Web Application Vulnerability Scanning

Web application servers provide active response to users accessing web pages, and web applications typically interact with a back-end database and other resources and are therefore vulnerable to attacks that are occurring through the http or https ports. Typical IP firewalls have opened these ports for your server to operate and may not be capable of monitoring or blocking these attacks because they are occurring inside the application server.

iBeta's Security Team can scan your web application server for the top 10 OWASP vulnerabilities as well as many others. Here are just some of the vulnerabilities:

OWASP TOP 10	Vulnerability
1	SQL Injection
2	Cross-Site Scripting (XSS)
2	DOM XSS
3	Weak HTTP Passwords
3	Authentication attacks
3	Weak FTP passwords
4	Checks for Backup Files or Directories
4	Cross Site Scripting in URI
4	Checks for Script Errors
4	Unrestricted File uploads Checks
4	Looks for Common Files
4	Discover Sensitive Files/Directories
4	Discovers Directories with Weak Permissions
4	Cross Site Scripting in Path and PHPSESSID Session Fixation.
5	Cross-Site Request Forgery (CSRF)
6*	Security Misconfiguration*
7*	Insecure Cryptographic Storage*
8	URL redirection
9	Finds Weak SSL Cyphers
10	Input Validation
Other Vulnerabilities	**We scan for more …**
	Code Execution
	HTTP Parameter Pollution
	File Inclusion
	Script Source Code Disclosure
	CRLF Injection
	Cross Frame Scripting (XFS)
	PHP Code Injection
	Path Disclosure (Unix and Windows)

	LDAP Injection
	Cookie Manipulation
	Arbitrary File creation
	Arbitrary File deletion
	Email Injection
	File Tampering
	Remote XSL inclusion
	Input Validation
	Buffer Overflows
	Sub-Domain Scanning
	HTTP Verb Tampering
	Directory Listings
	Source Code Disclosure
	Check for Common Files
	Check for Email Addresses
	Microsoft Office Possible Sensitive Information
	Local Path Disclosure
	Error Messages
	Trojan Shell Scripts
	Over 1200 Google Hacking Database Search Entries
	Finds All Open Ports on Servers
	Displays Network Banner of Port
	DNS Server Vulnerability: Open Zone Transfer
	DNS Server Vulnerability: Open Recursion
	DNS Server Vulnerability: Cache Poisoning
	Finds List of Writable FTP Directories
	FTP Anonymous Access Allowed
	Checks for Badly Configured Proxy Servers
	Checks for Weak SNMP Community Strings

* The OWASP-Top-10 #6 and #7 are not directly scanned for, but may be included in the items below. For example #6 – Security Misconfiguration is a broad topic that might include many of the others if the vulnerability is due to for example to a bad configuration file or the use of older vulnerable libraries. The #7 Insecure Cryptographic Storage is difficult to detect and exploit, but the impact is severe should the vulnerability be exploited. iBeta's team can consult with your developers on an hourly basis or review your web application code for vulnerabilities like this one.

References: http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf