

# Reconnaissance Assessment Report

**Target:** [testfire.net](#)

**Category:** Finance

**Assessment Date:** November 5, 2025

**Classification:** FOR OFFICIAL USE ONLY

## Executive Summary

This reconnaissance assessment identified [testfire.net](#) as a financial application running on Apache Tomcat with multiple domain associations. The infrastructure is hosted on Rackspace with adequate security controls including transfer prohibitions. The digital footprint reveals three interconnected domains with shared hosting infrastructure.

## 1.1 Domain Information

### 1.1 Registration Details

Attribute	Value
Domain	<a href="#">testfire.net</a>
Registrar	TurnCommerce, Inc.DBA <a href="#">NameBright.com</a>
Creation Date	2017-11-17
Expiration Date	2026-11-17
Domain Age	2,911 days
Registrar Status	clientTransferProhibited

---

## 2. Subdomain Enumeration Results

### 2.1 Discovered Subdomains

Subdomain	Status	Risk Level
<a href="#">altoro.testfire.net</a>	Active	Critical
<a href="#">demo.testfire.net</a>	Active	High
<a href="#">demo2.testfire.net</a>	Active	High
<a href="#">ftp.testfire.net</a>	Active	Critical

<i>Subdomain</i>	<i>Status</i>	<i>Risk Level</i>
<a href="#">rev11.testfire.net</a>	Active	Medium
<a href="#">localhost.testfire.net</a>	Active	High

---

### 3. Exposed Services Analysis

#### 3.1 Service Mapping

<b>Service</b>	<b>Port</b>	<b>Technology</b>	<b>Exposure</b>
Web Application	80	Apache Tomcat/Coyote JSP engine 1.1	Public
Secure Web	443	SSL/TLS	Public
Alternative Web	8080	Unknown Service	Public
FTP Service	21	FTP Protocol	Public

#### 3.2 Technology Stack

- **Web Server:** Apache Tomcat/Coyote JSP engine 1.1
  - **Programming Language:** Java
  - **Application:** Altoro Mutual (Financial)
  - **Session Management:** JSESSIONID with HttpOnly
  - **Hosting Provider:** Rackspace Backbone Engineering
-

## 4. Asset Mapping Log

### 4.1 Reconnaissance Timeline

Timestamp	Tool	Finding
2025-11-05 16:44:00	Shodan	Apache Tomcat on port 80
2025-11-05 16:45:00	WHOIS	Domain registration details
2025-11-05 16:46:00	Shodan	Open ports: 80,443,8080
2025-11-06 16:51:58	SubFinder	6 subdomains discovered
2025-11-06 16:52:00	Manual	Technology stack identification

### 4.2 Infrastructure Assets

Asset Type	Count	Details
Primary Domains	1	<a href="#">testfire.net</a>
Subdomains	6	Various purposes
IP Addresses	1	<b>65.61.137.117</b>
Open Ports	3	80, 443, 8080
Network Services	4	Web, Secure Web, Alt Web, FTP

### 4.2 Server Response Headers

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=FA065549AAAECF2ECE1DF729EBEE2D2B; Path=/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
```

## 5. OSINT Checklist Completion

### Completed Tasks

- **WHOIS Analysis** - Full registration details obtained
- **Subdomain Enumeration** - 6 subdomains discovered using SubFinder
- **Technology Identification** - Apache Tomcat/Java stack confirmed
- **Service Discovery** - 3 open ports and implied FTP service
- **Infrastructure Mapping** - Rackspace hosting identified

## Conclusion

The reconnaissance assessment reveals [testfire.net](#) as a well-established financial application with adequate security controls at the registrar level. The infrastructure shows standard enterprise hosting patterns with minor exposure concerns related to service versions and shared hosting