⟵ Home

Files or Directories Accessible to External Parties in InvoicePlane CRM

Mar 17, 2021

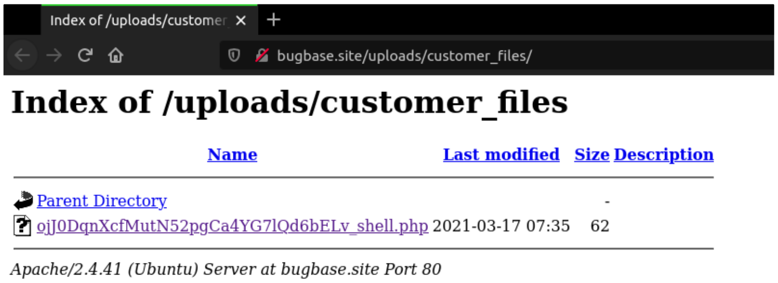
Summary

InvoicePlane is one of the popular open-source CRM. During the search for a PHP based open-source CRM in Github, this comes mostly within first ten.

The latest version of InvoicePlane (v1.5.11) has several vulnerabilities. Without further wasting your time let's dive into the details.

- CWE-552: Files or Directories Accessible to External Parties

As mentioned above, if the webserver is not configured properly, this allows unauthenticated directory listing and file download. Allowing an attacker to directory traversal and download files suppose to be private without authentication.


Index of /uploads/customer
bugbase.site/uploads/customer_files/

Index of /uploads/customer_files

Name	Last modified	Size	Description
Parent Directory		-	
ojJ0DqnXcfMutN52pgCa4YG7lQd6bELv_shell.php	2021-03-17 07:35	62	

Apache/2.4.41 (Ubuntu) Server at bugbase.site Port 80

The developer has implemented some preventive measures to avoid exploitation of this vulnerability like *htaccess* based directory access restriction and users can download the file via an authenticated URL instead of direct download. But none of these will work if the server is not configured properly. During the testing, it seems the default installation of Apache will not help with the implemented protection mechanism.

> .htaccess based mitigation will work only with the supported webserver.

notnnor
notnnor@gmail.com