

# [TOOL] IISShield – Application Layer Firewall

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0126.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 07/29/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 29 Jul 2003 23:13:02 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Get Thawte's New Step-by-Step SSL Guide for Apache.

<http://ad.doubleclick.net/clk;5903117;8265118;i>

-----

## IISShield – Application Layer Firewall

---

### DETAILS

IISShield is an IIS ISAPI Filter preventing any known and unknown attacks from disrupting IIS. The preventive approach of IISShield is an added value preventing IIS from even trying to interpret requests trying to break-in.

With a detailed logging engine, IISShield helps IIS administrators to know in advance and protect IIS from known or unknown HTTP attacks that flow over the Internet.

The configuration is quite detailed giving the ability to precisely decide over what is accepted and what is not regarding the HTTP Layer.

RFC Compliance is just one of the core features of IISShield offering an assurance of quality of service to the IIS Administrator.

Technical comparison with another well-known tool with similar capabilities is also provided outlining the powerful capabilities of IISShield.

Tool comparison:

Microsoft URLScan

Verb Allowed List: KodeIT IISShield – Yes, Microsoft URLScan – Yes

Verb Denial List: KodeIT IISShield – Yes, Microsoft URLScan – Yes

Securiteam: [TOOL] IISShield – Application Layer Firewall

Url Extension Allowed List: KodeIT IISShield – Yes, Microsoft URLScan – Yes  
 Url Extension Denial List: KodeIT IISShield – Yes, Microsoft URLScan – Yes

Dot In Path Detection: KodeIT IISShield – Yes, Microsoft URLScan – Yes  
 Url Schema Validation: KodeIT IISShield – Yes, Microsoft URLScan – No  
 Host Header Validation: KodeIT IISShield – Yes, Microsoft URLScan – No  
 Http Version Validation: KodeIT IISShield – Yes, Microsoft URLScan – No  
 RFC Compliant: KodeIT IISShield – Yes, Microsoft URLScan – No  
 Url & Query Size Limit: KodeIT IISShield – Yes, Microsoft URLScan – Yes  
 Header Name Size Limit: KodeIT IISShield – Yes, Microsoft URLScan – No  
 Header Value Size Limit (General): KodeIT IISShield – Yes, Microsoft URLScan – No  
 Header Value Size Limit (by Header Name): KodeIT IISShield – Yes, Microsoft URLScan – Yes  
 Payload Size Limit: KodeIT IISShield – Yes, Microsoft URLScan – Yes  
 Url Sequence Constraint: KodeIT IISShield – Yes, Microsoft URLScan – Yes  
 Query Sequence Constraint: KodeIT IISShield – Yes, Microsoft URLScan – No  
 Url Encoding Abuse Detection: KodeIT IISShield – Yes, Microsoft URLScan – Yes  
 Query Encoding Abuse Detection: KodeIT IISShield – Yes, Microsoft URLScan – No  
 Header Name & Header Value Encoding Abuse Detection: KodeIT IISShield – Yes, Microsoft URLScan – No  
 Header Name Denial: KodeIT IISShield – Yes, Microsoft URLScan – Yes  
 Url High Bit Detection: KodeIT IISShield – Yes, Microsoft URLScan – Yes  
 Query High Bit Detection: KodeIT IISShield – Yes, Microsoft URLScan – No  
 Header Name & Header Value (High Bit Detection On By Default): KodeIT IISShield – RFC Compliant, Microsoft URLScan – No  
 Payload High Bit Detection: KodeIT IISShield – Yes, Microsoft URLScan – Yes  
 Content-Length Value Limit: KodeIT IISShield – Yes, Microsoft URLScan – Yes  
 Filter Priority Setting: KodeIT IISShield – Yes, Microsoft URLScan – Yes  
 Simulation Mode: KodeIT IISShield – Yes, Microsoft URLScan – Yes

ADDITIONAL INFORMATION

The information has been provided by <<mailto:thalm@netcabo.pt>> thalm.

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
 To unsubscribe from the list, send mail with an empty subject line and body to:  
[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)  
 In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

## Securiteam: [TOOL] IISShield – Application Layer Firewall

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.