Host header attack

Host server is hosting many websites and web application on the same IP, so we need headers to know which site is the client calling.
So this is why host header attack is happening.

* Browse a website → send request to burpsuit → change host parameter to another website, so if the request directed you to the another website, there is a host header attack, else go home.

* Host header attack hunting

* Spider the host and in target burpsuit Tab try to Find URL having status code of 2xx or 3xx → Send them to repeater and test the following method

or 1) Change real host to bing.com.

or 2) Change Host from real website to bing.com & set X-Forwarded-Host to real website.

or 3) Set X-Forwarded-Host to bing.com & Host to realwebsite.

→ if non of the above methode works, it means the website is secure.

* Host header attack on password reset page.

Ebrahim Elhegazy:

exploit:

- access local resources
- Unvalidated redirections
- password reset vuln.
- XSS in Header attack.

* access local resource

Set any word in field Host: anyword -> server will send the value to the first virtual hostname he has.

* try Host: localhost, dev, stage, test

if the domain dev.any.com set Host: dev

* unvalidated redirection

```php
<?php
$host = "http://".$_SERVER['HTTP_HOST'];
echo $host."/login.php";
header("Location: $host/login.php");
?>
```

this is self behavoir

* password reset vulnerability

Create an account on the website -> reset password -> intercept request -> change Host: to any thing.
-> go to email see if he change the Host.

* XSS Via Host header

(it is self behavior).

Host: any.com "><svg onload=alert(1)>

> tool automatic virtual-host-discover

*password reset poisoning

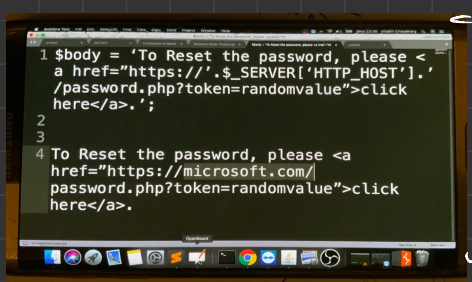
App
↓
Forget password page
↓
this page is vulnerable by
Host Header attack.
↓
input -> email-id :
↓
they will send you email
↓
email contents You can reset
your password via blew link :
http://target.com/password-reset.php ? token = ----

So if attacker can steal this token, he can reset your password.

* How we gonna take this token ?

example :

yammar.com
↓
forgot password
↓
input -> email :
they will send me an email like this :
https://yammer.com/token = ----



test if there is a header attack

I will capture this request with burpsuit and Change host to bing.com. So the the victim will receive a link like this https://bing.com/token = ----
then this is vulnerability. because if I put my site and on my site I have sniffer, so I will be able to steal the token and reset the password.