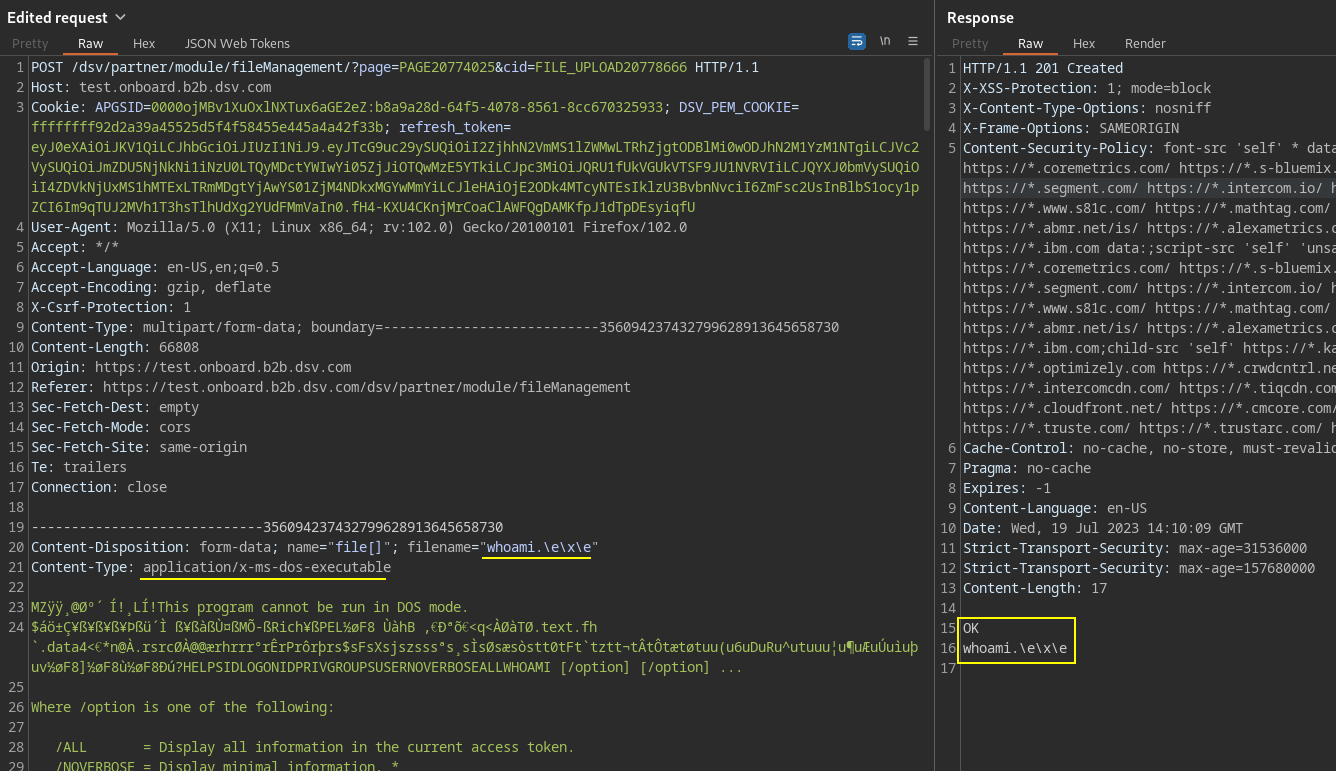
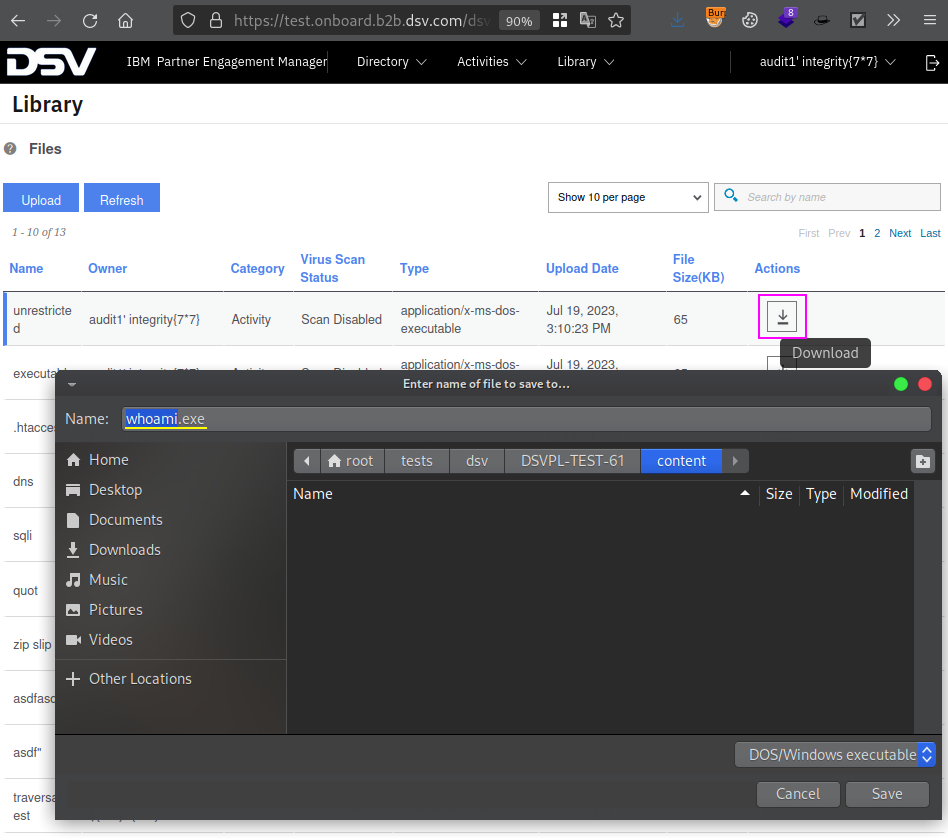
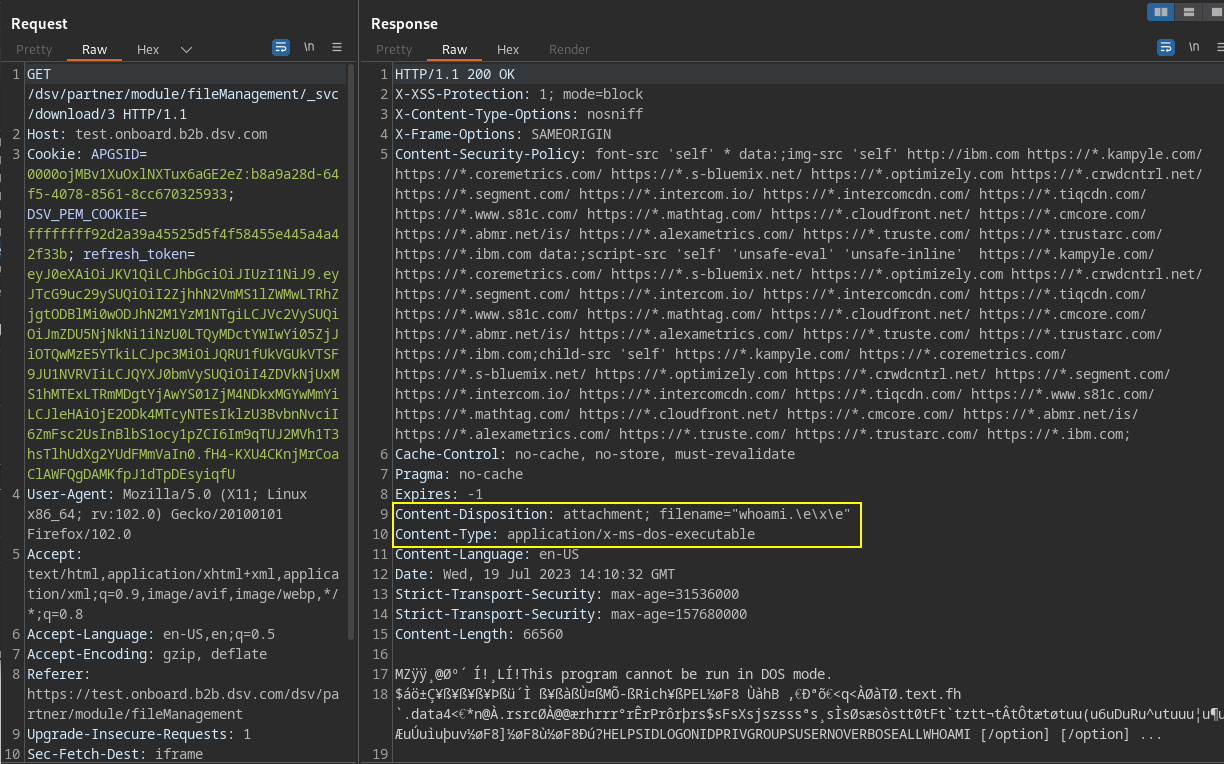
The application **test.onboard.b2b.dsv.com**is vulnerable to an unrestricted file upload on the path **/dsv/partner/module/fileManagement/** in the parameter **file**. Through this vulnerability it is possible to upload a windows executable file that that could have malicious behaviour.

Request uploading the file:



Downloading the file:





**Recommendations:**

* Use a whitelist approach to validate the file extension and name on the server side;
* Remove execution permissions on the directory where the upload is done.

**References:**

* OWASP Unrestricted File Upload - <https://ref.keepitsecure24.com/owasp-Unrestricted-File-Upload>
* OWASP File Upload Cheat Sheet - <https://ref.keepitsecure24.com/File-Upload-Cheat-Sheet>
* WSTG - Test Upload of Malicious Files - <https://ref.keepitsecure24.com/WSTG-BUSL-09>