Team – 1.4

Vulnerability assessment – testfire.net

Vulnerability Name: SQL injection

CWE: CWE – 89

OWASP Category: A03:2021 – Injection

Description: SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. This can be done by injecting malicious SQL code into the application's input fields. If the application does not properly validate the input, the attacker's code will be executed by the database, potentially giving the attacker access to sensitive data or allowing them to modify or delete data.

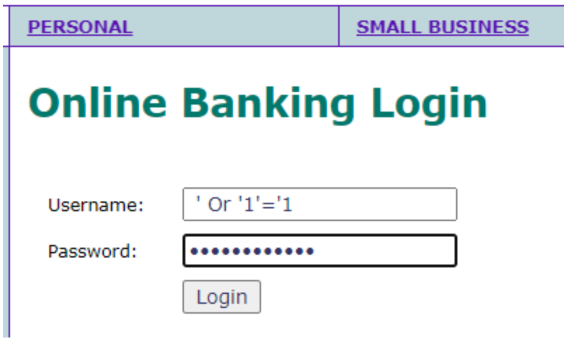
Business Impact: SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

Vulnerability Path: http://testfire.net/login.jsp

Vulnerability Parameter: http://testfire.net/bank/main.jsp

Steps to Reproduce:

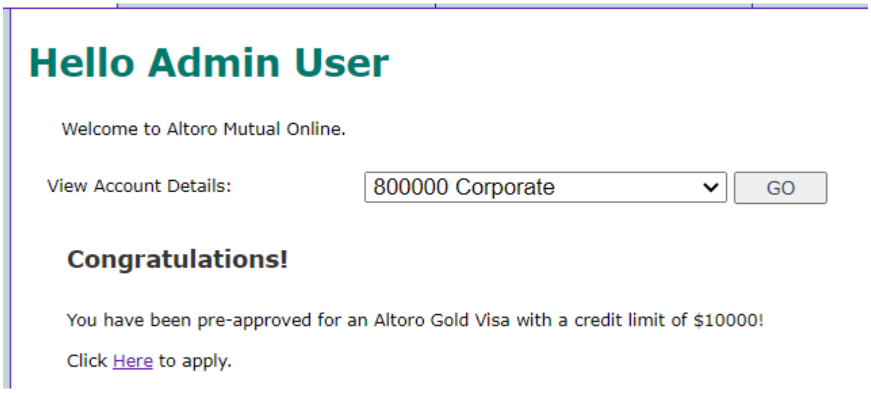
1) I was able to easily get through the login page of demo.testfire.net, accessible at http://testfire.net/login.jsp by using the payload ' Or '1'='1



Online Banking Login

Username: ' Or '1'='1

Password: ••••••••••••



Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

Vulnerability Name: Cross site scripting (XSS)

CWE: CWE-79

OWASP Category: A4: Cross-Site Scripting (XSS)

Description: Cross-site scripting (XSS) is a type of web security vulnerability that allows an attacker to inject malicious code into web pages viewed by other users. This code can then be executed when the victim views the page, potentially giving the attacker access to the victim's account, cookies, or other sensitive information.

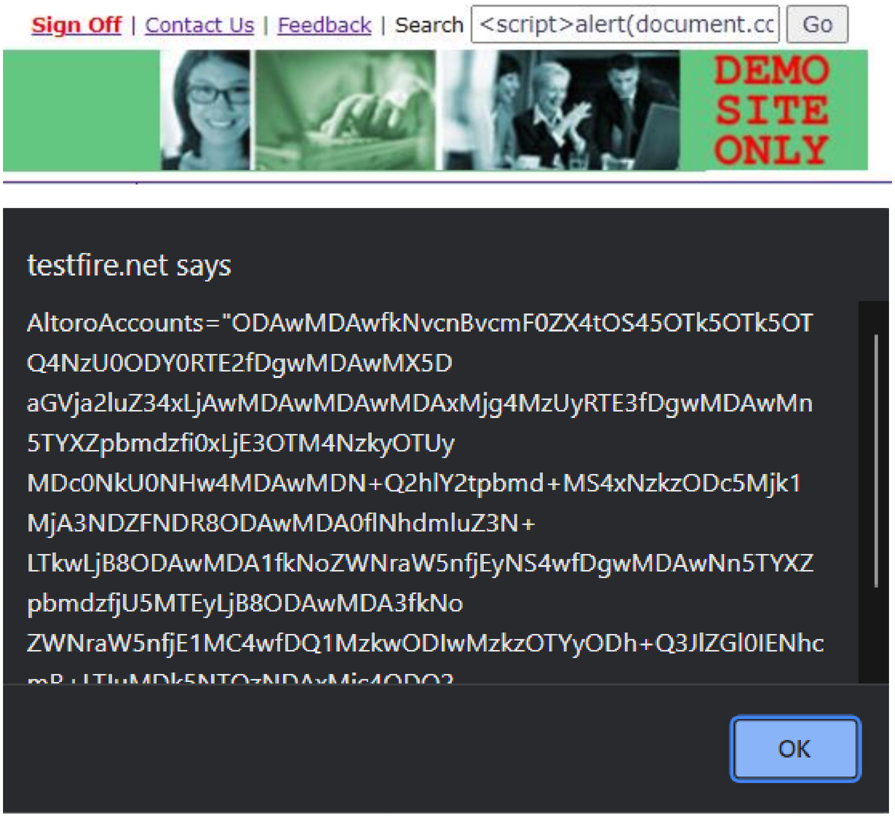
Business Impact: Attackers can masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account. XSS can also impact a business's reputation. An attacker can deface a corporate website by altering its content, thereby damaging the company's image or spreading misinformation.

Vulnerability Path: http://testfire.net/

Vulnerability Parameter: http://testfire.net/index.jsp

Steps to Reproduse:

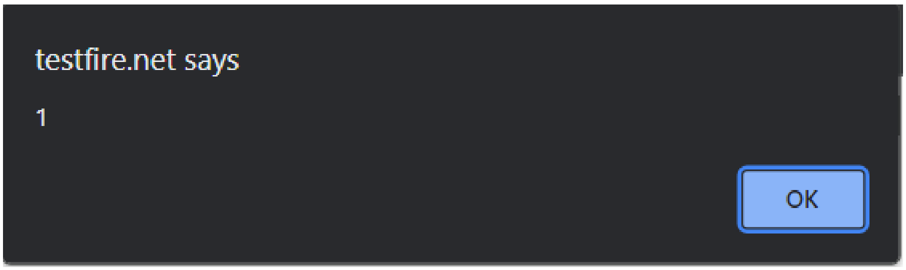
1) here you can retrive the cookie information using payload <script>alert(document.cookie)</script>


Sign Off | Contact Us | Feedback | Search
<script>alert(document.cc
Go
DEMO SITE ONLY
OK

testfire.net says

```
AltoroAccounts="ODAwMDAwfkNvcnBvcmF0ZX4tOS45OTk5OTk5OT
Q4NzU0ODY0RTE2fDgwMDAwMX5D
aGVja2luZ34xLjAwMDAwMDAwMDAxMjg4MzUyRTE3fDgwMDAwMn
5TYXZpbmdzfi0xLjE3OTM4NzkyOTUy
MDc0NkU0NHw4MDAwMDN+Q2hlY2tpbmd+MS4xNzkzODc5Mjk1
MjA3NDZFNDR8ODAwMDA0flNhdmluZ3N+
LTkwLjB8ODAwMDA1fkNoZWNraW5nfjEyNS4wfDgwMDAwNn5TYXZ
pbmdzfjU5MTEyLjB8ODAwMDA3fkNo
ZWNraW5nfjE1MC4wfDQ1MzkwODIwMzkzOTYyODh+Q3JlZGl0IENhc
```

2) Enter “<script>alert(1)</script>” in the search box returns with the output programmed by us. This shows the search box is vulnerable to Reflected XSS.



testfire.net says

1

Vulnerability Name: Insecure Direct Object Reference

CWE: CWE-639

OWASP Category: A1: Broken Access Control

Description: Insecure Direct Object Reference (IDOR) is a type of access control vulnerability that occurs when an application allows users to access objects directly without performing proper authorization checks. This can allow attackers to bypass authorization and access resources that they should not have access to, such as other users' data, sensitive files, or system functionality.

Business Impact: Insecure Direct Object Reference (IDOR) vulnerabilities can have a significant business impact on organizations of all sizes. By exploiting an IDOR vulnerability, an attacker could gain access to sensitive data, such as financial information, personal information, or trade secrets. They could also modify or delete data, or even take control of the application itself.

This could have a number of negative consequences for businesses, including:

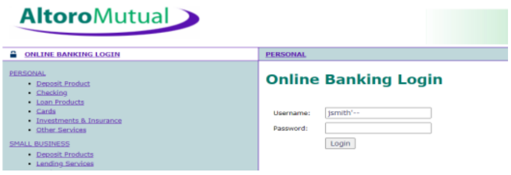
- Financial losses
- Damage to reputation
- Legal and regulatory fines
- Lost productivity
- Increased IT costs

Vulnerability Path: http://testfire.net/

Vulnerability Parameter: http://testfire.net/bank/transaction.jsp

Steps to Reproduse:

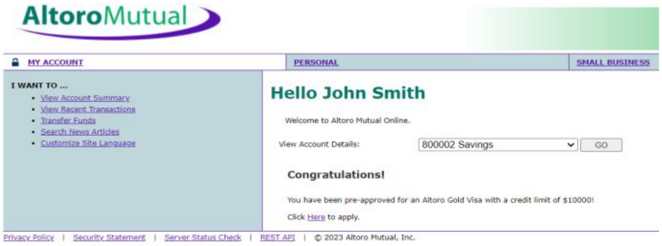
1) Enter the credentials to the sign in page.



Online Banking Login

Username: jsmith'--

Password:



AltoroMutual

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

Hello John Smith

Welcome to Altoro Mutual Online.

View Account Details: 800002 Savings GO

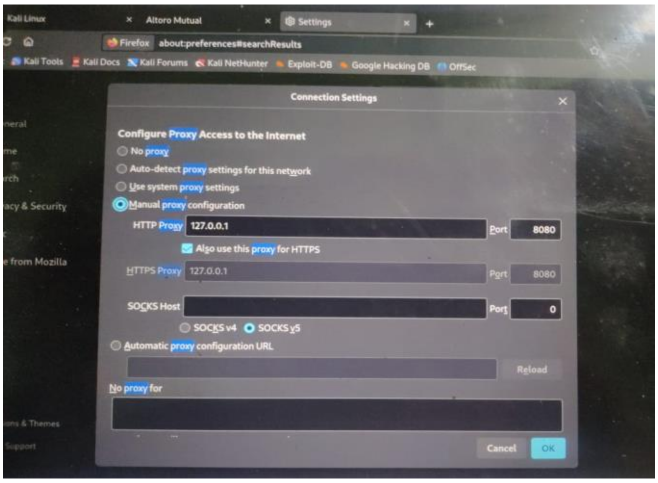
Congratulations!

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.

- inside the sign in page transfer money from savings account.
- To checking account.
- open Burp suite and change browser proxy setting



Connection Settings

Configure Proxy Access to the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for HTTPS

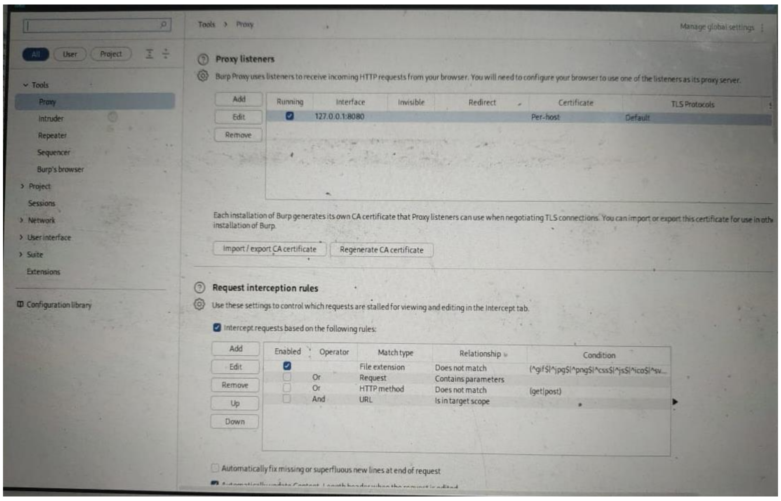
HTTPS Proxy 127.0.0.1 Port 8080

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for



Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	127.0.0.1:8080			Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in oth installation of Burp.

Request interception rules

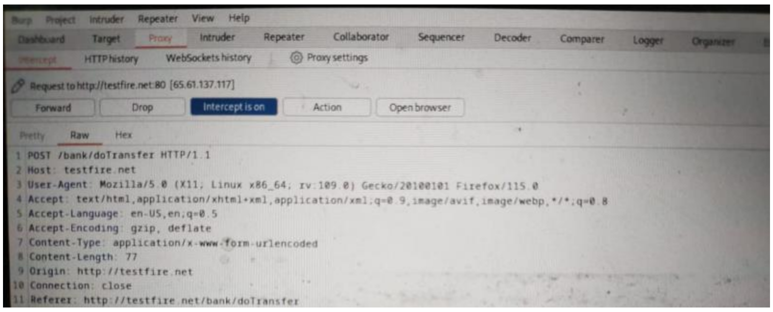
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$\|^ico$|^sv...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
□	And	URL	Is in target scope	

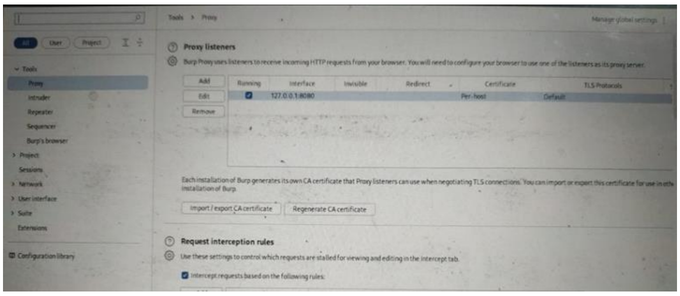
□ Automatically fix missing or superfluous new lines at end of request

- change receiver account. Number in intercept



Request to http://testfire.net:80 [65.61.137.117]

```
POST /bank/doTransfer 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: 77
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/bank/doTransfer
```



Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	127.0.0.1:8080			Per-host	Default

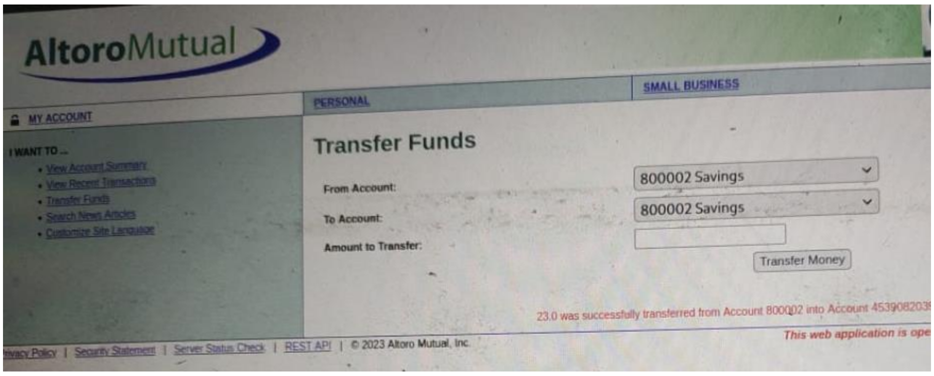
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in othe installation of Burp.

Request interception rules

Use these settings to control which requests are stalled for viewing and editing in the intercept tab.

☑ Intercept requests based on the following rules:

- transfer money



Transfer Funds

From Account: 800002 Savings

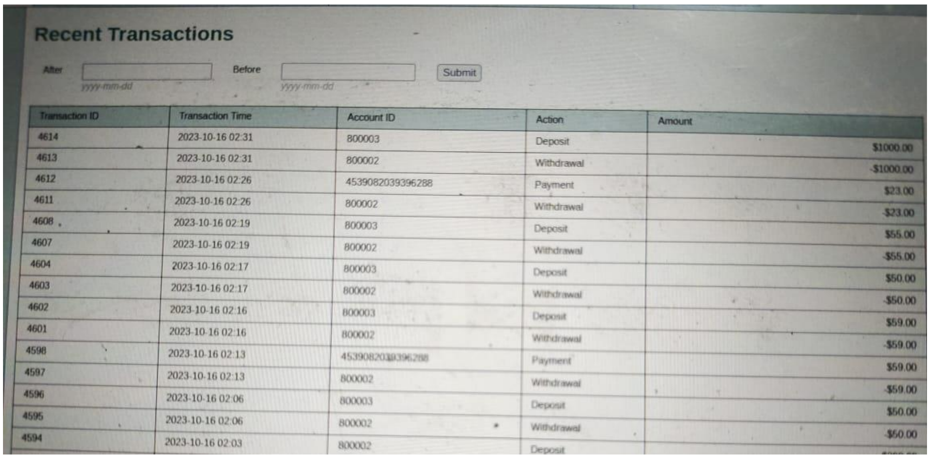
To Account: 800002 Savings

Amount to Transfer:

23.0 was successfully transferred from Account 800002 into Account 4539082039

This web application is ope

- check Recent transaction



Recent Transactions

Transaction ID	Transaction Time	Account ID	Action	Amount
4614	2023-10-16 02:31	800003	Deposit	$1000.00
4613	2023-10-16 02:31	800002	Withdrawal	-$1000.00
4612	2023-10-16 02:26	4539082039396288	Payment	$23.00
4611	2023-10-16 02:26	800002	Withdrawal	-$23.00
4608	2023-10-16 02:19	800003	Deposit	$55.00
4607	2023-10-16 02:19	800002	Withdrawal	-$55.00
4604	2023-10-16 02:17	800003	Deposit	$50.00
4603	2023-10-16 02:17	800002	Withdrawal	-$50.00
4602	2023-10-16 02:16	800003	Deposit	$59.00
4601	2023-10-16 02:16	800002	Withdrawal	-$59.00
4598	2023-10-16 02:13	4539082039396288	Payment	$59.00
4597	2023-10-16 02:13	800002	Withdrawal	-$59.00
4596	2023-10-16 02:06	800003	Deposit	$50.00
4595	2023-10-16 02:06	800002	Withdrawal	-$50.00
4594	2023-10-16 02:03	800002	Deposit	[illegible]

Vulnerability Name: Information Disclosure or Sensitive Data Exposure

CWE: CWE-200

OWASP Category: A3:2017-Sensitive Data Exposure

Description: Sensitive Data Exposure occurs when an organization unknowingly exposes sensitive data or when a security incident leads to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to sensitive data.

Business Impact: Risks of sensitive data exposure include identity theft, financial fraud, reputation damage, regulatory penalties, and loss of trust among customers or clients.

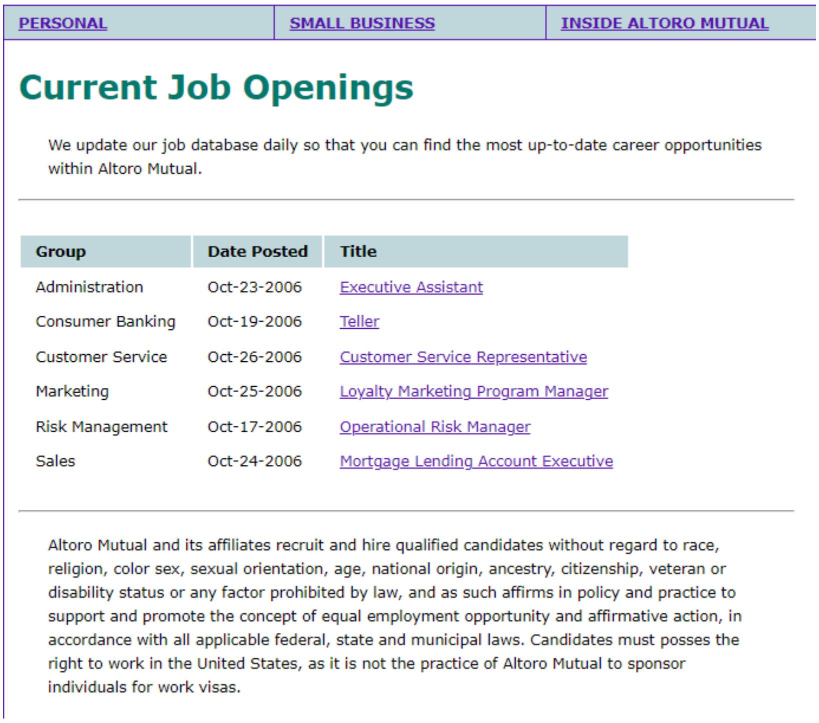
Vulnerability Path: http://testfire.net/

Vulnerability Parameter: http://testfire.net/index.jsp?content=inside_jobs.htm

Steps to Reproduse:

1) The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

   - Screenshot of the rendered page containing this vulnerability.



Current Job Openings

We update our job database daily so that you can find the most up-to-date career opportunities within Altoro Mutual.

Group	Date Posted	Title
Administration	Oct-23-2006	Executive Assistant
Consumer Banking	Oct-19-2006	Teller
Customer Service	Oct-26-2006	Customer Service Representative
Marketing	Oct-25-2006	Loyalty Marketing Program Manager
Risk Management	Oct-17-2006	Operational Risk Manager
Sales	Oct-24-2006	Mortgage Lending Account Executive

Altoro Mutual and its affiliates recruit and hire qualified candidates without regard to race, religion, color sex, sexual orientation, age, national origin, ancestry, citizenship, veteran or disability status or any factor prohibited by law, and as such affirms in policy and practice to support and promote the concept of equal employment opportunity and affirmative action, in accordance with all applicable federal, state and municipal laws. Candidates must posses the right to work in the United States, as it is not the practice of Altoro Mutual to sponsor individuals for work visas.

Vulnerability Name: Broken Authentication

CWE: CWE-287

OWASP Category: A2:2017- Broken Authentication

Description: When attackers are able to compromise passwords, keys or session tokens, user account information, and other details to assume user identities. Due to poor design and implementation of identity and access controls, the prevalence of broken authentication is widespread.

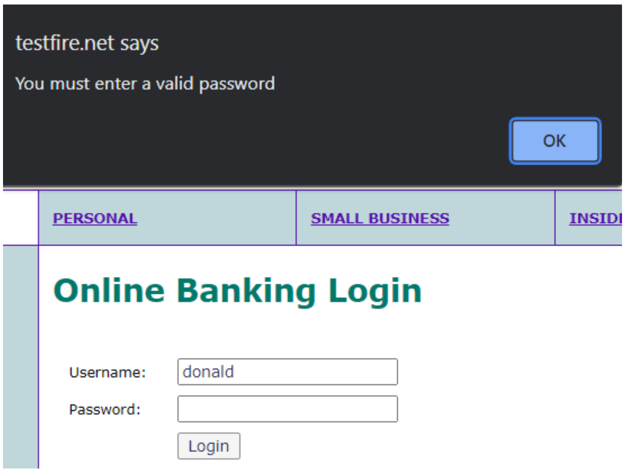
Business Impact: Attackers can also manipulate or delete user data, impersonate legitimate users, perform fraudulent transactions, or even escalate their privileges within the application.

Vulnerability Path: http://testfire.net/

Vulnerability Parameter: http://testfire.net/index.jsp?content=inside_jobs.htm

Steps to Reproduse:

1) give Username without password. We can see that it uses client-side JS validation



testfire.net says

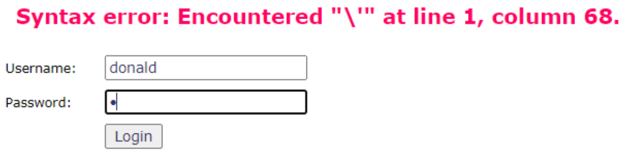
You must enter a valid password

Online Banking Login

Username: donald

Password:

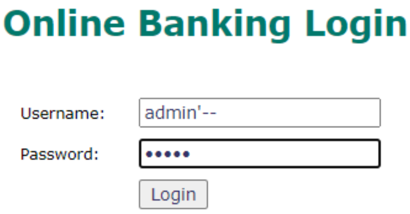
Enter your name into the username and a single tick into the password



Syntax error: Encountered "\'" at line 1, column 68.

Username: donald

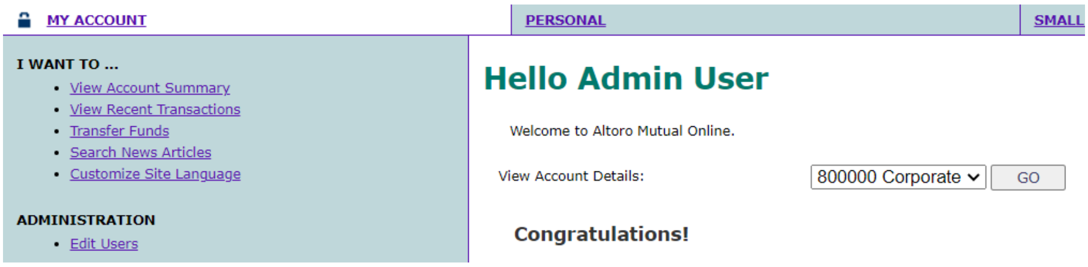
Password: •



Online Banking Login

Username: admin'--

Password: •••••



Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate

Congratulations!