Host Headers attack

Host headers attack is a piece of information that you can use in addition to IP address and port number to uniquely identify a web domain or as an application server .

بمعنى إن لو ربطت أكتر من موقع بنفس ال IP من خلاله هعرف أفتحه من أي موقع من خلال ال Host

EX: www.hello.com: 8443 → *port*

"ممكن أزوده أولًا" *additional*

Note : لو أنا غيرت قيمة ال Host لحاجة مش مفهومة تلقائي بيحولني لأول Virtual host

Virtual host : is a provider of web services that include server functions

And internet connection services .

توضيح : هي قيمة virtual بتساعدني في فكرة أكتر من موقع في نفس ال IP بحيث مثلًا لو الuser دخل www.non.com افتحله اللي في ال virtual رقم كذا .

Unvalidated redirection :

أي header

```
<? Php
$ host = "http://". S _ SERVER [ ' HTTP _ Hast ' ] ;
      echo $ host . "// Login.php";
          header [ "location :$ host / login.php"];
```

إطبعه

حول اليوزر للصفحة دي ?>

Password Reset:

one of Common functionality in most app is the ability to reset user's password . the user clicks a forgot passwords link and the server sends a password reset link to the email account Configured for the user account the link includes a one time token and allows the user to set a new password without having to specify the old one.

EX:

$resetPasswordURL = "https://{$_SERVER['HTTP_HOST']}/reset-password.php?token=12345678-1234-1234-1234-12345678901";

توضيح : هي ثغرة بتمكني إني أقدر أغير باسورد اليوزر عن طريق إني أغير الصفحة اللي هيروح عليها لصفحة خاصة بيا و بالتالي أقدر أشوف ال lags عليها.

اسم الموقع + virtual host name enumartion

tool

https://hackerone.com/reports/698416

https://hackerone.com/reports/13286

https://hackerone.com/reports/158019

https://hackerone.com/reports/182670

https://hackerone.com/reports/170333

https://hackerone.com/reports/601287

https://hackerone.com/reports/221908

https://hackerone.com/reports/180196

https://hackerone.com/reports/167809

https://hackerone.com/reports/158482

https://hackerone.com/reports/94637

https://hackerone.com/reports/7357

https://hackerone.com/reports/283786

https://hackerone.com/reports/301592

https://hackerone.com/reports/277192

https://github.com/udacity/fcnd-issue-reports/issues/361

https://hackerone.com/reports/170333

/https://pethuraj.com/blog/how-i-earned-800-for-host-header-injection-vulnerability

https://sites.google.com/site/testsitehacking/10k-host-header

/https://www.acunetix.com/blog/articles/automated-detection-of-host-header-attacks