**Practice Website Vulnerabilities**

**Vulnerability Name**: ICMP Timestamp Request Remote Date Disclosure

**CWE**:  [200](http://cwe.mitre.org/data/definitions/200)

**Description**: The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. Timestamps returned from machines running Windows Vista / 7 / 2008 /2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

**Business Impacts**: Revealing system information can provide attackers with valuable insights into your network architecture and infrastructure. This information can be exploited to plan and execute more targeted attacks.

**Vulnerability Pub Date**: January 1, 1995

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

**Vulnerability Name**: OS Identification

**Description**: Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

**Business Impacts**: An OS identification vulnerability might reveal the specific operating system version and its associated vulnerabilities. Attackers can use this information to target known vulnerabilities in the OS, potentially gaining unauthorized access to the system. This could lead to data breaches, data loss, and damage to the organization's reputation.

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

**Vulnerability Name**: Device Type

**Description**: Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

**Business Impacts**: When vulnerabilities are exploited and lead to incidents like data breaches or service disruptions, an organization's reputation can suffer. Customers may lose trust, leading to a loss of business and difficulty acquiring new customers.

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

--------------------------------------------------------------------------------------------------------------------------------------

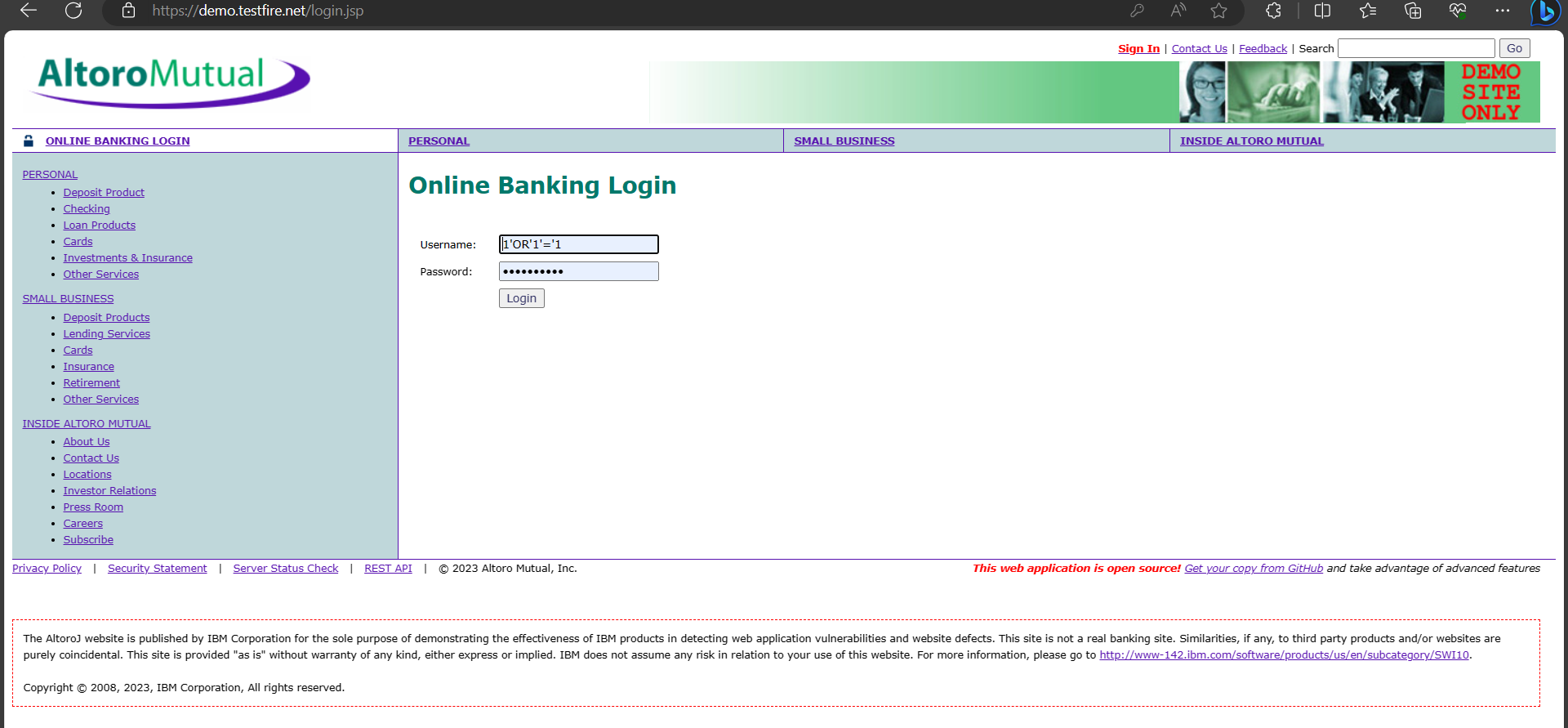
**Vulnerability Name**: SQL Injection Vulnerability (for login bypass)

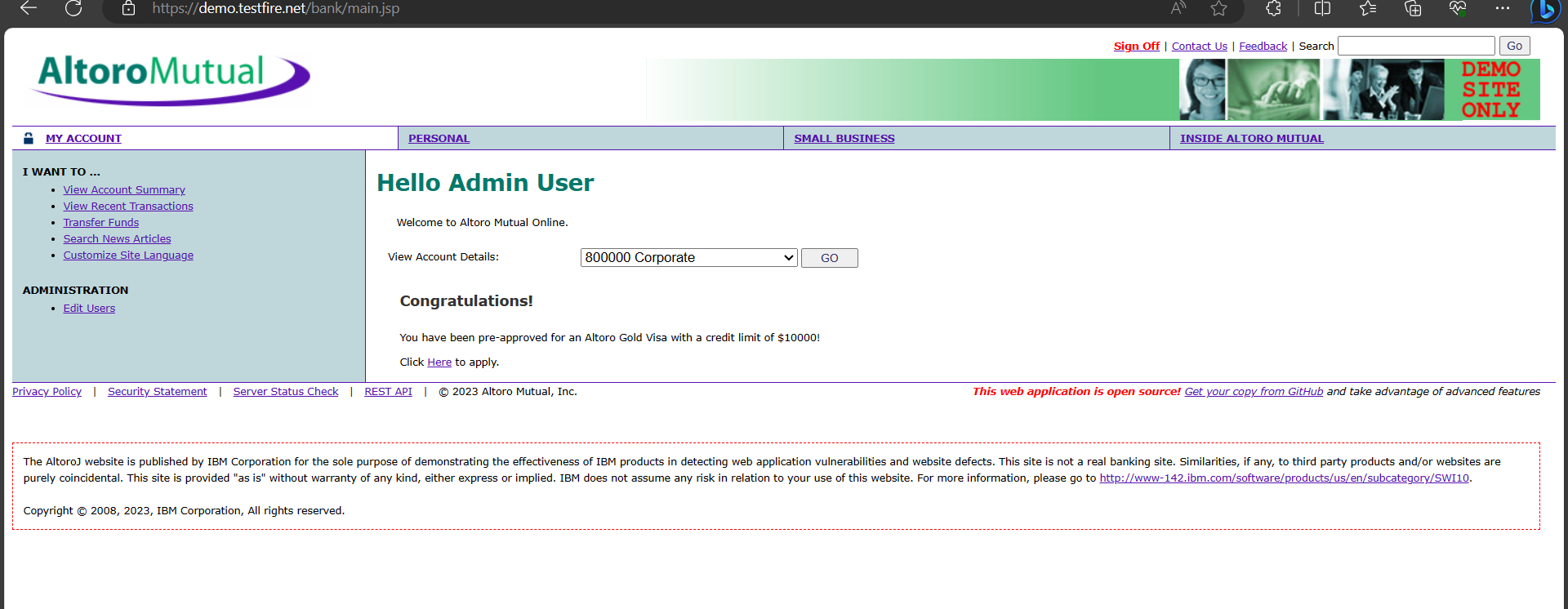
**Vulnerability Level:** High

**Description:** The test website <https://testfire.net/> is vulnerable to SQL injection attacks, and allows even basic SQL injection attacks, enabling attackers to obtain successful unauthorized access as admin or any user of the website.

**Business impacts:** SQL injection vulnerability leading to unauthorized access can result in severe data breaches, compromising customer trust and potentially leading to legal repercussions and financial losses.

**Vulnerability path: https://demo.testfire.net/login.jsp**

****

****

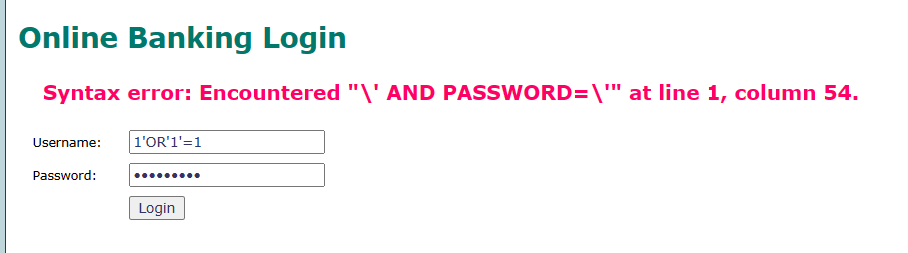
**Vulnerability Name**: Displaying internal server error from tomcat

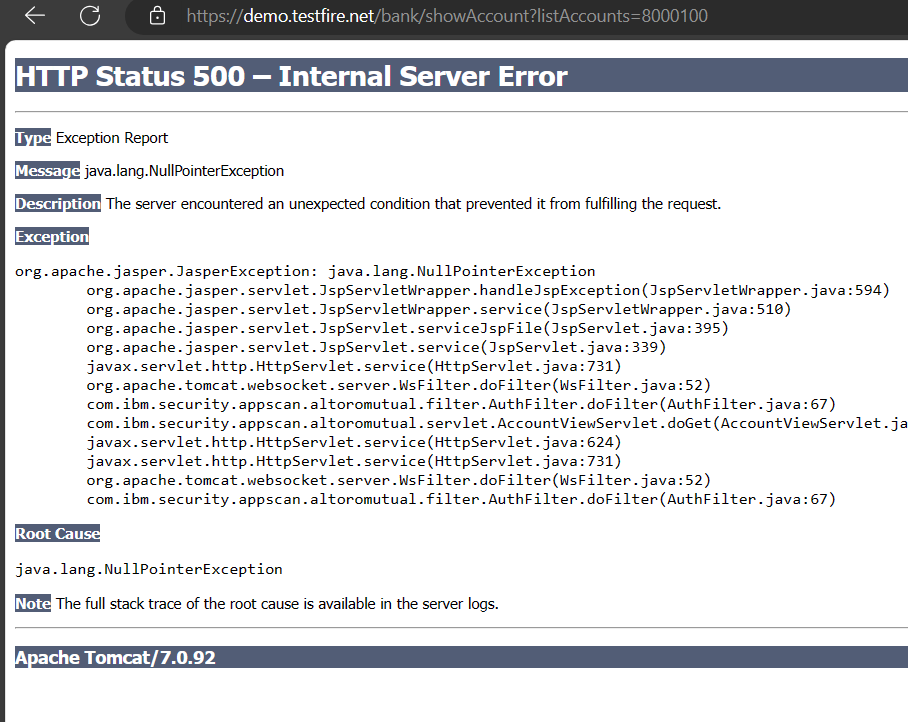
**Vulnerability Level:** High

**Description:** The website displays all the internal server error along with the entire error trace stack, also displays the Apache tomcat version. The allows attackers to debug or understand the code logics and also find vulnerabilities associated with that specific tomcat server version.

**Business impacts:** This vulnerability can expose sensitive system information, enabling attackers to identify weaknesses and potentially exploit them, leading to security breaches, data loss, and reputational damage with significant business and financial consequences.

**Vulnerability path:** [**https://demo.testfire.net/login.jsp**](https://demo.testfire.net/login.jsp)

****

****

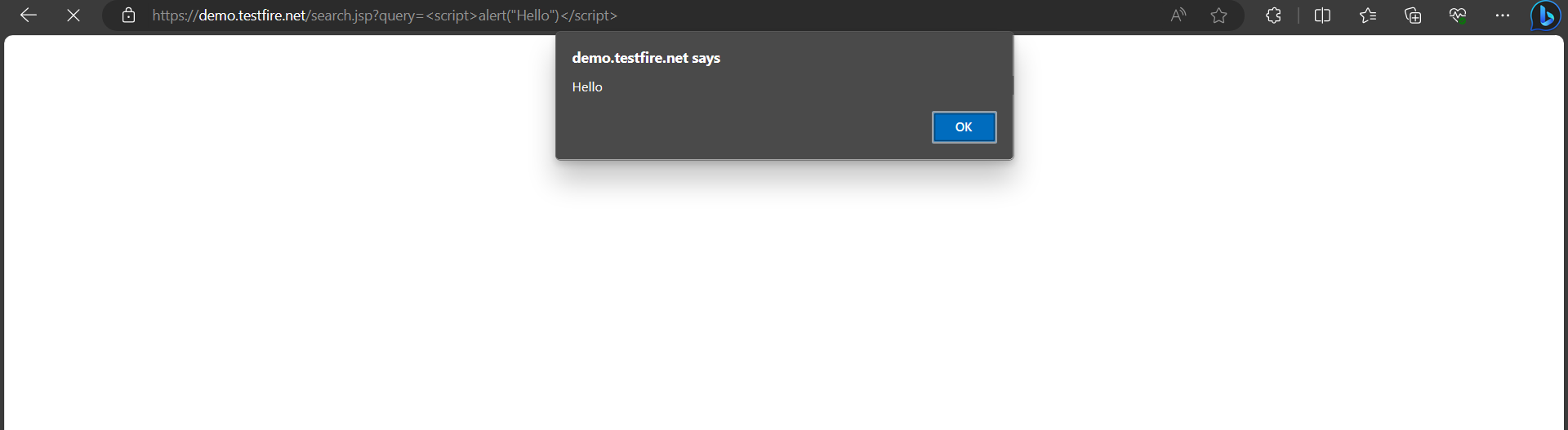
**Vulnerability Name**: Cross site Scripting XSS

**Vulnerability Level:** Moderate

**Description:** Improper query field validation or input filed validation. The website doesn’t sanitize the input or query fields. Attackers will be able to send crafted inputs to users and can steal sensitive data like cookies and gain access.

**Business Impact:** Cross-Site Scripting (XSS) can have various business impacts, including compromised user data, damaged reputation, legal liabilities, and financial losses due to potential theft or manipulation of sensitive information, leading to decreased customer trust and operational disruptions.

**Vulnerability path: https://demo.testfire.net/search.jsp?query**

****

**Vulnerability name :** Insecure Direct Object Reference.

**CWE :** 639.

**Description :** Insecure Direct Object Reference is an access control problem that allows an attacker to view data by manipulating an identifier.

**Business impact :** Insecure Direct Object References (IDOR) occur when an application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources in the system directly, for example database records or files.

**Vulnerability path :** [**https://demo.testfire.net/**](https://demo.testfire.net/)

**Vulnerability name :** Security Misconfiguration.

**CWE :** OWASPA05 Category.

**Description :** Security misconfigurations are security controls that are inaccurately configured or left insecure, putting your systems and data at risk. Basically, any poorly documented configuration changes, default settings, or a technical issue across any component in your endpoints could lead to a misconfiguration.

**Business impact :** It a misconfigured database server can cause data to be accessible through a basic web search. If this data includes administrator credentials, an attacker may be able to access further data beyond the database, or launch another attack on the company's servers.

**Vulnerability path :** [**https://demo.testfire.net/**](https://demo.testfire.net/)

**Vulnerability Name**:HTTP Server type and Version

**CWE**: 444

**Description**: This plugin attempts to determine the type and the version of the remote web server.

**Business Impacts**: Knowing the server type and version allows an attacker to focus on the vulnerabilities of that specific version, whereas someone without this knowledge would have to try different vulnerabilities by brute- force. In addition, some servers disclose the operating system version within HTTP response headers. For example, Apache often discloses UNIX or Windows whilst Microsoft-IIS only runs on Windows, and each version of IIS only runs on a single version of Windows.

**Vulnerability Pub Date**: 1/4/2000

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

**Vulnerability Name**: Traceroute Infromation

**Description**: A traceroute provides a map of how data on the internet travels from its source to its destination

**Business Impacts**: One way that a traceroute can be used to determine if a website is hacked is by looking for any unexpected or unfamiliar IP addresses or domains in the traceroute results. If a hacker has gained access to a website, they may have inserted their own code or servers into the website's infrastructure, which would likely show up in a traceroute as an unexpected IP address or domain. Additionally, if a website is experiencing a DDoS attack, the traceroute may show a large number of requests originating from a single IP address or domain, which could indicate that the website is under attack.

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

**Vulnerability Name**: Additional DNS Hostnames

**Description**: Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for hosts discovered on a web server. Different web servers may be hosted on name-based virtual hosts.

**Business Impacts**: An attacker with the ability to conduct a successful cache poisoning attack can cause a nameserver's clients to contact the incorrect, and possibly malicious, hosts for particular services. Consequently, web traffic, email, and other important network data can be redirected to systems under the attacker's control.

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