

# **Web Application Security Assessment using Vulnerability Assessment and Penetration Testing (VAPT) Methodology**

**An Industrial/Practical Training Report**

Submitted to the Faculty of Engineering of  
**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA,  
KAKINADA**

In partial fulfillment of the requirements for the award of the Degree of

**BACHELOR OF TECHNOLOGY**  
In  
**COMPUTER SCIENCE AND ENGINEERING**

By

Yarroju Rudra Prakash	20481A05P5
Tellakula Tharuni	20481A05M7
Somala Anu	20481A05L9

Under the EnviablE and Esteemed Guidance of  
**Dr. N. Rajeswari, M. Tech PhD**  
Professor, Department of CSE



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SESHADRI RAO GUDLAVALLERU ENGINEERING COLLEGE**

(An Autonomous Institute with Permanent Affiliation to JNTUK, Kakinada)

**SESHADRIRAO KNOWLEDGE VILLAGE**

**GUDLAVALLERU – 521356**

**ANDHRA PRADESH**

**2023-24**

**SESHADRI RAO  
GUDLAVALLERU ENGINEERING COLLEGE**

(An Autonomous Institute with Permanent Affiliation to JNTUK, Kakinada)  
SESHADRI RAO KNOWLEDGE VILLAGE, GUDLAVALLERU

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**



**CERTIFICATE**

This is to certify that the project report entitled “**Web Application Security Assessment using Vulnerability Assessment and Penetration Testing (VAPT) Methodology**” is a bonafide record of work carried out by **Yarroju Rudra Prakash (20481A05P5), Tellakula Tharuni (20481A05M7), Somala Anu (20481A05L9)** under the guidance and supervision of **Dr. N. Rajeswari** in the partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science and Engineering of Jawaharlal Nehru Technological University Kakinada, Kakinada** during the academic year 2023-24.

**Project Guide**

**(Dr. N. Rajeswari)**

**Head of the Department**

**(Dr. M. Babu Rao)**

**External Examiner**

## ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of people who made it possible and whose constant guidance and encouragements crown all the efforts with success.

We would like to express our deep sense of gratitude and sincere thanks to **Dr. N. Rajeswari**, M. Tech, PhD, Department of Computer Science and Engineering for her constant guidance, supervision and motivation in completing the project work.

We feel elated to express our floral gratitude and sincere thanks to **Dr. M. Babu Rao** , Head of the Department, Computer Science and Engineering for his encouragements all the way during analysis of the project. His annotations, insinuations and criticisms are the key behind the successful completion of the project work.

We would like to take this opportunity to thank our beloved principal **Dr. G. V. S. N. R. V. Prasad** for providing a great support for us in completing our project and giving us the opportunity for doing project.

Our Special thanks to the faculty of our department and programmers of our computer lab. Finally, we thank our family members, non-teaching staff and our friends, who had directly or indirectly helped and supported us in completing our project in time.

### Team members

Yarroju Rudra Prakash	(20481A05P5)
Tellakula Tharuni	(20481A05M7)
Somala Anu	(20481A05L9)



## **INTERNSHIP REPORT APPROVAL FORM**

Date

With immense pleasure, this is to approve that the students of Seshadri Rao Gudlavalleru Engineering College i.e **Yarroju Rudra Prakash (20481A05P5), Tellakula Tharuni (20481A05M7), Somala Anu (20481A05L9)** successfully completed their Project and Project Report on “**Web Application Security Assessment using Vulnerability Assessment and Penetration Testing (VAPT) Methodology**” under our guidance.

We are highly impressed with the work that they have done and commend them on their quick grasping skills. They have shown good intent to learn and have put the knowledge gained into application in the form of this project. We appreciate the hard work and commitment shown by them.

We, hereby approve that this document is completely checked and accepted by SmartBridge Technical Team. It's been an absolute pleasure to educate and mentor these students. We hope that this document will also serve as a Letter of Recommendation, to whomsoever applied.

We wish them success in all future endeavors and a great career ahead.

**Jayaprakash Netha,**  
**Program Manager**

## **ABSTRACT**

With the growing reliance on web applications for various functionalities, ensuring the security of these applications has become a paramount concern. This paper aims to explore and discuss the methodologies and practices involved in conducting a comprehensive security assessment of web applications using Vulnerability Assessment and Penetration Testing (VAPT) methods.

Furthermore, the paper highlights the critical role of tools and frameworks employed in VAPT assessments, including popular tools such as Burp Suite, OWASP ZAP, Nmap, and others. It discusses their functionalities in detecting vulnerabilities like SQL injection, Cross-Site Scripting (XSS), authentication flaws, and more.

Moreover, the research examines the challenges and limitations associated with VAPT methodologies, emphasizing the importance of ethical considerations, legal compliance, and the need for continuous testing and remediation.

In conclusion, this paper emphasizes the significance of VAPT as an indispensable approach for evaluating and fortifying the security posture of web applications, offering insights into best practices and recommendations for organizations aiming to secure their web-based assets effectively.

## **INDEX**

<b>SL. NO</b>	<b>TITLE</b>	<b>PAGE NO</b>
1.	INTRODUCTION	1
1.1	Introduction	1
1.2	Objectives of the Project	1
1.3	Problem Statement	3
2.	LITERATURE REVIEW	5
3.	PROPOSED METHOD	6
3.1	Methodology	6
3.2	Implementation	7
3.3	Data Preparation	20
4.	RESULTS AND DISCUSSION	22
5.	CONCLUSION	26
6.	REFERENCE	27

Mapping of course outcomes with graduated POs and PSOs

## **1. INTRODUCTION**

### **1.1 INTRODUCTION**

In an era dominated by digital technology, the security of web applications is of paramount importance. With cyber threats constantly evolving, businesses and organizations must adopt proactive measures to protect their applications and sensitive data. This is where Vulnerability Assessment and Penetration Testing (VAPT) come into play. VAPT is a structured and comprehensive approach to evaluating and enhancing the security of full-stack web applications. VAPT methodology combines two distinct yet complementary processes: Vulnerability Assessment, which identifies and prioritizes potential weaknesses, and Penetration Testing, which assesses the application's resilience to real-world attacks. This dynamic methodology is a vital component of any organization's cybersecurity strategy. In this exploration of Web Application Security Assessment using VAPT, we will delve into the intricacies of this methodology, from the initial preparations to the final reporting stage. We will examine how to identify and address vulnerabilities, simulate attacks, and ultimately fortify web applications against a multitude of threats. The aim of this methodology is not only to discover and remediate security flaws but also to enhance the overall robustness of web applications. Through this comprehensive guide, we will equip you with the knowledge and tools to safeguard your web applications effectively, ensuring the confidentiality, integrity, and availability of critical data. As the digital landscape continues to evolve, understanding and implementing VAPT methodology becomes an indispensable part of securing your web applications in an ever-changing and potentially hazardous online environment.

### **1.2 OBJECTIVES OF THE PROJECT**

The objectives of a Full-stack Web Application Security Assessment using Vulnerability Assessment and Penetration Testing (VAPT) methodology project are as follows:

#### **Identify Vulnerabilities:**

The primary goal is to identify vulnerabilities in the web application, including but not limited to common issues such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms.

**Prioritize Risks:**

Assess the severity and impact of identified vulnerabilities to prioritize them. This ensures that high-risk issues are addressed promptly, reducing potential security threats.

**Simulate Real Attacks:**

Through penetration testing, simulate real-world attacks on the application to understand its resilience and response to threats. This helps in identifying weaknesses in the application's security defenses.

**Enhance Security:**

Provide actionable recommendations and solutions to mitigate vulnerabilities and strengthen the application's security posture. This includes code fixes, configuration changes, and best practices.

**Compliance and Regulations:**

Ensure that the web application complies with relevant industry standards and regulations, such as GDPR, HIPAA, or PCI DSS, depending on the application's domain.

**Protect Sensitive Data:**

Protect sensitive user data and ensure data confidentiality, integrity, and availability by identifying data leakage vulnerabilities and implementing encryption where necessary.

**Prevent Unauthorized Access:**

Verify that the application has robust access control mechanisms in place to prevent unauthorized access to sensitive functionality and data.

**Evaluate Business Logic Flaws:**

Identify and address business logic flaws that may not be apparent through automated scanning but can pose significant security risks.

**Test Security Controls:**

Evaluate the effectiveness of security controls, including firewalls, intrusion detection systems, and other security measures in place.

**Build Security Awareness:**

Raise awareness among development and operational teams regarding security best practices, thereby fostering a culture of security within the organization.

**Documentation and Reporting:**

Create comprehensive reports that detail the assessment findings, recommendations, and any remediation actions taken. These reports serve as a valuable reference for stakeholders.



**Continuous Improvement:**

Establish a framework for ongoing monitoring and periodic assessments to adapt to emerging threats and changes in the web application. This ensures that security remains robust over time.

These objectives collectively contribute to the overarching goal of fortifying the web application against potential security threats and providing assurance to both the organization and its users that their data is protected in an increasingly digital and interconnected world.

### **1.3 PROBLEM STATEMENT**

In today's digital landscape, the proliferation of full-stack web applications has become ubiquitous, serving as the backbone for businesses, governments, and individuals. While these applications bring convenience and efficiency, they are also prime targets for malicious actors seeking to exploit vulnerabilities for financial gain, data breaches, or other nefarious purposes. The problem at hand is the growing need to address the critical issue of web application security,

continues to pose a significant and evolving challenge. The following issues and concerns underscore the problem:

**Rapidly Evolving Threat Landscape:**

The threat landscape for web applications is constantly evolving, with new attack vectors and vulnerabilities emerging regularly. This poses a constant challenge for organizations to keep their applications secure.

**Inadequate Security Posture:**

Many organizations lack a comprehensive approach to secure their web applications. This often leads to suboptimal security controls, vulnerabilities, and the risk of data breaches.

**Lack of Awareness:**

Both development and operational teams may lack the awareness and expertise required to effectively secure web applications, resulting in coding errors and misconfigurations that create security holes.

**Compliance and Regulatory Pressure:**

Organizations must adhere to industry-specific regulations and compliance standards. Non-compliance can lead to legal consequences, fines, and damage to reputation.

**Data Breach Consequences:**

Data breaches can have severe consequences, including financial losses, loss of customer trust, legal action, and reputational damage.

**Complexity and Scale:**

As web applications become more complex and interconnected, assessing and mitigating security risks across multiple layers of the stack becomes a formidable challenge.

**Resource Constraints:**

Limited resources, including time, budget, and skilled security professionals, can hinder an organization's ability to conduct thorough security assessments.

**Need for Proactive Measures:**

Traditional reactive security measures are no longer sufficient. To address the problem effectively, organizations must adopt proactive security practices and integrate them into the software development lifecycle. The problem statement, therefore, centers on the imperative need for a systematic and robust Full-stack Web Application Security Assessment methodology using VAPT. This methodology aims to provide organizations with the tools and guidance needed to identify and remediate vulnerabilities, strengthen their security posture, and ultimately safeguard their web applications against an ever-advancing array of threats.

## 2. LITERATURE REVIEW

A literature review on the topic of Full-stack Web Application Security Assessment using Vulnerability Assessment and Penetration Testing (VAPT) Methodology reveals several key findings and existing research in the field of cybersecurity. Many studies provide in-depth analyses of these vulnerabilities.

**Frameworks and Tools:** Research papers often discuss various frameworks, methodologies, and tools used in VAPT, including OWASP (Open Web Application Security Project) guidelines, NIST (National Institute of Standards and Technology) standards, and popular security scanning tools like Nessus and Burp Suite.

**VAPT in Specific Domains:** Studies have examined the application of VAPT in specific domains, such as healthcare, e-commerce, and finance, addressing industry-specific challenges and regulatory compliance.

**Automation and Artificial Intelligence:** Recent literature highlights the use of automation and AI in VAPT, discussing the role of machine learning and AI algorithms in vulnerability detection and security testing.

**Evolving Threat Landscape:** Ongoing research discusses the ever-evolving threat landscape and the need for VAPT to adapt to emerging security risks, including IoT (Internet of Things) vulnerabilities and cloud-based threats.

**Business Impact and Risk Assessment:** Some studies focus on the business impact of web application vulnerabilities, including financial losses, reputational damage, and legal consequences. They emphasize the importance of risk assessment in VAPT.

**Ethical Hacking and Responsible Disclosure:** Research explores the ethical considerations in penetration testing and vulnerability disclosure, emphasizing responsible and legal practices.

**Regulations and Compliance:** Papers discuss the relevance of VAPT in complying with data protection and cybersecurity regulations, such as GDPR, HIPAA, and PCI DSS.

**Best Practices and Case Studies:** Various publications present best practices for VAPT and real-world case studies that illustrate successful security assessments and remediation.

**Continuous Monitoring and Improvement:** Literature underlines the need for continuous monitoring and improvement in VAPT methodologies to address emerging threats and maintain security over time.

Overall, the literature review provides valuable insights into the methodologies, best practices, challenges, and evolving trends in Full-stack Web Application Security Assessment using Vulnerability Assessment and Penetration Testing. This body of knowledge forms the foundation for organizations to develop and implement effective security strategies for their web applications.

### 3. PROPOSED METHOD

#### 3.1 METHODOLOGY

A comprehensive Full-stack Web Application Security Assessment using Vulnerability Assessment and Penetration Testing (VAPT) typically follows a structured methodology. Here's a high-level overview of the process:

**Planning and Scope Definition:**

Determine the scope of the assessment, including the web application, its components, and any specific testing objectives. Identify legal and compliance requirements that must be adhered to.

**Information Gathering:**

Gather information about the web application, its architecture, technologies used, and potential entry points. Identify the application's functionalities, APIs, and dependencies.

**Vulnerability Assessment:**

Use automated scanning tools to identify common vulnerabilities such as SQL injection, Cross-Site Scripting (XSS), and more. Perform source code review if applicable. Analyze the results and prioritize vulnerabilities based on their severity.

**Penetration Testing:**

Conduct manual testing to identify more complex and critical vulnerabilities. Attempt to exploit vulnerabilities to assess their impact. Test for issues like authentication bypass, privilege escalation, and data exposure.

**Reporting:**

Document all identified vulnerabilities, their severity, and potential impact. Provide clear and actionable recommendations for remediation. Categorize findings based on their criticality.

**Validation and Retesting:**

Confirm that reported vulnerabilities have been fixed. Retest to ensure that the fixes did not introduce new issues.

**Client Communication:**

Regularly update the client on the assessment progress and findings. Discuss potential risks and mitigation strategies.

**Documentation and Compliance:**

Ensure that the assessment process adheres to legal and compliance requirements. Document all testing procedures and results for auditing purposes.

**Post-Assessment Actions:**

Provide guidance on ongoing security practices and measures to maintain the application's security. Schedule periodic re-assessments to stay proactive against evolving threats.

**Final Report and Sign-off:**

Present a detailed report to the client, including an executive summary and technical details. Obtain client sign-off indicating the completion of the assessment.

**Follow-Up and Support:**

Offer post-assessment support to assist with the implementation of recommended security measures. Stay available for questions or clarifications. It's important to tailor the methodology to the specific context of the web application, and the VAPT team should have the necessary expertise to perform the assessment effectively. Additionally, it's crucial to approach the assessment ethically and responsibly, respecting the confidentiality of the client's data and systems.

### 3.2 IMPLEMENTATION

We have implemented the VAPT methods on Altoro Manual site. During the testing of Altoro Mutual, we focused on identifying vulnerabilities related to SQL injection, Cross-Site Scripting, and HTML injection. Our approach involved using both automated tools and manual techniques to identify potential vulnerabilities.

Tools used are Kali Linux, Burp Suite, Firefox Browser, DNS Enum, DNS Recon, Who Is

1. **Vulnerability Name:** Cross-Site Scripting (Reflected)

**CWE :** CWE-79

**OWASP Category:** A03:2021 – Injection

**Description:** Untrusted data enters a web application, typically from a web request.

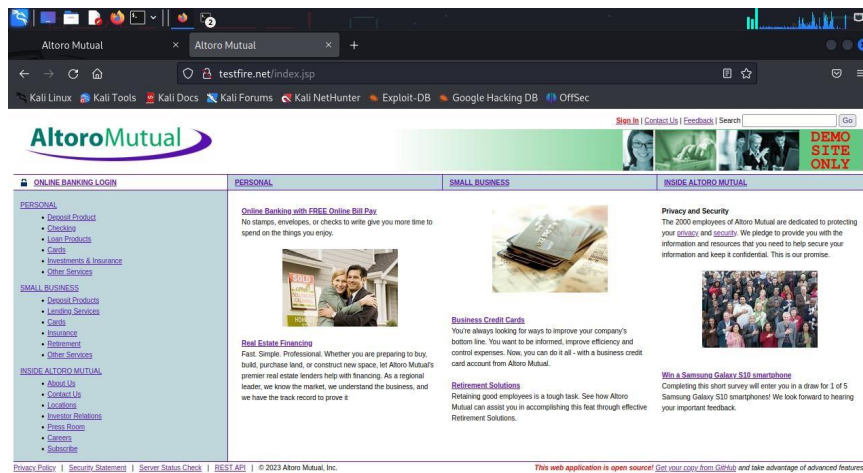
**Vulnerability Path:** <http://testfire.net/search.jsp?query=>

**Vulnerability**

**Parameter:** <http://testfire.net/search.jsp?query=%3Cscript%3Ealert%28%22XSS+attack%22%29%3C%2Fscript%3E>

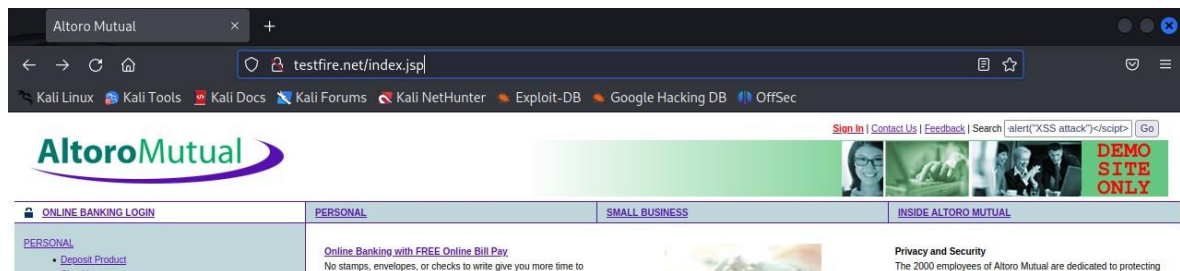
## Steps to Reproduce :

Step 1: Access the URL testfire.net



Step 2: Go to the Search and enter a xss payload

`<script>alert('XSS Attack')</script>`



## 2. Vulnerability Name :- SQL Injection

**CWE :** - CWE-89

**OWASP Category :-** A03:2021 – Injection

**Description :-** Consider the following SQL query:

`SELECT * FROM Users WHERE Username='$username' AND Password='$password'`

A similar query is generally used from the web application in order to authenticate a user.

If the query returns a value it means that inside the database a user with that set of credentials exists, then the user is allowed to login to the system, otherwise access is denied. The values of the input fields are generally obtained from the user through a web form. Suppose we insert the following Username and Password values:

`$username = '1' or '1' = '1'`

`$password = '1' or '1' = '1'`

The query will be:

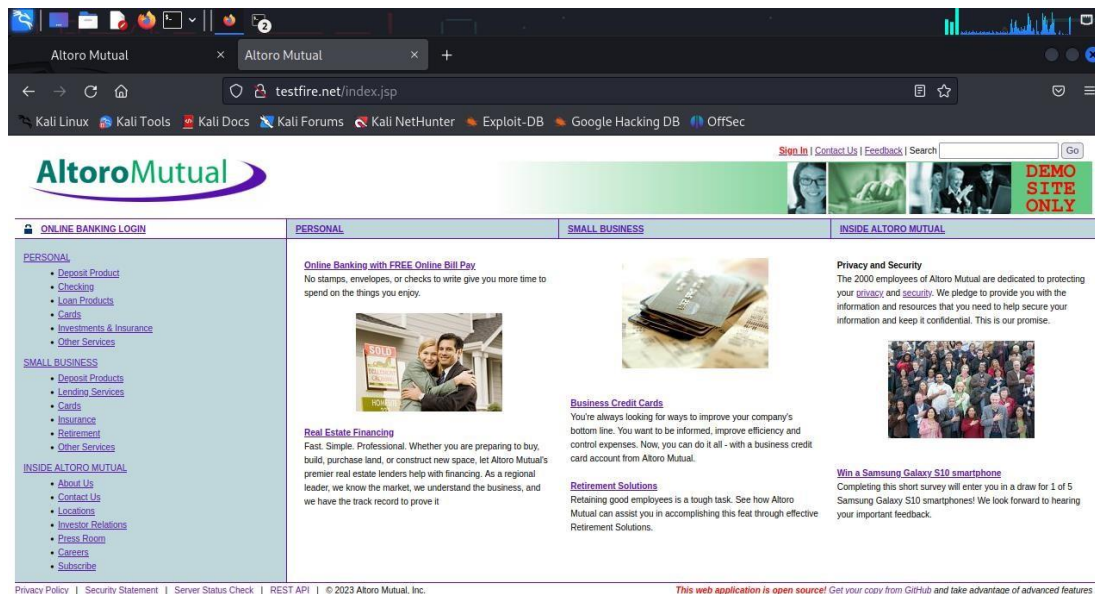
```
SELECT * FROM Users WHERE Username='1' OR '1' = '1' AND Password='1' OR '1' = '1'
```

**Vulnerability Path:** <http://testfire.net/login.jsp>

**Vulnerability Parameter:** <http://testfire.net/bank/main.jsp>

**Steps to Reproduce :-**

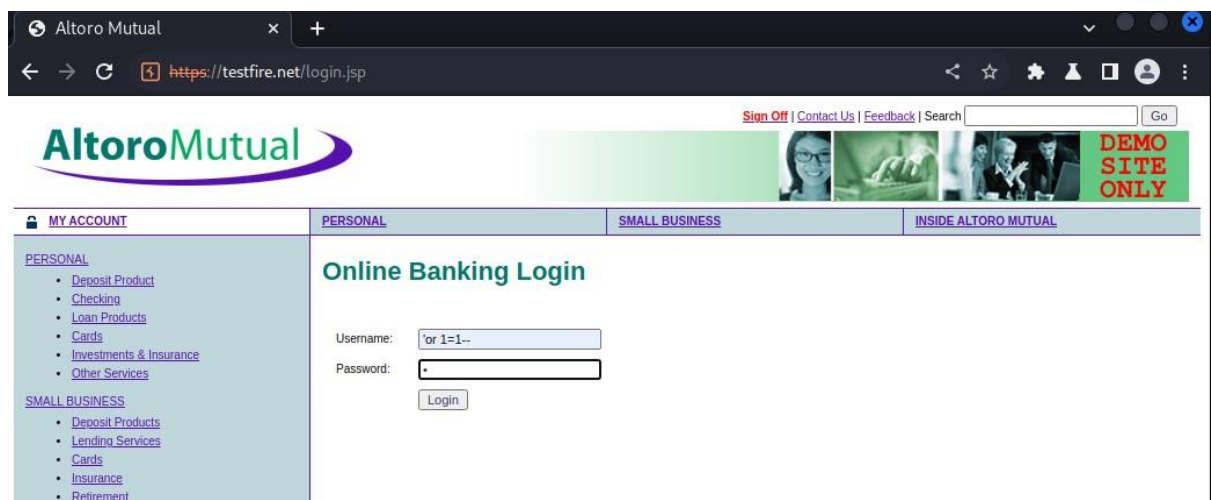
Step-1: Access the Url



Step-2: Now give an sql payload as input

Username: 'or 1=1--

Password: 1



### 3. Vulnerability Name :- HTML Injection-Reflected (POST)

**CWE :-** CWE-79

**OWASP Category :-** A03:2021 – Injection

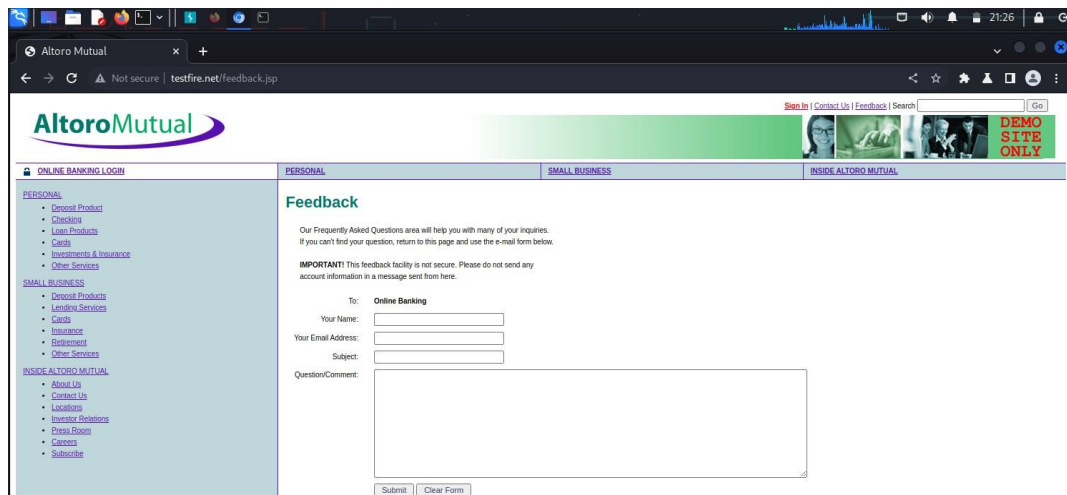
**Description :-** HTML Injection also known as Cross Site Scripting. It is a security vulnerability that allows an attacker to inject HTML code into web pages that are viewed by other users.

**Vulnerability Path:** <http://testfire.net/feedback.jsp>

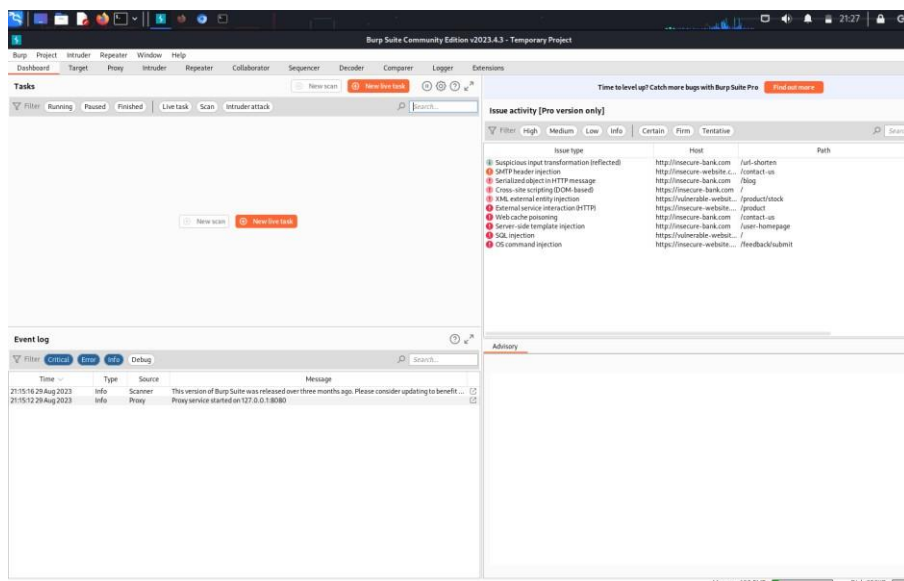
**Vulnerability Parameter:-** <http://testfire.net/sendFeedback>

#### Steps to Reproduce :-

Step-1: Access the url:

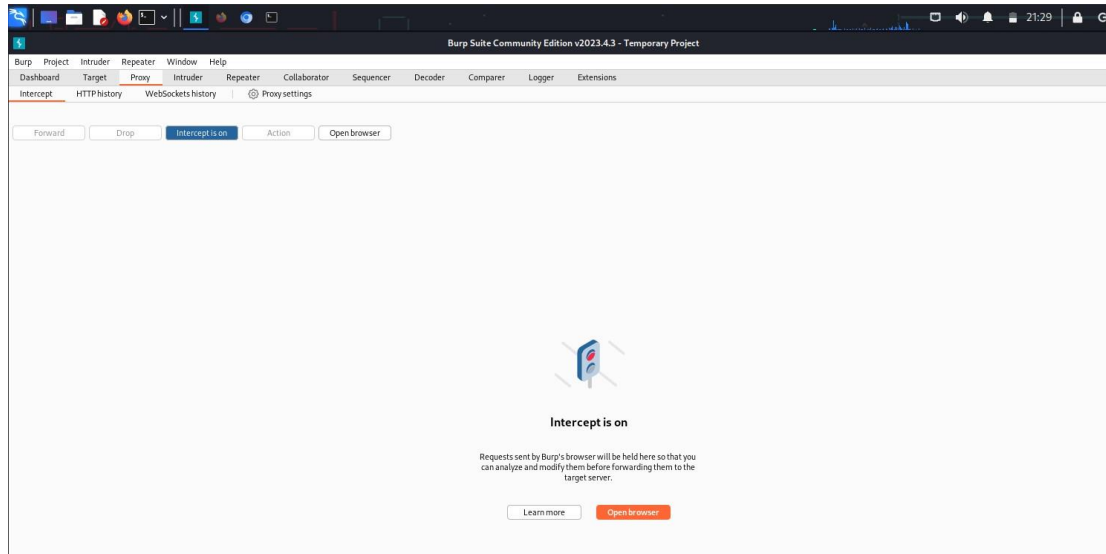


Step-2: Now give some dummy data and open burp suite and wait for the request while making the proxy on.

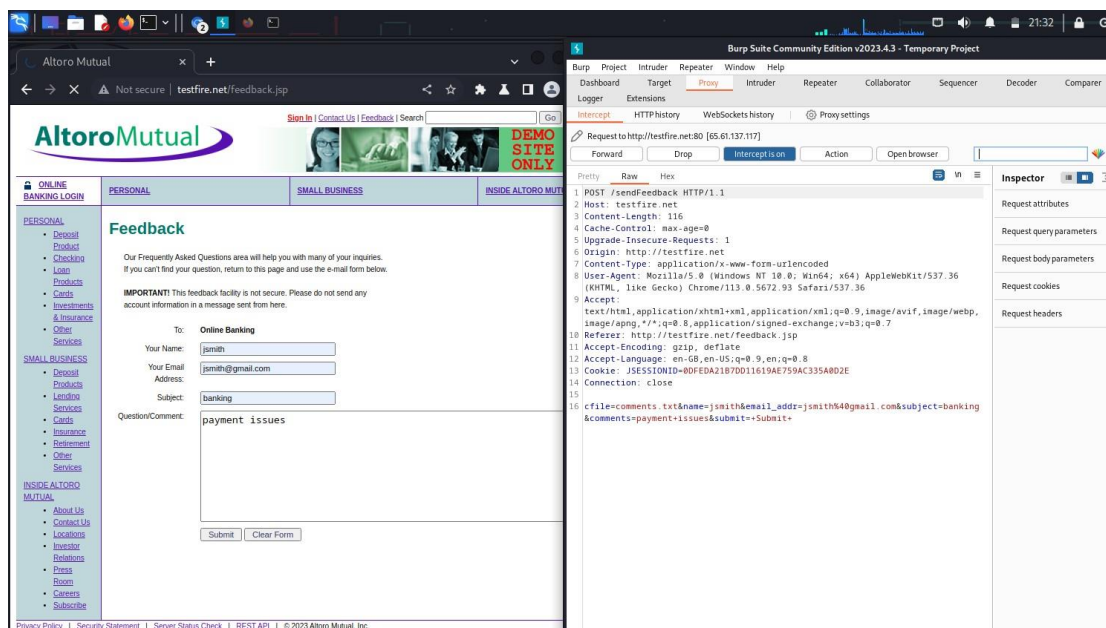




### Step-3: Go to proxy and turn the intercept on

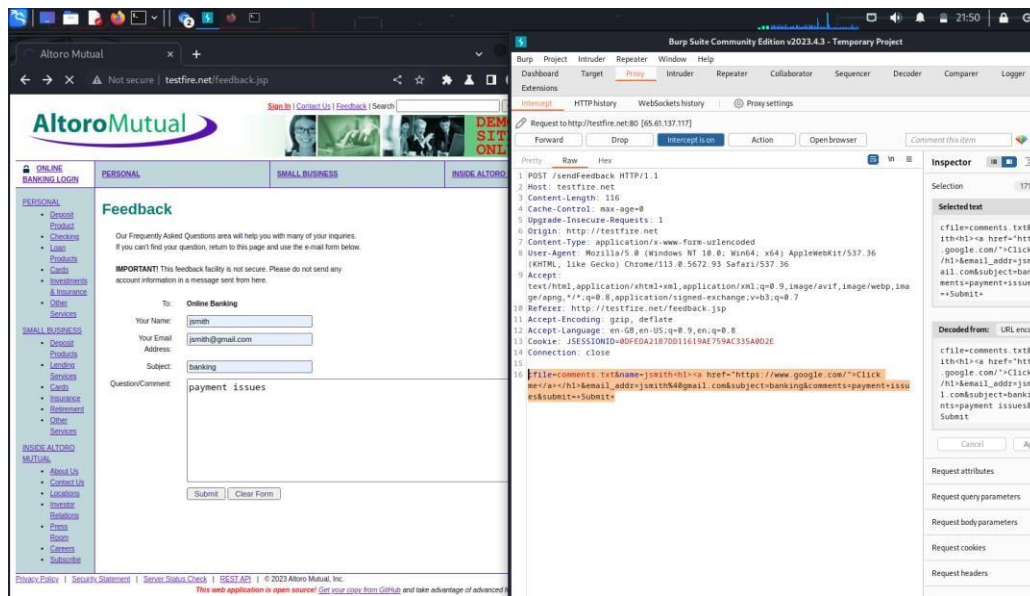


### Step-4: We successfully intercepted the request and can see the request data in raw form.



### Step-5: Now you can see the given first name and email clearly and we inserted a anchor tag in between the first name value.

<h1><a href="https://www.google.com/>Click me</a></h1>



#### 4. Vulnerability Name :- IDOR Vulnerability

**CWE :-** CWE-639

**OWASP Category :-** A04:2007 – Insecure Direct Object Reference

#### Description :-

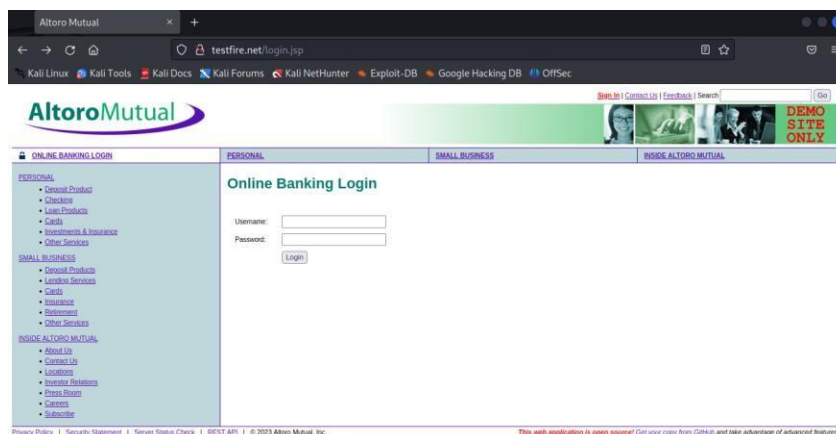
Insecure Direct Object Reference (IDOR) is a critical web application security vulnerability that arises from improper authorization and access control. It is essential for developers and security professionals to be aware of this vulnerability and take proactive measures to prevent and mitigate it in their applications.

**Vulnerability Path:** <http://testfire.net/login.jsp>

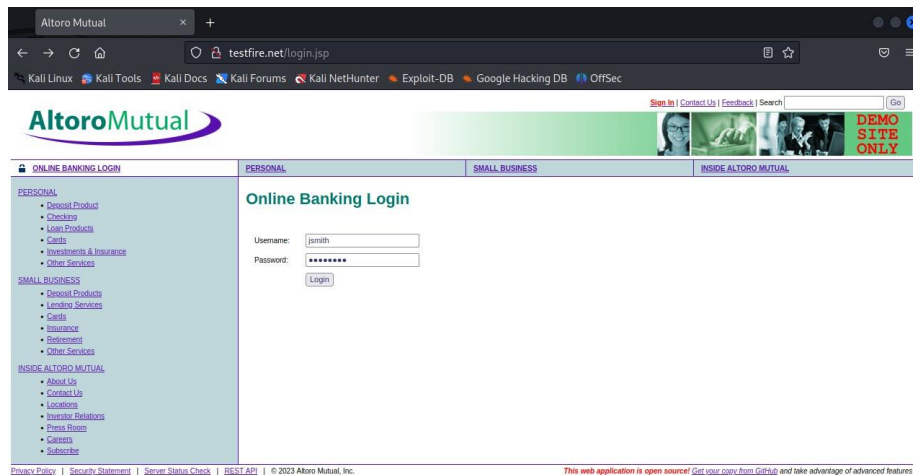
**Vulnerability Parameter:-** <http://testfire.net/sendFeedback>

#### Steps to Reproduce :-

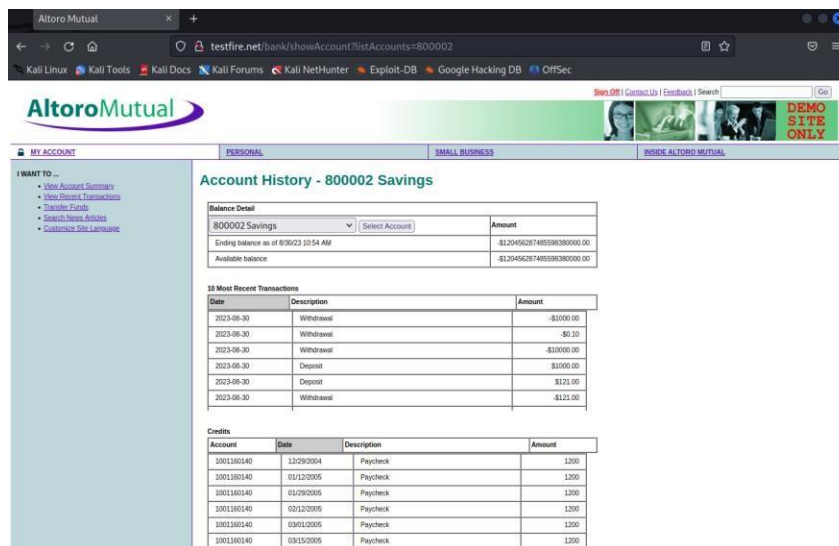
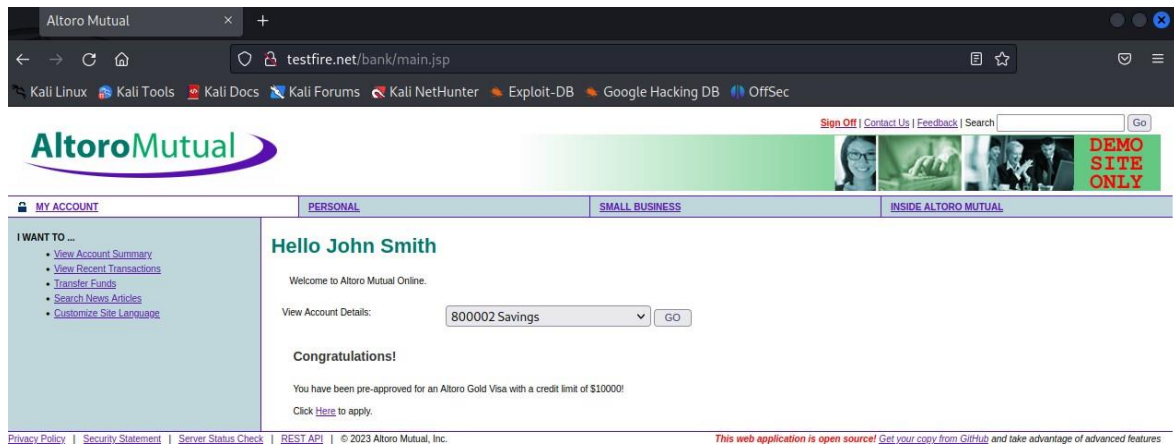
Step-1: Access the url:



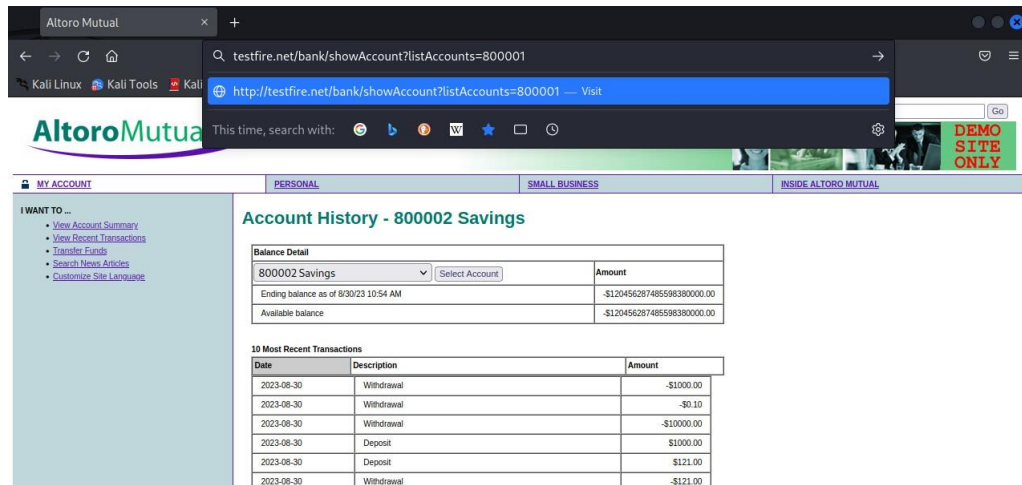
Step-2: Login into the bank account Username: jsmith password: demo1234



Step-3: Check the account details of jsmith



Step-4: In URL <http://testfire.net/bank/showAccount?listAccounts=800002> change the account to 800001



## 5. Vulnerability Name :- Brute Force

**CWE :-** CWE-307

**OWASP Category :-** A2:2017-Broken Authentication

**Description :-**

Brute force is a straightforward and systematic method of attempting to discover a password, encryption key, or access code by trying all possible combinations until the correct one is found. It is a common and often time-consuming technique used in cybersecurity attacks and password cracking.

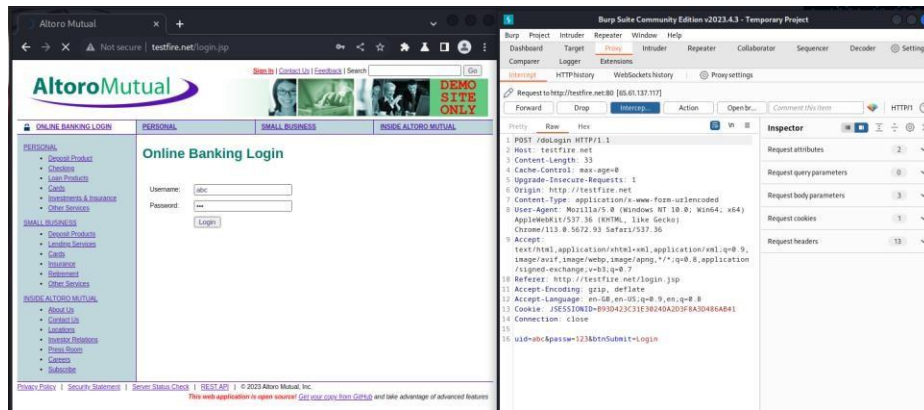
**Vulnerability Path:** <http://testfire.net/login.jsp>

**Vulnerability Parameter:-** <http://testfire.net/sendFeedback>

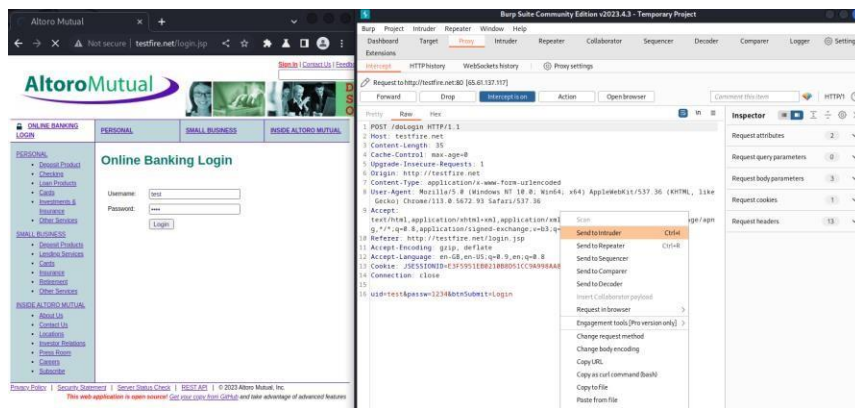
**Steps to reproduce:**

Step-1: Access the url

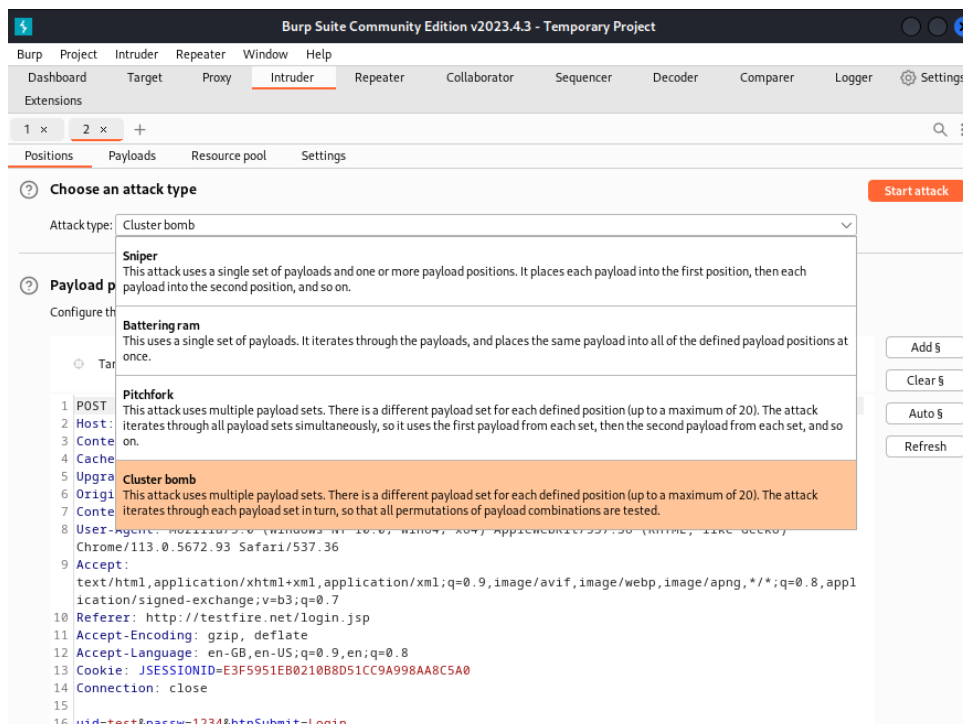
Step-2: Try to login with a random credentials. Using Burp suite Intercept the login request



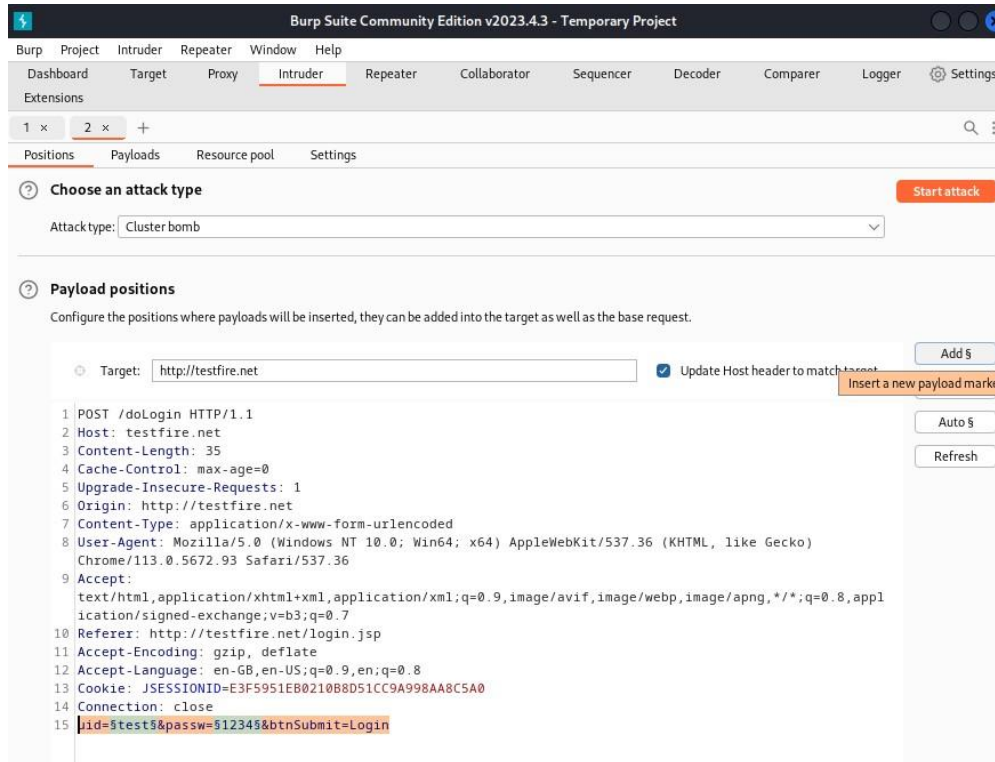
Step-3: Send the request to the intruder



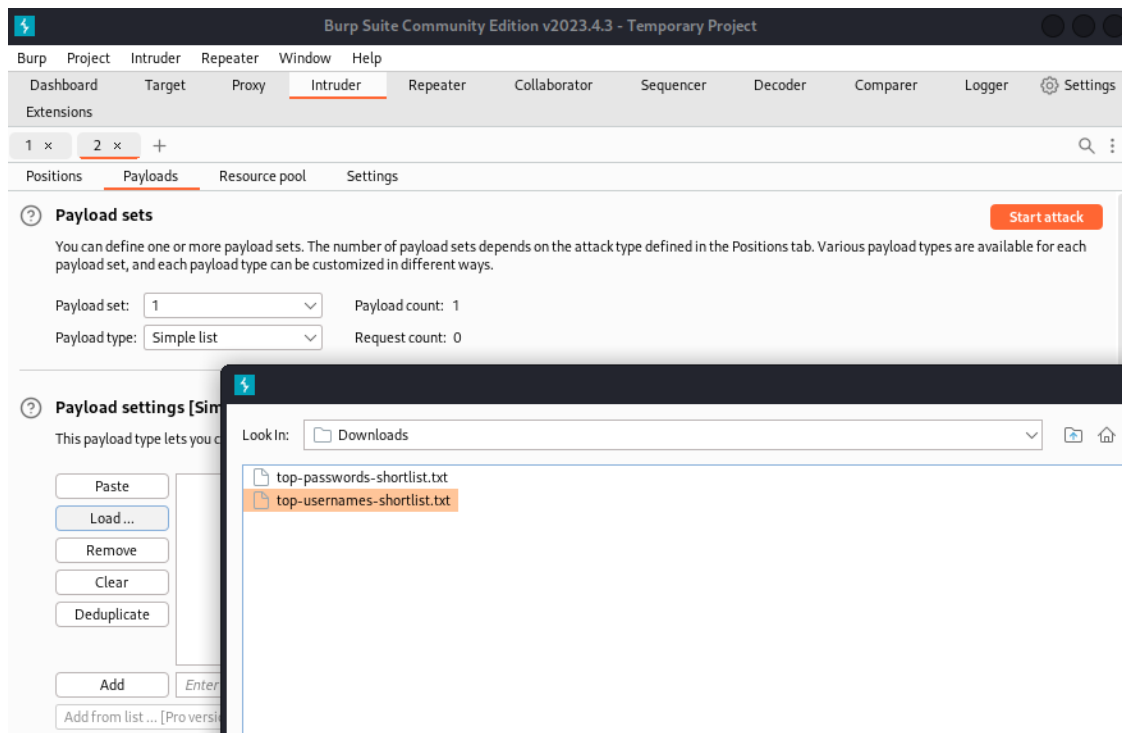
Step-4: Select the attack type as Cluster Bomb as we have to payload two values(username & password)



### Step-5: Select the Username & password values and click 'add \$' to brute force

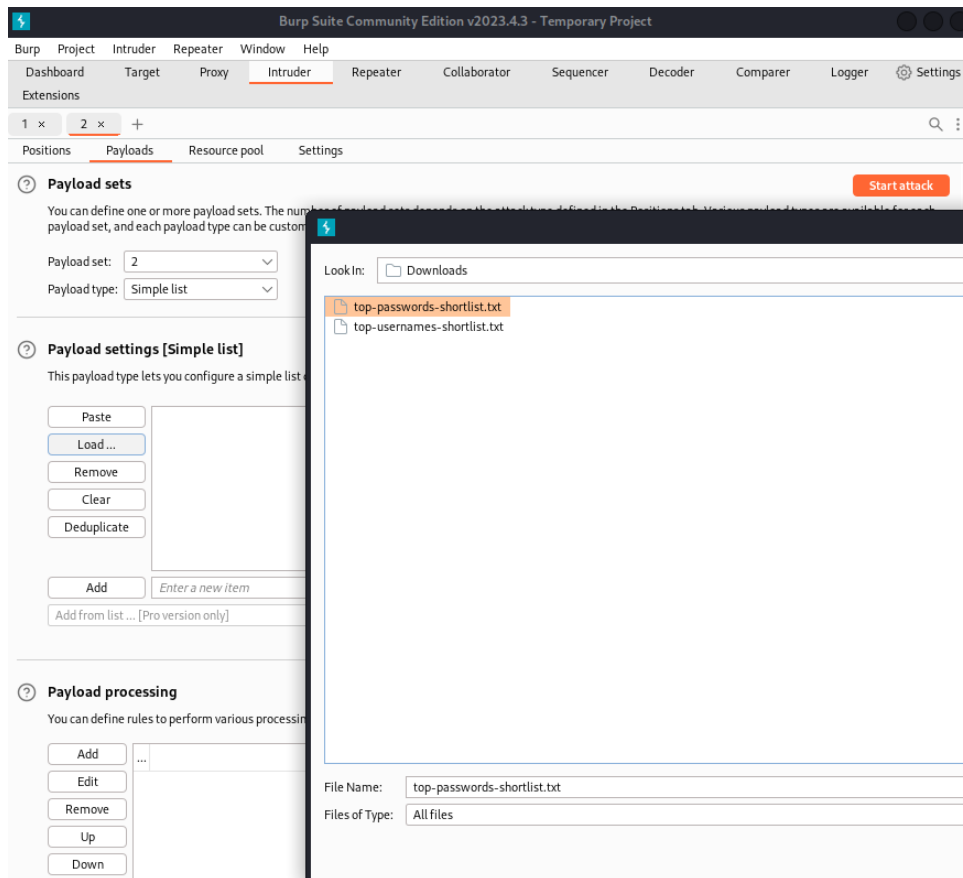


### Step-6: For payload set 1 add username word list

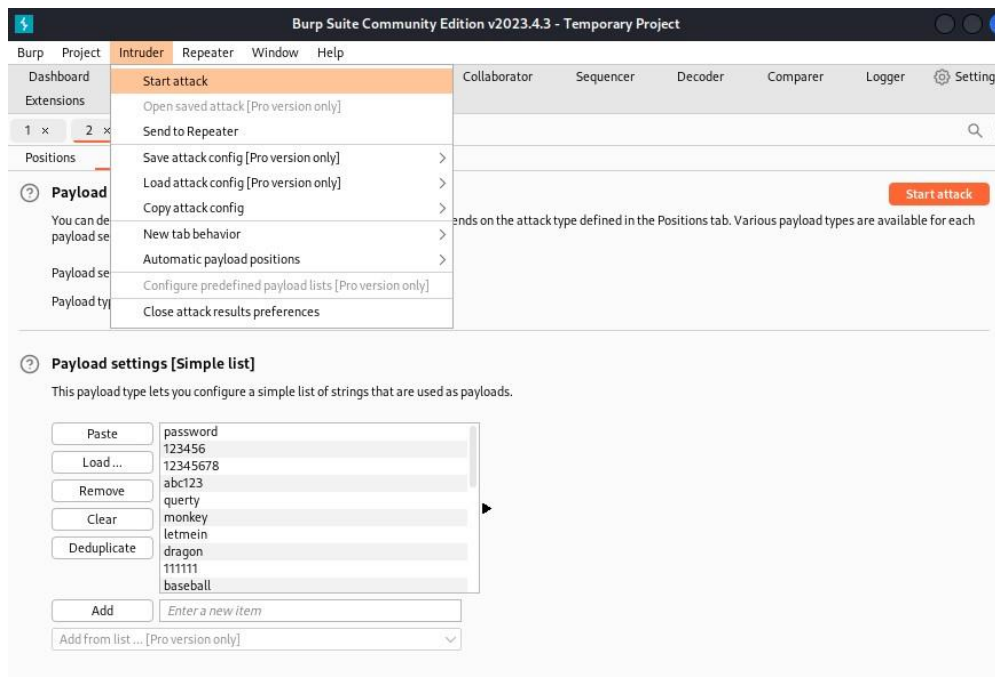




## Step-7: For payload set 2 add password word list

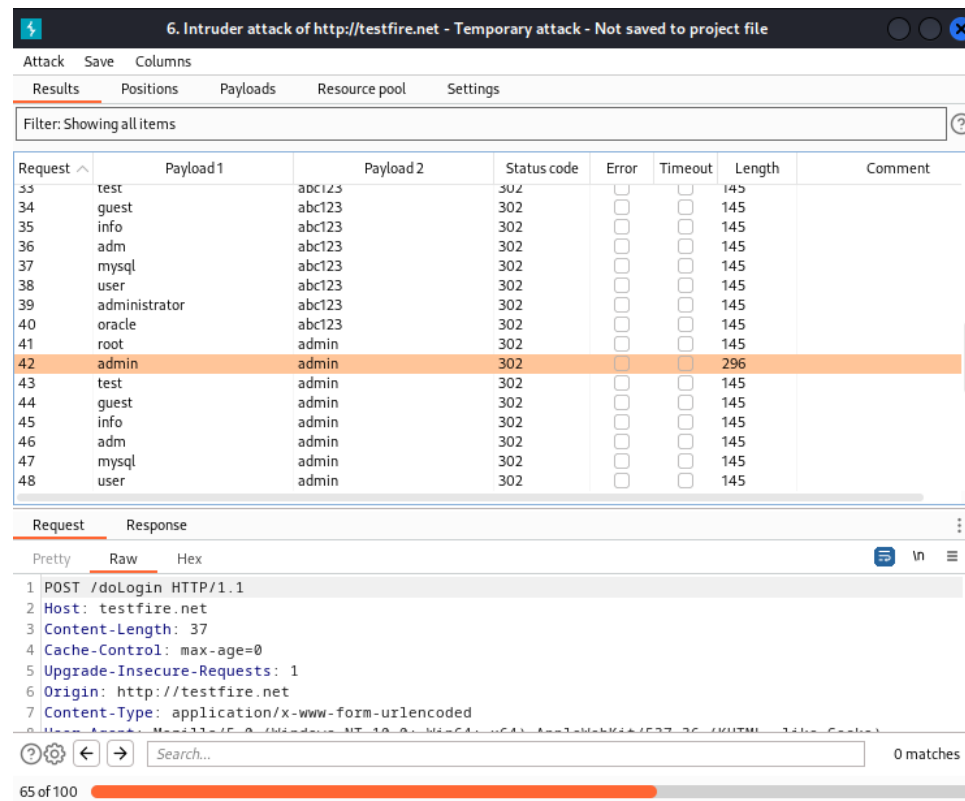


## Step-8: Start the attack



Step-9: Check the Length for a difference in value

Here for username: admin and password: admin we got a Length value: 296



6. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
33	test	abc123	302			145	
34	guest	abc123	302			145	
35	info	abc123	302			145	
36	adm	abc123	302			145	
37	mysql	abc123	302			145	
38	user	abc123	302			145	
39	administrator	abc123	302			145	
40	oracle	abc123	302			145	
41	root	admin	302			145	
42	admin	admin	302			296	
43	test	admin	302			145	
44	guest	admin	302			145	
45	info	admin	302			145	
46	adm	admin	302			145	
47	mysql	admin	302			145	
48	user	admin	302			145	

Request Response

Pretty Raw Hex

```

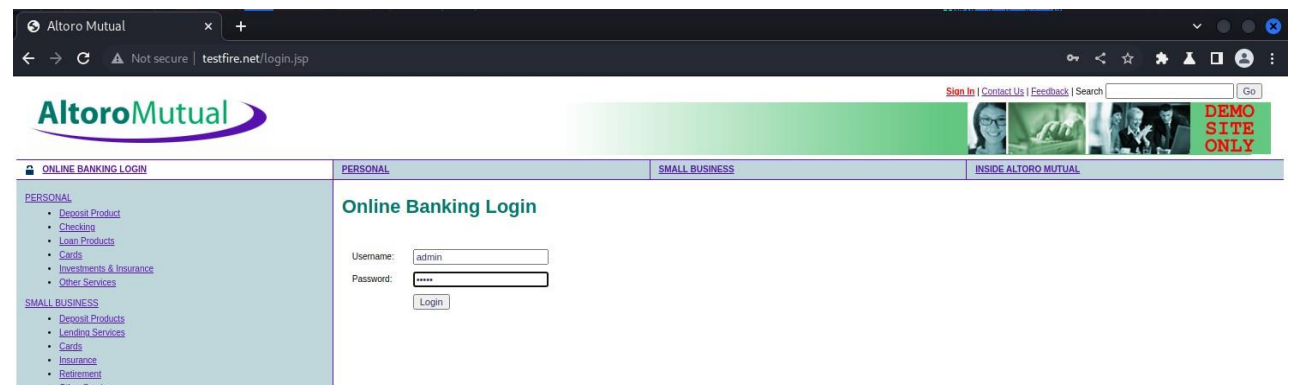
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 Content-Length: 37
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://testfire.net
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.84 Safari/537.36

```

0 matches

65 of 100

Step- 10: Now Check the username and password



Altoro Mutual

Sign In | Contact Us | Feedback | Search

ONLINE BANKING LOGIN PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

PERSONAL

- Deposit Products
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

Online Banking Login

Username: admin

Password: \*\*\*\*\*

Login

### 3.3 DATA PREPARATION

**Altoro Manual:** Altoro Mutual was a fictional banking website created by IBM for the purpose of demonstrating security vulnerabilities and showcasing how IBM security products could address these issues. The website was used as a training tool in cybersecurity courses, workshops, and demonstrations. It was designed intentionally with



various security vulnerabilities to simulate real-world scenarios and demonstrate how hackers might exploit weaknesses in a web application.

**DNS Enum:** DNS enumeration, or DNS (Domain Name System) enumeration, is the process of gathering information about a domain or network by querying DNS servers. This method involves extracting different types of DNS records to gather information about hosts, subdomains, mail servers, and other resources associated with a particular domain. DNS enumeration can be used for legitimate purposes, such as network administration, troubleshooting, or understanding the structure of a network. However, it's also a technique commonly utilized by hackers and penetration testers to gather valuable information about a target network, which can be exploited for various purposes.

```
(rishi@kali)-[~]
$ dnsenum testfire.net
dnsenum VERSION:1.2.6

testfire.net

Host's addresses:

testfire.net.          48681    IN      A       65.61.137.117

Name Servers:

usc3.akam.net.         13490    IN      A       96.7.50.64
asia3.akam.net.        67210    IN      A       23.211.61.64
ns1-206.akam.net.      27364    IN      A       193.108.91.206
usw2.akam.net.         60783    IN      A       184.26.161.64
eur2.akam.net.         74198    IN      A       95.100.173.64
usc2.akam.net.         67567    IN      A       184.26.160.64
eur5.akam.net.         67839    IN      A       23.74.25.64
ns1-99.akam.net.       27292    IN      A       193.108.91.99
```

```
Mail (MX) Servers:

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for testfire.net on usc3.akam.net ...
AXFR record query failed: REFUSED
Trying Zone Transfer for testfire.net on asia3.akam.net ...
AXFR record query failed: REFUSED
Trying Zone Transfer for testfire.net on ns1-206.akam.net ...
AXFR record query failed: REFUSED
Trying Zone Transfer for testfire.net on usw2.akam.net ...
AXFR record query failed: REFUSED
Trying Zone Transfer for testfire.net on eur2.akam.net ...
AXFR record query failed: REFUSED
Trying Zone Transfer for testfire.net on usc2.akam.net ...
AXFR record query failed: REFUSED
Trying Zone Transfer for testfire.net on eur5.akam.net ...
AXFR record query failed: REFUSED
Trying Zone Transfer for testfire.net on ns1-99.akam.net ...
AXFR record query failed: REFUSED

@route forcing with /usr/share/dnsenum/dns.txt:

ftp.testfire.net.      86256    IN      CNAME   testfire.net.
testfire.net.          48589    IN      A       65.61.137.117
```

**DNS Recon:** DNS reconnaissance, also known as DNS recon, refers to the process of gathering information about a target's network infrastructure, domain names, subdomains, and associated IP addresses using DNS-related techniques. This reconnaissance is crucial for understanding a network's structure and identifying potential vulnerabilities or entry points.

```
(rishi@kali)~$ dnsrecon -d testfire.net
[*] std: Performing General Enumeration against: testfire.net...
[-] DNSSEC is not configured for testfire.net
[*] SOA asia3.akam.net 23.211.61.64
[*] NS usw2.akam.net 184.26.161.64
[*] Bind Version for 184.26.161.64 "42475.168"
[*] NS usc2.akam.net 184.26.160.64
[*] Bind Version for 184.26.160.64 "29251.67"
[*] NS eur5.akam.net 23.74.25.64
[*] Bind Version for 23.74.25.64 "42608.6"
[*] NS eur2.akam.net 95.100.173.64
[*] Bind Version for 95.100.173.64 "43223.22"
[*] NS usc3.akam.net 96.7.50.64
[*] Bind Version for 96.7.50.64 "32886.207"
[*] NS asia3.akam.net 23.211.61.64
[*] Bind Version for 23.211.61.64 "32865.234"
[*] NS ns1-206.akam.net 193.108.91.206
[*] Bind Version for 193.108.91.206 "33301.38"
[*] NS ns1-206.akam.net 2600:1401:2::ce
[*] NS ns1-99.akam.net 193.108.91.99
[*] Bind Version for 193.108.91.99 "33301.25"
[*] NS ns1-99.akam.net 2600:1401:2::63
[*] A testfire.net 65.61.137.117
[*] TXT testfire.net v=spf1 mx/24 -all
[*] TXT _dmarc.testfire.net v=DMARC1; p=reject; fo=1; rua=mailto:dmarc_rua@emaildefense.proofpoint.com; ruf=mailto:dmarc_ruf@emaildefense.proofpoint.com
[*] Enumerating SRV Records
[+] 0 Records Found
```

**Whois:** A WHOIS tool is an internet utility used to retrieve information about domain names, IP addresses, and their registrants or owners. It provides publicly available registration data maintained by domain name registrars and registries. This information can include details about the domain's owner, registration and expiration dates, contact information, name servers, and more. Using WHOIS information responsibly is essential, and accessing it should align with the terms of service provided by the registrar or registry.

```
(rishi@kali)~$ whois testfire.net
Domain Name: TESTFIRE.NET
Registry Domain ID: 8363973_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
Updated Date: 2023-07-19T05:05:02Z
Creation Date: 1999-07-23T13:52:32Z
Registry Expiry Date: 2024-07-23T13:52:32Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: ASIA3.AKAM.NET
Name Server: EUR2.AKAM.NET
Name Server: EUR5.AKAM.NET
Name Server: NS1-206.AKAM.NET
Name Server: NS1-99.AKAM.NET
Name Server: USC2.AKAM.NET
Name Server: USC3.AKAM.NET
Name Server: USW2.AKAM.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-08-14T16:25:55Z <<<
```

```

domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

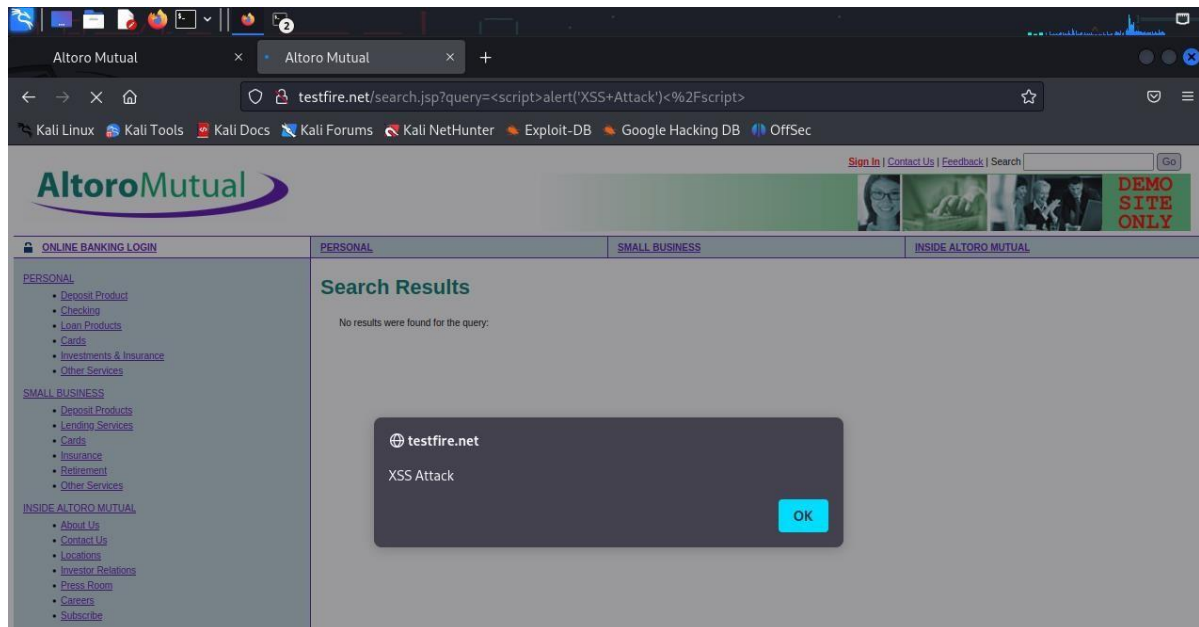
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.

Domain Name: testfire.net
Registry Domain ID: 8363973_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2023-07-19T01:05:02Z
Creation Date: 1999-07-23T09:52:32Z
Registrar Registration Expiration Date: 2024-07-23T13:52:32Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Not Disclosed
Registrant Organization: Not Disclosed
Registrant Street: Not Disclosed
Registrant City: Sunnyvale
Registrant State/Province: CA
Registrant Postal Code: 94085
Registrant Country: US
Registrant Phone: +Not Disclosed
Registrant Phone Ext:
Registrant Fax: +Not Disclosed
Registrant Fax Ext:
Registrant Email: Not Disclosed
Registry Admin ID:
Admin Name: Not Disclosed
Admin Organization: Not Disclosed
Admin Street: Not Disclosed
Admin City: Sunnyvale
Admin State/Province: CA
Admin Postal Code: 94085
Admin Country: US
Admin Phone: +Not Disclosed
Admin Phone Ext:
Admin Fax: +Not Disclosed
Admin Fax Ext:
Admin Email: Not Disclosed
Registry Tech ID:
Tech Name: Not Disclosed
Tech Organization: Not Disclosed
Tech Street: Not Disclosed
Tech City: Sunnyvale
Tech State/Province: CA
Tech State/Province: CA
Tech Postal Code: 94085
Tech Country: US
Tech Phone: +Not Disclosed
Tech Phone Ext:
Tech Fax: +Not Disclosed
Tech Fax Ext:
Tech Email: Not Disclosed
Name Server: ns1-99.akam.net
Name Server: eur5.akam.net
Name Server: eur2.akam.net
Name Server: ns1-206.akam.net
Name Server: usw2.akam.net
Name Server: usc3.akam.net
Name Server: asia3.akam.net
Name Server: usc2.akam.net
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-07-19T01:05:02Z <<<

```

## 4. RESULTS AND DISCUSSION

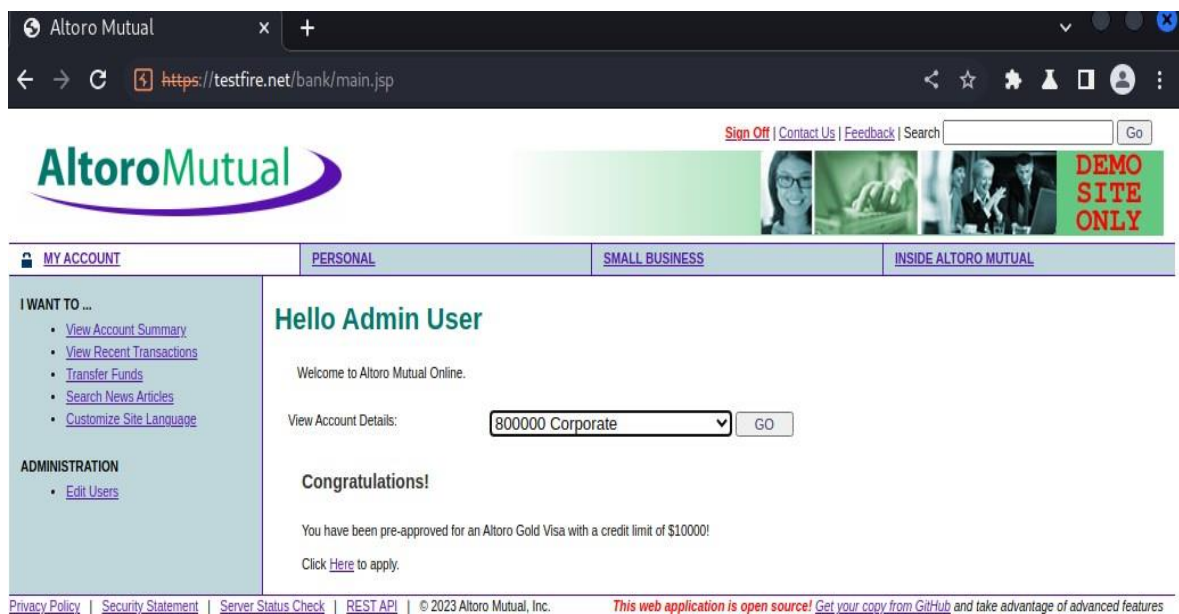
**Cross-Site Scripting:** The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. At a later time, the dangerous data is subsequently read back into the application and included in dynamic content. From an attacker's perspective, the optimal place 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. After implementing the XSS attack, there will be a pop up which is given in our xss payload.



**SQL Injection:** A SQL injection attack consists of insertion or “injection” of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file

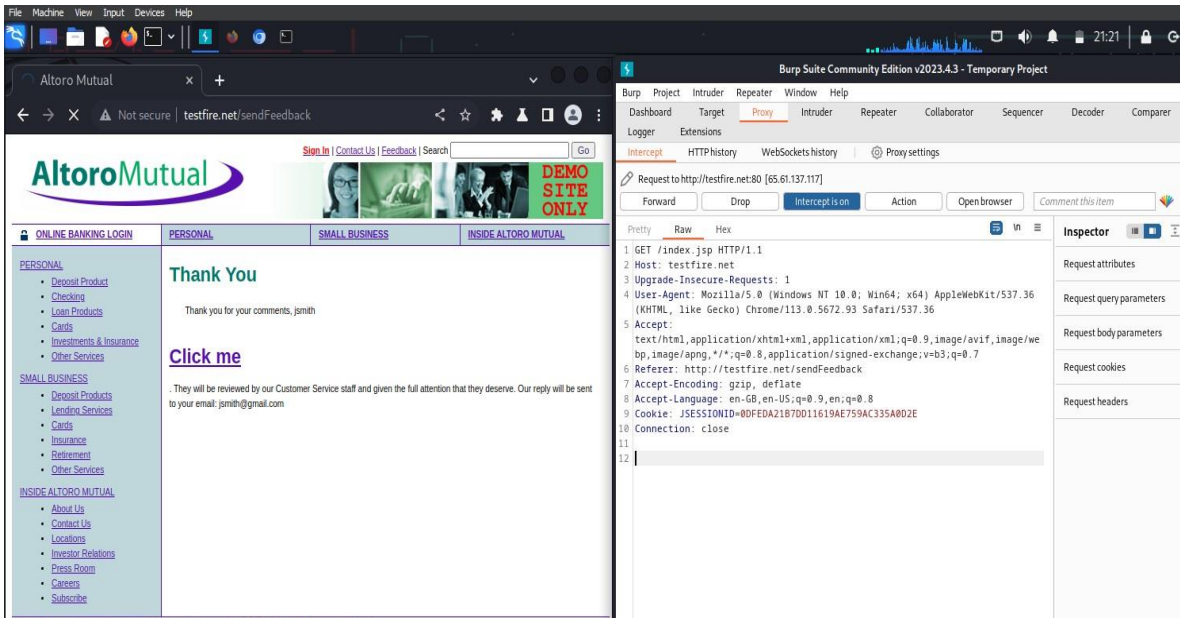


system and in some cases issue commands to the operating system. SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server. SQL Injection is very common with PHP and ASP applications due to the prevalence of older functional interfaces. After we implemented the SQL injection, we have logged in as admin user.



**HTML-Injection Reflected:** A phony form might be used by the attacker to steal password information saved in the browser or to fool a user into entering their login information. Malicious actors may be granted administrative access to the online application if the targeted user has those rights. By carrying out an assault that is visible to the public, the attacker might seriously damage the image of the business, organization, or even nation. Users or clients may make poor judgments and lose faith in your cybersecurity procedures if a high-value page is vandalized or exploited to propagate misinformation. HTML injection might be used as a technique by the attacker to progress to more severe assaults like CSRF. The attacker creates malicious links with his HTML content inserted into them, then emails the URLs to the victim.

Because the page is hosted on a reputable domain, the user views it, which causes his identity to be stolen. After the performing the attack we successfully proved that there is no input validation, as our input reflected on the site



**IDOR Vulnerability:** In the business context, an Insecure Direct Object Reference (IDOR) vulnerability can have serious and wide-ranging consequences. IDOR vulnerabilities can lead to unauthorized access to sensitive data, which may include customer records, financial information, intellectual property, and confidential documents. Such unauthorized access can result in data breaches, causing significant reputational damage and undermining customer trust, leading to a potential loss of customers. Furthermore, these vulnerabilities can have financial implications. They can be exploited to manipulate financial records or transactions, potentially leading to financial losses, such as unauthorized fund transfers or fraudulent activities. In cases involving personal data, organizations may face legal and regulatory consequences, including fines and legal actions, for non-compliance with data protection regulations. The impact extends to the organization's reputation, which is a critical asset in business. News of a data breach or security incident can harm an organization's reputation, making it difficult to attract new customers and potentially causing customer churn. competitive edge.

Additionally, competitors may take advantage of IDOR vulnerabilities to access sensitive business information, gaining a IDOR vulnerabilities can disrupt business operations, damage reputation, result in financial losses, IDOR vulnerabilities can disrupt business operations, damage reputation, result in financial losses, and lead to legal and regulatory challenges. After the attack can access the details of the account 800001

**AltoroMutual**

**Account History - 800001**

**Balance Detail**

Account	Amount
800002 Savings	\$100000.00
Ending balance as of 8/30/23 10:57 AM	\$100000.00
Available balance	\$100000.00

**30 Most Recent Transactions**

Date	Description	Amount
2023-08-30	Deposit	\$100.00
2023-08-30	Deposit	\$100.00
2023-08-30	Deposit	\$100.00
2023-08-30	Deposit	\$100.00
2023-08-30	Deposit	\$100.00
2023-08-30	Deposit	\$100.00
2023-08-30	Deposit	\$100.00
2023-08-30	Deposit	\$100.00
2023-08-30	Deposit	\$100.00
2023-08-30	Deposit	\$100.00

**Credits**

Account	Date	Description	Amount
1001100140	12/29/2004	Paycheck	1200
1001100140	01/12/2005	Paycheck	1200
1001100140	01/29/2005	Paycheck	1200
1001100140	02/12/2005	Paycheck	1200
1001100140	03/01/2005	Paycheck	1200
1001100140	03/15/2005	Paycheck	1200

**Brute Force:** Brute force attacks can have significant business impacts, primarily due to the potential compromise of sensitive information and the resources to mitigate and recover from such attacks. First and foremost, the unauthorized access to sensitive data can lead to data breaches, which may expose customer records, financial information, intellectual property, and confidential documents. This can have severe reputational consequences, eroding trust and confidence among customers and business partners. Loss of customer trust can result in customer churn, decreased business, and a negative impact on an organization's brand and market position. After the attack we have successfully logged in as an Admin.

**AltoroMutual**

**Hello Admin User**

Welcome to Altoro Mutual Online.

View Account Details:

**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 | BEST API | © 2023 Altoro Mutual, Inc.

## 5. CONCLUSION

As we came across different vulnerabilities within the given website we have come to the following conclusions. Note that proper output encoding, escaping, and quoting is the most effective solution for preventing XSS, although input validation may provide some defense-in-depth. Do not rely on client-side input validation. It is better to use a database user with restricted privileges. Use prepared statements and query parameterization. Scan your code for SQL injection vulnerabilities.

It is therefore essential to have appropriate data validation in place to prevent such attacks. Every input should be checked if it contains any script code or any HTML code. One should check, if the code contains any special script or HTML brackets. The most common way of detecting HTML injection is by looking for HTML elements in the incoming HTTP stream that contains the user input. A naive validation of user input simply removes any HTML-syntax substrings (like tags and links) from any user-supplied text. Implement Proper Access Controls. Avoid Direct Object References in URLs or Parameters. Apply Input Validation and Sanitization. Use Unique and Randomized Identifiers

With the number of data breaches on the rise, companies urgently look for new ways to protect their data. The internet is overflowing with information on how companies can protect their data. The truth is that businesses of all sizes need to utilize an excellent VAPT solution to safeguard the data. In this blog post, we've discussed the importance of a VAPT solution and how it can help protect your business from malicious attacks. The best part is that it's affordable for all businesses.



## 6. REFERENCE

Tajpour Atefeh, Maslin Masrom, Mohammad Zaman Heydari and Suhaimi Ibrahim, "SQL injection detection and prevention tools assessment", Computer Science and Information Technology (ICCSIT) 2010 3rd IEEE International Conference, vol. 9, pp. 518-522, 2010.

S. Ali, S.K. Shahzad and H. Javed, "SQLIPA: An Authentication Mechanism Against SQL Injection", European Journal of Scientific Research, vol. 38, no. 4, pp. 604-611, 2009.

S. J. Sadana and N. Selam, "Analysis of Cross Site Scripting Attack", Proc. International Journal of Engineering Research and Applications (IJERA), vol. 1, no. 4, pp. 1764-1773, 2011.

R. Kumar, "Mitigating the authentication vulnerabilities in Web applications through security requirements", Information and Communication Technologies (WICT), vol. 60, pp. 651-663, 2011.

A. Avancini and M. Ceccato, "Towards Security Testing with Taint Analysis and Genetic Algorithms", ICSE Workshop on Software Engineering for Secure Systems, vol. 5, pp. 65-71, 2010.

L. S. Shar, H. B. K. Tan and L. C. Briand, "Mining SQL injection and cross site scripting vulnerabilities using hybrid program analysis", Proc. of Int. Conf. on Software Engineering (ICSE '13), pp. 642-651, 2013.

**SESHADRI RAO**  
**GUDLAVALLERU ENGINEERING COLLEGE**

(An Autonomous Institute with Permanent Affiliation to JNTUK, Kakinada)  
Seshadri Rao Knowledge Village, Gudlavalleru

**Department of Computer Science and Engineering**

**Program Outcomes (POs)**

**Engineering Graduates will be able to:**

- 1. Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
- 2. Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
- 3. Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
- 4. Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions., component, or software to meet the desired needs.
- 5. Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
- 6. The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
- 7. Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
- 8. Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

- 9. Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
- 10. Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
- 11. Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
- 12. Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

### **Program Specific Outcomes (PSOs)**

PSO1 : Design, develop, test and maintain reliable software systems and intelligent systems.

PSO2 : Design and develop web sites, web apps and mobile apps.

## PROJECT PROFORMA

Classification of Project	Application	Product	Research	Review
	√			

**Note: Tick Appropriate category**

Project Outcomes	
Course Outcome (CO1)	Acquire technical competence in the specific domain during the training.
Course Outcome (CO2)	Identify the problem statement based on the requirements of the industry
Course Outcome (CO3)	Adapt project management skills on par with industrial standards.
Course Outcome (CO4)	Develop a system model to obtain a solution and generate a report.

## Mapping Table

CS3523: INTERNSHIP/ INDUSTRIAL TRAINING/ PRACTICAL TRAINING															
Course outcomes	Program Outcomes and Program Specific Outcome														
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12		PSO1	PSO2
CO1	3	2	2	2	2			2	2	2	1	2		2	
CO2	3	3	2	2	1			2	2	2	1	2		2	2
CO3	1		1		1	1	1	2	2	2	3	2		2	
CO4	3	2	3	3	3	2	1	2	2	2	3	2		2	2
INTERNSHIP/ INDUSTRIAL TRAINING/ PRACTICAL TRAINING	3	2	2	2	2	1	1	2	2	2	2	2		2	1

**Note: Map each project outcomes with POs and PSOs with either 1 or 2 or 3 based on level of mapping as follows:**

1-Slightly (Low) mapped      2-Moderately (Medium) mapped    3-Substantially (High) mapped

Name: Yarroju Rudra Prakash  
Roll No: 20481A05P5



Name: Tellakula Tharuni  
Roll No:20481A05M7



Name: Somala Anu  
Roll No: 20481A05L9

