

bWAPP

Host Header Attack (Cache Poisoning)

Tổng quan về Host Header Attack:

- Host Header Attack là gì?

Host Header Attack (hay còn gọi là host header injection hoặc host header poisoning) là một loại lỗ hổng trong các ứng dụng web trong đó kẻ tấn công thao túng tiêu đề máy chủ trong yêu cầu HTTP để khai thác khả năng xử lý tiêu đề của ứng dụng. Tiêu đề máy chủ là một phần của giao thức HTTP chỉ định tên máy chủ của trang web. Nó được máy chủ web sử dụng để xác định máy chủ ảo hoặc trang web mà yêu cầu dành cho. Trong một cuộc tấn công tiêu đề máy chủ, kẻ tấn công có thể sửa đổi giá trị tiêu đề máy chủ để lừa ứng dụng web xử lý yêu cầu như thể nó được dành cho một trang web khác.

Giờ ta sẽ khai thác lỗ hổng này trên trang web bWAPP

Đây là hiển thị của trang web

/ Host Header Attack (Cache Poisoning) /

Click [here](#) to go back to the portal.

Khi ta ấn vào nút “here” thì nó sẽ trả về trang web đầu tiên

/ Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project! It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

----- bWAPP v2.2 -----

/ A1 - Injection /

HTML Injection - Reflected (GET)

HTML Injection - Reflected (POST)

HTML Injection - Reflected (Current URL)

HTML Injection - Stored (Blog)

iFrame Injection

LDAP Injection (Search)

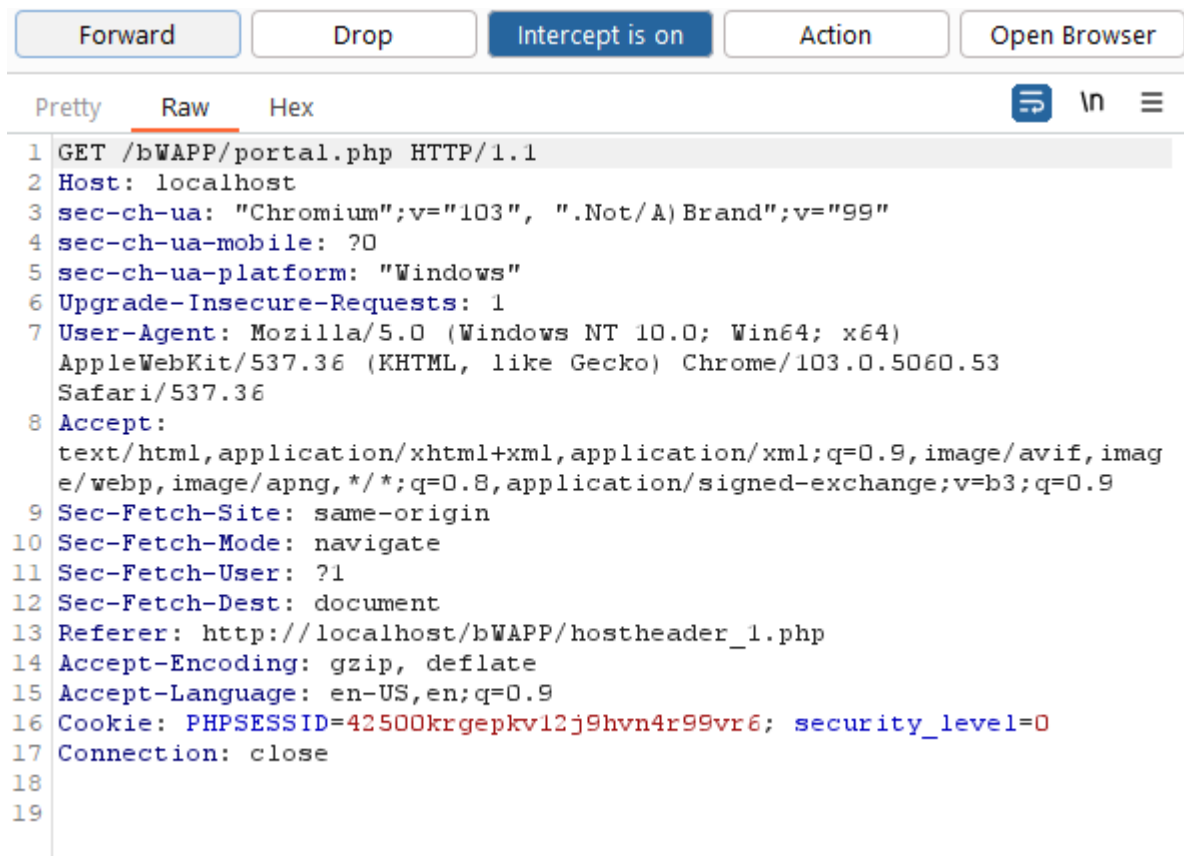
Mail Header Injection (SMTP)

Hack

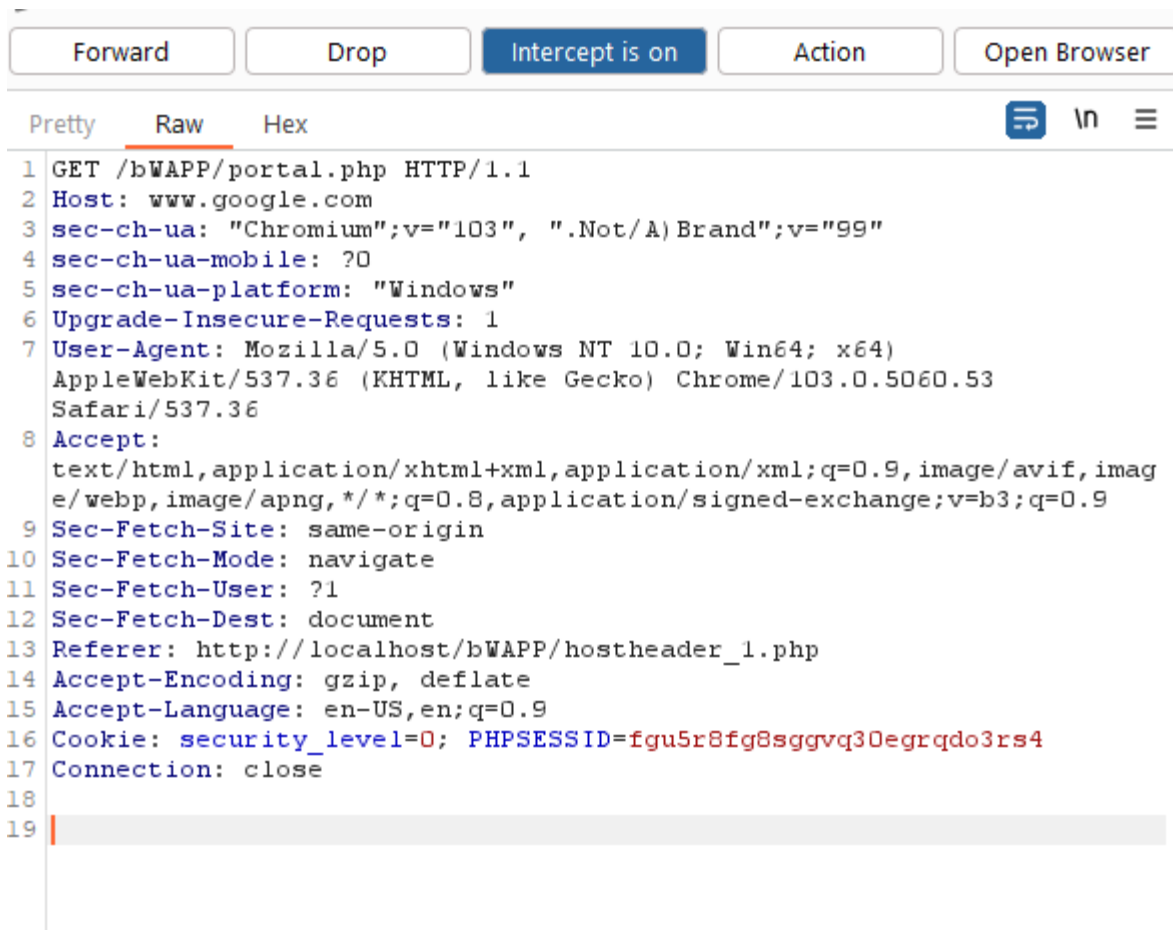


NATION
CENTER
MIS
EXP
C H I

Giờ ta sẽ thử mở Burp Suite và cho trang web này vào Proxy sau đó bật Intercept lên để xem ta có gì



Đây là kết quả sau khi ta ấn nút here, giờ ta sẽ thử đổi host của nó thành một cái gì khác xem sao



Và đây là kết quả ta nhận được

bWAPP

an extremely buggy web app !

[Bugs](#) [Change Password](#) [Create User](#) [Set Security Level](#) [Reset Credits](#) [Blog](#) [Logout](#) [Welcome Ndx](#)

Host Header Attack (Cache Poisoning)

Click [here](#) to go back to the portal.



bWAPP is licensed under © 2014 MME BVBA / Follow [@MME_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive [training](#)?



Set your security level:

Current: **low**

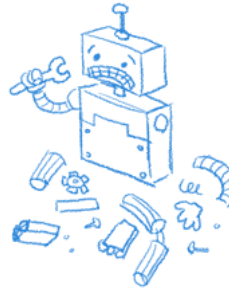
Choose your bug:

Sau khi ta tắt Intercept và click here thì đây là kết quả ta nhận được



404. That's an error.

The requested URL /bWAPP/portal.php was not found on this server. That's all we know.



Đường link đã chuyển đến

<http://www.google.com/bWAPP/portal.php>

Vậy là chúng ta đã thành công Host Header Attack.

Lên đến level Medium thì ta đã không thể tìm như vậy nữa nên gần như không thể khai thác tiếp được level trên