10-16 03:35	800001	Deposit	$600.00
4623	2023-10-16 03:35	800000	Withdrawal	-$600.00
4616	2023-10-16 03:10	800000	Deposit	$87446.00
4615	2023-10-16 03:10	800001	Withdrawal	-$87446.00

Business Impact:

To effectively mitigate the business impact of CWE-639, organizations must make it a top priority to fortify their access control and authorization mechanisms. This entails the implementation of robust security measures, the regular conduct of comprehensive security assessments, and the deployment of intrusion detection systems to promptly identify and counter unauthorized access attempts. These measures stand as absolutely critical in the defense of sensitive data, the overall security of systems, and the preservation of the organization's esteemed reputation