



Welcome to webApp.**secure**[™] LiveCD

Find out how easy it is to secure your web assets.

webScurity Inc.
9298 Central Ave NE
Suite 402
Minneapolis MN 55434
USA
866.SECURITY Toll Free (US)
763.786.2009 Twin Cities Metro/International
763.786.3680 Fax
www.webscurity.com

©2010 webScurity Inc. All rights reserved.

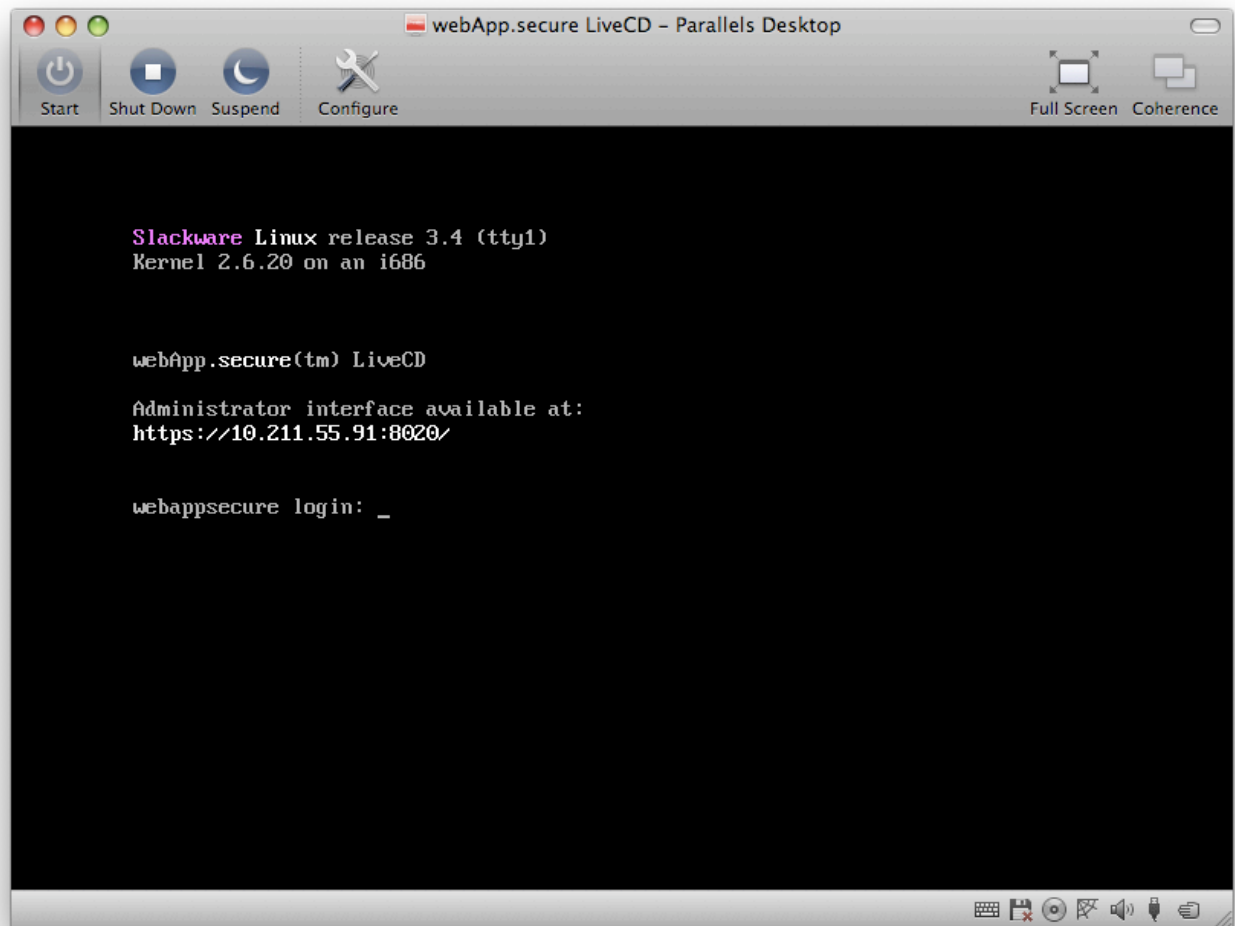
webApp.**secure**, **Intended Use Guidelines**, and
web/**insite** are trademarks of webScurity Inc.

This product includes the Spidermonkey JavaScript
Interpreter, which is code covered by the Netscape Public
License, v1.1. The original code is available from
www.mozilla.org.

First Things First	4
Admin Interface Access	5
Quick UI Tour	6
Server Setup	7
User-defined Policies	8
User-defined Policies (non-HTML content)	9
Real-time Attack Notification	10
SMTP	10
HTTP	11
Trusted Hosts	12
Advanced Settings	13
Performance Tuning	13
Miscellaneous	14
Error URLs	15
HTTP Method(s)	16
Secure Sockets Layer	17
Application Manipulation Protection	19
Form Validation	19
Cookie Validation	20
Attack Insight	21
Alert Navigator	22
Alert Detail	23
Adding a Policy	24
OpenSSL	25
Mozilla Spidermonkey	26

First Things First

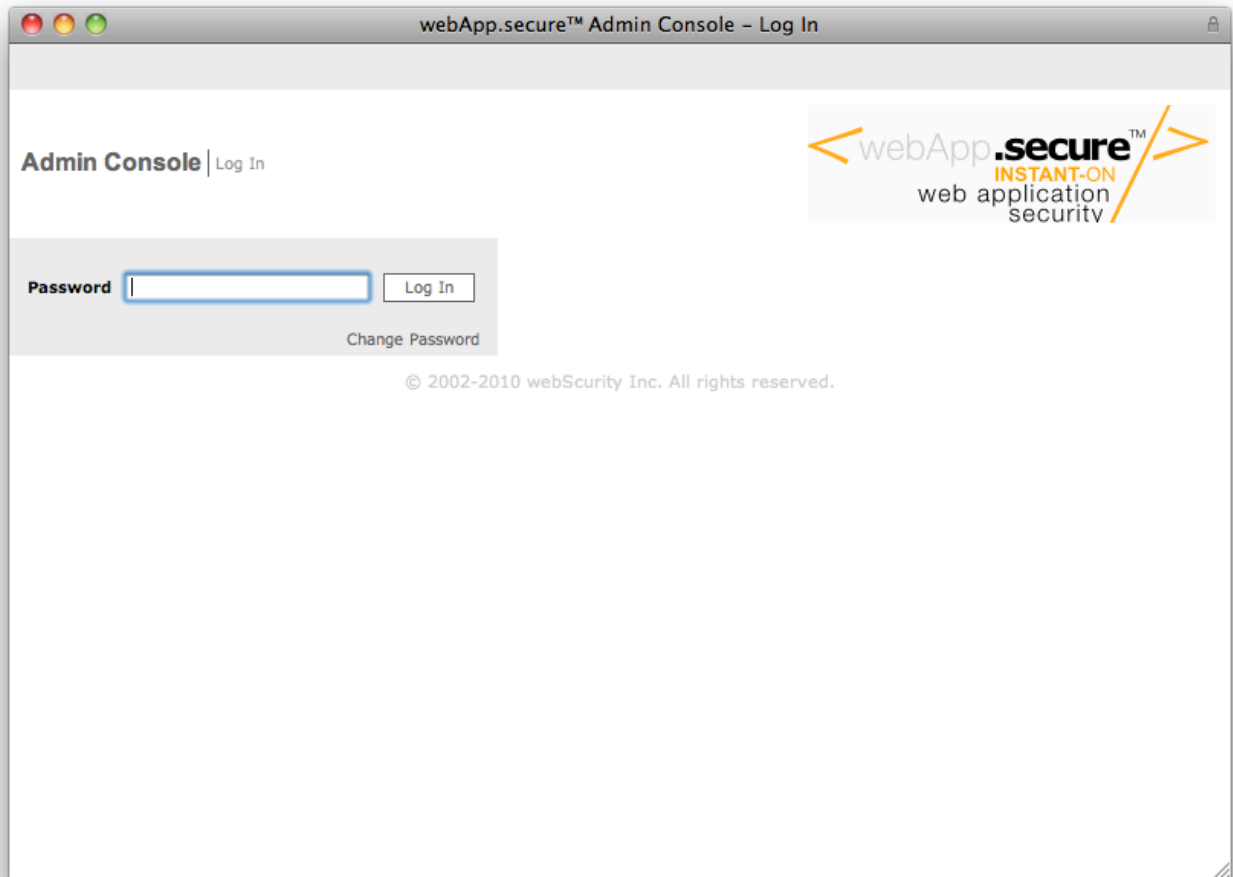
Boot the ISO image after burning to a CD or as a virtual machine using your favorite VM software. No hard disk drive is required (or used) in either physical or virtual configurations.



Use the URL displayed at boot (<https://10.211.55.91:8020/> in the above example) to access the administration interface from any browser.

Admin Interface Access

A URL to access the admin interface is displayed at boot time. Please note “https” protocol on port 8020.



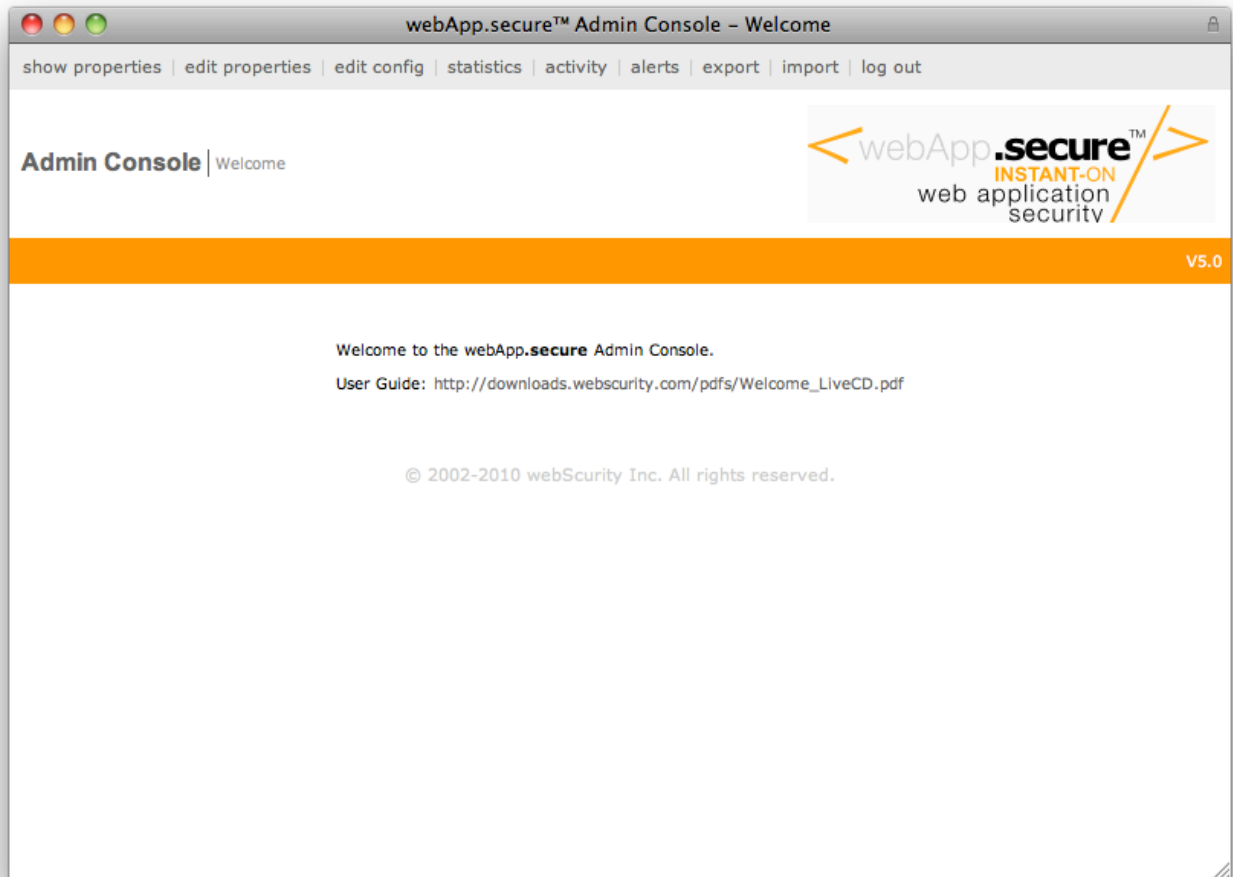
Default password is “admin” (lower case, no quotes).

Log in using the default password “admin” (lower case, no quotes).

To change the password, click the “Change Password” link before logging in. Not available in LiveCD version.

Quick UI Tour

After log in, the welcome landing page shown below is displayed.



Welcome page displayed after login with main menu options across the top.

show properties

Display currently defined property settings.

edit properties

Modify current property settings.

edit config

Modify startup settings.

statistics

Display current run-time statistics.

activity

Display the contents of the plain text activity log.

alerts

Display the contents of the XML alert log.

export

Export the current property settings.

import

Import previously exported property settings.

Server Setup

The following properties specify the reverse-proxy, TCP/IP communication settings of the Web server and webApp.secure.

The screenshot shows the 'webApp.secure™ Admin Console - Edit Properties' window. The top navigation bar includes links: show properties | edit properties | edit config | statistics | activity | alerts | export | import | log out. The main header displays 'Admin Console | Edit Properties' and the webApp.secure logo with the tagline 'INSTANT-ON web application security'. Below the header is a tabbed interface with tabs: Server Info, User-Defined Policies, Alerts, Logging, Advanced, SSL, Input Validation, and Remote Admin. The 'Server Info' tab is selected. It contains the following fields and controls:

- Web server name*: A text input field.
- Web server port*: A text input field containing '80'.
- Listen IP*: A text input field.
- Listen port*: A text input field containing '80'.
- Bind IP: A text input field.
- Internet host name(s): A text input field with 'Add' and 'Remove' buttons to its right.

At the bottom of the form area, there is a note: '* Requires restart to take effect.' and two buttons: 'Cancel' and 'Submit'. The footer of the window states: '© 2002-2010 webScurity Inc. All rights reserved.'

Web Server Name

Identifies the internal reference of the Web server webApp.secure is protecting (i.e. 192.168.0.2), typically an IP address or internal server name.

Web Server Port

Identifies the TCP port number of the Web server webApp.secure is protecting (i.e. 80).

Listen IP

Not available in LiveCD version.

Listen Port

The TCP port number webApp.secure will use for unencrypted traffic (i.e. 80).

Bind IP

Not available in LiveCD version.

Internet Host Name(s)

One or more external host names (domain name) of the website(s) webApp.secure is protecting (i.e. www.mydomain.com). Add an entry for each name-based virtual website hosted on the Web server.

User-defined Policies

Entry Points are one or more URI's that are accessible without restriction from the outside – i.e. a “starting point” for the website/application. web/insite™ begins automatically identifying the Intended Use Guidelines™ from this (these) point(s).

webApp.secure™ Admin Console – Edit Properties

show properties | edit properties | edit config | statistics | activity | alerts | export | import | log out

Admin Console | Edit Properties

webApp.secure™
INSTANT-ON
web application security

Server Info | User-Defined Policies | Alerts | Logging | Advanced | SSL | Input Validation | Remote Admin

Entry Points | Unprotected Dirs | Form-related | Filters

Entry point

/

☐ https-only ☐ ignore-case ☐ regex

Add Remove

Cancel Submit

© 2002-2010 webScurity Inc. All rights reserved.

The root URI (/) is set up by default and it is common to also specify the root document name (i.e. /index.html) specifically.

Use wildcard characters “*” (one or more alpha-numeric characters), “?” (single alpha-numeric character), and “#” (single numeric character) to specify entry points that may have a variable component.

Check the “https-only” checkbox if the entry point should be accessed through an encrypted connection only. Check the “ignore-case” checkbox if the entry point validation should be case-insensitive.

Entry Point	Would Allow	Would Deny
/default.asp?var=*	/default.asp?var=123 /default.asp?var=123&var2=456	/default.asp /default.asp?x=123 /default.aspXvar=123
/default.asp?var=##	/default.asp?var=12	/default.asp?var=1 /default.asp?var=123 /default.asp?var=ab
/default.asp?v1=*&v2=##&v3=???	/default.asp?v1=1a&v2=12&v3=abc /default.asp?v1=a&v2=34&v3=123	/default.asp?v1=1a&v2=1a&v3=1a

User-defined Policies (non-HTML content)

Unprotected Directories (paths) are one or more URI's that are accessible without restriction from the outside. These should be paths to images or other non-HTML content.

Unprotected Directories can be useful to specify access to resources that webApp.**secure** is not able to automatically recognize as part of the website Intended Use Guidelines.

Check the “https-only” checkbox if the unprotected directory should be accessed through an encrypted connection only. Check the “ignore-case” checkbox if the unprotected directory validation should be case-insensitive.

Unprotected Dir	Would Allow	Would Deny
/images/*.gif	/images/123.gif /images/moreimages/abc.gif	/images/123.GIF /images/123.jpg
/*.gif	/images/123.gif /images/moreimages/abc.gif	/images/123.GIF /images/123.jpg
/include/*.js	/include/func.js	/include/funcs.javascript
/pdfs/*.pdf	/pdfs/123.pdf /pdfs/morepdfs/abc.pdf	/pdfs/123.PDF /pdfs/abc.pd

Real-time Attack Notification

Choose from 2 available real-time alert mechanisms that best suites your environment. Email and HTTP alerts let you know what's going on.

SMTP

Configure to send an SMTP mail message to one or more recipients when activity is blocked. Details of the alert will be contained in the body of the email in well-formed XML format (see [Attack Insight](#) section for details).

The screenshot shows the 'webApp.secure™ Admin Console - Edit Properties' window. The top navigation bar includes links: show properties | edit properties | edit config | statistics | activity | alerts | export | import | log out. The main header area displays 'Admin Console | Edit Properties' and the 'webApp.secure™ INSTANT-ON web application security' logo. Below the header is a tabbed interface with tabs: Server Info, User-Defined Policies, Alerts, Logging, Advanced, SSL, Input Validation, and Remote Admin. The 'Alerts' tab is active, and within it, the 'SMTP' sub-tab is selected. The configuration area for SMTP includes: 'Enable' (radio button) and 'Disable' (radio button, selected); 'Server name' (text input); 'Server port' (text input with value '25'); 'Subject' (text input with value 'webApp.secure alert message'); 'From' (text input with value 'webApp'); 'Recipient(s)' (text input with an 'Add' button); 'User ID' (text input); and 'Password' (text input). There is a 'Remove' button below the recipient list. At the bottom are 'Cancel' and 'Submit' buttons. The footer text reads: © 2002-2010 webScurity Inc. All rights reserved.

Server Name

The email server name or IP address (i.e. "mail.mydomain.com").

Server Port

The email server TCP port number (i.e. "25").

Subject

Text to appear in the subject line to help identify the origin of the alert email (i.e. "Alert from Web server 1").

From

A "from" email address. (i.e. "server1@mydomain.com").

Recipient(s)

One or many recipient email addresses (i.e. "admin@mydomain.com").

HTTP

Configure to send an HTTP POST request to a user-supplied URL when activity is blocked. Details of the alert will be contained in the payload of the request in well-formed XML format (see [Attack Insight](#) section for details).

webApp.secure™ Admin Console – Edit Properties

show properties | edit properties | edit config | statistics | activity | alerts | export | import | log out

Admin Console | Edit Properties

webApp.secure™
INSTANT-ON
web application security

Server Info | User-Defined Policies | Alerts | Logging | Advanced | SSL | Input Validation | Remote Admin

SMTP | HTTP | Network | Trusted Hosts

☐ Enable ☒ Disable

Server name

Server port

From

Action

Cancel Submit

© 2002-2010 webScurity Inc. All rights reserved.

Server Name

The HTTP server name or IP address (i.e. “192.168.0.100”).

Server Port

The HTTP server TCP port number (i.e. “80”).

Action

The URI of the receiving script (i.e. “/cgi-bin/alert.cgi”).

From

An optional name to help the receiving CGI script (see Action above) identify the origin of the alert message.

Trusted Hosts

Optional list of origin IP addresses that represent “trusted hosts”. Malicious activity from these IP addresses will be blocked, but not reported or alerted. This is useful for scheduled penetration testing to avoid being alerted for every blocked request generated by the testing device every time it runs.

webApp.secure™ Admin Console – Edit Properties

show properties | edit properties | edit config | statistics | activity | alerts | export | import | log out

Admin Console | Edit Properties

webApp.secure™
INSTANT-ON
web application security

Server Info | User-Defined Policies | Alerts | Logging | Advanced | SSL | Input Validation | Remote Admin

SMTP | HTTP | Network | Trusted Hosts

☐ Enable ☒ Disable

Trusted Host IP(s)

© 2002-2010 webScurity Inc. All rights reserved.

Trusted Host IP(s)

One or more IP addresses identified as a “trusted source IP” (i.e. “192.168.0.100”).

Use a dash to specify a range of IP addresses (i.e. “192.168.0.100-150”).

Advanced Settings

The Advanced section allows you to tailor performance and other settings to your environment.

Performance Tuning

TCP/IP-related settings that can enhance performance and impose limitations on how client socket connections are serviced.

The screenshot shows the 'webApp.secure™ Admin Console - Edit Properties' window. The top navigation bar includes links: show properties | edit properties | edit config | statistics | activity | alerts | export | import | log out. The main header shows 'Admin Console | Edit Properties' and the 'webApp.secure™ INSTANT-ON web application security' logo. Below the header is a tabbed interface with tabs: Server Info, User-Defined Policies, Alerts, Logging, Advanced (selected), SSL, Input Validation, and Remote Admin. Under the 'Advanced' tab, there are sub-tabs: Performance Tuning (selected), Misc, Error URLs, and HTTP Methods. The 'Performance Tuning' sub-tab contains three input fields: 'Max connections**' with a value of 5000, 'Max listen queue*' with a value of 511, and 'Keep-alive timeout (seconds)' with a value of 15. Below these fields are two footnotes: '* Requires restart to take effect.' and '** Requires restart on non-Windows® platforms to take effect.' At the bottom of the form are 'Cancel' and 'Submit' buttons. The footer of the window states '© 2002-2010 webScurity Inc. All rights reserved.'

Max Connections

The maximum number of simultaneous client connections (sockets) that will be served. Once the threshold is reached, the operating system's listen queue will be used. 5000 is the default value.

Max Listen Queue

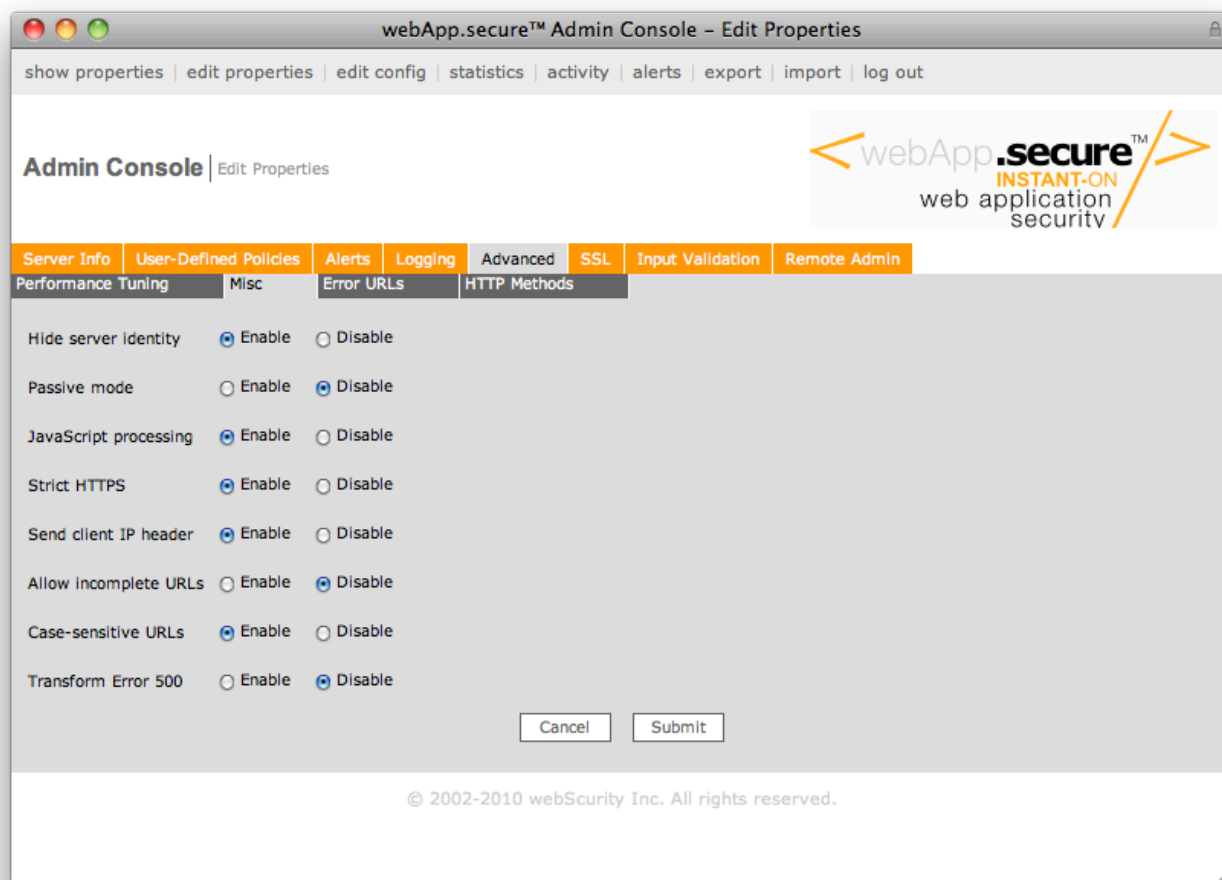
The maximum number of pending connections in the operating system's listen queue. 511 is the default value.

Keep Alive Timeout

The number of seconds to wait for subsequent requests before closing a connection. 15 seconds is the default value.

Miscellaneous

A variety of binary (enable/disable) options can be configured in the Misc section.



Hide Server Identity

Enable (default) to avoid disclosing the Web server's identity to prevent banner-grabbing.

Passive Mode

Disable (default) to identify, report, and block malicious activity. Enable to operate in "report-only" mode - all requests are forwarded on to the Web server (nothing is blocked).

JavaScript Processing

Enable (default) to interpret client-side JavaScript to extract Intended Use Guidelines™.

Strict HTTPS

Enable (default) to strictly enforce access to https resources through an encrypted connection.

Allow Incomplete URLs

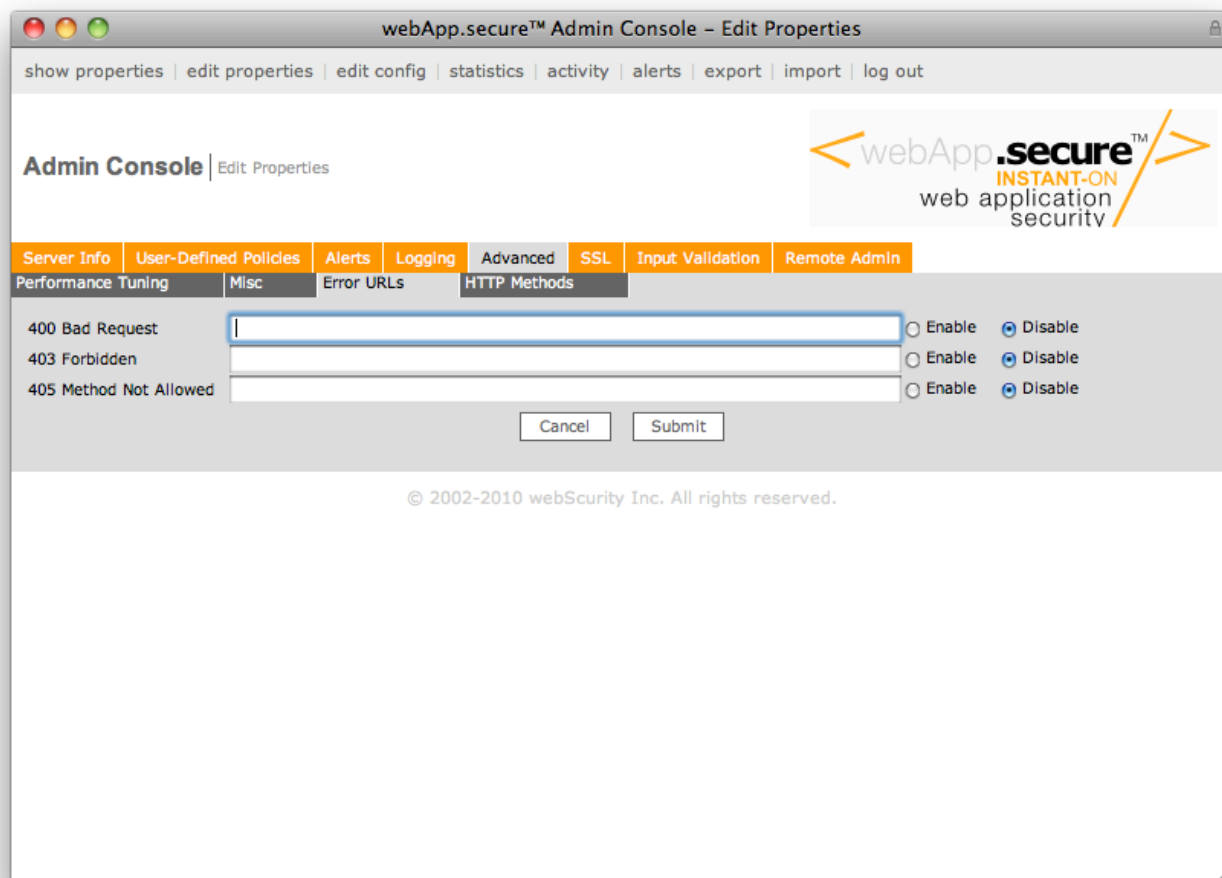
Enable to allow "incomplete" URLs where the Intended Use Guidelines might show "http://www.domain.com/test/", but the user enters "http://www.domain.com/test" (no trailing slash) in their browser's address bar. When enabled, both would be allowed. When disabled (default), the latter would not. Disabled is the most commonly used setting.

Case-sensitive URLs

Enable (default) to perform URL validation in a case-sensitive manner.

Error URLs

Rather than returning the standard HTTP error codes 400 Bad Request, 403 Forbidden, and 405 Method Not Allowed for blocked requests, an optional, fully-qualified URL can be configured to redirect the user. A 302 Found response code with the fully-qualified URL in the Location: response header, causing an automatic redirection.



webApp.secure™ Admin Console – Edit Properties

show properties | edit properties | edit config | statistics | activity | alerts | export | import | log out

Admin Console | Edit Properties

webApp.secure™
INSTANT-ON
web application security

Server Info | User-Defined Policies | Alerts | Logging | Advanced | SSL | Input Validation | Remote Admin

Performance Tuning | Misc | Error URLs | HTTP Methods

400 Bad Request	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
403 Forbidden	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
405 Method Not Allowed	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

© 2002-2010 webScurity Inc. All rights reserved.

400 Bad Request

Fully-qualified URL to redirect what would normally be HTTP error code 400 Bad Request.

403 Forbidden

Fully-qualified URL to redirect what would normally be HTTP error code 403 Forbidden.

405 Method Not Allowed

Fully-qualified URL to redirect what would normally be HTTP error code 405 Method Not Allowed.

HTTP Method(s)

One or many HTTP request methods that will be allowed. POST, HEAD, and GET are recommended and are the default values.

The screenshot shows the 'webApp.secure™ Admin Console - Edit Properties' window. The top navigation bar includes links: show properties | edit properties | edit config | statistics | activity | alerts | export | import | log out. The main header displays 'Admin Console | Edit Properties' and the 'webApp.secure™ INSTANT-ON web application security' logo. Below the header is a tabbed interface with tabs: Server Info, User-Defined Policies, Alerts, Logging, Advanced, SSL, Input Validation, and Remote Admin. Under the 'Advanced' tab, there are sub-tabs: Performance Tuning, Misc, Error URLs, and HTTP Methods. The 'HTTP Methods' sub-tab is active. It contains an input field with a cursor, an 'Add' button, and a list box containing 'GET', 'HEAD', and 'POST'. To the right of the list box is a 'Remove' button. At the bottom of the form area are 'Cancel' and 'Submit' buttons. The footer text reads: © 2002-2010 webScurity Inc. All rights reserved.

Type the name in the input box, click the “Add” button, followed by the “Submit” button to add a method to the list.
Highlight a name in the list, click the “Remove” button, followed by the “Submit” button to remove a method from the list.

Secure Sockets Layer

Use the SSL properties to enable encrypted traffic support. webApp.**secure** must decrypt https traffic before forwarding valid transactions on to the Web server, but re-encrypting may not be necessary for every implementation (“Encrypt to Web server” property).

The screenshot shows the 'webApp.secure™ Admin Console - Edit Properties' window. The top navigation bar includes links: show properties | edit properties | edit config | statistics | activity | alerts | export | import | log out. The main header displays 'Admin Console | Edit Properties' and the webApp.secure logo with the tagline 'INSTANT-ON web application security'. Below the header is a tabbed interface with tabs: Server Info, User-Defined Policies, Alerts, Logging, Advanced, SSL (selected), Input Validation, and Remote Admin. The SSL tab contains the following settings:

- ☐ Enable ☒ Disable
- Listen IP*: [text input field]
- Listen port*: [text input field with value 443]
- Web server port*: [text input field with value 443]
- Certificate File*: [Choose File button] no file selected
- Certificate Key File*: [Choose File button] no file selected
- CA Certificate File*: [Choose File button] no file selected
- Prompt for pass phrase*: [No] (dropdown menu)
- Encrypt to Web server: [Yes] (dropdown menu)
- Allow SSLv2*: [No] (dropdown menu)
- Allow weak ciphers*: [No] (dropdown menu)

* Requires restart to take effect.

Buttons: Cancel, Submit

© 2002-2010 webScurity Inc. All rights reserved.

Listen IP

Not available in LiveCD version.

Listen port

The TCP port webApp.**secure** should listen on for encrypted traffic (i.e. 443), normally the standard https port 443 will be used. Requires restart.

Web server port

The TCP port number of the Web server for encrypted (https) traffic. This value is not used unless Encrypt to web server is enabled (see above). Requires restart.

Certificate, Key, and CA Files

Upload server certificate files. The certificate and key files must be uploaded if SSL is enabled. Apache-compatible certificates are required. Please see <http://www.webscurity.com/reference.htm> for certificate conversion instructions and tips.

Prompt for pass phrase

Not available in LiveCD version.

Encrypt to Web server

Select Yes (default) to re-encrypt validated traffic forwarded on to the Web server. When set to Yes, the Web server port property must also be populated with an appropriate value (see above).

Allow SSLv2

Select Yes to allow SSLv2 client connections (not recommended). Default is No.

Application Manipulation Protection

Application manipulation attack protection settings can be tailored to your environment.

Form Validation

Use this section to control how/if HTML form elements will be validated.

webApp.secure™ Admin Console – Edit Properties

show properties | edit properties | edit config | statistics | activity | alerts | export | import | log out

Admin Console | Edit Properties

Server Info | User-Defined Policies | Alerts | Logging | Advanced | SSL | Input Validation | Remote Admin

Forms | Cookies

☒ Enable ☐ Disable

Special character filters

Field Type	Special Character Filter	Send alert	Block
TEXT	<>"';()	Yes	No
TEXTAREA	<>"';()	Yes	No
PASSWORD	<>"';()	Yes	No

Form cleanup ☒ Enable ☐ Disable

15 Days
0 Hours

Cancel Submit

© 2002-2010 webScurity Inc. All rights reserved.

Special Character Filters

Specify the dangerous characters that will be transparently filtered from user input for each HTML field type (*TEXT*, *TEXTAREA*, *PASSWORD*) to combat SQL/command injection and cross-site scripting attacks.

TEXT

Characters that should be stripped from *TEXT* type (<input type="text" ... />) form fields.

TEXTAREA

Characters that should be stripped from *TEXTAREA* type (<textarea ... />) form fields.

PASSWORD

Characters that should be stripped from *PASSWORD* type (<input type="password" ... />) form fields.

Form Cleanup

Enable to cleanup of HTML form Intended Use Guidelines™ older than Days and Hours (see below).

Days, Hours

Establishes the timeframe for cleanup of HTML form Intended Use Guidelines older than Days and Hours.

Cookie Validation

Use this section to control how/if HTTP name/value pair cookies will be validated.

The screenshot shows the 'webApp.secure™ Admin Console - Edit Properties' window. The top navigation bar includes links: show properties | edit properties | edit config | statistics | activity | alerts | export | import | log out. The main header shows 'Admin Console | Edit Properties' and the 'webApp.secure™ INSTANT-ON web application security' logo. The left sidebar has tabs: Server Info, User-Defined Policies, Alerts, Logging, Advanced, SSL, Input Validation, and Remote Admin. The 'Input Validation' tab is active, and the 'Cookies' sub-tab is selected. The 'Cookies' settings are as follows:
 - Enable: ☒ Enable, ☐ Disable
 - Strict: ☐ Enable, ☒ Disable
 - Transition period: ☒ Enable, ☐ Disable
 - Transition period values: 6 Days, 0 Hours
 - Cookie cleanup: ☒ Enable, ☐ Disable
 - Cookie cleanup values: 15 Days, 0 Hours
 At the bottom are 'Cancel' and 'Submit' buttons. The footer text reads: © 2002-2010 webScurity Inc. All rights reserved.

Strict

Enable if requests that contain an altered cookie should be blocked and not forwarded on to the Web server.

When disabled (default), requests that contain altered cookie values will be forwarded on to the Web server, but the cookie will be completely stripped.

Transition Period

Enable (default) to allow for a “transition period” of Days and Hours (see below) from the time cookie validation is enabled. This allows cookie attributes and values that cannot be validated to be allowed rather than rejected.

Days, Hours

Establishes the timeframe for the transition period measured in Days and Hours. (Default is 6 days.)

Cookie Cleanup

Enable (default) to cleanup of HTTP cookie Intended Use Guidelines™ older than Days and Hours (see below).

Days, Hours

Establishes the timeframe for cleanup of HTTP cookie Intended Use Guidelines older than Days and Hours. (Default is 15 days.)

Attack Insight

Malicious activity is logged to a well-formed XML file. The format of the alert message (in the alert log file, and delivered via email or HTTP) is:

<alert><date-time /></alert>

The date and time of the request (i.e. "Tue Feb 24 03:03:46 2008").

<alert><alert-msg /></alert>

webApp.secure™-generated message regarding the alert.

<alert><ip /></alert>

The origin IP address of the client that made the request (i.e. "192.168.0.2").

<alert><remote-name /></alert>

The origin host name of the client that made the request (i.e. "remotehost.isp.net").

<alert><request /></alert>

The HTTP request line (i.e. "GET /scripts/nsiislog.dll HTTP/1.0").

<alert><action /></alert>

The action taken by webApp.secure ("Denied" or "Would Deny" (if running in Passive Mode)).

<alert><request-URI /></alert>

The URI component of the HTTP request line (i.e. "/scripts/nsiislog.dll").

<alert><method /></alert>

The HTTP request method (i.e. "GET").

<alert><status-code /></alert>

The HTTP status code returned to the client (i.e. "403").

NOTE: A status code of 200 generally means the request was not blocked, but special characters were filtered, which would be indicated in <alert-msg /> (see above).

<alert><reason /></alert>

The webApp.secure attack category (i.e. "Forceful Browsing").

<alert><content-type /></alert>

The request content type.

<alert><host /></alert>

The value from the request "Host:" HTTP header.

Sample

```
<alerts>
  <alert>
    <date-time>Tue Feb 24 03:03:46 2008</date-time>
    <alert-msg>http://www.mysite.com/attackurl not allowed</alert-msg>
    <ip>67.123.123.123</ip>
    <remote-name>remotehost.isp.net</remote-name>
    <request>GET /attackurl HTTP/1.1</request>
    <request-URI>/attackurl</request-URI>
    <method>GET</method>
    <status-code>403</status-code>
    <reason>Forceful Browsing</reason>
    <content-type></content-type>
    <user-agent>Mozilla/5.0</user-agent>
    <host>www.mysite.com</host>
  </alert>
</alerts>
```

Alert Navigator

As described in the [Attack Insight](#) section, malicious activity is logged to a well-formed XML file. The alerts contained within can be viewed from the “alerts” main menu item.

webApp.secure™ Admin Console – Alerts

show properties

edit properties

edit config

statistics

activity

alerts

export

import

log out

Admin Console

Alerts

<

webApp.secure™

>

INSTANT-ON

web application security

/usr/local/wa/logs/alert.xml

V5.0

Date/Time	Message	Origin IP	Status Code
06-01-2010 02:09:40	filtered 1 special character(s) from field 'password' in form 'login'	10.211.55.2 ttylinux_host.domain.net	400
06-01-2010 02:10:13	hidden field 'acct' in form 'checkSearch' has been altered. Should be '123456' - now '423456'.	10.211.55.2 ttylinux_host.domain.net	400
06-01-2010 02:11:34	https://www.bankco.com/cgi-bin/bankco.cgi?action=detail&acct=423456 not allowed	10.211.55.2 ttylinux_host.domain.net	403
06-01-2010 02:12:13	value '323456' not valid for select option 'to' in form 'select_account'	10.211.55.2 ttylinux_host.domain.net	400
06-01-2010 02:12:41	https://www.bankco.com/cgi-bin/bankco.cgi?action=accounts&uid=3 not allowed	10.211.55.2 ttylinux_host.domain.net	403

1-5 of 5 alerts

export

© 2002-2010 webScurity Inc. All rights reserved.

Click the **alerts** main menu option to view contents of alerts log.

Date/Time

Date and time of the event. This is a clickable link that will display further details of the alert (see [Alert Detail](#) on the following page).

Message

Description of the event.

Origin IP

Origin IP address that submitted the request that triggered the event.

Status Code

The HTTP status code returned (or would have been returned if running in Passive Mode) in response to the blocked activity.

Export Button

Click the “export” button to export the alert.xml file to a local storage location.

Alert Detail

Detail of the alert can be displayed by clicking the Date/Time link on the desired row.

webApp.secure™ Admin Console – Alerts > Detail

Admin Console | Alerts > Detail

webApp.secure™
INSTANT-ON
web application security

/usr/local/wa/logs/alert.xml V5.0

Date/Time	Tue Jun 1 02:11:34 2010
Message	https://www.bankco.com/cgi-bin/bankco.cgi?action=detail&acct=423456 not allowed
From IP	10.211.55.2
From Name	ttylinux_host.domain.net
User Agent	Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
HTTP Request	GET /cgi-bin/bankco.cgi?action=detail&acct=423456 HTTP/1.1
Host	www.bankco.com
URI	/cgi-bin/bankco.cgi?action=detail&acct=423456
Reason	Parameter Tampering
Status Code	403

Add Policy

3 of 5 alerts

<<prev

close

next>>

© 2002-2010 webSecurity Inc. All rights reserved.

Display a menu

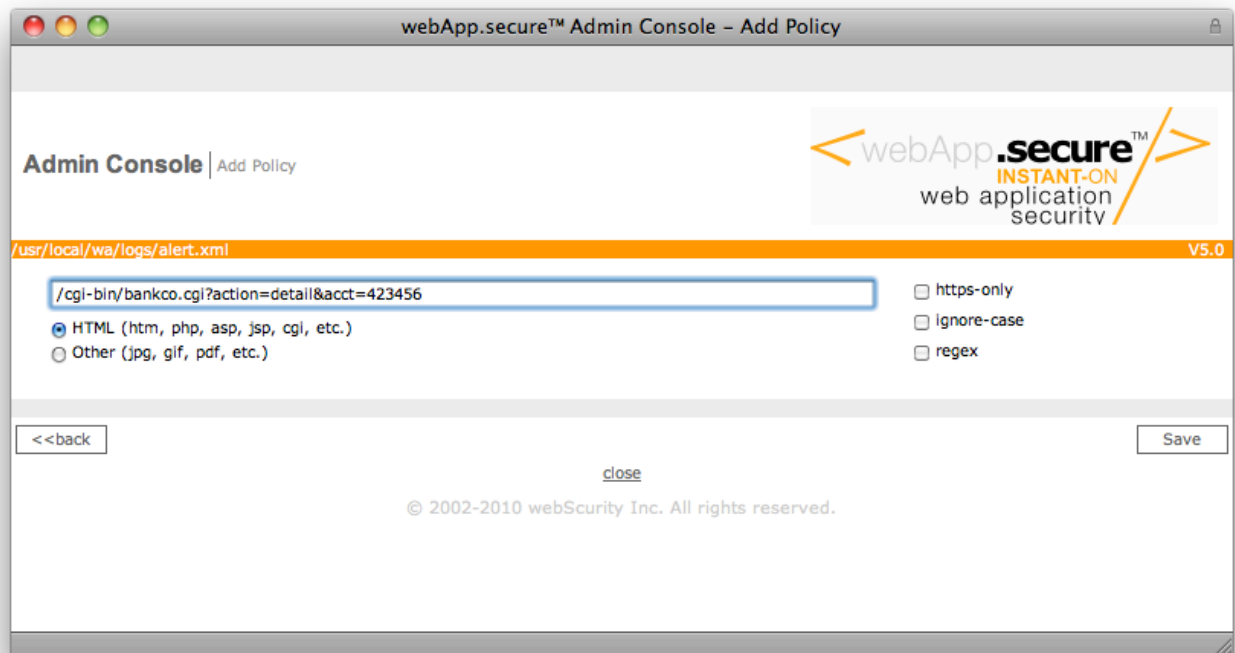
Details of a single alert are displayed when the date/time is clicked.

Add Policy

In many cases, an “Add Policy” link will appear in lower center of the page. As the name suggests, clicking the link will add a user-defined policy. Depending on the nature of the policy, another page may be displayed to gather more information (see next page for example). If a policy already exists for the alert, the “Add Policy” link will be replaced with “Remove Policy” and “Edit Policy” links.

Adding a Policy

Below is an example of a page that displays when the “[Add Policy](#)” (see previous page) link is clicked. This page allows the policy to be customized according to your specific needs.



The screenshot shows the 'webApp.secure™ Admin Console - Add Policy' window. The header includes the 'Admin Console | Add Policy' breadcrumb and the 'webApp.secure™ INSTANT-ON web application security' logo. Below the header, there is a status bar with the path '/usr/local/wa/logs/alert.xml' and 'V5.0'. The main content area features a text input field containing '/cgi-bin/bankco.cgi?action=detail&acct=423456'. Below the input field are two radio buttons: 'HTML (htm, php, asp, jsp, cgi, etc.)' (selected) and 'Other (jpg, gif, pdf, etc.)'. To the right of these are three checkboxes: 'https-only', 'ignore-case', and 'regex'. At the bottom of the form are '<<back' and 'Save' buttons. A 'close' link is centered below the buttons, and a copyright notice '© 2002-2010 webSecurity Inc. All rights reserved.' is at the very bottom.

Example policy for a URL query string parameter-tampering alert.

URI Input Box

The URI of the blocked request is displayed and can be altered to meet specific needs. Most often, if the URI component of the alert is edited, it is to incorporate wildcard characters to allow for varying query string values (see [User-defined Policies \(HTML content\)](#) for details).

Content Type Radio Buttons

- *HTML*: check this option if the content delivered by the URI will be HTML (policy is implemented as an Entry Point).
- *Other*: check this option if the content delivered by the URI will not be HTML (policy is implemented as an Unprotected Dir).

https-only Checkbox

Check this option if the URI should only be accessed over an encrypted connection (https).

ignore-case Checkbox

Check this option if the URI a case-insensitive comparison should be used.

regex Checkbox

Not available in LiveCD version.

OpenSSL

webApp.secure™ utilizes the "OpenSSL Toolkit" functionality provided by "The Open SSL Project" at <http://www.openssl.org>.

The OpenSSL Toolkit is licensed under a dual-license (the OpenSSL license and the original SSLeay license). See the license text below.

OpenSSL License

Copyright (c) 1998-2000 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"
THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)". The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.

Mozilla Spidermonkey

webApp.**secure** utilizes the Spidermonkey JavaScript Interpreter provided by Mozilla at <http://www.mozilla.org>.

Netscape Public License v1.1

AMENDMENTS

The Netscape Public License Version 1.1 ("NPL") consists of the Mozilla Public License Version 1.1 with the following Amendments, including Exhibit A-Netscape Public License. Files identified with "Exhibit A-Netscape Public License" are governed by the Netscape Public License Version 1.1.

Additional Terms applicable to the Netscape Public License.

I. Effect.

These additional terms described in this Netscape Public License -- Amendments shall apply to the Mozilla Communicator client code and to all Covered Code under this License.

II. "Netscape's Branded Code" means Covered Code that Netscape distributes and/or permits others to distribute under one or more trademark(s) which are controlled by Netscape but which are not licensed for use under this License.

III. Netscape and logo.

This License does not grant any rights to use the trademarks "Netscape", the "Netscape N and horizon" logo or the "Netscape lighthouse" logo, "Netcenter", "Gecko", "Java" or "JavaScript", "Smart Browsing" even if such marks are included in the Original Code or Modifications.

IV. Inability to Comply Due to Contractual Obligation.

Prior to licensing the Original Code under this License, Netscape has licensed third party code for use in Netscape's Branded Code. To the extent that Netscape is limited contractually from making such third party code available under this License, Netscape may choose to reintegrate such code into Covered Code without being required to distribute such code in Source Code form, even if such code would otherwise be considered "Modifications" under this License.

V. Use of Modifications and Covered Code by Initial Developer.

V.1. In General.

The obligations of Section 3 apply to Netscape, except to the extent specified in this Amendment, Section V.2 and V.3.

V.2. Other Products.

Netscape may include Covered Code in products other than the Netscape's Branded Code which are released by Netscape during the two (2) years following the release date of the Original Code, without such additional products becoming subject to the terms of this License, and may license such additional products on different terms from those contained in this License.

V.3. Alternative Licensing.

Netscape may license the Source Code of Netscape's Branded Code, including Modifications incorporated therein, without such Netscape Branded Code becoming subject to the terms of this License, and may license such Netscape Branded Code on different terms from those contained in this License.

VI. Litigation.

Notwithstanding the limitations of Section 11 above, the provisions regarding litigation in Section 11(a), (b) and (c) of the License shall apply to all disputes relating to this License.

EXHIBIT A-Netscape Public License.

"The contents of this file are subject to the Netscape Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.mozilla.org/NPL/> Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License. The Original Code is Mozilla Communicator client code, released March 31, 1998. The Initial Developer of the Original Code is Netscape Communications Corporation. Portions created by Netscape are Copyright (C) 1998-1999 Netscape Communications Corporation. All Rights Reserved. Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the "[_____] License"), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [_____] License and not to allow others to use your version of this file under the NPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [_____] License. If you do not delete the provisions above, a recipient may use your version of this file under either the NPL or the [_____] License."

MOZILLA PUBLIC LICENSE

Version 1.1

1. Definitions.

- 1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.
- 1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.
- 1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.
- 1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.
- 1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.
- 1.5. "Executable" means Covered Code in any form other than Source Code.
- 1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.
- 1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.
- 1.8. "License" means this document.
- 1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.
- 1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:
 - A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.
 - B. Any new file that contains any part of the Original Code or previous Modifications.
- 1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.
- 1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.
- 1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.
- 1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and
(b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

(c) the licenses granted in this Section 2.1(a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) the licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims.

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs.

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent

licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions.

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. TERMINATION.

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

(a) such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

(b) any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. U.S. GOVERNMENT END USERS.

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. MULTIPLE-LICENSED CODE.

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the NPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

EXHIBIT A -Mozilla Public License.

``The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.mozilla.org/MPL/>

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____. Portions created by _____ are Copyright (C) _____. All Rights

Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the "[_____] License"), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [_____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [_____] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [_____] License."