arachnys / cabot Public

Code Issues 150 Pull requests 17 Actions Projects Security ...

New issue

Jump to bottom

Security Fix for Stored Cross-site Scripting (XSS) - huntr.dev #694

Merged **dbuxton** merged 2 commits into `arachnys:master` from `418sec:1-pip-cabot` on Jan 5, 2021

Conversation 3 Commits 2 Checks 0 Files changed 2

huntr-helper commented on Sep 17, 2020 • edited

https://huntr.dev/users/alromh87 has fixed the Stored Cross-site Scripting (XSS) vulnerability 🔨. alromh87 has been awarded $25 for fixing the vulnerability through the huntr bug bounty program 💵. Think you could fix a vulnerability like this?

Get involved at https://huntr.dev/

Q | A
Version Affected | ALL
Bug Fix | YES
Original Pull Request | 418sec#1
Vulnerability README | https://github.com/418sec/huntr/blob/master/bounties/pip/cabot/1/README.md

User Comments:

📊 Metadata *

Bounty URL: **https://www.huntr.dev/bounties/1-pypi-cabot/**

⚙️ Description *

Executed Persistent stored XSS in cabot check settings, as well as the address field.

💻 Technical Description *

Fixed by using builtin django autoescape and URLValidator

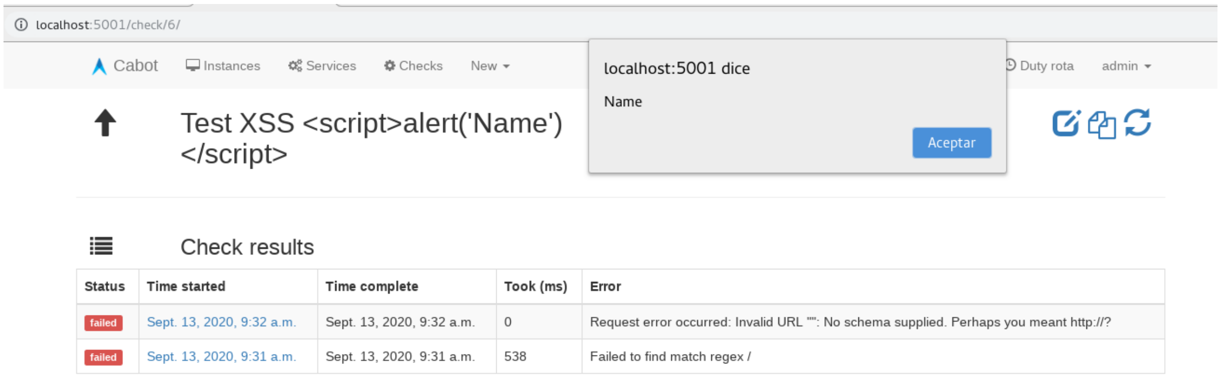
Altough Django has inbuilt protection agains XSS it was disabled for the test result.error by using `{% autoescape off %}`, just to be sure I wasn't breaking any needed functionality I inspected history to depict the porpouse of this change

- Ofending line was introduced in `558f18c` #diff-480f9da2f76d81e98bfb4c99316b90c6R52
- For allowing embeding links in the response `558f18c` #diff-9ff30487dc763b21d6a7742d19eb2268R442
- Function was removed a few commits later making the use of `{% autoescape off %}` unnecesary

As an extra I added URLValidator in the Http test model

🐛 Proof of Concept (PoC) *

1. Setup cabot to reproduce the vulnerability
2. Create an account now login to the account
3. Go to checks Create and navigate to http check.
4. In the Endpoint column append a XSS payload.
   `<script>alert('Hi')</script>`
5. Now we can see a failed check now click run button in that checks
6. XSS triggered
7. XSS will trigger in check result for every time executed for both Test name and Endpoint



localhost:5001/check/6/

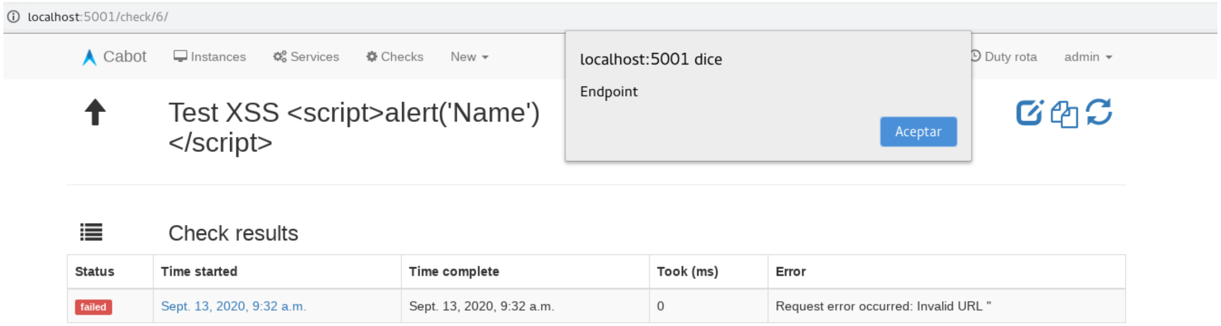
localhost:5001 dice

Name

Test XSS <script>alert('Name')</script>

Check results

Status	Time started	Time complete	Took (ms)	Error
failed	Sept. 13, 2020, 9:32 a.m.	Sept. 13, 2020, 9:32 a.m.	0	Request error occurred: Invalid URL "": No schema supplied. Perhaps you meant http://?
failed	Sept. 13, 2020, 9:31 a.m.	Sept. 13, 2020, 9:31 a.m.	538	Failed to find match regex /



localhost:5001 dice

Endpoint

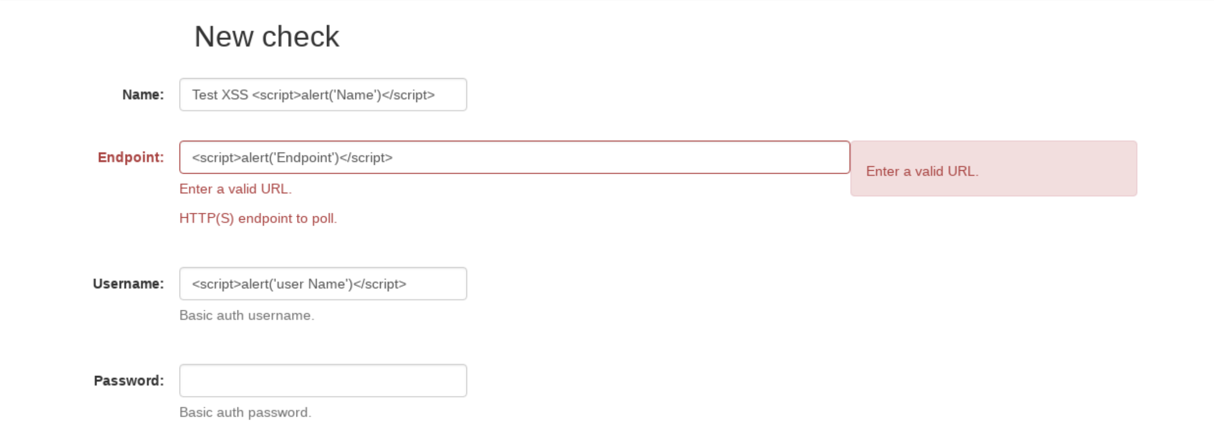
Test XSS <script>alert('Name')</script>

Check results

Status	Time started	Time complete	Took (ms)	Error
failed	Sept. 13, 2020, 9:32 a.m.	Sept. 13, 2020, 9:32 a.m.	0	Request error occurred: Invalid URL ''

Proof of Fix (PoF) *

After fix No code is executed for remote user



New check

Name: Test XSS <script>alert('Name')</script>

Endpoint: <script>alert('Endpoint')</script>

Enter a valid URL.

HTTP(S) endpoint to poll.

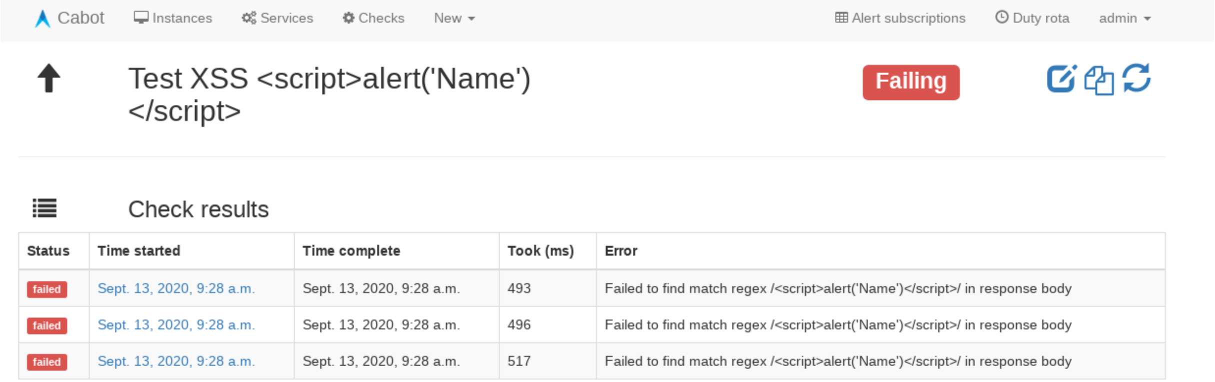
Enter a valid URL.

Username: <script>alert('user Name')</script>

Basic auth username.

Password:

Basic auth password.



Test XSS <script>alert('Name')</script>

Check results

Status	Time started	Time complete	Took (ms)	Error
failed	Sept. 13, 2020, 9:28 a.m.	Sept. 13, 2020, 9:28 a.m.	493	Failed to find match regex /<script>alert('Name')</script>/ in response body
failed	Sept. 13, 2020, 9:28 a.m.	Sept. 13, 2020, 9:28 a.m.	496	Failed to find match regex /<script>alert('Name')</script>/ in response body
failed	Sept. 13, 2020, 9:28 a.m.	Sept. 13, 2020, 9:28 a.m.	517	Failed to find match regex /<script>alert('Name')</script>/ in response body

Fix will also handle previously stored offending endpoints with XSS

👍 User Acceptance Testing (UAT)

After fix functionality is unafected

alromh87 and others added 2 commits 2 years ago

`Fix XSS` 1870857

`Merge pull request #1 from alromh87/master` … b788986

FuccDucc commented on Jan 5, 2021 • edited

The cabot project is dead (inactive repository), but i hope they realize this is a serious vulnerability.. it is CVE-2020-7734, scored as 8.2 HIGH on https://nvd.nist.gov/vuln/detail/CVE-2020-7734

So **@dbuxton** or **@frankh** please do something and merge this important security fix

Also see https://snyk.io/vuln/SNYK-PYTHON-CABOT-609862 for more details. They were right to say "There is no fixed version for cabot" under remediation.

With all sources combined, the public knowledge of the specifics of this vulnerability is enough to make exploitation by a lot of people possible. So it's not safe for it to be unpatched this long.

Merge it and deploy a new release or hotfix

👍 1

dbuxton merged commit `eb0b354` into `arachnys:master` on Jan 5, 2021

dbuxton commented on Jan 5, 2021 Contributor

Thanks for the feedback. Exploitation of this requires admin access, so we did not prioritize it, but as the fix is simple and uncontroversial it's now merged.

❤ 2

FuccDucc commented on Jan 5, 2021 • edited ▾

Nice..

The last release `0.11.7` dates back to 2017, and there's a lot of later commits in master.

How about making a new release that will include this security patch and also serve not to let all of those other updates go to waste? **@dbuxton**

Reviewers

No reviews

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

4 participants