THE RED USERS TASK 2

PENETRATION TESTING ON WEB APPLICATIONS

VENKATESH VOOTA

20TH AUG 2024

Table of Contents

INTRODUCTION TO PROJECT:

The project titled "Penetration Testing on Web Applications" was created Vulnerabilities and Penetration Testing (VAPT) are both security services that focus on identifying vulnerabilities in the network, server and system infrastructure. Both the services serves a different purpose and are carried out to achieve different but complimentary goals. Vulnerability Assessment focuses on internal organizational security, while Penetration Testing focuses on external real-world risk. Vulnerability Assessment (VA) is a rapid automated review of network devices, servers and systems to identify key vulnerabilities and configuration issues that an attacker may be able to take advantage off. Its generally conducted within the network on internal devices and due to its low footprint can be carried out as often as every day. Penetration Testing (PT or PenTest) is an in-depth expert-driven activity focused on identifying various possible routes an attacker could use to break into the network. In-addition with the vulnerabilities it also identifies the potential damage and further internal compromise an attacker could carry out once they are past the perimeter. Web Application Penetration Testing is security testing methods for security holes or vulnerabilities in web applications and corporate websites. Due to these vulnerabilities, websites are left open for exploitation.

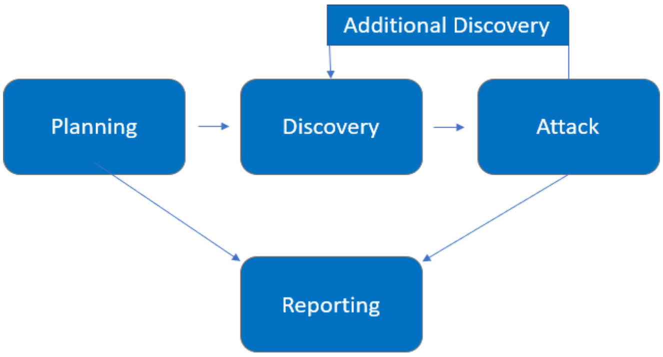
In this Project, Penetration Testing is conducted on Open source wed application and the web application name is Altoro Mutual (testfire.net). It is a banking web application and it is provided by HCL company A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

ASSESSMENT OVERVIEW:

Our Task to evaluate the security posture of its Company infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the OWASP Testing Guide, and customized testing frameworks.

Phases of penetration testing activities include the following:

- **Planning** – Customer goals are gathered and rules of engagement obtained.
- **Discovery** – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- **Attack** – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- **Reporting** – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



DIFFERENT TYPES OF WEB APPLICATION PENETRATION TESTING TOOLS:

The project was conducted through the use of one Penetration Tester on Kali Linux. The rationale behind using various sources and methods was to ensure a comprehensive and wide range of vulnerabilities to be detected. It was also to ensure a lack of overreliance on one source, but to implement various sources to increase accuracy in results and findings.

TOOLS:

1. **NMAP**:

   NMAP is short for Network Mapper. It is an open-source tool that helps you map a network by scanning ports, discovering operating systems, and creating an inventory of devices and the services running on them. It sends differently structured packets for different transport layer protocols which return with IP addresses and other information. You can use this information for Metasploit currently includes nearly 1677 exploits along with almost 500 payloads that include

● Command shell payloads

● Dynamic payloads

● Meterpreter payloads

● Static payloads

The framework also includes listeners, encoders, post-exploitation code, and whatnot.

● Host discovery

● OS fingerprinting

● Service discovery

● Security auditing

You can use the tool for a large network with thousands of devices and ports.

2. **Wireshark:**

Wireshark is another famous open-source tool that you can use for protocol analysis. It allows you to monitor network activities at a microscopic level. It is a growing platform with thousands of developers contributing from across the world.

With Wireshark you can perform

● Live capture and offline analysis

● Inspection of hundreds of different protocols

● Browse captured data via GUI

● Decrypt protocols

● Read live data from Ethernet, and a number of other mediums

● Export output to XML, PostScript, CSV, or plain text

Wireshark is the industry standard for protocol analysis in many different sectors. If you know what you are doing, it is a great tool to use.

3. **Metasploit**:

   Metasploit is a Ruby-based open-source framework, used by both ethical hackers and malicious actors to probe systematic vulnerabilities on networks and servers. The Metasploit framework also contains portions of fuzzing, anti-forensic, and evasion tools. It is easy to install and can work on a wide range of platforms regardless of the languages they run on. The popularity and the wide availability of Metasploit among professional hackers make it an important tool for Penetration Testers as well.

4. **Burp Suite:**

   Burp Suite is a set of penetration testing tools by Portswigger Web Security. It is used by ethical hackers, pen-testers, and security engineers. It is like a one-stop-shop for bug bounty hunters and security researchers. Let us take a look at a few tools included in Burp Suite.

   ● Spider: It is a web crawler. You can use it to map the target application. It lets you create an inventory of all the endpoints, monitor their functionalities, and look for vulnerabilities.

   ● Proxy: As explained earlier, a proxy sits between the browser and the internet to monitor, and modify the requests and responses in transit.

- Intruder: It runs a set of values through an input point and lets you analyze the output for success, failure and content length.

These aside the suite includes Repeater, Sequencer, Decoder, Extender, and some other add-on tools.

FINDING SEVERITY RATINGS:

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

RISK FACTORS

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability’s effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

SCOPE

Assessment	Details
Web Application Penetration test	https://testfire.net

Scope Exclusions

Our Project did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

TESTING SUMMARY

The Web Application assessment evaluated TestFire Web Application security posture. From an internal perspective, the pen tester performed manual vulnerability assessment against the website link provided by testfire to evaluate the overall patching health of the website. The pen tester found many vulnerabilities on the web app and exploited it.

The pen tester used some manual techniques to exploit basic level of vulnerabilities and was successfully able to get admin access to the web app using various exploitation methods. The security of the web app is completely compromised by basic level of exploitation which are mentioned below along with the evidence. Since it was a time bound assessment so most the vulnerabilities were reported by the pen tester in the given time. However, there are more serious exploits still present in the system but due to the time limit only some of them are reported.

KEY STRENGTHS AND WEAKNESSES:

The following identifies the key strengths identified during the assessment:

The following identifies the key weaknesses identified during the assessment:

1. Default credentials were used in web app
2. Broken Authentication.
3. Improper input validation on various input parameters
4. Internal server error being displayed.
5. Insecure direct object reference allowed.
6. Injection allowed on various input parameters.
7. No mechanism to stop brute force of login information
8. Displaying user information on web page.
9. GitHub source code link of web app displayed on screen.

VULNERABILITY SUMMARY & REPORT CARD

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Web Application Penetration Test Findings

1	4	1	1	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Web Application Penetration Test		
1: Apache Tomcat insecure default administrative password	High	Change the default password
2: Insecure Direct Object reference	High	Validate and filter any sort of input even if it's not malicious.
3: SQL Injection Vulnerability allowing login bypass.	Critical	Use parametrized query instead of string concatenation within the query.
4: Login Brute on username and password.	High	Restrict multiple requests from a same source.
5: Improper input Validation.	High	Proper validation and filter of input to be performed.
6: Reflected XSS.	Moderate	Implement proper filtration of various characters during input.
7. Displaying user info on web app	Low	Properly check for any user info displayed on screen.
8. Displaying internal server error.	Informational	Properly check error log and error messages displayed on screen.

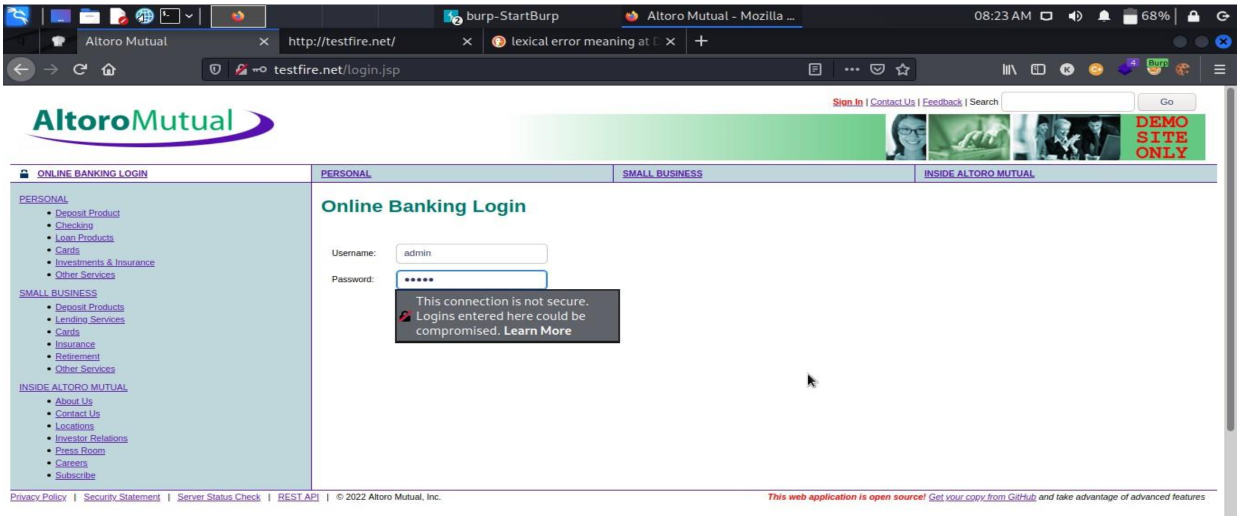
TECHNICAL FINDINGS

Web Application Penetration Test Findings

Finding 001: Apache Tomcat Insecure Default Administrative Password (High)

Description:	Test fire allows the use of default admin password being used on the login page due to which any unauthenticated user knowing the default password available on the internet can gain access to the admin account and have admin privileges.
Risk:	Likelihood: High – This attack is effective on web app and have major consequences to it. Impact: Very High – This attack gives admin privilege to a user who can make any changes on the web application.
System:	All
Tools Used:	Manually
References:	https://www.acunetix.com/vulnerabilities/web/apache-geronimo- default-administrative-credentials/

Evidence

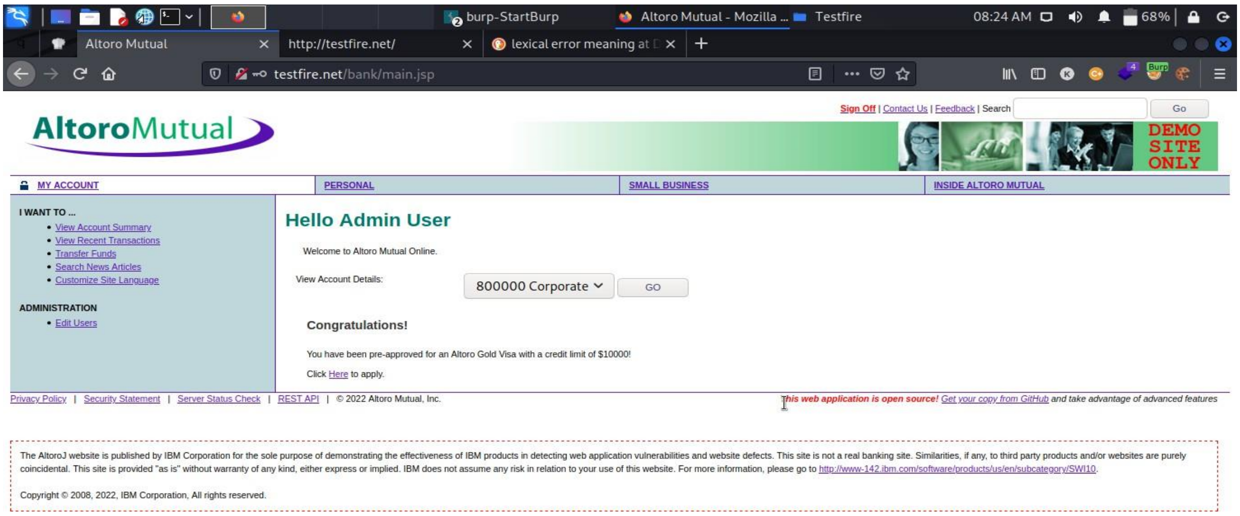


Online Banking Login

Username: admin

Password: •••••

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



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.

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 provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2022, IBM Corporation, All rights reserved.

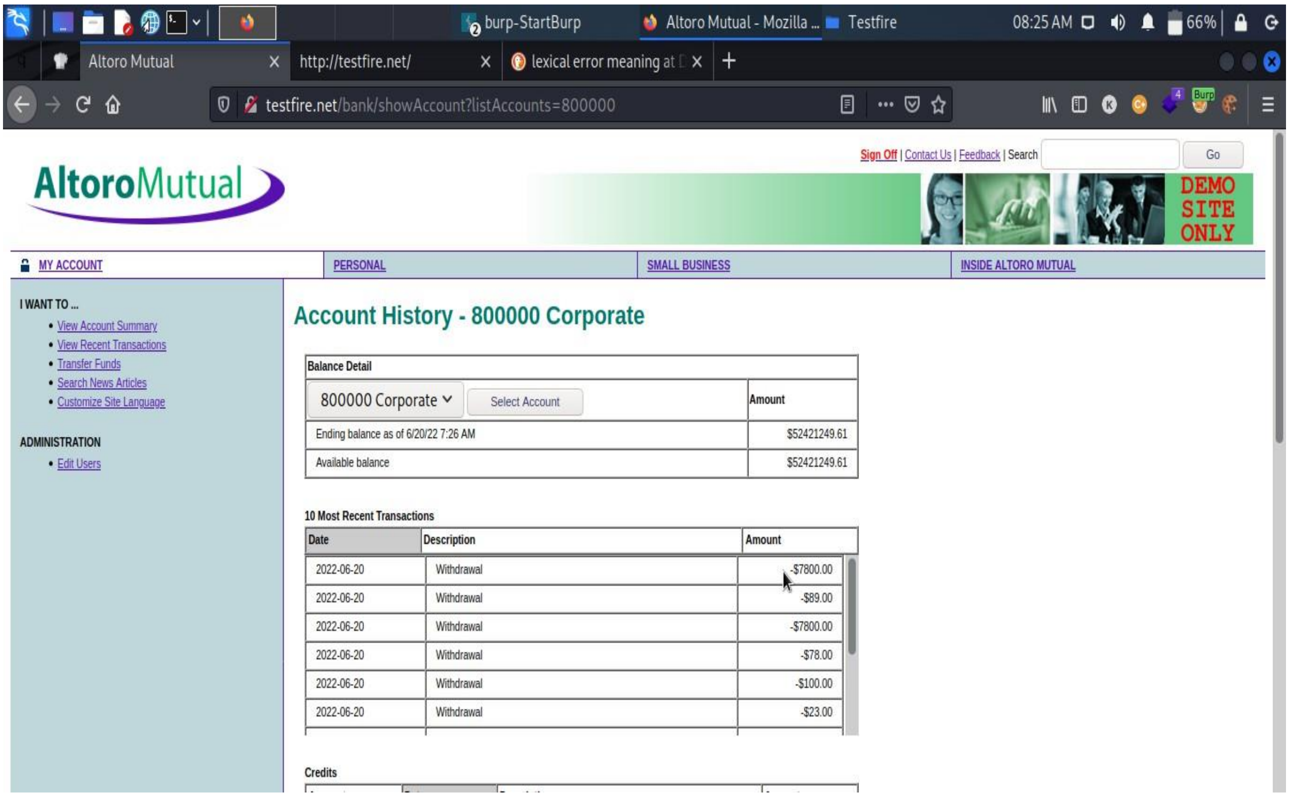
REMEDIATION

Change the Administrative Default username and password

Finding 002: Insecure Direct object Reference (High)

Description:	This vulnerability allows any user to view all account info of different user without authentication. The user just has to change the account number of the get request and he/she will be able to view sensitive account information about a different user.
Risk:	Likelihood: High – This attack is effective and can display sensitive account information about a different user Impact: Very High – Changing get request directly from the allows user to view account information about different user.
System:	All
Tools Used:	Manually
References:	https://www.cvedetails.com/cve/CVE-2022-29627

Evidence



testfire.net/bank/showAccount?listAccounts=800000

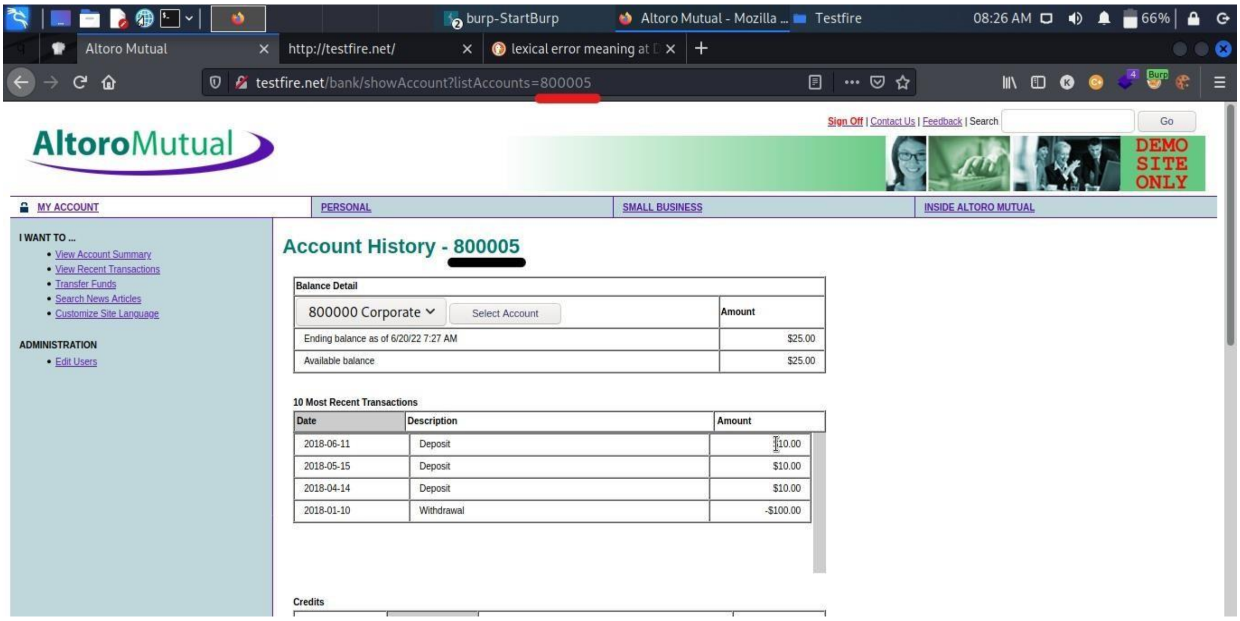
Account History - 800000 Corporate

Balance Detail	
800000 Corporate Select Account	Amount
Ending balance as of 6/20/22 7:26 AM	$52421249.61
Available balance	$52421249.61

10 Most Recent Transactions

Date	Description	Amount
2022-06-20	Withdrawal	-$7800.00
2022-06-20	Withdrawal	-$89.00
2022-06-20	Withdrawal	-$7800.00
2022-06-20	Withdrawal	-$78.00
2022-06-20	Withdrawal	-$100.00
2022-06-20	Withdrawal	-$23.00

Credits



testfire.net/bank/showAccount?listAccounts=800005

Account History - 800005

Balance Detail	Amount
Ending balance as of 6/20/22 7:27 AM	$25.00
Available balance	$25.00

10 Most Recent Transactions

Date	Description	Amount
2018-06-11	Deposit	$10.00
2018-05-15	Deposit	$10.00
2018-04-14	Deposit	$10.00
2018-01-10	Withdrawal	-$100.00

Credits

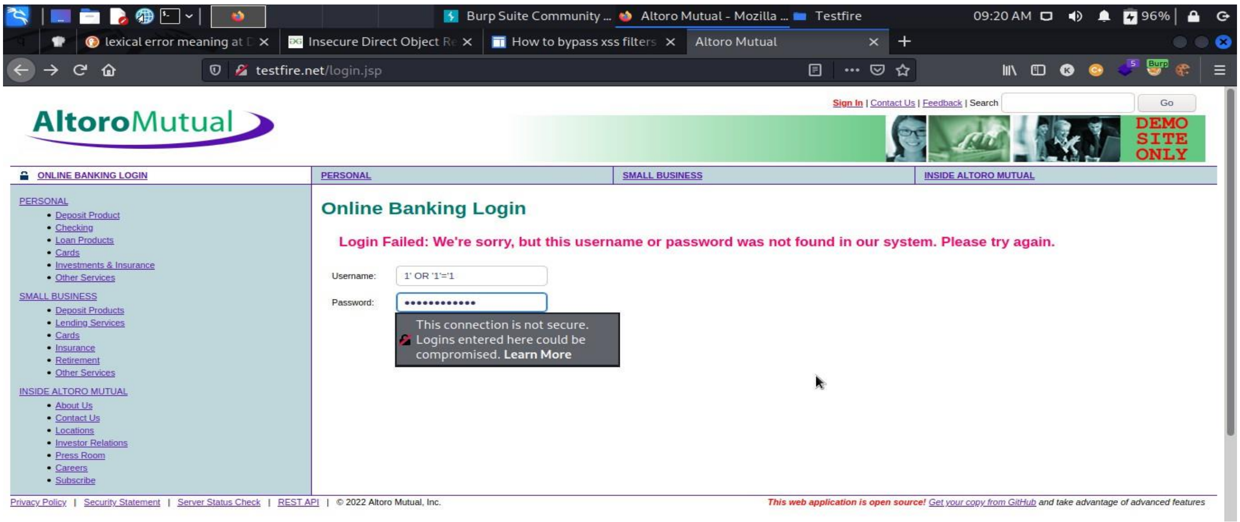
REMEDIATION

Proper implementation of security standards on the get and past request.

Finding 003: SQL Injection Vulnerability allowing login bypass (Critical).

Description:	TestFire allowed a successful SQL injection attack can result in unauthorized access to admin account and user accounts as well using the same method the login security if the web app was fully compromised.
Risk:	Likelihood: Critical – This attack allowed admin as well as user login acces to the web application. Impact: Critical – After gaining admin privilege the user has all acces to the backend of the system
System:	All
Tools Used:	Manually
References:	https://portswigger.net/web-security/sql-injection

Evidence



testfire.net/login.jsp

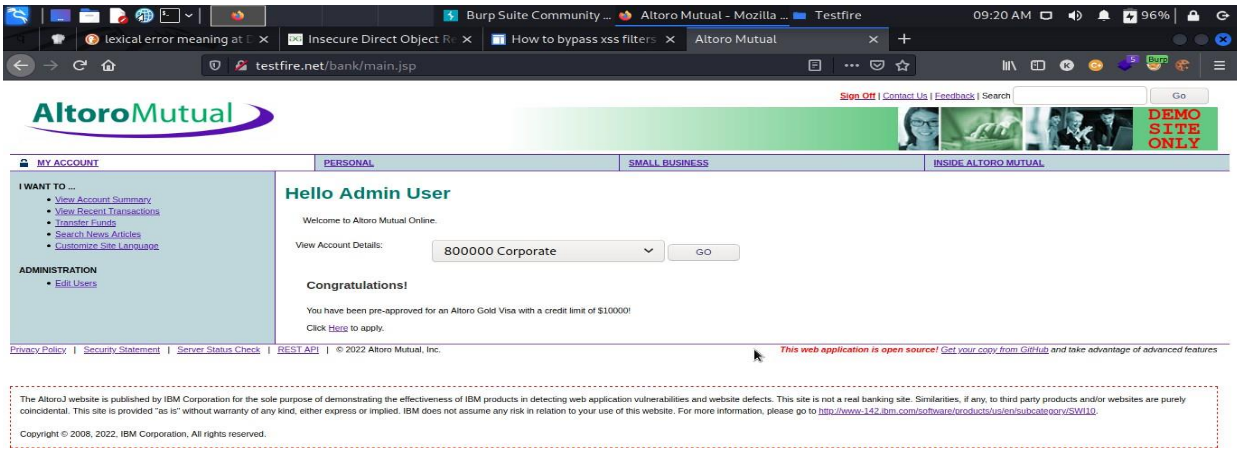
Online Banking Login

Login Failed: We're sorry, but this username or password was not found in our system. Please try again.

Username: 1' OR '1'='1

Password: ••••••••••••

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



testfire.net/bank/main.jsp

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

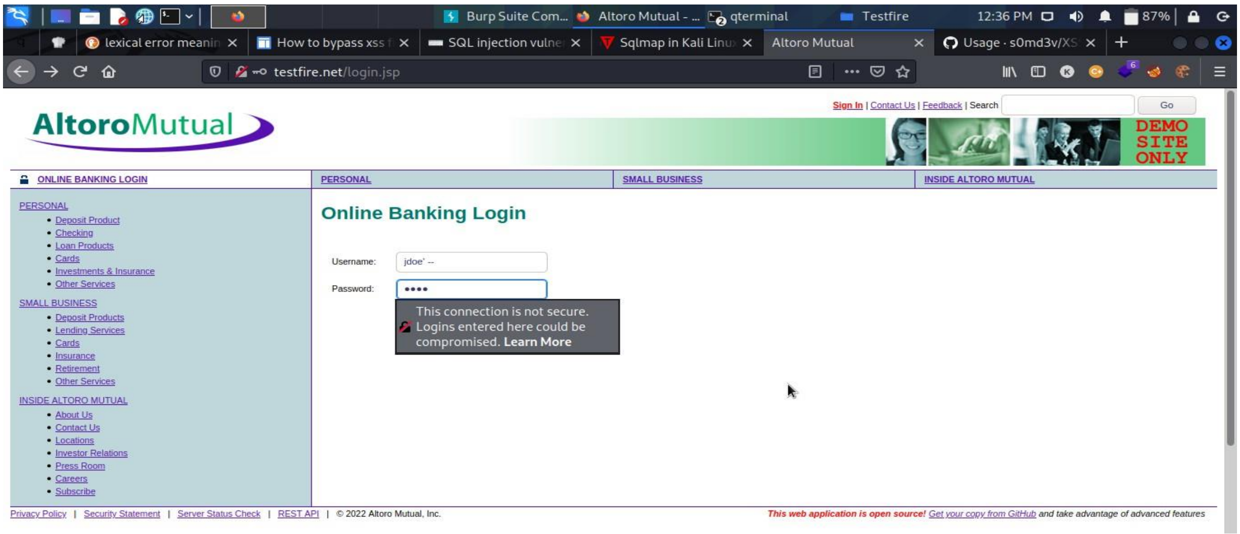
You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

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 provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2022, IBM Corporation, All rights reserved.

Burp Suite Community ...
Altoro Mutual - Mozilla ...
Testfire
09:20 AM
96%
Sign Off | Contact Us | Feedback | Search
Go
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
Edit Users
Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features



testfire.net/login.jsp

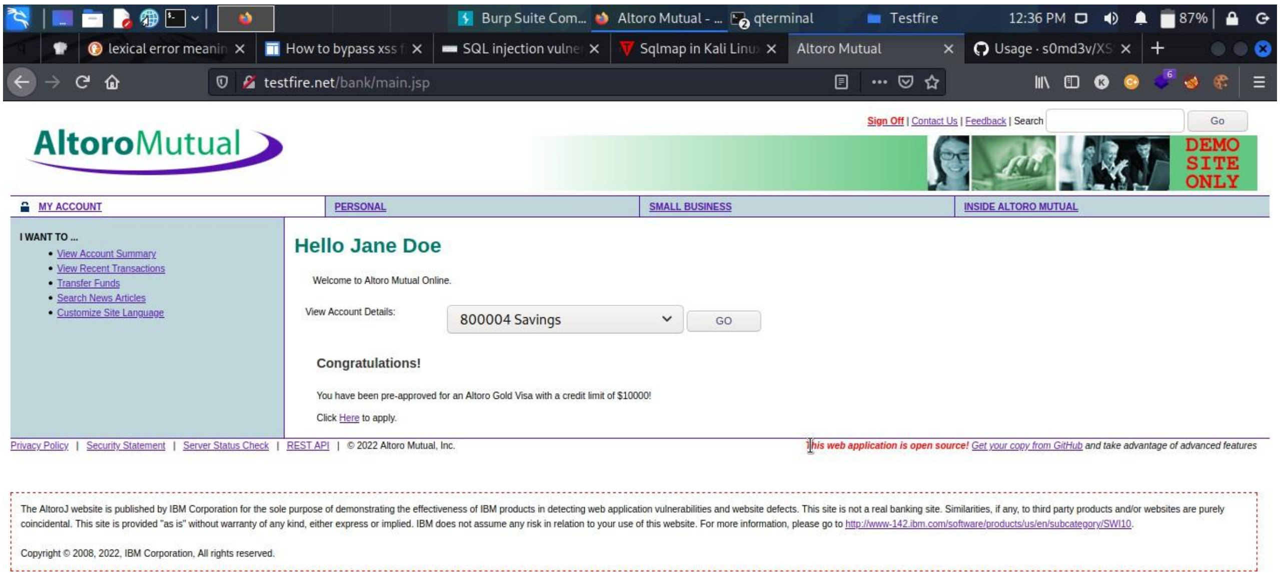
Online Banking Login

Username: jdoe' --

Password: ••••

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

Burp Suite Com...
Altoro Mutual - ...
qterminal
Testfire
12:36 PM
87%
lexical error meanin
How to bypass xss
SQL injection vulne
Sqlmap in Kali Linu
Altoro Mutual
Usage · s0md3v/XS
Sign In | Contact Us | Feedback | Search
Go
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features



I WANT TO ...

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

Hello Jane Doe

Welcome to Altoro Mutual Online.

View Account Details: 800004 Savings

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 | © 2022 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

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 provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2022, IBM Corporation, All rights reserved.

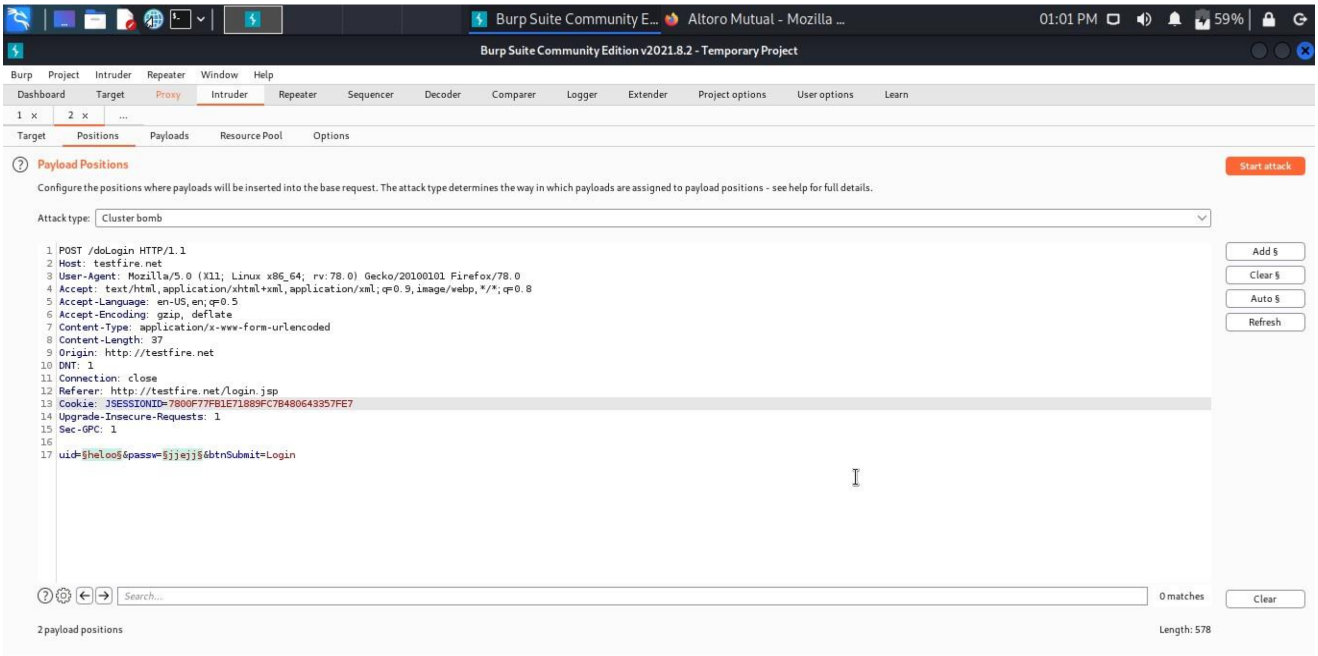
REMEDIATION

Proper Input Validation And filtering of username and password.

Finding 004: Login Brute force of username and password (High)

Description:	Testfire allowed multiple spraying of username and password on the web app without any restriction.
Risk:	Likelihood: High – The penetration tester sprayed hundreds of username and password on the web application. Impact: Very High – The attacker can get the username and password of the admin and users.
System:	All
Tools Used:	Burpsuite
References:	https://www.alpinesecurity.com/blog/brute-forcing-login-page-with-burp-suite/

Evidence



Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

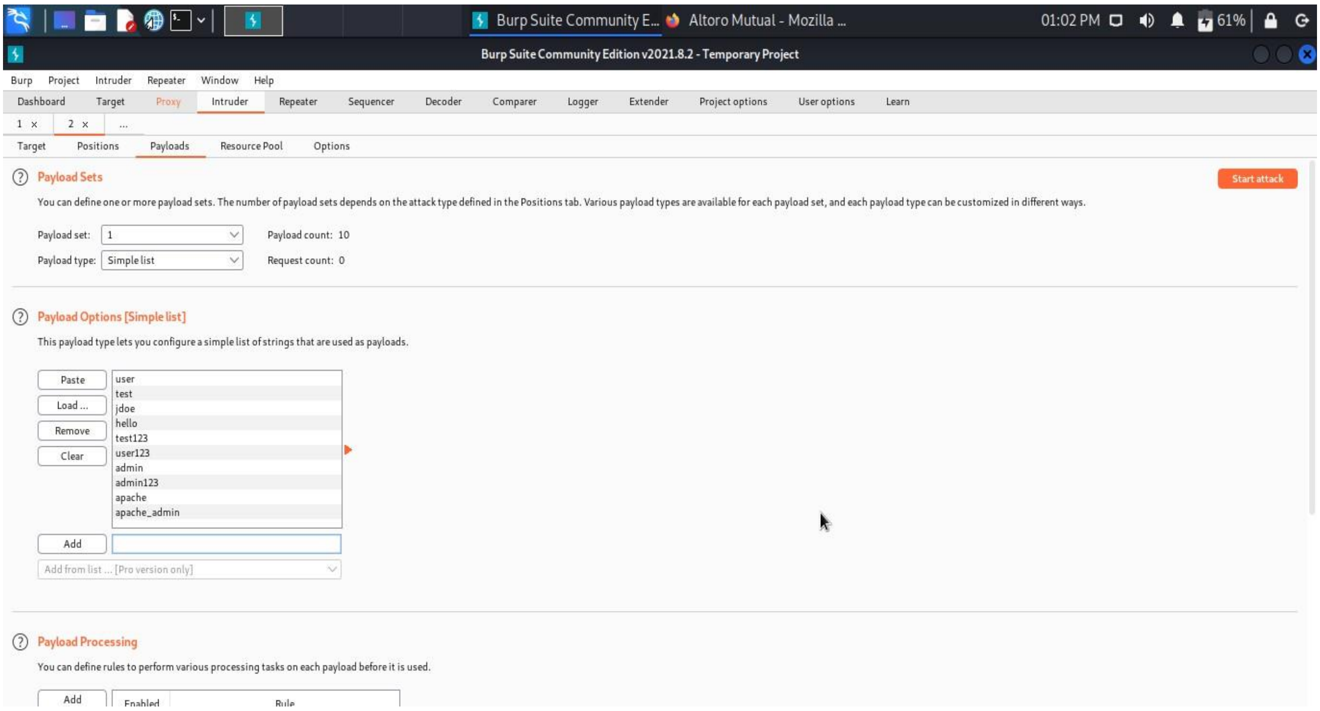
Attack type: Cluster bomb

```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: 37
Origin: http://testfire.net
DNT: 1
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=7800F77FB1E71889FC7B480643357FE7
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

uid=§heloo§&passw=§jjejj§&btnSubmit=Login
```

2 payload positions

Length: 578



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 10

Payload type: Simple list Request count: 0

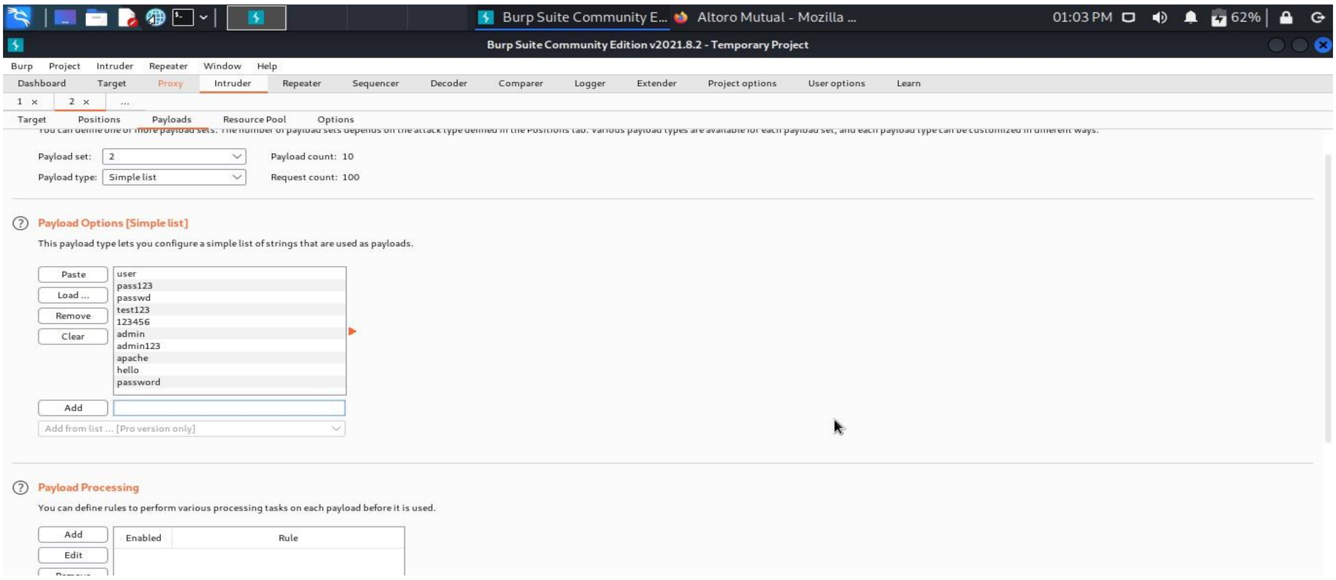
Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
user
test
jdoe
hello
test123
user123
admin
admin123
apache
apache_admin
```

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.



You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 10

Payload type: Simple list Request count: 100

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

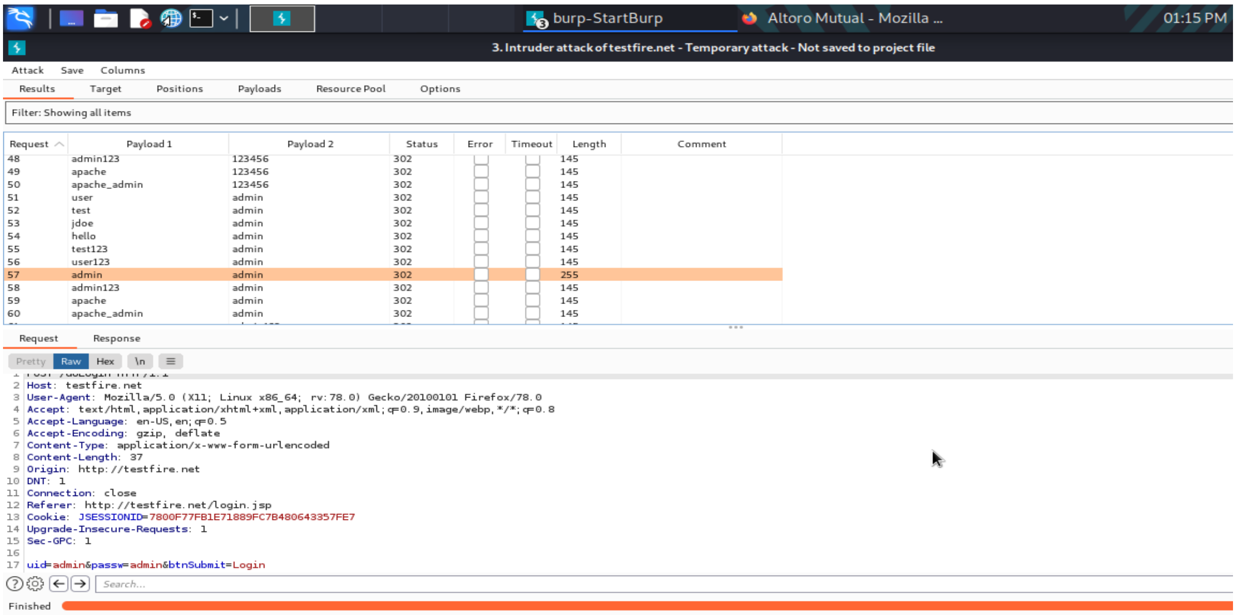
```
user
pass123
passwd
test123
123456
admin
admin123
apache
hello
password
```

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule



3. Intruder attack of testfire.net - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
48	admin123	123456	302	□	□	145	
49	apache	123456	302	□	□	145	
50	apache_admin	123456	302	□	□	145	
51	user	admin	302	□	□	145	
52	test	admin	302	□	□	145	
53	jdoe	admin	302	□	□	145	
54	hello	admin	302	□	□	145	
55	test123	admin	302	□	□	145	
56	user123	admin	302	□	□	145	
57	admin	admin	302	□	□	255	
58	admin123	admin	302	□	□	145	
59	apache	admin	302	□	□	145	
60	apache_admin	admin	302	□	□	145	

```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: 37
Origin: http://testfire.net
DNT: 1
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=7800F77FB1E71889FC7B480643357FE7
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

uid=admin&passw=admin&btnSubmit=Login
```

Finished

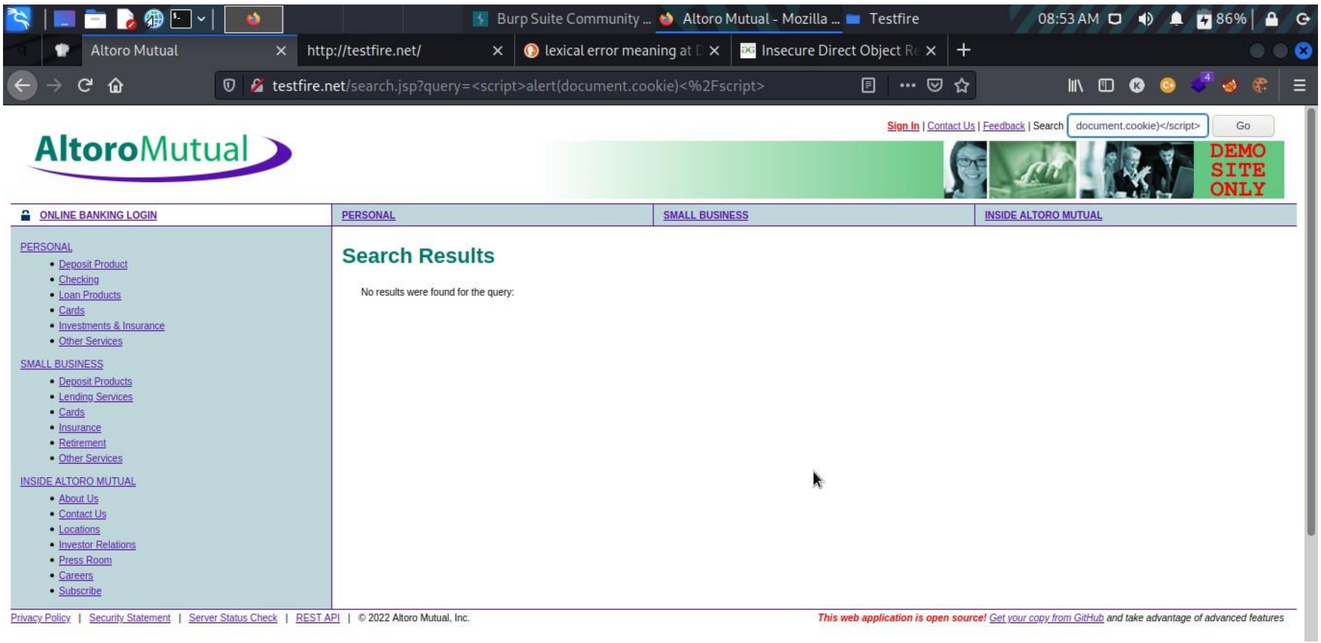
REMEDIATION

Most instances of SQL injection can be prevented by using parameterized queries (also known as prepared statements) instead of string concatenation within the query.

Finding -005: Reflected XSS (Moderate).

Description:	The pen tester was able to send a crafted input on the search field which in result lead to a pop up alert displaying the session cookie.
Risk:	Likelihood: High – Attacker can send crafted input to users and can steal the cookie. Impact: Moderate - If exploited, an attacker can send crafted input to other user and can acquire their session cookie.
System:	All
Tools Used:	Manually
References:	https://www.cvedetails.com/cve/CVE-2022-27926

Evidence

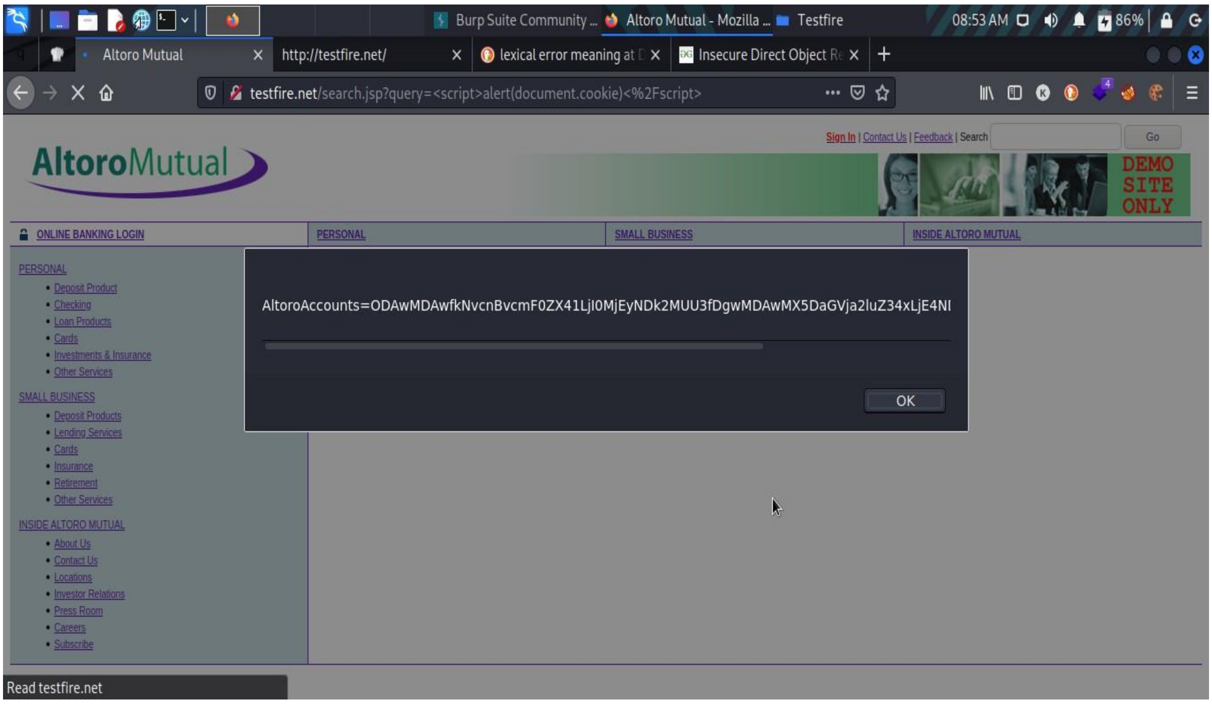


testfire.net/search.jsp?query=<script>alert(document.cookie)<%2Fscript>

document.cookie)</script>

Search Results

No results were found for the query:



testfire.net/search.jsp?query=<script>alert(document.cookie)<%2Fscript>

AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX41LjI0MjEyNDk2MUU3fDgwMDAwMX5DaGVja2luZ34xLjE4NI

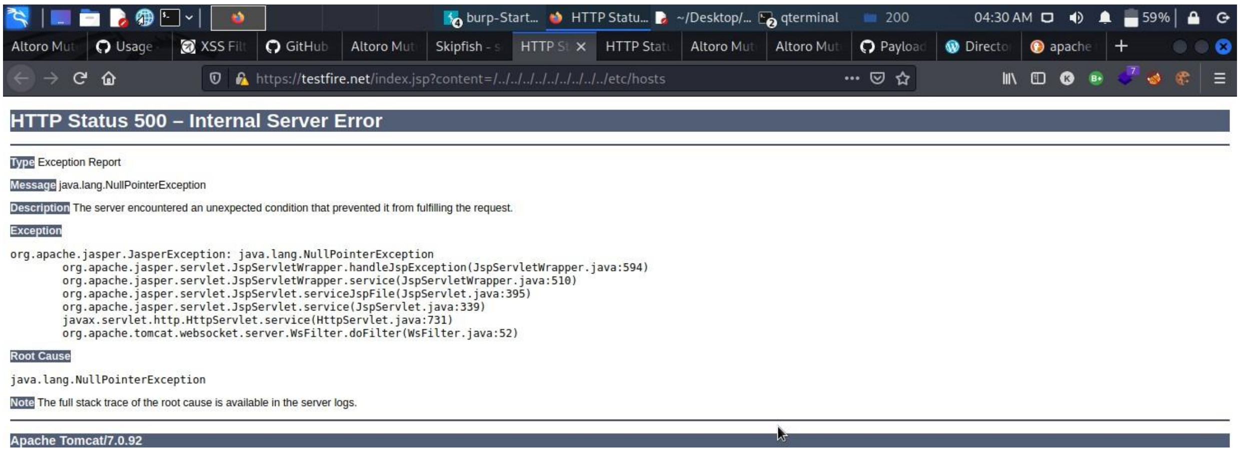
REMEDIATION

Proper implementation of input filtering on various character on the search field.

Finding -006: Displaying internal server error (informational).

Description:	Testfire displayed the error message displayin the apache tomcat version being used in the backend which can help attacker to frame the attack accordingly.
Risk:	Likelihood: High – An attacker can discover the version of the server being used Impact: Very High – Attacker can exploit according to the version of apache being used and frame attack accordingly.
Tools Used:	Manually
References:	N/A

Evidence



https://testfire.net/index.jsp?content=/../../../../../../../../../etc/hosts

HTTP Status 500 – Internal Server Error

Type Exception Report

Message java.lang.NullPointerException

Description The server encountered an unexpected condition that prevented it from fulfilling the request.

Exception

```
org.apache.jasper.JasperException: java.lang.NullPointerException
	org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
	org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:510)
	org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
	org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
	javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
	org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
```

Root Cause

```
java.lang.NullPointerException
```

Note The full stack trace of the root cause is available in the server logs.

Apache Tomcat/7.0.92

REMEDIATION

Developer should do proper review of error messages and error log before hosting the web app

CONCLUSION:

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber-crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cybercrimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

REFERENCES:

REFERENCE 1: APACHE TOMCAT INSECURE DEFAULT ADMINISTRATIVE PASSWORD
https://www.acunetix.com/vulnerabilities/web/apache-geronimo- default-administrative-credentials/

REFERENCE 2: INSECURE DIRECT OBJECT REFERENCE
https://www.cvedetails.com/cve/CVE-2022-29627

REFERENCE 3: SQL INJECTION VULNERABILITY
https://portswigger.net/web-security/sql-injection

REFERENCE 4: LOGIN BRUTE FORCE
https://www.alpinesecurity.com/blog/brute-forcing-login-page-with-burp-suite/

REFERENCE 5: REFLECTED XSS
https://www.cvedetails.com/cve/CVE-2022-27926