Account Takeover [namelessmc.com] in namelessmc/nameless

0

Valid Reported on Aug 6th 2022

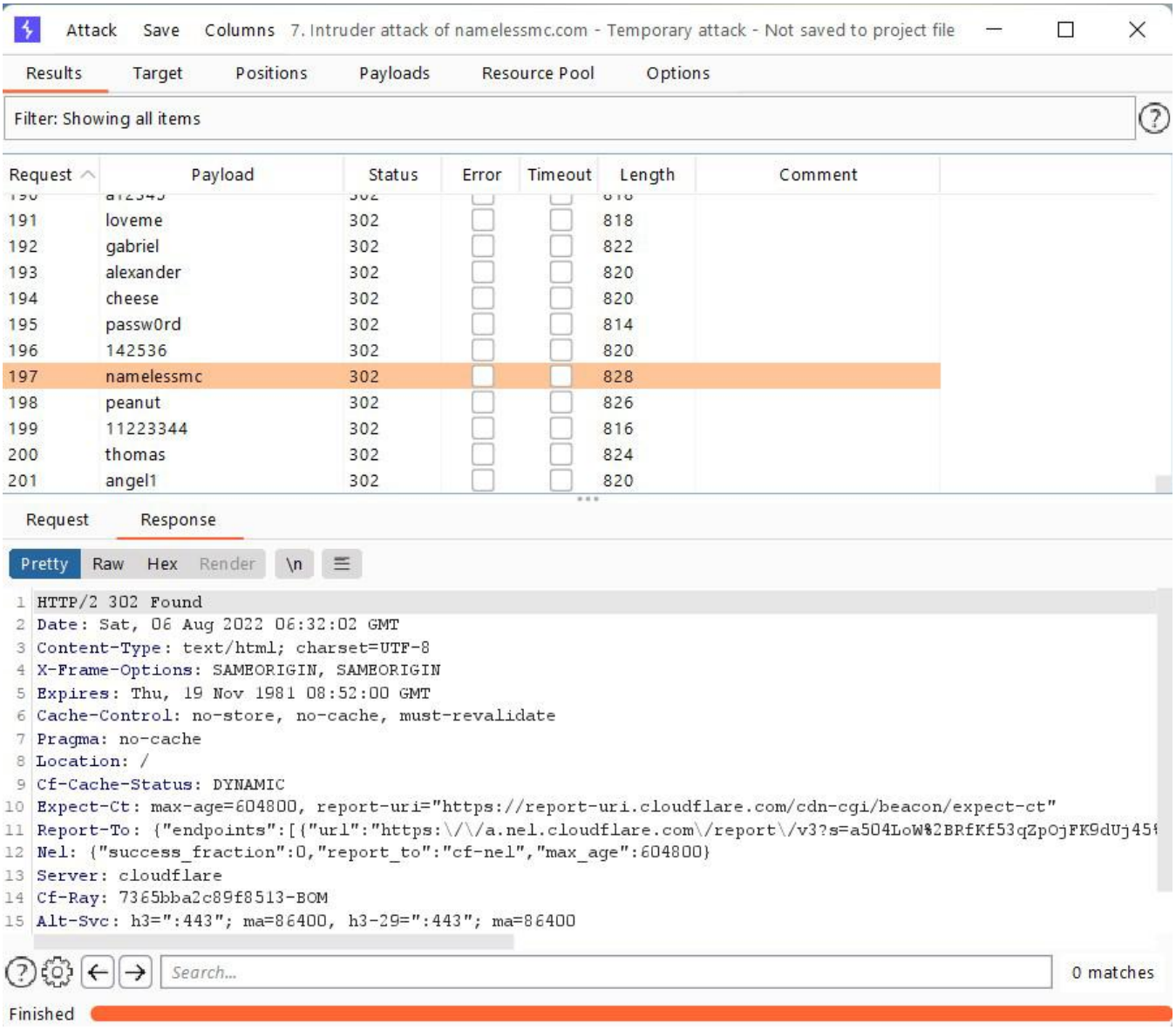
Description:

Hello team, while i was testing on `https://namelessmc.com/login/` i noticed that there is no ratelimit protection on POST login form, so an attacker can takeover the account by brute forcing the password field

Steps to reproduce:

1- go to `https://namelessmc.com/login/`
2- Enter username and any password
3- Capture the request with burpsuite and start bruteforcing with our wordlist

POC Screenshot:



Patch recommendation:

Add ratelimit protecion on POST login endpoints/parameters

Impact

Account takeover

Occurrences

login.php L1-L331

CVE
CVE-2022-2821

(Published)

Vulnerability Type
CWE-304: Missing Critical Step in Authentication

Severity
Critical (9.8)

Registry
Other

Affected Version
2.0.0

Visibility
Public

Status
Fixed

Found by

AGNIHACKERS
@agnihackers
amateur

This report was seen 614 times.

We are processing your report and will contact the **namelessmc/nameless** team within 24 hours. 4 months ago

We have contacted a member of the **namelessmc/nameless** team and are waiting to hear back 4 months ago

Sam validated this vulnerability 4 months ago

AGNIHACKERS has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

AGNIHACKERS 4 months ago Researcher

@maintainer are you happy to assign a CVE? please confirm, then only admin can move further

AGNIHACKERS 4 months ago Researcher

@Sam waiting for bounty . This is critical vulnerability.

AGNIHACKERS 4 months ago Researcher

@admin can you pls assign a CVE for this?

Jamie Slome 4 months ago Admin

Happy to assign a CVE once we get the go-ahead from the maintainer 👍

AGNIHACKERS 4 months ago Researcher

@maintainer are you happy to assign a CVE ? Please confirm

We have sent a fix follow up to the **namelessmc/nameless** team. We will try again in 7 days.
4 months ago

AGNIHACKERS 4 months ago Researcher

@maintainer are you happy to assign a CVE ? Please confirm

Sam 3 months ago

Hi, apologies for the delay.

Yes I am happy to go ahead with assigning a CVE.

Sam marked this as fixed in **v2.0.2** with commit **98fe4b** 3 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

login.php#L1-L331 has been validated ✔

AGNIHACKERS 3 months ago Researcher

@admin maintainer as given the permission for assigning CVE. So please assign a CVE for this report

Jamie Slome 3 months ago Admin

Sorted 👍

AGNIHACKERS 3 months ago Researcher

@admin waiting for bounty . This is critical vulnerability.

Jamie Slome 3 months ago Admin

There is no bounty for this report. You should see the potential bounty for a report when you submit it.

Sign in to join this conversation