

PRACTICAL NO - 6

AIM: Simulate persistent Cross Site Scripting attack.

The image displays two screenshots of the AltoroMutual website, demonstrating a Cross Site Scripting (XSS) attack.

Top Screenshot (Initial State): The browser address bar shows `altoro.testfire.net`. The website features a navigation menu with categories: ONLINE BANKING LOGIN, PERSONAL, SMALL BUSINESS, and INSIDE ALTORO MUTUAL. The PERSONAL section includes links for Deposit Products, Checking, Loan Products, Cards, Investments & Insurance, and Other Services. The SMALL BUSINESS section includes links for Deposit Products, Lending Services, Cards, Insurance, Retirement, and Other Services. The INSIDE ALTORO MUTUAL section includes links for About Us, Contact Us, Locations, Investor Relations, Press Room, Careers, and Subscribe. The main content area displays various services like Online Banking with FREE Online Bill Pay, Real Estate Financing, Business Credit Cards, Retirement Solutions, and Privacy and Security. A footer notice states: "This web application is open source! Get your copy from GitHub and take advantage of advanced features".

Bottom Screenshot (XSS Attack Result): The browser address bar shows `altoro.testfire.net/search.jsp?query=tycs+ekta+yadav`. The search results section displays "No results were found for the query: tycs ekta yadav". The footer notice remains the same.