

Affected Items Report

Acunetix Security Audit

05 September 2024

Scan of https://www.drspinecrm.in/drspine-CRM/login.php

Scan details




Scan information	
Start time	05/09/2024, 11:43:54
Start url	https://www.drspinecrm.in/drspine-CRM/login.php
Host	https://www.drspinecrm.in/drspine-CRM/login.php
Scan time	2 minutes, 53 seconds
Profile	Full Scan

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	12
 High	0
 Medium	7
 Low	4
 Informational	1

Affected items

Web Server	
Alert group	.htaccess file readable
Severity	Medium
Description	This directory contains an .htaccess file that is readable. This may indicate a server misconfiguration. htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.
Recommendations	Restrict access to the .htaccess file by adjusting the web server configuration.
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	<p>This alert requires manual confirmation</p> <p>Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.</p> <p>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.</p>
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	Application error message
Severity	Medium
Description	<p>This alert requires manual confirmation</p> <p>Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.</p> <p>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.</p>
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	Application error message
Severity	Medium
Description	<p>This alert requires manual confirmation</p> <p>Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.</p>

	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	CRLF injection/HTTP response splitting (Web Server)
Severity	Medium
Description	<p>This script is possibly vulnerable to CRLF injection attacks.</p> <p>HTTP headers have the structure "Key: Value", where each line is separated by the CRLF combination. If the user input is injected into the value section without properly escaping/removing CRLF characters it is possible to alter the HTTP headers structure.</p> <p>HTTP Response Splitting is a new application attack technique which enables various new attacks such as web cache poisoning, cross user defacement, hijacking pages with sensitive user information and cross-site scripting (XSS). The attacker sends a single HTTP request that forces the web server to form an output stream, which is then interpreted by the target as two HTTP responses instead of one response.</p>
Recommendations	You need to restrict CR(0x13) and LF(0x10) from the user input or properly encode the output in order to prevent the injection of custom HTTP headers.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	Development configuration file
Severity	Medium
Description	A configuration file (e.g. Vagrantfile, Gemfile, Rakefile, ...) was found in this directory. This file may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.
Recommendations	Remove or restrict access to all configuration files accessible from internet.
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	<p>This alert requires manual confirmation</p> <p>Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.</p> <p>Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.</p>
	<p>Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.</p> <p>The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes.</p>

Recommendations	<ul style="list-style-type: none"> • The anti-CSRF token should be unique for each user session • The session should automatically expire after a suitable amount of time • The anti-CSRF token should be a cryptographically random value of significant length • The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm • The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent) • The server should reject the requested action if the anti-CSRF token fails validation <p>When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected.</p>
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	<p>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.</p> <p>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.</p>
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	Login page password-guessing attack
Severity	Low
Description	<p>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.</p> <p>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.</p>
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	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	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	<p>The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code similar to:</p> <pre><INPUT TYPE="password" AUTOCOMPLETE="off"></pre>
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Scanned items (coverage report)

<https://www.drspinecrm.in/>

<https://www.drspinecrm.in/drspine-CRM>

<https://www.drspinecrm.in/drspine-CRM/> headername: headervalue

<https://www.drspinecrm.in/drspine-CRM/.htaccess>

<https://www.drspinecrm.in/drspine-CRM/backups>

<https://www.drspinecrm.in/drspine-CRM/composer.lock>

<https://www.drspinecrm.in/drspine-CRM/config.php>

<https://www.drspinecrm.in/drspine-CRM/css>

<https://www.drspinecrm.in/drspine-CRM/css/login.css>

<https://www.drspinecrm.in/drspine-CRM/dist>

<https://www.drspinecrm.in/drspine-CRM/dist/img>

<https://www.drspinecrm.in/drspine-CRM/images>

<https://www.drspinecrm.in/drspine-CRM/login.php>

<https://www.drspinecrm.in/drspine-CRM/logindb.php>

<https://www.drspinecrm.in/drspine-CRM/plugins>

<https://www.drspinecrm.in/drspine-CRM/vendor>