Th3G3nt3lman Follow
Jun 4, 2017 · 2 min read

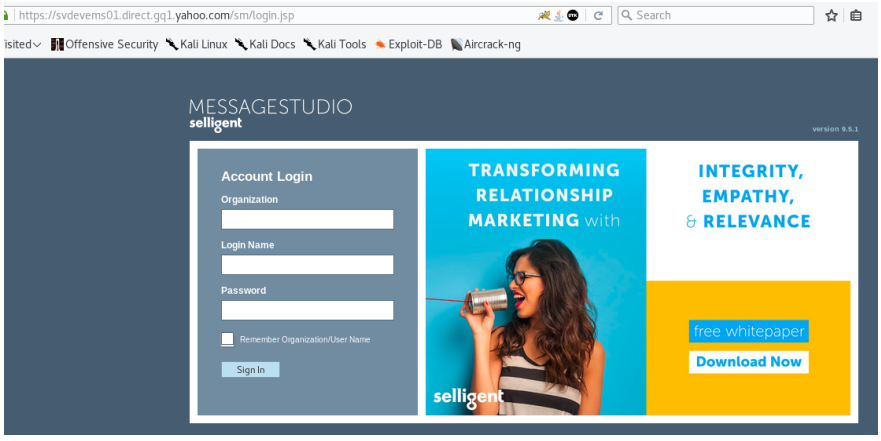
How I got 5500$ from Yahoo for RCE

Hi Guys,

I always believed that sharing is caring, and i have been learning from multiple security researchers in the bug bounty field, so i decided to share my few findings with you as it might help others who started in the Bug Bounty journey.

As you already know few months back a critical venerability have been discovered in apache Struts2 (CVE-2017–5638) leads to a remote code execution, the easy exploit for the same have been published and a lot of web applications were getting exploited in massive way.

After almost 3 weeks of the Struts2 exploit being published and during my Recon process i came across this link: https://svdevems01.direct.gq1.yahoo.com/sm/login.jsp which is a login page for the selligent Messages studio solution used by yahoo.



Tried to find vulnerabilities there and i failed until i found this endpoint : https://svdevems01.direct.gq1.yahoo.com/sm/login/loginpageconte

ntgrabber.do , for those who don't know if you find endpoints with .action, .do , .go that means the web application running struts2.

So as i said the exploit was published and easy to use but also it didn't work for this target even though it was confirmed that its vulnerable, that means there was WAF or something blocking my attacks.

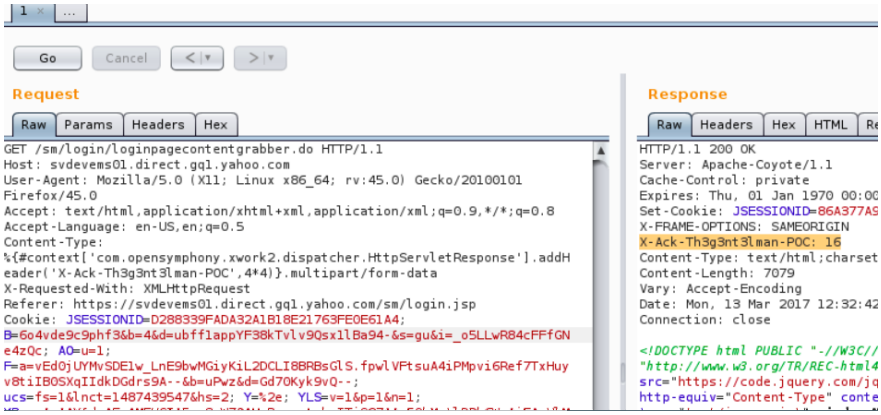
I couldn't stop here as its vulnerable and for reporting it i have to provide a valid POC for the same, After some searches i found a twitter post with a payload that can bypass WAF to exploit this vulnerability.

The detection method i found makes use of the Content-Type HTTP header to send a specially crafted packet. The header is shown below:

Content-Type: %{#context['com.opensymphony.xwork2.dispatcher.HttpServletResponse'].addHeader('X-Ack-Th3g3nt3lman-POC',4*4)}.multipart/form-data

The new request asks the web server to multiple two numbers and can be used to request the web server to perform any other operation. In the example above the two numbers are ***4*** and ***4***. and the answer from the web server, was ***16*** which concluded that the server is vulnerable.

The response as per the below picture will contain the new header ***X-Ack-Th3g3nt3lman-POC: 16***



That was fair enough to report the bug for yahoo through hackerone, Yahoo Triaged the report within 30 minutes, took the application offline to fix the issue and i confirmed the fix after that, within a week i was awarded with 5500$ for this finding.

Hope You liked this finding and i apologize for my weak English if there is any mistakes in this post.