

Phishing Report of <https://demo.testfire.net/>

 **Vulnerability Name:** Authentication Bypass

Description

Authentication bypass occurs when an attacker gains unauthorized access to a system without completing the intended authentication process. This typically exploits flaws in input validation, session management, or logic errors in authentication workflows.

A common example is using SQL injection to manipulate login queries. If multi-factor authentication (MFA) is not enforced, attackers can gain access using only compromised credentials.

Attack Steps

Step 1:

Searched for vulnerable login pages using Google dork:
inurl:admin login php site:demo.testfire.net

Step 2:

Accessed the admin login page of the target website.

Step 3:

Analyzed login logic:

User Id	Password	Result
True	True	True
True	False	False
False	True	False
False	False	False

Step 4:

Injected SQL payload in the login field:

```
1' OR '1'='1
```

This bypassed authentication and granted admin access.

System State

Before Exploit:

- Login page accessible without input validation
- No multi-factor authentication
- Database vulnerable to SQL injection

After Exploit:

- Admin access gained without valid credentials
- Sensitive data exposed
- System integrity compromised

⚠ Mistakes by Roles & Suggested Fixes

👤 Web Developer Mistake

Issue: Input fields allow special characters, enabling SQL injection.

Suggestions:

- ✓ Use input validation (e.g., regex for alphanumeric usernames)
- ✓ Implement server-side validation
- ✓ Use prepared statements or ORM to prevent SQL injection
- ✓ Integrate security libraries (e.g., OWASP ESAPI)

🗄 Database Administrator Mistake

Issue: Database lacks encryption, exposing sensitive data.

Suggestions:

- ✓ Encrypt data at rest using AES-256
- ✓ Hash passwords with bcrypt or Argon2
- ✓ Enable Transparent Data Encryption (TDE)
- ✓ Rotate encryption keys regularly

🌐 Network Administrator Mistake

Issue: Firewall misconfiguration allows unauthorized access.

Suggestions:

- ✓ Apply least privilege rules for inbound/outbound traffic
- ✓ Block unused ports and monitor logs
- ✓ Deploy IDS/IPS systems
- ✓ Conduct regular firewall audits and penetration tests

✓ Final Recommendations

- Enforce **multi-factor authentication (MFA)**
- Conduct **regular vulnerability assessments**
- Train developers on **secure coding practices**
- Maintain **incident response plans** for breach scenarios

Before Attack:

AltoroMutual Sign In | Contact Us | Feedback | Search | Go

ONLINE BANKING LOGIN PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

PERSONAL

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

SMALL BUSINESS

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

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it.

Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc. *This web application is open source! Get your copy from GitHub and take advantage of advanced features*

The Altoro website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/appscan/>.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.

After Attack:

AltoroMutual Sign Off | Contact Us | Feedback | Search | Go

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

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.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc. *This web application is open source! Get your copy from GitHub and take advantage of advanced features*

The Altoro website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/appscan/>.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.