

Arbitrary File Write FreeTAKServer-UI (Remote Code Execution) #29

Open Securitybits-io opened this issue on Feb 16 · 0 comments

Assignees



Labels enhancement

Milestone \Rightarrow 2.3

Securitybits-io commented on Feb 16

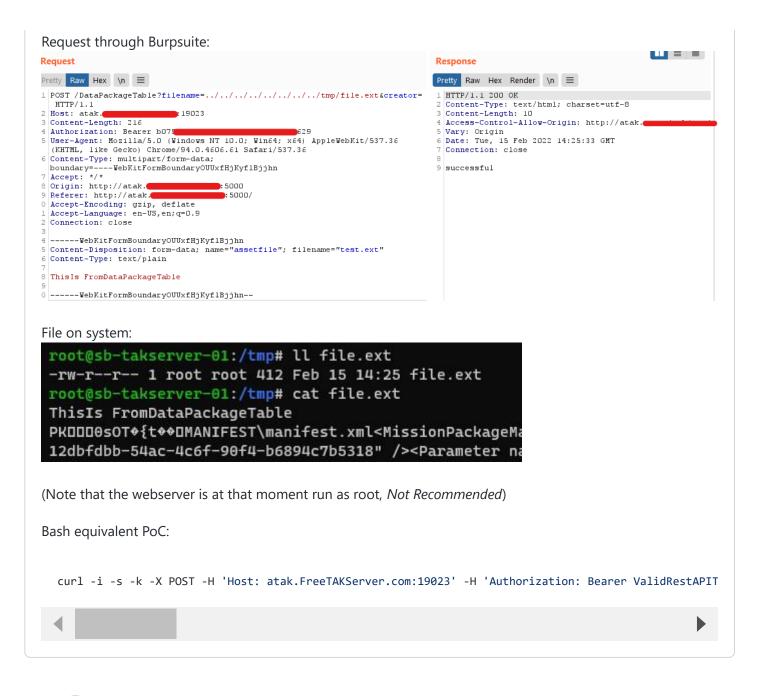
User Interface Datapackage

From the WebUI it is possible to (once logged in) upload DataPackages directly to the server so that it is possible to download the zipped files on the EUD in the field.

The route /DataPackageTable takes an argument ?filename= which is not sanitized for either the Path or the Filename outside of the UI, which creates the issues that you can place any file, anywhere on the system. Albeit going this route will add some junk XML data into the end of the file, this making it extremely hard to achieve code execution through Python or Flask Templating.

This was achieved using a transparent proxy to catch and modify the webrequest, but can also be achieved using something like Curl

Proof Of Concept



- A brothercorvo assigned dlc-ariel on Sep 6
- ⇔ brothercorvo added this to the 2.3 milestone on Sep 6
- brothercorvo added the enhancement label on Sep 6

Assignees



Labels

| enhancement | | |
|------------------------------|--|--|
| Projects | | |
| None yet | | |
| Milestone | | |
| 2.3 | | |
| Development | | |
| No branches or pull requests | | |
| 2 | | |

3 participants





