



Elegant MicroWeb
Delivering the Value of Technology

Case Study

Web Application Security and Accessibility Standards Compliance

SECURITY



➤ www.ElegantMicroWeb.com

Elegant MicroWeb Technologies Pvt. Ltd.
A-305, Shapath - IV, Opp. Karnavati Club,
SG Highway, Ahmedabad-380051 India
Email: info@ElegantMicroWeb.com



ISO 9001:2008



Case Study

Web Application Security and Accessibility Standards Compliance

Client

A leading Internet Community, Consultation and eDemocracy Solution Provider in UK

The Company

The UK-based client of Elegant Microweb is a leading Internet Community, Market Research, Consultation and eDemocracy solution provider. The company's mission is to enhance participation, promote engagement and consultation, trigger thought leadership, and champion innovations that advance the greater cause of democracy by harnessing latest advances in Information Technology. The client's customer base includes:

- Local UK Government authorities
- Office of the Deputy Prime Minister
- Scottish Parliament
- Welsh assembly

- General Medical council and similar organizations
- Other public sector institutions and organizations in the UK

The Objectives

Each organization's IT strategy must include robust application security implementation and compliance with various industry and government standards.

Enterprises need to ensure compliance with these standards in order to work effectively with various stakeholders and their systems. At the same time, they also need to shield themselves against security threats since even a slight security breach can damage the organization's reputation and have legal as well as financial implications.

The client's primary market comprises highly reputed public sector organizations in the United Kingdom. The client wished to offer fool-proof, certified and secure web applications to all their customers. Apart from data and application security, implementation of accessibility standards as well as inter government data interchange standards compliance were also crucial for customers.



Case Study




Web Application Security and Accessibility Standards Compliance

To meet the client objectives, world-class Application Security and Standards Compliance services were provided. This helped the client to retain and expand their customer base, boost confidence levels and have an extra edge in the targeted market.

The Solution

Application & Data Security:

The following security issues for web security compliance were identified. Each issue was categorized by vulnerability and level of threat. Stringent security audit by a highly reputed third party security expert was executed for each of these issues, and final certification for compliance was issued to the product thus ensuring complete web security for users as well as the organizations' data.

Symbol	Explanation
	A high risk issue was found which represents a critical threat that should be immediately resolved
	A moderate risk issue was found that should be promptly investigated
	A low risk issue was found that should be reviewed to ensure the network is inline with good security practice



Case Study

Web Application Security and Accessibility Standards Compliance



High Risk Issues

Sr. No	Vulnerability	Description and summary recommendation
1	Handled Cross-site Scripting	Cross-Site Scripting occurs when dynamically generated web pages display user input such as login information that is not properly validated, allowing an attacker to embed malicious scripts into the generated page and further execute the script on the machine of any user who views the site. Our system restricts this type of attacks.
2	Handled Cross-site Request Forgery	HTML tags are validated in the input fields to prevent XSS attacks.

3	Input Validations	Prevention mechanism against <ul style="list-style-type: none">• SQL injections• Operating system commands XSS attacks
4	Handled Cross-site Request Forgery	Prevention mechanism against MS SQL server specific SQL commands (with specific system table names and stored procedures)
5	Client and Server side Session Management	Prevent reuse of session IDs



Case Study

Web Application Security and Accessibility Standards Compliance



Moderate Risk Issues

Sr. No	Vulnerability	Description and summary recommendation
1	Authenticated Admin Section	This policy states that any area of the website or web application that contains sensitive information or provides access to privileged functionality requires authentication before allowing access.
2	Login sent over encrypted connections	All areas of a web application that could possibly contain sensitive information or provide access to privileged functionality should utilize SSL to prevent login information from being stolen.

3	Secure directories	Common Web Site Structure Directories Download/Upload Directories General Business Directories Web Application Common Directories.
4	Forgot password mechanism	System uses a e-mail based verification system to reset the password and create new password.
5	Stringent Password Policy	System has a difficult-to-crack password policy that uses a complex combination of Numerical, Capital letters and Special characters.



Case Study

Web Application Security and Accessibility Standards Compliance



Low Risk Issues

Sr. No	Vulnerability	Description and summary recommendation
1	Custom application error messages	Detailed error reporting should never be provided on a production web application. Error messages tend to leak useful information about the application and can possibly make way for attacks.
2	Privacy policy	Provide a clearly published privacy policy with description of intended purpose, use of data, methods for limiting use and disclosure of the information, list of third parties to whom the information may be disclosed and contact information for inquires and/or complaints, if any.

Accessibility and Government Data Interchange compliances:

Following accessibility and data interchange standards were implemented.

- W3C
- Bobby AA
- e-GMS
- e-GIF
- Cross Browser Compatibility with Internet explorer, Mozilla, Safari, Netscape, Opera on Windows and Mac OS



Case Study

Web Application Security and Accessibility Standards Compliance

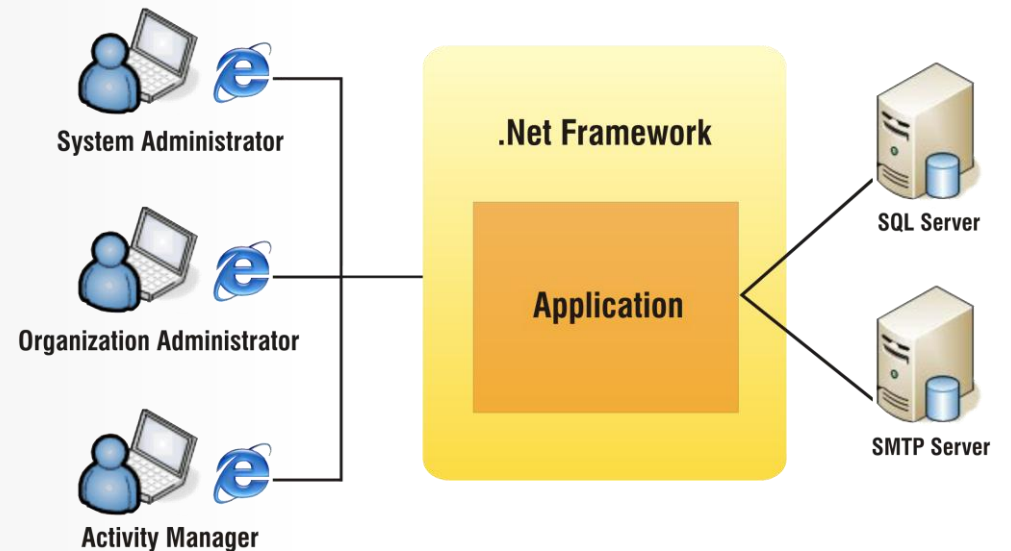
The Technology

The Application architecture is based on popular Microsoft Platforms, with a IIS Web Server running on Windows 200x Platforms, and MS-SQL Server as Backend with ASP / .Net / HTML front-end.

Platform:

- Operating System: Windows 2000 or higher
- Web Server: Internet Information Server 5.0 or higher
- Database Server: MS SQL Server 2000
- Other Services: SMTP service
- Framework: .Net framework 2.x

Technical Architecture:





Case Study

Web Application Security and Accessibility Standards Compliance

Elegant MicroWeb Role

- Research, Identification and Interpretation of best application security practices and numerous accessibility and government recommended standards
- Mapping these standards to technology platforms and finding implementation workarounds
- Identification, resolution and implementation of all recommendations in the standards
- Testing the system from functional as well as security perspectives
- Coordinating with a third party, security verification agency
- Handing over the system

Conclusion

The client wanted to have all standards to be implemented fully since most of their customers belonged to the public sector and following government directives was mandatory. Elegant MicroWeb completed the project successfully within the prescribed budget and coordinated with third party security audit agencies to get through the complex certification process.

Elegant Microweb provided the client with a third party certified; secure application conforming to all mandatory accessibility and government data interchange compliances. This implementation proved to be a winning formula for the client, and resulted in more confidence and greater acceptance levels of their services in the markets that they served.



Case Study

Web Application Security and Accessibility Standards Compliance

Contact Us

Elegant MicroWeb Technologies Pvt. Ltd.

A-305, Shapath - IV, Opp. Karnavati Club,
SG Highway, Ahmedabad-380051 India
Email: contact@ElegantMicroWeb.com
URL: www.ElegantMicroWeb.com

EMR5127C - CaseStudy – Web Application Security and Accessibility Standards Compliance - Version 1.2 - Published 2009
Copyright © Elegant MicroWeb Technologies Pvt. Ltd (EMTPL), all rights reserved

This document contains information that is proprietary and confidential to EMTPL, which shall not be disclosed, transmitted, or duplicated, used in whole or in part for any purpose other than its intended purpose. Any use or disclosure in whole or in part of this information without express written permission of EMTPL is prohibited.

Any other company and product names mentioned are used for identification purpose only, and may be trademarks of their respective owners and duly acknowledged