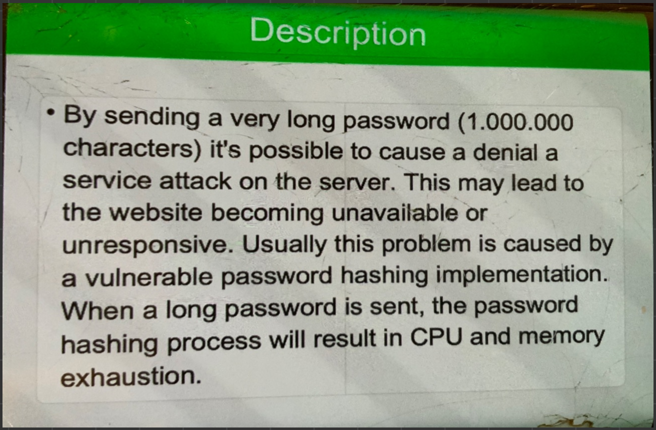
Long password Dos Attack

* Easy to find



Description

- By sending a very long password (1.000.000 characters) it's possible to cause a denial a service attack on the server. This may lead to the website becoming unavailable or unresponsive. Usually this problem is caused by a vulnerable password hashing implementation. When a long password is sent, the password hashing process will result in CPU and memory exhaustion.

* How to hunt ?

1. Try to sign up with long password.

a very long password ....
more then 1000 char.

* if any application or website accepting more then 500 characters then this is vulnerablility.

Background process:

plain text → hashing
↓
require resources like (RAM, CPU)

So if attacker entered more then 1000 character this need more resources, so Dos attack.

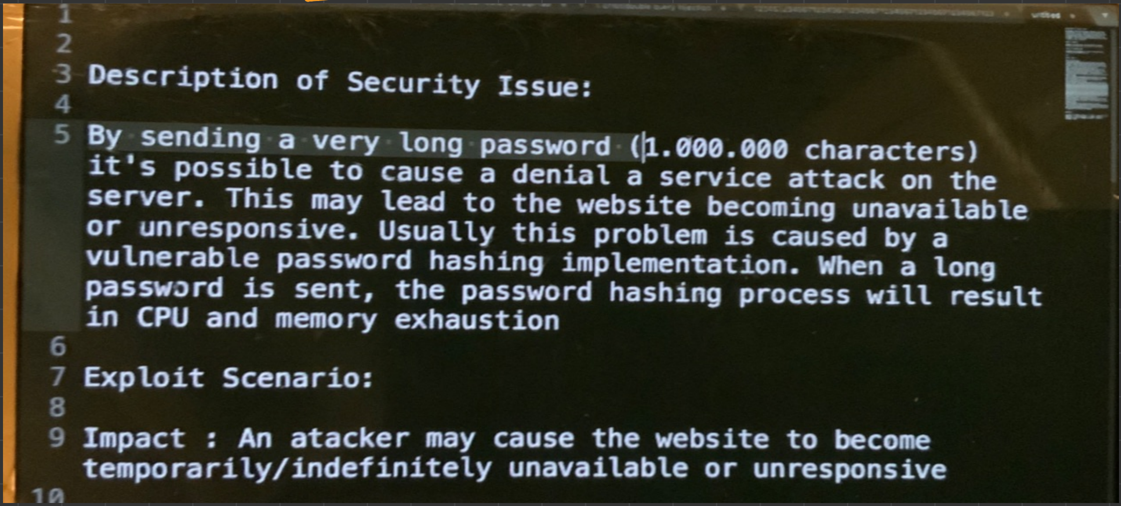
Solution:

there should be some limite.

Steps:

1. Sign in
2. intercept
3. put long password
4. accept ? — yes → vulnerable
   — no → secure

Report

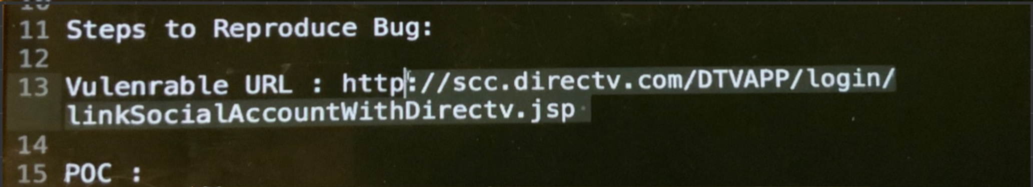


Description of Security Issue:

By sending a very long password (1.000.000 characters) it's possible to cause a denial a service attack on the server. This may lead to the website becoming unavailable or unresponsive. Usually this problem is caused by a vulnerable password hashing implementation. When a long password is sent, the password hashing process will result in CPU and memory exhaustion

Exploit Scenario:

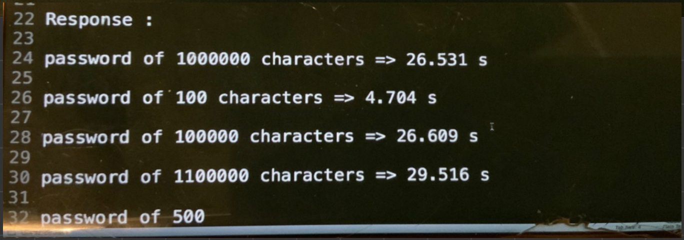
Impact : An atacker may cause the website to become temporarily/indefinitely unavailable or unresponsive



Steps to Reproduce Bug:

Vulenrable URL : http://scc.directv.com/DTVAPP/login/linkSocialAccountWithDirectv.jsp

POC :



```
Response :

password of 1000000 characters => 26.531 s

password of 100 characters => 4.704 s

password of 100000 characters => 26.609 s

password of 1100000 characters => 29.516 s

password of 500
```