M10915027 石成峰 HW3

[Get Started]

1. 先呼叫create創立一個題目的合約。
2. 呼叫題目合約中的callme將win變為true。
3. 將server給的token傳進validate放出信號讓server收到。
4. server收到後給出flag。

[Private]

1. 從合約中可以看出constructor之後flag的值就沒有變動。
2. 查詢合約位址的第一個儲存位置得到flag。

[ReEntrancy]

1. 撰寫一個hack合約，他的receive會再次呼叫withdraw。
2. 發布hack合約，讓他呼叫create創建題目。
3. 讓hack呼叫題目的withdraw，收到錢後會再次呼叫。
4. 由於還沒有結束所以沒有扣錢，可以再次收到。
5. 將題目的錢領光後送出token給validate。
6. server收到信號後給出flag。

[Bet]

1. 發布hack合約，讓他呼叫create創建題目。
2. 讓hack用題目的算法算出他的getRandom函數。
3. 使用算出來的值呼叫題目的Bet。
4. 由於在同一個時間及區塊上所以值會一樣。
5. 將題目的錢贏光後送出token給validate。
6. server收到信號後給出flag。