

Forum:[Hack Forums](#)

Thread: [HTTP Form-Based Digest Authentication](#)

DramaKing - November 12, 2022, 3:19 pm

I'm currently trying to find a way to bruteforce the password of a Reolink IP camera. I've tried OWASP ZAP, Burp Suite, hydra and the http-brute NSE script. None seem to work against this particular type of authentication. Medusa just returns a success message regardless of what credentials I feed it. HTTP POST request below.

```
POST http://192.168.1.20/cgi-bin/api.cgi?cmd=Login HTTP/1.1
Host: 192.168.1.20
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: /
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 338
Origin: https://192.168.1.20
Connection: keep-alive
Referer: https://192.168.1.20/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```

```
[{"cmd":"Login","action":0,"param":{"Version":1,"Digest":{"UserName":"admin","Realm":"IPC","Method":"POST","Uri":"cgi-bin/api.cgi?cmd=Login","Nonce":"f9e8a87b55a7ac5325f554caec14d6ccfa592c571ffbb4ed","Nc":"00000002","Cnonce":"cd63f2fdc350341e2c64375f8c841efdb219f265ca1610dc","Qop":"auth","Response":"ce9b0ce612622b727aa20209c0f8ce6b"}}}]
```

Brief - November 14, 2022, 6:28 am

That's some weird HTTP POST request right there. I cannot tell by looking at the request. In my experience, I had a similar issue like Medusa when my IP was blocked and Hydra output success for all wordlist. If I were you, I'll look into CORS policy and X-Requested header. If any of you know how they work for this particular site, I'd like to learn it.