Affected Items Report

Acunetix Security Audit

30 May 2018

Generated by Acunetix

Scan of http://www.altoromutual.com

Scan details

Scan information	
Start time	30/05/2018, 17:34:04
Start url	http://www.altoromutual.com
Host	http://www.altoromutual.com
Scan time	47 minutes, 38 seconds
Profile	Full Scan

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	63
High	16
Medium	16
Low	16
Informational	15

Affected items

Web Server	
Alert group	**Blind SQL Injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Blind SQL Injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Blind SQL Injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	

Alert group	**Blind SQL Injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Blind SQL Injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Cross site scripting**
Severity	High
Description	This script is possibly vulnerable to Cross Site Scripting (XSS) attacks. Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.
Recommendations	Your script should filter metacharacters from user input.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Cross site scripting**
Severity	High
Description	This script is possibly vulnerable to Cross Site Scripting (XSS) attacks. Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot

	know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.
Recommendations	Your script should filter metacharacters from user input.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Cross site scripting**
Severity	High
Description	This script is possibly vulnerable to Cross Site Scripting (XSS) attacks. Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.
Recommendations	Your script should filter metacharacters from user input.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Cross site scripting**
Severity	High
Description	This script is possibly vulnerable to Cross Site Scripting (XSS) attacks. Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.
Recommendations	Your script should filter metacharacters from user input.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Directory traversal**
Severity	High
Description	This script is possibly vulnerable to directory traversal attacks. Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.
Recommendations	Your script should filter metacharacters from user input.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Microsoft IIS tilde directory enumeration**
Severity	High
Description	It is possible to detect short names of files and directories which have an 8.3 file naming scheme equivalent in Windows by using some vectors in several versions of Microsoft IIS. For instance, it is possible to detect all short-names of ".aspx" files as they have 4 letters in their extensions. This can be a major issue especially for the .Net websites which are vulnerable to direct URL access

	as an attacker can find important files and folders that they are not normally visible.
Recommendations	Consult the "Prevention Technique(s)" section from Soroush Dalili's paper on this subject. A link to this paper is listed in the Web references section below.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**SQL injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**SQL injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**SQL injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.

Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**SQL injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**SQL injection**
Severity	High
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Application error message**
Severity	Medium
Description	This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception. This may be a false positive if the error message is found in documentation pages.
Recommendations	Review the source code for this script.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Application error message**
Severity	Medium

Description	This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception. This may be a false positive if the error message is found in documentation pages.
Recommendations	Review the source code for this script.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Application error message**
Severity	Medium
Description	This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception. This may be a false positive if the error message is found in documentation pages.
Recommendations	Review the source code for this script.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Application error message**
Severity	Medium
Description	This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception. This may be a false positive if the error message is found in documentation pages.
Recommendations	Review the source code for this script.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Application error message**
Severity	Medium
Description	This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception. This may be a false positive if the error message is found in documentation pages.
Recommendations	Review the source code for this script.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Application error message**
Severity	Medium
Description	This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception. This may be a false positive if the error message is found in documentation pages.
Recommendations	Review the source code for this script.

Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Application error message**
Severity	Medium
Description	This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception. This may be a false positive if the error message is found in documentation pages.
Recommendations	Review the source code for this script.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Application error message**
Severity	Medium
Description	This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception. This may be a false positive if the error message is found in documentation pages.
Recommendations	Review the source code for this script.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Application error message**
Severity	Medium
Description	This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception. This may be a false positive if the error message is found in documentation pages.
Recommendations	Review the source code for this script.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Directory listing**
Severity	Medium
Description	The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
Recommendations	You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Directory listing**
Severity	Medium
Description	The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
Recommendations	You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**HTML form without CSRF protection**
Severity	Medium
Description	This alert may be a false positive, manual confirmation is required. Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.
Recommendations	Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**HTML form without CSRF protection**
Severity	Medium
Description	This alert may be a false positive, manual confirmation is required. Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.
Recommendations	Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**HTML form without CSRF protection**
Severity	Medium
Description	This alert may be a false positive, manual confirmation is required. Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.
Recommendations	

	Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**HTML form without CSRF protection**
Severity	Medium
Description	This alert may be a false positive, manual confirmation is required. Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.
Recommendations	Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**User credentials are sent in clear text**
Severity	Medium
Description	User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.
Recommendations	Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**ASP.NET debugging enabled**
Severity	Low
Description	ASP.NET debugging is enabled on this application. It is recommended to disable debug mode before deploying a production application. By default, debugging is disabled, and although debugging is frequently enabled to troubleshoot a problem, it is also frequently not disabled again after the problem is resolved.
Recommendations	Check References for details on how to fix this problem.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**ASP.NET version disclosure**
Severity	Low
Description	The HTTP responses returned by this web application include anheader named **X-AspNet-Version**. The value of this header is used by Visual Studio to determine which version of ASP.NET is in use. It is not necessary for production sites and should be disabled.
	Apply the following changes to the web.config file to prevent ASP.NET version disclosure:

Recommendations	`<System.Web>`
	` <httpRuntime enableVersionHeader="false" />`
	`</System.Web>`

Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Clickjacking: X-Frame-Options header missing**
Severity	Low
Description	Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.
Recommendations	Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Cookie(s) without HttpOnly flag set**
Severity	Low
Description	This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.
Recommendations	If possible, you should set the HTTPOnly flag for this cookie.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**OPTIONS method is enabled**
Severity	Low
Description	HTTP OPTIONS method is enabled on this web server. The OPTIONS method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI.
Recommendations	It's recommended to disable OPTIONS Method on the web server.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Possible relative path overwrite**

Severity	Low
Description	Manual confirmation is required for this alert. Gareth Heyes introduced a technique to take advantage of CSS imports with relative URLs by overwriting their target file. This technique can be used by an attacker to trick browsers into importing HTML pages as CSS stylesheets. If the attacker can control a part of the imported HTML pages he can abuse this issue to inject arbitrary CSS rules.
Recommendations	If possible, it's recommended to use absolute links for CSS imports. The problem can be partially mitigated by preventing framing. To prevent framing configure your web server to include an X-Frame-Options: deny header on all pages.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Possible relative path overwrite**
Severity	Low
Description	Manual confirmation is required for this alert. Gareth Heyes introduced a technique to take advantage of CSS imports with relative URLs by overwriting their target file. This technique can be used by an attacker to trick browsers into importing HTML pages as CSS stylesheets. If the attacker can control a part of the imported HTML pages he can abuse this issue to inject arbitrary CSS rules.
Recommendations	If possible, it's recommended to use absolute links for CSS imports. The problem can be partially mitigated by preventing framing. To prevent framing configure your web server to include an X-Frame-Options: deny header on all pages.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Possible relative path overwrite**
Severity	Low
Description	Manual confirmation is required for this alert. Gareth Heyes introduced a technique to take advantage of CSS imports with relative URLs by overwriting their target file. This technique can be used by an attacker to trick browsers into importing HTML pages as CSS stylesheets. If the attacker can control a part of the imported HTML pages he can abuse this issue to inject arbitrary CSS rules.
Recommendations	If possible, it's recommended to use absolute links for CSS imports. The problem can be partially mitigated by preventing framing. To prevent framing configure your web server to include an X-Frame-Options: deny header on all pages.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Possible relative path overwrite**
Severity	Low
Description	Manual confirmation is required for this alert. Gareth Heyes introduced a technique to take advantage of CSS imports with relative URLs by overwriting their target file. This technique can be used by an attacker to trick browsers into importing HTML pages as CSS stylesheets. If the attacker can control a part of the imported HTML pages he can abuse this issue to inject arbitrary CSS rules.
	If possible, it's recommended to use absolute links for CSS imports. The problem can be partially

Recommendations	mitigated by preventing framing. To prevent framing configure your web server to include an X-Frame-Options: deny header on all pages.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Possible relative path overwrite**
Severity	Low
Description	Manual confirmation is required for this alert. Gareth Heyes introduced a technique to take advantage of CSS imports with relative URLs by overwriting their target file. This technique can be used by an attacker to trick browsers into importing HTML pages as CSS stylesheets. If the attacker can control a part of the imported HTML pages he can abuse this issue to inject arbitrary CSS rules.
Recommendations	If possible, it's recommended to use absolute links for CSS imports. The problem can be partially mitigated by preventing framing. To prevent framing configure your web server to include an X-Frame-Options: deny header on all pages.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Possible relative path overwrite**
Severity	Low
Description	Manual confirmation is required for this alert. Gareth Heyes introduced a technique to take advantage of CSS imports with relative URLs by overwriting their target file. This technique can be used by an attacker to trick browsers into importing HTML pages as CSS stylesheets. If the attacker can control a part of the imported HTML pages he can abuse this issue to inject arbitrary CSS rules.
Recommendations	If possible, it's recommended to use absolute links for CSS imports. The problem can be partially mitigated by preventing framing. To prevent framing configure your web server to include an X-Frame-Options: deny header on all pages.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Possible relative path overwrite**
Severity	Low
Description	Manual confirmation is required for this alert. Gareth Heyes introduced a technique to take advantage of CSS imports with relative URLs by overwriting their target file. This technique can be used by an attacker to trick browsers into importing HTML pages as CSS stylesheets. If the attacker can control a part of the imported HTML pages he can abuse this issue to inject arbitrary CSS rules.
Recommendations	If possible, it's recommended to use absolute links for CSS imports. The problem can be partially mitigated by preventing framing. To prevent framing configure your web server to include an X-Frame-Options: deny header on all pages.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	

Alert group	**Possible relative path overwrite**
Severity	Low
Description	Manual confirmation is required for this alert. Gareth Heyes introduced a technique to take advantage of CSS imports with relative URLs by overwriting their target file. This technique can be used by an attacker to trick browsers into importing HTML pages as CSS stylesheets. If the attacker can control a part of the imported HTML pages he can abuse this issue to inject arbitrary CSS rules.
Recommendations	If possible, it's recommended to use absolute links for CSS imports. The problem can be partially mitigated by preventing framing. To prevent framing configure your web server to include an X-Frame-Options: deny header on all pages.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Possible sensitive directories**
Severity	Low
Description	A possible sensitive directory has been found. This directory is not directly linked from the website.This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
Recommendations	Restrict access to this directory or remove it from the website.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Possible sensitive directories**
Severity	Low
Description	A possible sensitive directory has been found. This directory is not directly linked from the website.This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
Recommendations	Restrict access to this directory or remove it from the website.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Possible sensitive files**
Severity	Low
Description	A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.
Recommendations	Restrict access to this file or remove it from the website.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Broken links**

Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Broken links**
Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Broken links**
Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Broken links**
Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Broken links**
Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Broken links**

Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Broken links**
Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Broken links**
Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Broken links**
Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Broken links**
Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Broken links**

Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Content type is not specified**
Severity	Informational
Description	This page does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.
Recommendations	Set a Content-Type header value for this page.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Email address found**
Severity	Informational
Description	One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
Recommendations	Check references for details on how to solve this problem.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Microsoft IIS version disclosure**
Severity	Informational
Description	The HTTP responses returned by this web application include a header named **Server**. The value of this header includes the version of Microsoft IIS server.
Recommendations	Microsoft IIS should be configured to remove unwanted HTTP response headers from the response. Consult web references for more information.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Password type input with auto-complete enabled**
Severity	Informational
Description	When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.
Recommendations	The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code similar to:

	`<INPUT TYPE="password" AUTOCOMPLETE="off">`
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Scanned items (coverage report)

http://www.altoromutual.com/
http://www.altoromutual.com/|~.aspx
http://www.altoromutual.com/admin
http://www.altoromutual.com/bank
http://www.altoromutual.com/bank/20060308_bak
http://www.altoromutual.com/bank/account.aspx
http://www.altoromutual.com/bank/account.aspx.cs
http://www.altoromutual.com/bank/apply.aspx
http://www.altoromutual.com/bank/apply.aspx.cs
http://www.altoromutual.com/bank/bank.master
http://www.altoromutual.com/bank/bank.master.cs
http://www.altoromutual.com/bank/customize.aspx
http://www.altoromutual.com/bank/customize.aspx.cs
http://www.altoromutual.com/bank/login.aspx
http://www.altoromutual.com/bank/login.aspx.cs
http://www.altoromutual.com/bank/logout.aspx
http://www.altoromutual.com/bank/logout.aspx.cs
http://www.altoromutual.com/bank/main.aspx
http://www.altoromutual.com/bank/main.aspx.cs
http://www.altoromutual.com/bank/members
http://www.altoromutual.com/bank/mozxpath.js
http://www.altoromutual.com/bank/queryxpath.aspx
http://www.altoromutual.com/bank/queryxpath.aspx.cs
http://www.altoromutual.com/bank/servererror.aspx
http://www.altoromutual.com/bank/transaction.aspx
http://www.altoromutual.com/bank/transaction.aspx.cs
http://www.altoromutual.com/bank/transfer.aspx
http://www.altoromutual.com/bank/transfer.aspx.cs
http://www.altoromutual.com/bank/ws.asmx
http://www.altoromutual.com/business_cards.htm
http://www.altoromutual.com/business_insurance.htm
http://www.altoromutual.com/business_other.htm
http://www.altoromutual.com/business_retirement.htm
http://www.altoromutual.com/comment.aspx
http://www.altoromutual.com/comments.txt
http://www.altoromutual.com/default.aspx
http://www.altoromutual.com/disclaimer.htm
http://www.altoromutual.com/feedback.aspx
http://www.altoromutual.com/images
http://www.altoromutual.com/inside.htm
http://www.altoromutual.com/inside_about.htm
http://www.altoromutual.com/inside_contact.htm
http://www.altoromutual.com/inside_investor.htm
http://www.altoromutual.com/inside_points_of_interest.htm
http://www.altoromutual.com/inside_press.htm
http://www.altoromutual.com/pr
http://www.altoromutual.com/pr/docs.xml
http://www.altoromutual.com/pr/draft.rtf
http://www.altoromutual.com/pr/q3_earnings.rtf
http://www.altoromutual.com/retirement.htm
http://www.altoromutual.com/search.aspx
http://www.altoromutual.com/security.htm
http://www.altoromutual.com/servererror.aspx
http://www.altoromutual.com/static
http://www.altoromutual.com/style.css
http://www.altoromutual.com/subscribe.aspx
http://www.altoromutual.com/subscribe.swf
http://www.altoromutual.com/survey_questions.aspx
http://www.altoromutual.com/test.aspx