Host Header Injection

1-تعريفها: أحيانا بيكون في ويب سيرفر عليه أكتر من من ويب ابليكشن ف لما نيجي نبعت ريكوست لـ IP موقع من التلاتة المفروض الويب سيرفر يعرف الريكوست لاي موقع بالظبط وعشان كده موجود الهيدر الي اسمه Host عشان يحدد السيرفر منه انا بطلب أي موقع من المواقع الي ليها نفس الـIP.

2-بستغلها إزاي: هو في طريقتين عشان تستغل الثغرة دي:

- الاولي عن طريق إنك بتغير الـ Host Header وتخليه حاجة أي موقع زي evil.com أوbing.com
- التانية عن طريق الـ X-Forwarded-Host Header وده وظيفته إنه بيعيد كتابة الـ Host Header
- وهنا مثال للكود الضعيف :

```
<script src="http://<?php echo _SERVER['HOST'] ?>/script.js">
```

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

فـ هنا لو بدلنا الـ HTTP Host Header بـ أي Host تاني هيكمل عادي.

3-بتسبب ايه: ثغرة الـ Host Header Injection بتسبب حاجتين رئيسيتين:

- Web cache Posioning : ودي فيها بنتلاعب بالـ cache بتاع الموقع ونقدم محتوى غير الموجود, يعني الينكات الي موجودة في الموقع بتخليها تروح ع موقع من اختيارك وكأنها مواقع معتمدة لان اللينك بتاعها جاي من الموقع الأصلي نفسه.
- abuses of alternative channels for conducting sensitive operations, such as password resets : في الطبيعي لما بنعمل reset password ونكتب الاميل بتاعنا بيروح يعمل توكين ويبعته في لينك على الاميل الي كتبناه وبالتالي لما ندوس عليه هيودينا على صفحة تغيير الباسورد للاميل ده, طيب ولو كتبنا الـ Hostموقع من عندنا إحنا وموقع يكون تبعنا؟ كده الموقع هيبعت التوكين للموقع بتاعي وهنا هاخد التوكين واروح اغير انا الباسورد للـvictim.

4-بلاقيها إزاي بالبرب:

- 1-أول حاجة بتعمل intercept لريكوست الدومين الرئيسي زيwww.example.com
- 2-بتعمل spider للريكوست دي وبعدين بتشوف أي URL تكون الـ status code بتاعته 300/200
- 3-أول حاجة بتجرب تغير الـ Host وبعدين بتحاول تضيف X-Forwarded-Host لو فشلت الأولى, بس الـ Hostيكون فيه الـ invalid host والـ X-Forwarded-Host يكون الـ real host وبعدين تبدلهم.
- 4-جرب الخطوة (3) على URl يكون 201 وبعدين على URL يكون 301.
  ```

- -5وانت بتجرب تغير الـ Host او باقي الخطوات سيرش على الـ invalid host الي كتبته في الـ response عشان ممكن متكونش open redirect ولكن تكون web cache poisoning.

-5سيناريوهات:

- -1بتجرب في الدومين الرئيسي/اي صبدومين تغير الـ Host وبعدين تشوف الـ location واخد قيمة ايه أو هل في لينك اتغيرت قيمته في الصفحة واخد قيمة الـ Host الجديد؟
- -2لو حصل وإن الموقع منع تغيير الـ Host وبيجبلك response 404 Not-Found هنا بتستخدم X-Forwarded-Hostعشان تعمل bypass.
- -3طريقة تاني لـلـ Bypass وهو إنك بتستخدم إتنين Host الأول بيكون بتاع الموقع الصحيح والتاني بيكون الـ malicious.
- -4لو الثغرة دي موجودة في صفحة reset password, فـ أنت لما بتيجي تعمل reset password هو بيـ createلينك وبيعته للاميل المحدد, فـ اللينك الي بيتـ create بياخد قيمة الـ Host HEADER ف لو كتبت evil.comمثلا, بيروح يبقى اللينك :

https://evil.com/reset-password.php?token=765694144h5g8525f52v2255fd55d5

ف الـ victim لما يدوس على اللينك انا هاخد التوكين واروح اغير الباسورد وعشان يبقى الامر اسهل بتخبي اللينك جوا button بحيث الـ victim ميشوفش اللينك.

- أي function التطبيق بيبعت فيها لينك على الاميل او بيـ create لينك تقدر تجرب فيه الثغرة.
- لو حصل web cache poisoning والـ invaild host اتطبع في الصفحة ممكن تجرب تكتب XSS Payload.
- ممكن تيجي تدخل على admi panel فيرفض بناءاً على الـ HOST header لو كان interal بيوافق، ف وقتها بتخلي قيمة الـ HOST header هي الـ localhost.
- لو الموقع بيعمل cache للصفحة الرئيسية أو صفحات تاني، جرب تغير قيمة الـ HOST لو الريسبونس 504 جرب تضيف HOST header تاني وتكون قيمته هي السيرفر الخاص بيك، وشوف في الريسبونس الدومين بيتضاف فين، لو في ملف JS ف اعمل ملف جافاسكريبت يكون الكود بتاعه إن يبعت الكوكي بتاعة اليوزر للسيرفر بتاعك مثلا، وبعدين تحاول تعمل cache للصفحة دي بحيث كل يوزر هيطلب الصفحة هيتنفذ عليه الكود.
- لو الـ Load-balancer أو revers-proxy بيعمل Routing للريكوستس بناءاً على الـHost header ف ممكن نستغله في إننا نعمل SSRF attack ونخليه يعمل تيست لـ Internal IP ranges لعل نلاقي IP ونلاقي عليه حاجة مهمة وده بيُسمى Routing-based SSRF.
- لو بتغير في الـ HOST وبيديك 403 ف جرب تستخدم الـ URL كامل في الريكوست زي https://example.com وبعدين تغير الـ HOST، غالبا هنا هيعمل check للـ Absolute URL وهيعدي الـ HOST عادي.
- جرب سيناريو Password reset poisoning via dangling markup وده ف حالة إنه بيبعتلك الباسورد في الأميل، ف بتحاول تاخد جزء من الريسبونس الي فيه الباسورد وتبعته على الميل بتاعك.

-6نمنعها إزاي:

- هنروح لملف الـ config.ini ونضيف السطر ده

```
[APPLICATION]

BASE_URL=example.com
```

وبعدين الكود نخليه بالشكل ده (بدل الكود الضعيف في النقطة 2(

```
resetPasswordURL = "https://" . get_config('APPLICATION', 'BASE_URL') . "/reset-password.php?token=12345678-1234-1234-1234-12345678901";
```