Blocking Web Application Attacks

https://campus.barracuda.com/doc/112165976/

Web applications are constantly under threat from attackers who exploit vulnerabilities to inject malicious code or manipulate data. Barracuda WAF-as-a-Service safeguards your applications by identifying and blocking these attacks at the request level.

How it Works

The Barracuda WAF-as-a-Service analyzes incoming requests for patterns associated with various attack types. These patterns include techniques used in attacks like:

- **Cross-Site Scripting (XSS)**: Injecting malicious scripts into web pages to steal data or hijack user sessions.
- **Remote File Inclusion (RFI)**: Forcing the server to execute code from an external source.
- **SQL Injection**: Injecting malicious SQL code into requests to manipulate databases.
- **Directory Traversal**: Accessing unauthorized files or directories on the server.
- **OS Command Injection**: Executing arbitrary operating system commands on the server.

Block or Log Attacks

If a request matches an attack pattern, the Barracuda WAF-as-a-Service takes action based on your configuration:

- **Block**: The malicious request is blocked entirely, preventing the attack from reaching your application.
- **Log**: The request is logged for further analysis, while still being blocked to prevent harm.

Predefined Attack Patterns

The Barracuda WAF-as-a-Service provides a comprehensive list of predefined patterns for various attack types. The following table lists the predefined patterns for attack types:

Attack Type	Description	Pattern Name(s)

Cross-Site Scripting - strict		• opening-html-tag • closing-html-tag • script-comments • arbitrary-tag-injection • script-string-concat
Cross-Site Scripting	Techniques to inject malicious scripts into web pages.	• onevent-references-misc-3 • onevent-references • onevent-references-misc-2 • onevent-references-misc-1 • url-references • script-tag • xss-style-attr • script-in-tag-attribute • evasion-via-data-uri-scheme • unsafe-tag • script-tag-utf-7 • onevent-references-misc-generic • evasion-via-html-named-char-ref
Remote File Inclusion - strict		• external-file-reference
Remote File Inclusion	Forcing the server to execute code from an external source.	• php-file-inclusion
SQL Injection - strict	Injecting malicious SQL code to manipulate databases.	• sql-union-command-strict • sql-comments-strict • sql-tautology-conditions-like-dbcmd-strict • sql-select-command-strict • sql-sleep-dos-attempt-strict • sql-tautology-conditions-string-strict • asp-search-manipulation
SQL Injection - medium		• sql-declare-simple • sql-quote-variant • sql-blind-injection • sql-tautology-conditions-json-bypass-string • sql-tautology-conditions-in-dbcmd • sql-tautology-conditions-simple • sql-quote • sql-command-injection • sql-union-command • oracle-command-injection • sql-tautology-conditions-between-dbcmd • sql-cast-simple • ms-sql-procedures • sql-select-command • sql-comments • sql-tautology-conditions-like-dbcmd • sql-tautology-conditions-simple-string • sql-exec-simple • sql-tautology-conditions-extract

Directory Traversal - strict	Accessing unauthorized files or directories on the server.	• tilde-strict • dot-dot-slash-strict
Directory Traversal - medium		• dot-dot-slash • tilde
OS Command Injection - strict	Executing arbitrary operating system commands on the server.	• python-commands • log4j-rce-colon-vuln-strict • misc-commands • log4j-rce-substitution-vuln-strict • misc-commands-injections-end • arbitrary-cmd-injection-substrings • unix-shell-commands • arbitrary-unix-shell-commands • misc-commands-injections • c-language-functions • arbitrary-string-concatenation • php-injection • arbitrary-cmd-injection-dollar-ifs • misc-commands-start
OS Command Injection		• c-language-function-substrings • windows-commands • SSI-injection-command • bash-shell-shock-injection-vulnerability • misc-command-substrings • log4j-rce-vulnerability • windows-command-substrings • unix-shell-command-substrings • perl-language-functions
LDAP Injection - medium	Manipulating directory services like LDAP.	• ldap-injection-command • ldap-injection-command-substrings
Python PHP Attacks - medium	Exploiting vulnerabilities in these languages.	• python-cfm-command-substrings • php-commands • php-command-substrings
HTTP Specific Attacks - medium	Attacks targeting specific functionalities within HTTP.	• owa-ssrf-powershell-vulnerability • aws-server-metadata-check-variant • aws-server-metadata-url-check • web-client-commands • aws-server-metadata-check • HTTP-response-splitting-attempt • aws-server-metadata-check-2
Apache Struts Attacks - medium	Apache Struts attack refers to exploiting vulnerabilities in web applications built with the Apache Struts framework.	• apache-struts-vulnerability-http • apache-struts-vulnerability-java
Apache Struts Attacks - strict		• apache-struts-method-vulnerability • apache-struts-redirect-vulnerability • apache-struts-java-lang-vulnerability

By identifying and blocking these attack patterns, Barracuda WAF-as-a-Service helps keep your web applications secure and your data protected.