









Rhino Security Labs

-  **Client:** Rhino Security Labs
-  **Site:** rhinosecuritylabs.com
-  **Industry:** Cybersecurity
-  **Country:** USA
-  **Size of the Team:** 1 person
-  **Duration:** ongoing, 6 months



Technologies Used:



CLOJURE



POSTGRES



CLOSTACHE



ANGULAR



CSS 3



HTML 5



OUR CLIENT

The main objectives of Rhino Security Labs' services are to identify security vulnerabilities, protect architecture and mitigate risks. The company is known for its insight into the needs of retail and healthcare, financial services and technology as well as other vertical markets. All security assessment and management services can be tailored to the needs of specific businesses, be it a multinational corporate giant or a budding start-up.

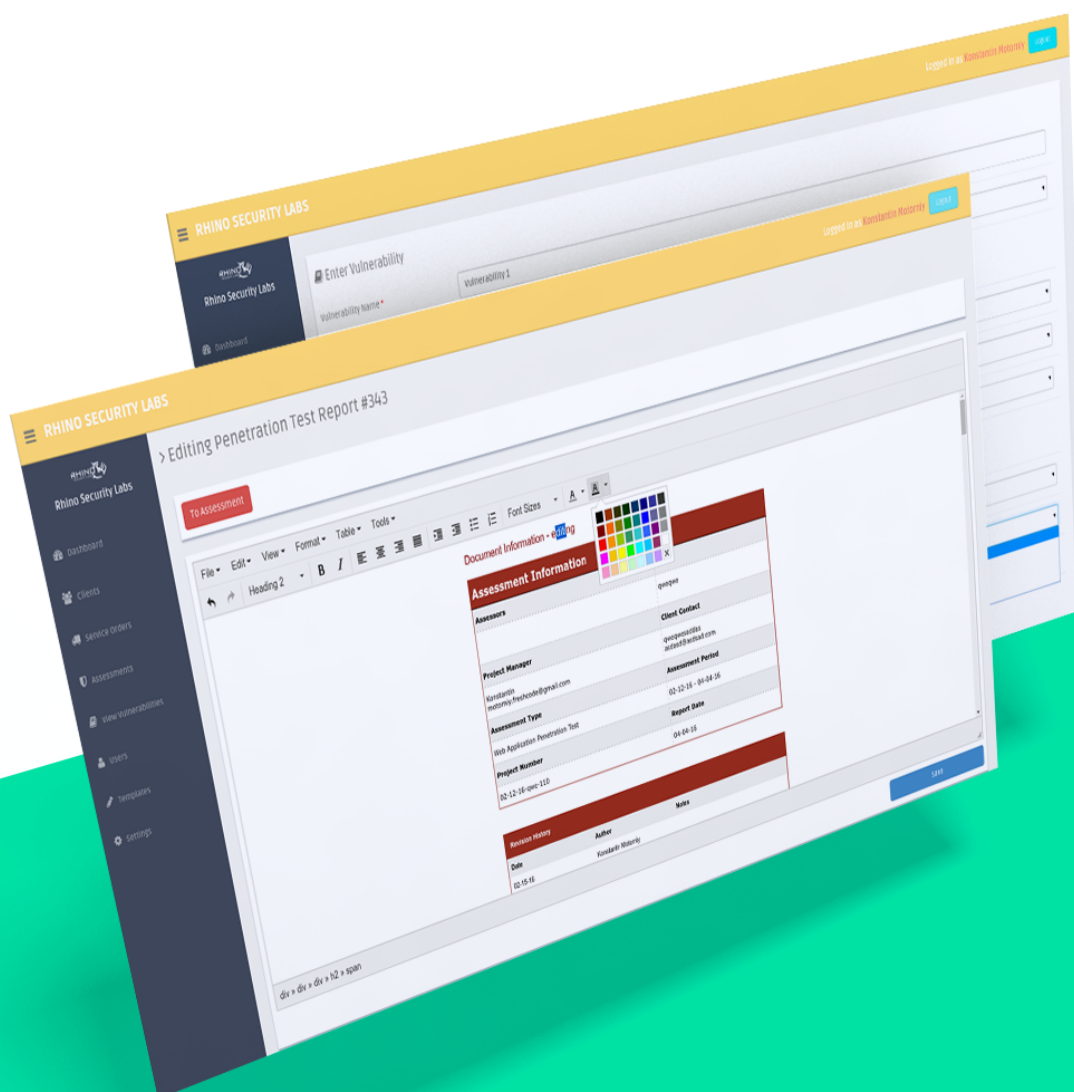




BUSINESS ISSUES

Security assessment report building application was in order to replace manual report generation. Our main objectives included:

- ▶ Replacing manual report building tool with automated application
- ▶ Using XML parser to improve third-party applications security data aggregation efficiency and time
- ▶ Creating flexible online PDF editor for reports' templates
- ▶ Providing several data access layers
- ▶ Additional report types generation according to the type of security vulnerabilities





SOLUTIONS

Our team created a flexible, easy-to-use web-application for automatic PDF reports generation using XML parser to effectively aggregate external applications' data on security vulnerabilities. Detailed reports are automatically filled with information on vulnerabilities' background, threat level and possible solutions. Generated PDF report as well as PDF report templates can be edited using online template engine. To guarantee data security and prevent any security leaks during report generation our developers created additional tools, including the custom screen-shot editor.

One of the most daunting tasks was creating several data access layers: two for admins and several layers for basic users with possibilities to generate and edit reports as well as the database.

Report generation tool recognizes three main types of security vulnerabilities and chooses report template accordingly. Future development will see template tree broadening with individual templates for new types of vulnerabilities, further integration with other tools and creating reports' export system.

The screenshot displays the 'Rhino Security Labs' web application interface. The top navigation bar is orange and contains the company logo, name, and contact information. The left sidebar is dark blue and lists various menu items. The main content area is white and shows the 'Edit Service Order' form for 'Super Mega Company 77'. The form is divided into several sections: 'Personnel', 'Services', 'Time and Cost', and 'Cost Summary'. The 'Time and Cost' section includes input fields for 'Project Timetable', 'Days', 'Hours per Day', 'Pen-Testers', 'Start Date (Optional)', and 'End Date (Optional)'. The 'Cost Summary' section features a table with columns for 'Service', 'Price', 'Quantity', and 'Total'. The table contains one row for 'Digital Forensic Investigation, Analysis, and Data Recovery' with a price of \$12.00, a quantity of 5, and a total of \$60.00. There is also a 'Discount' field set to 10.0 and a 'Total' field set to \$60.00. At the bottom of the form, there are buttons for 'Save Service Order' and 'Download PDF'.

Service	Price	Quantity	Total
Digital Forensic Investigation, Analysis, and Data Recovery	\$12.00	5	\$60.00

BUSINESS VALUE

This solution accelerated Rhino Security Labs' performance and improved service quality. As a result our client is experiencing an increase in a number of customers.