### Ovirt engine URL redirection vulnerability

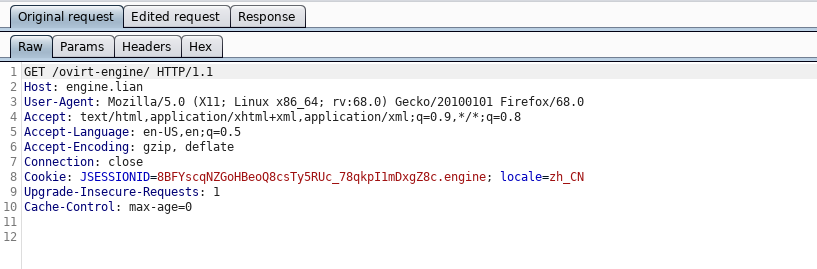
#### Vulnerability profile:

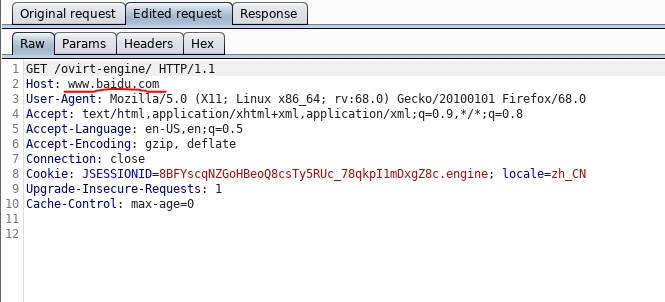
There is a URL redirection vulnerability in ovirt.-engine before version 4.3.9.An attacker can construct malicious URL parameters to redirect users to arbitrary URLs. By using this vulnerability, users can be induced to visit a page, Mount horses, password records, download arbitrary files, etc.

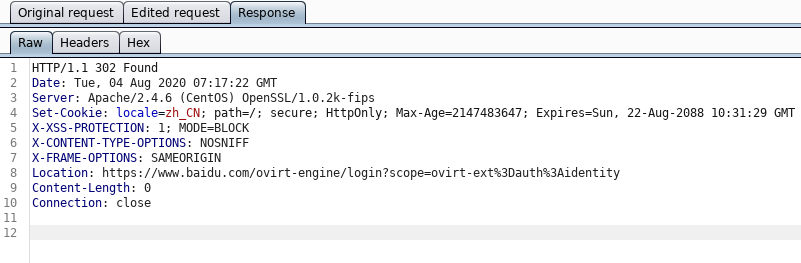
#### Affected version:

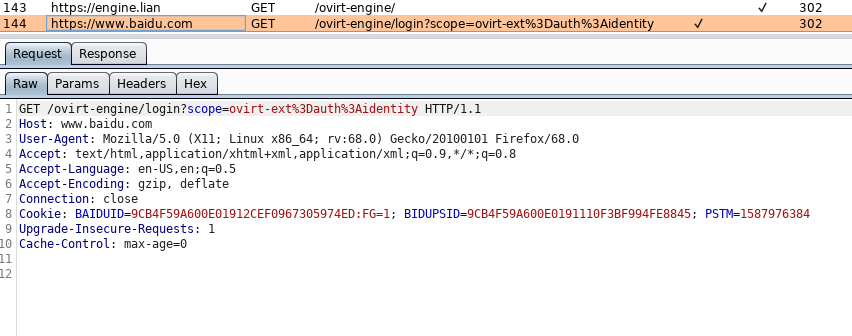
Ovirt engine 4.4 and earlier

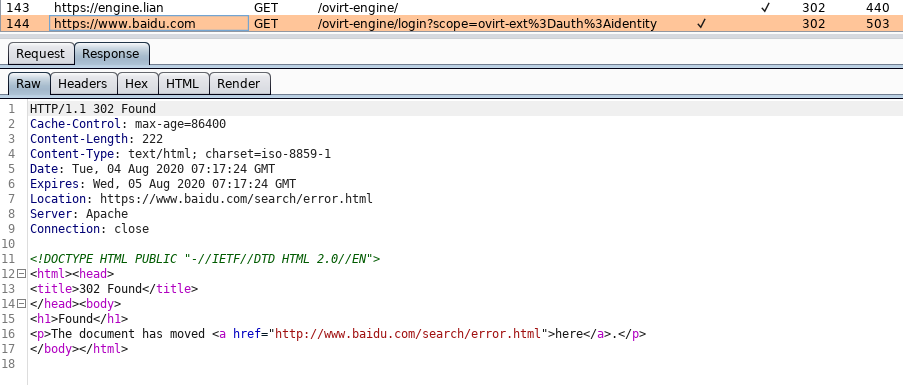
**Vulnerability verification:**

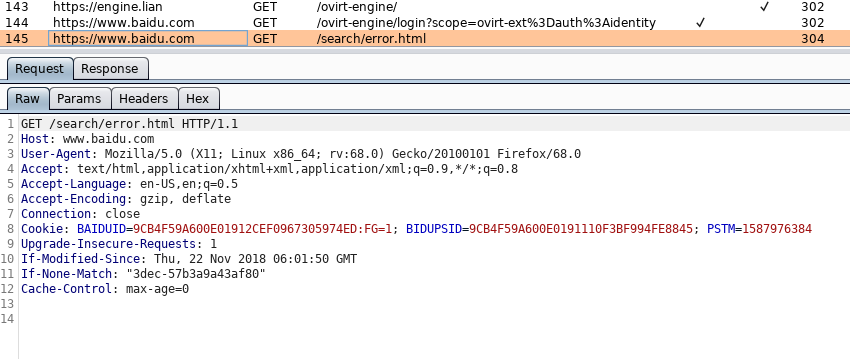
The vulnerability may be located in multiple pages, this test is the service home page, as follows: 

The vulnerability trigger point is located in the host parameter of the header. The system will jump the page according to the parameter, and the host can be modified directly, as shown below.

The response is 

After that, the system jumps to send the request header, and the host is our modified value 



Request failed, jump to www.baidu.com Error handling page. 



**Trigger condition:**

There are no restrictions