WebDNA
Software Corporation
16192 Coastal Highway • Lewes, DE 19958
support@webdna.us • http://webdna.us

WebDNA Security

The **WebDNA** Sandbox is a key security feature for multi-domain hosting solutions

WebDNA allows the hosting provider to lock down individual websites into their own Sandboxes, preventing any of that website's code from accessing files or folders -- or executing external code -- that is outside the realm of that website.

Security in data, code, and communications

WebDNA has long supported mechanisms for ensuring the security of data and communications. Built-in encryption and decryption tags allow for storing sensitive data in encrypted form. Secure Socket Layer (SSL) support in the TCP connect context provides secure communications when sensitive data is being transmitted to and from the website. For hosting providers, the secure access of files, assets, and scripts from WebDNA pages is enhanced by the secure website Sandbox environment which completely isolates a given website into its own set of folders, databases, preferences, privileges, and execution.

WebDNA's Sandbox creates a localized, restricted environment

The Sandbox feature of WebDNA lets a WebDNA administrator create a restricted virtual environment for each WebDNA website hosted on a single server by designating a particular folder as a WebDNA Sandbox. This means that any WebDNA template running from within that folder hierarchy will not be able to view, manipulate, delete, or create any files outside of the immediate root Sandbox folder. This enables a WebDNA ISP to allow multiple WebDNA developers access to the same server knowing that each site is 'locked down' to its own root folder, where no WebDNA code can possibly access anything outside of its own Sandbox environment.

This localized security extends beyond access from the WebDNA templates used in the site. It also provides a secure mechanism for executing external scripts written in other languages or command line scripts. The WebDNA language does provide for the execution of external scripts, but in a Sandbox, these script contexts are restricted to a "reference only" mode. This means that in order to run any external command script, a system administrator must first add the script to a database of approved scripts for that Sandbox, giving it a reference ID. Then, the WebDNA template can only access that script via the unique reference ID, making it impossible for WebDNA code to execute unapproved, and potentially harmful, external scripts.

Security beyond access

The WebDNA Sandbox does more than sequester and secure folders, files and command scripts within a website. It also individualizes the overall behavior of the sandbox, because each sandbox has its own Sandbox Prefs, which includes nearly every preference you would find in the master WebCatalog Prefs file. Each Sandbox includes its own private Triggers process, Emailer process, Users database, and Admin section, which includes nearly all the templates you would find in the main WebDNA admin pages. In essence, a WebDNA sandbox defines a completely self-contained and secure virtual environment that cannot access, or be influenced by, any other website that co-exists on the same server.