acunetix

Affected Items Report

Acunetix Security Audit

23 August 2019

Generated by Acunetix

Scan of joptii.azurewebsites.net

Scan details

Scan information	
Start time	23/08/2019, 09:16:32
Start url	http://joptii.azurewebsites.net/
Host	joptii.azurewebsites.net
Scan time	16 minutes, 8 seconds
Profile	Full Scan
Server information	Microsoft-IIS/10.0
Responsive	True
Server OS	Windows
Server technologies	ASP

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	13
High	0
Medium	6
Low	3
Informational	4

Affected items

Web Server	
Alert group	**Application error message**
Severity	Medium
Description	This alert requires manual confirmation Application error or warning messages may expose sensitive information about an application's internal workings to an attacker. Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
Recommendations	Verify that this page is disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Error message on page**
Severity	Medium
Description	This alert requires manual confirmation Application error or warning messages may expose sensitive information about an application's internal workings to an attacker. Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
Recommendations	Verify that this page is disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Error message on page**
Severity	Medium
Description	This alert requires manual confirmation Application error or warning messages may expose sensitive information about an application's internal workings to an attacker. Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
Recommendations	Verify that this page is disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Error message on page**
Severity	Medium
Description	This alert requires manual confirmation Application error or warning messages may expose sensitive information about an application's internal workings to an attacker. Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.
Recommendations	Verify that this page is disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.
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	**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 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.

Recommendations	Apply the following changes to the web.config file to prevent ASP.NET version disclosure:
	
	`<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	**Login page password-guessing attack**
Severity	Low
Description	A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works. This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.
Recommendations	It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Stack Trace Disclosure (ASP.NET)**
Severity	Low
Description	A stack trace was identified on this page. The web application has generated an error message that includes sensitive information about its environment, users, or associated data. The stack trace can disclose potentially sensitive information such as: physical file paths of relevant files, source code fragments, version information of various packages, database information, error messages, ... It's recommended to handle exceptions internally and do not display errors containing potentially sensitive information to a user.

Recommendations	To prevent the information disclosure you can implement custom error pages by applying the following changes to your **web.config** file.
	
	`<System.Web>`
	`  <customErrors mode="On" defaultRedirect="~/error/GeneralError.a`
	`  <error statusCode="403" redirect="~/error/Forbidden.aspx"`
	`  <error statusCode="404" redirect="~/error/PageNotFound.asp`
	`  <error statusCode="500" redirect="~/error/InternalError.as`
	`  </customErrors>`
	`</System.Web>`

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

Web Server	
Alert group	**Content Security Policy (CSP) not implemented**
Severity	Informational

Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.
	
	Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:
	
	`Content-Security-Policy:`
	`  default-src 'self';`
	`  script-src 'self' https://code.jquery.com;`
	
	It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Recommendations	It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Error page web server version disclosure**

Severity	Informational
Description	Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker. Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.
Recommendations	Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.
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://joptii.azurewebsites.net/
http://joptii.azurewebsites.net/|~.aspx
http://joptii.azurewebsites.net/account
http://joptii.azurewebsites.net/bundles/
http://joptii.azurewebsites.net/bundles/jqueryval
http://joptii.azurewebsites.net/Content/
http://joptii.azurewebsites.net/Content/Template/
http://joptii.azurewebsites.net/Content/Template/css/
http://joptii.azurewebsites.net/Content/Template/css/sb-admin.css
http://joptii.azurewebsites.net/Content/Template/js/
http://joptii.azurewebsites.net/Content/Template/js/demo/
http://joptii.azurewebsites.net/Content/Template/vendor/
http://joptii.azurewebsites.net/Content/Template/vendor/bootstrap/
http://joptii.azurewebsites.net/Content/Template/vendor/bootstrap/js/
http://joptii.azurewebsites.net/Content/Template/vendor/bootstrap/js/bootstrap.bundle.min.js
http://joptii.azurewebsites.net/Content/Template/vendor/fontawesome-free/
http://joptii.azurewebsites.net/Content/Template/vendor/fontawesome-free/css/
http://joptii.azurewebsites.net/Content/Template/vendor/fontawesome-free/css/all.min.css
http://joptii.azurewebsites.net/Content/Template/vendor/fontawesome-free/js/
http://joptii.azurewebsites.net/Content/Template/vendor/fontawesome-free/webfonts/
http://joptii.azurewebsites.net/Content/Template/vendor/fontawesome-free/webfonts/fa-brands-400.woff2
http://joptii.azurewebsites.net/Content/Template/vendor/fontawesome-free/webfonts/fa-regular-400.woff2
http://joptii.azurewebsites.net/Content/Template/vendor/fontawesome-free/webfonts/fa-solid-900.woff2
http://joptii.azurewebsites.net/Content/Template/vendor/jquery-easing/
http://joptii.azurewebsites.net/Content/Template/vendor/jquery-easing/jquery.easing.min.js
http://joptii.azurewebsites.net/Content/Template/vendor/jquery/
http://joptii.azurewebsites.net/Content/Template/vendor/jquery/jquery.min.js
http://joptii.azurewebsites.net/forgot-password.html
http://joptii.azurewebsites.net/jEAGqFXa8T
http://joptii.azurewebsites.net/register.html
http://joptii.azurewebsites.net/scripts/