PerfectForms™ – Application Security

© 2011 PerfectForms

PerfectForms™ Application Security

The systems architecture of PerfectForms™ has been designed with optimal security built-in from the ground up. All communications channels have been encrypted using SSL (Secure Sockets Layer), effectively preventing replay attacks. All user input is white list validated, which prevents SQL injection even in cases of escaped alternate encodings like Unicode. During communication between client and server, our application uses a HTTPS (HTML Transfer Protocol over Secure Socket Layer) session with 128-bit encryption.

Adding more security to PerfectForms™ SSL is the use of custom keys. All user sessions have a custom key for each request and PerfectForms™ sends a unique response key for each request. Each generated key is used only once in order to guard against automated load attacks.

Because systems are only as secure as their weakest link, real product security is achieved by implementing processes around product development and deployment, and a culture of security is important to maintaining security over time. At PerfectForms™, we understand that security is an ongoing process and we have taken steps to ensure that it is a core competency of our company. We have periodic developer training on security best practices.

We adhere to rigorous certification processes to maintain this standard. All code undergoes a peer review process, which can reveal simple and complex security assumptions. Our entire code-base undergoes continuous testing and daily automated testing using multiple simulated user environments and network configurations. This approach catches potential timing, processor speed, memory and network related vulnerabilities. In addition, our code undergoes third-party static analysis nightly which can reveal a host of potential security vulnerabilities including buffer overflows, user input validation or memory management issues. Our subsystem and deployment architectures undergo periodic review by an internal panel of experts. Finally, we employ a lightweight, rapid development process that allows us to quickly detect, correct and deploy fixes for any software vulnerabilities.

The PerfectForms™ Web servers are protected via firewall. This prevents compromise through management channels, as only ports 80, 443 and 1935 are open for TCP communication. The Web servers are updated whenever a patch is available and a roll-back mechanism is in place to make sure any bad patches can be quickly reverted. The Web servers are also behind a load balancer, meaning servers are rotated in and out of service as needed, ensuring continuous service even during maintenance. In addition, load balancing allows any server with unusual behavior to be isolated rapidly and removed from service.

Backend servers are further isolated from the Internet and will only respond to requests from known, authenticated, internal Web servers. This includes mail servers, SQL servers and the Flash media servers. These servers are not directly accessible and are also protected by firewall and load balancing.

Any Web application which results in the generation of e-mail will be attacked by spammers looking for an open mail relay. PerfectForms™ has been designed to prevent compromise of the mail server. The mail server is protected by a firewall that blocks all incoming requests to the mail server. The firewall

© 2011 PerfectForms

only allows outbound mail and the mail server only accepts authenticated mail requests from firewall protected, internal Web servers. These mail requests must have the right credentials and type of data to be accepted. Mass mail requests – both e-mails with too many destinations and e-mails repeated with only the "To:" address changed – can be blocked and will not propagate.

Finally, the database is further isolated from direct external visibility. It is only accessible via secure private channel within the network and known, specified systems (Web servers). Packets from all other hosts are dropped by the firewall before they even get to the database. This helps prevent side channel attacks because the databases are only accessible to the SQL server via direct, known channels. The client data on the forms database is in a protected, masked format that cannot be read by the human eye.

PerfectForms™ utilizes industry best practices to help ensure the security of its client is not compromised. PerfectForms™ has been designed to eliminate many threats and limit exposure to other threats. While no useful Web product can ever be assumed "100% secure", PerfectForms™ strikes a strong balance, offering an easy-to-use product that protects its users from detectable vulnerabilities.

© 2011 PerfectForms