**bWAPP**

**Session Management**

Tổng quan về Session Management:

**- Session Management là gì?**

Session Management là thông tin tạm thời và tương tác trao đổi giữa máy khách và máy chủ, Session Management là quá trình theo dõi hoạt động của người dùng trong các phiên tương tác với hệ thống máy tính, chẳng hạn như: đăng nhập, đăng xuất, … Session Management có thể liên quan đến việc yêu cầu người dùng đăng nhập lại nếu phiên đã hết hạn. Nếu lỗ hổng được kể tấn công tìm thấy, ké tấn công có thể khai thác lỗ hổng xác thực bị hỏng hoặc chiếm đoạt tài khoản

Chúng ta sẽ đi qua toàn bộ các bài liên quan đến Session Management gồm 5 bài: “Administrative Portals”, “Cookies (HTTPOnly)”, “Cookies (Secure)”, “Session ID in URL”, “Strong Sessions”

**Session Mgmt. - Administrative Portals**

Đầu tiên chúng ta sẽ thử với level Low trước

Đây là giao diện của trang web



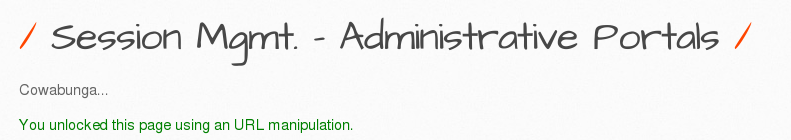
Và chúng ta có thể nhìn thấy đường trang web đã bị chặn và có thể nhìn thấy trên URL

<http://localhost/bWAPP/smgmt_admin_portal.php?admin=0>

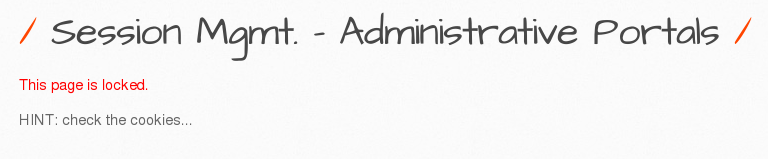
Có admin = 0 và giờ ta sẽ thử điều chỉnh admin = 1 xem ta sẽ thu được gì

[http://localhost/bWAPP/smgmt\_admin\_portal.php?admin=](http://localhost/bWAPP/smgmt_admin_portal.php?admin=0)1

Và ta sẽ có kết quả



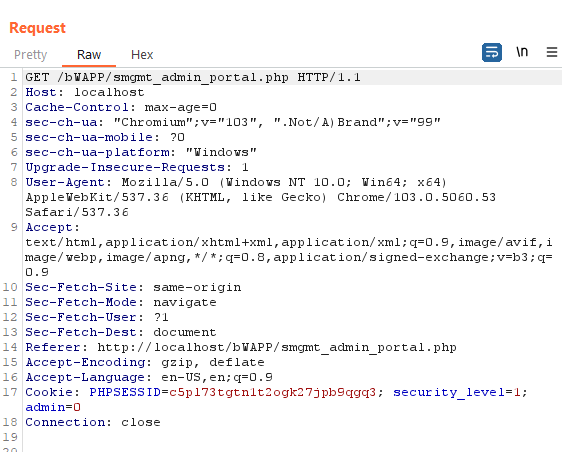
Vậy là ta đã thành công đi qua level Low giờ ta sẽ chuyển sang level Medium



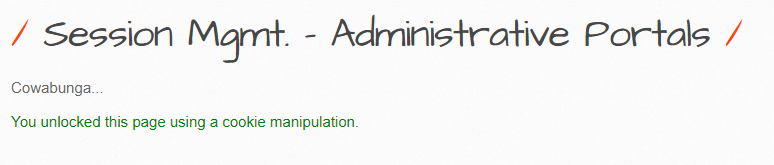
Trang web lại tiếp tục bị khóa và trên URL cũng không để lộ phân quyền của user trên URL nữa

http://localhost/bWAPP/smgmt\_admin\_portal.php

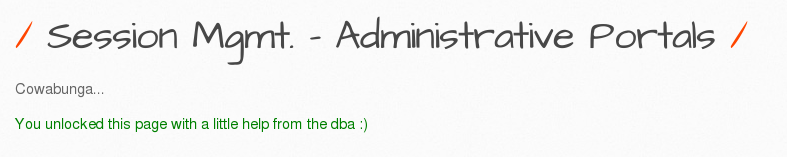
Vậy chúng ta sẽ sử dụng Burp Suite để xem ta có thể làm gì với nó



Sau khi sử dụng Burp Suite ta đã có thể nhìn thấy được Cookie để truy cập và hơn nữa ta thấy được admin=0. Vậy cũng giống như với level Low ta sẽ thay đổi admin=1 xem kết quả ta nhận được là gì



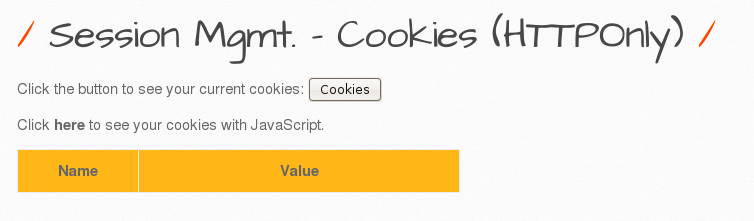
Vậy chúng ta đã thành công đi qua level Medium của bài này và giờ ta sẽ thử xem level High của nó sẽ như thế nào



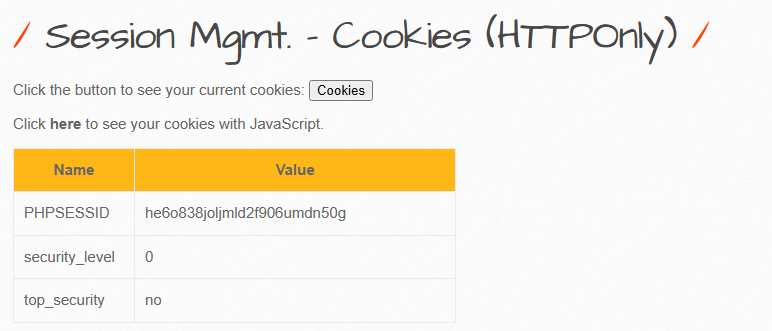
Có vẻ như trang web đã không bị khóa và chúng ta đã được giúp đỡ bởi Database Administator và không có gì để khai thác ở level này nữa. Vậy là ta đã thành công đi qua cả 3 level của bài Administrative Portals

**Session Mgmt. - Cookies (HTTPOnly)**

Đây là giao diện của trang web



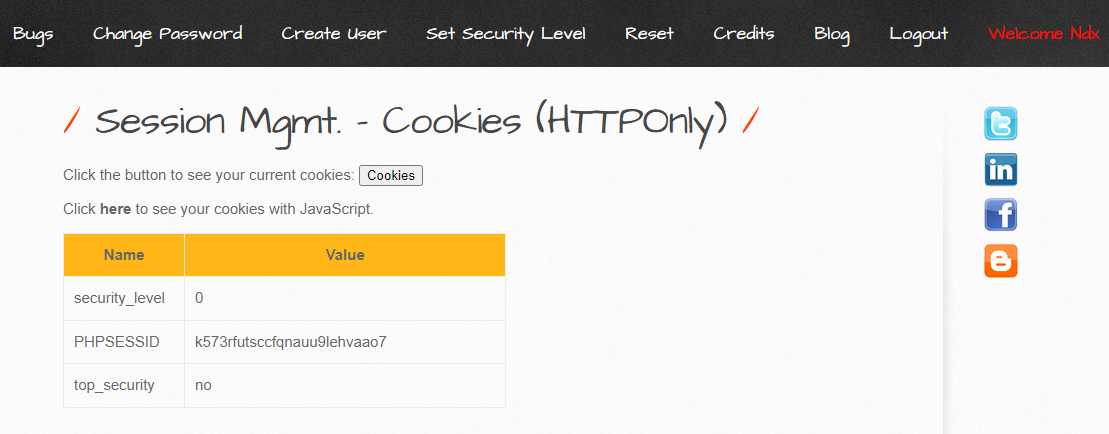
Ta ấn vào nút Cookies để xem Cookies của user bee



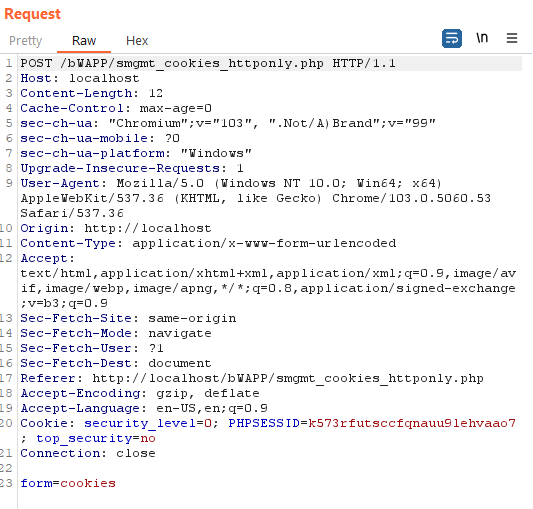
he6o838joljmld2f906umdn50g

Giờ ta sẽ tạo một tài khoản để có thể lấy một Cookies khác. Và tôi đã tạo một user là NDX và có Cookies là

k573rfutsccfqnauu9lehvaao7



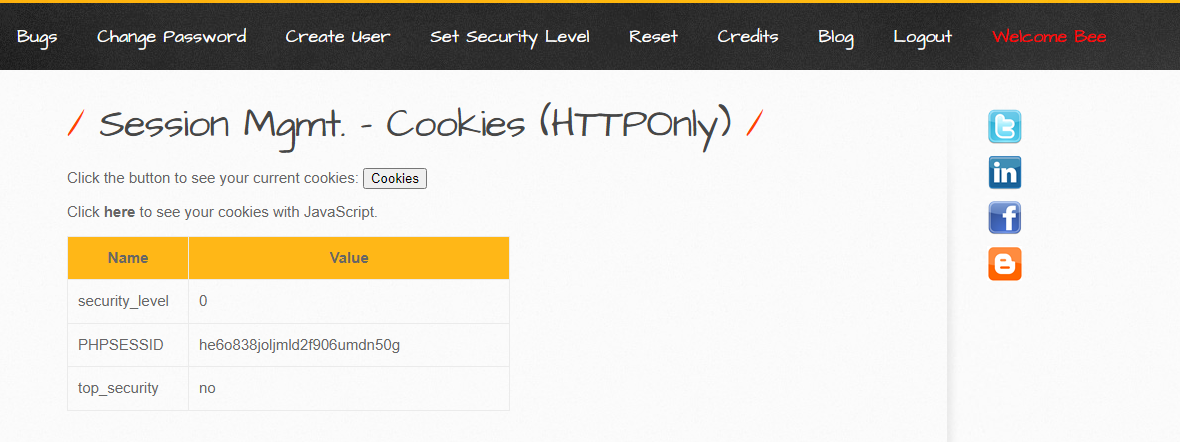
Giờ ta sẽ vào Burp Suite



Ta sẽ thay đổi cookie của user NDX thành cookie của user bee



Và ta sẽ có kết quả là chúng ta có thể vào được user bee khi chúng ta có cookie của user đó



Điều này chỉ có thể thực hiện khi cookies của user bee vẫn còn có hiệu lực

Và với level Medium thì các thức thực hiện cũng giống hệt với level low. Còn với level High thì trong source code của trang web ta có thể thấy được

case "2" :

// The cookie will be available within the entire domain

// The cookie expires at end of the session

// Sets the Http Only flag

setcookie("top\_security", "yes", time()+300, "/", "", false, true);

break;

Là nó sẽ ngay lập tức hết phiên nên gần như không có lỗ hổng mà ta có thể khai thác được tiếp

**Session Mgmt. - Cookies (Secure)**

Đối với bài này thì cách thức làm bài giống hệ như với Session Mgmt. - Cookies (HTTPOnly)

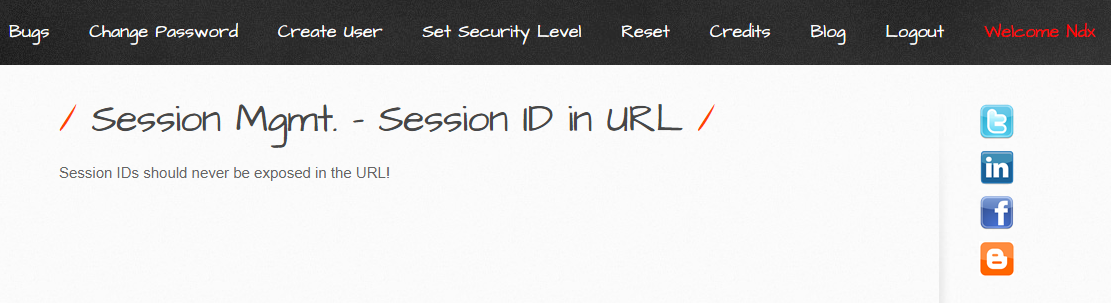
Sự khác bieeth của HttpOnly và Secure

HttpOnly có tác dụng làm cho cookie chỉ được thao tác bởi server mà không bị thao tác bởi các script phía người dùng

Secure có tác dugnj làm cho trình duyệt phải sử dụng kết nối bảo mật mã hóa, nhưng nó chỉ hoạt động khi server có sử dụng SSL(HTTPs). Nhưng tuy rằng thông tin đã được mã hóa thì vẫn có thể bị truy cập bởi bên thứ 3

**Session Mgmt. - Session ID in URL**

Đối với bài này thì cookie đã bị lộ ra ngay trên URL



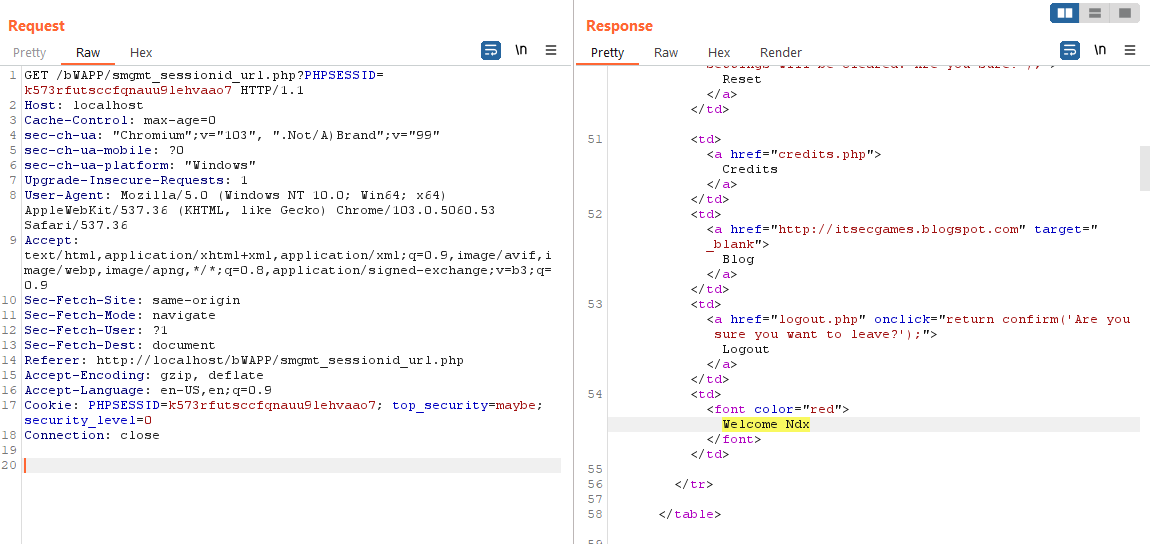
Trang web này có URL như sau

<http://localhost/bWAPP/smgmt_sessionid_url.php?PHPSESSID=k573rfutsccfqnauu9lehvaao7>

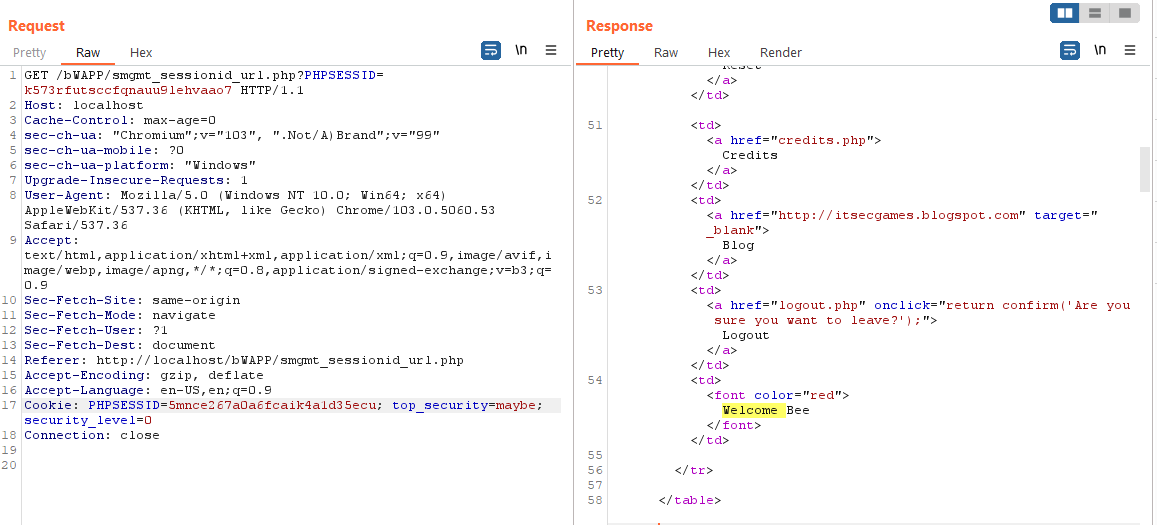
Giờ ta đã biêt được cookie của user Ndx giờ ta sẽ xem cookie của user bee

<http://localhost/bWAPP/smgmt_sessionid_url.php?PHPSESSID=5mnce267a0a6fcaik4a1d35ecu>

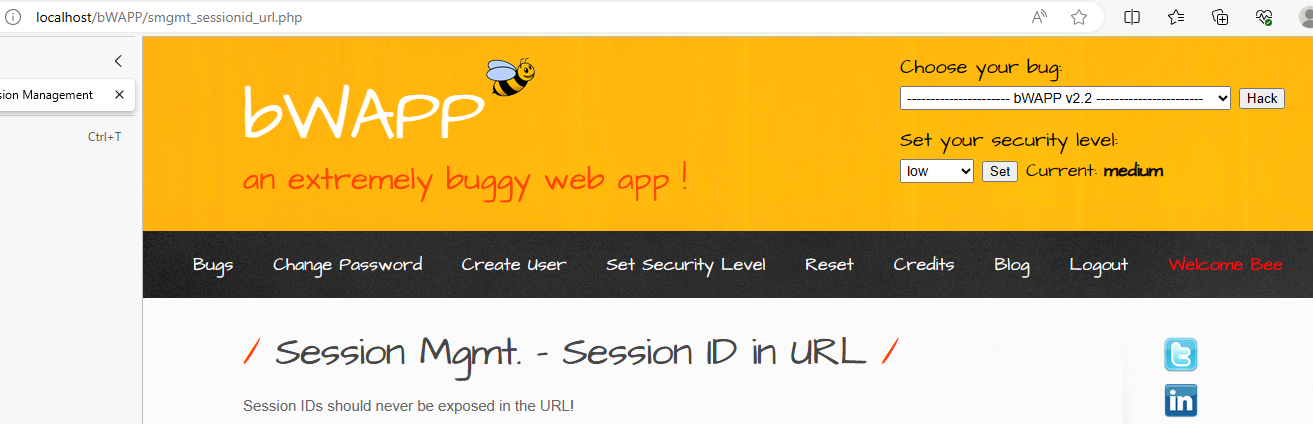
Giờ ta sẽ tiếp tục sử dụng Burp Suite để có thể thử nhiều hơn



Hiện tại đây là trang web có cookie của user Ndx giờ ta sẽ thay cookie sang của user bee



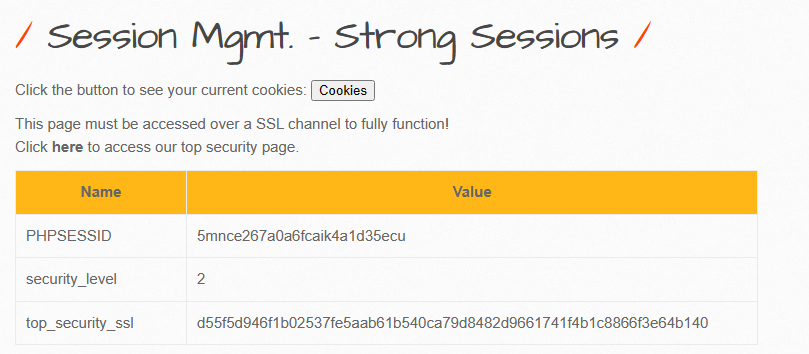
Vậy là chúng ta đã thành công đi qua level Low của bài này ta sẽ lên thử level Medium của nó



Trang web đã không còn hiển thị cookie trên URL nữa vậy là không còn gì chúng ta có thể khai thác tại bài này nữa ta sẽ đi qua bài tiếp theo

**Session Mgmt. - Strong Sessions**

Ở bài này cho ta thấy được khi kết hợp cả 2 HTTPOnly và Secure thì trang web của bạn sẽ được bảo mật hơn nhưng ở level Low và Medium vẫn chỉ là lấy cookie của các user chèn vào Burp Suite để truy cập bất hợp pháp khi ở level Medium bạn chỉ nên lấy cookie để có thể truy cập còn ở Level High bạn sẽ phải có cả cookie và SSL channel của phiên đăng nhập đó thì bạn mới có thể đi qua được



Và tôi nghĩ là ở những trang web bên ngoài cũng không ai để lộ SSL ra cả nên có vẻ level High đã là một cách bảo vệ phiên tốt nhất có thể, không những vậy những trang web hiện nay còn ẩn cả cookie của phiên đăng nhập và phải có những biện pháp khác mới có thể lấy được cookie của người dùng nên tôi nghĩ như vậy đã là cách bảo vệ phiên đăng nhập tốt mà ta có thể làm