

Introduction

“Today over 80% of attacks against a company’s network come at the ‘Application Layer’ not the Network or System layer.”

Immunity against security threats is becoming one of the leading challenges for **Enterprise community**. The race to “go online” and develop competitive services are enabling enterprise communities to launch web applications rapidly with less attention to security risk’s making the sites vulnerable.

Interestingly many corporate sites are vulnerable to hackers in touch of a button

Need

Web applications perform multiple functions across the web. They include information transactions pertaining to health/medical records, banking information, credit card information and customer feedback etc.

It is very important to consider web application security because

- **The firewall does not help. By definition, http traffic must be allowed to go through the firewall. Otherwise no web application is possible.**
- **SSL does not help either.**
- **People don’t usually think about securing web applications**
- **Usually web sites are protected by well configured firewalls and attacking your web application might be one of the only ways for a hacker to get in.**

Risks Involved:

Web applications belonging to industry verticals like Banking & finance, healthcare, retail, Government etc are being attacked daily by wide variety of hackers. The end results of a security breach are usually devastating: such as

- **Decreased top & bottom line revenues**
- **Decreased credibility in the market**
- **Legal liability**
- **Sudden plunge in customer trust.**
- **Expenditure on Recovery and Fixes.**

Our Solution

Taking Enterprise to the Next level of Security

Enterprise must be able to detect the loopholes in their web applications. To enable this process software and security professionals can evaluate the severity of the loopholes and can patch them as quickly as possible.

A typical methodology might be to evaluate the portfolio of applications on web connected devices and assess each layer of application logic for potential vulnerabilities by

- **Performing technical due diligence on a given WEB Application.**
- **Finding new ways to break into the application**
- **Identifying potential holes in the application that might endanger organizations**

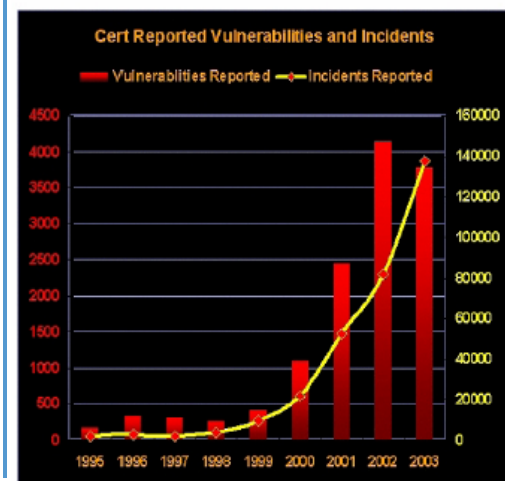
Based on the above process and open web application security project (OWASP) we probe in to both known and unknown vulnerabilities.

Benefits

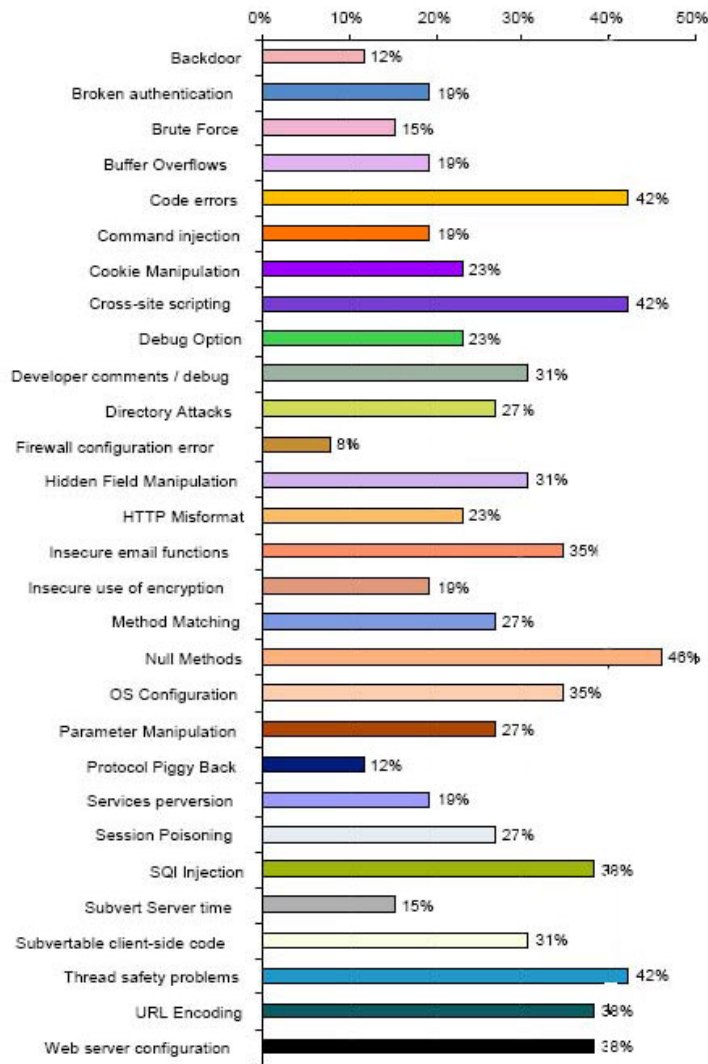
- **Delivers timely and valuable application vulnerability information to assist in developing proactive protection measures.**
- **Provides advice and actionable data needed to quickly address security holes provided by experts.**
- **Protects business and information assets against hacking and loss of valuable data.**
- **Assists in increase of customer confidence and trust on the application.**
- **Prevents loss of customer’s confidential information.**
- **Overcoming legal hassles due to failure of the application security.**
- **Reduces the cost of recovery and fixes due to loss of information.**
- **Increase in credibility in the market.**

Deliverables:

Once testing process is completed, Reports are generated and delivered to the Enterprise under test .These reports are configured to make the user comprehend the impact of the test. This is articulated to the fact that the report is delivered with proper and clear communication.



Different Types of Attacks on Web Applications



For Further Details About this service Contact us at www.coesecurity.com

Email: sales@coesecurity.com