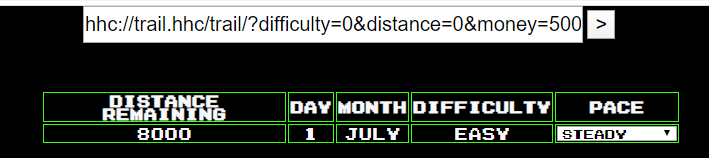
# Basic Web Attacks—Holiday Hack Trail—KEY

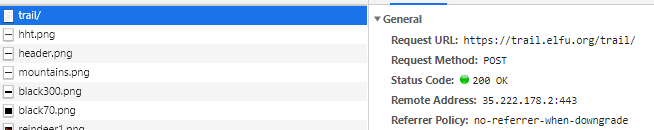
## Easy Mode

### Questions

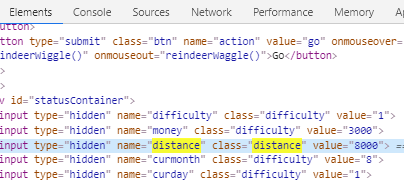
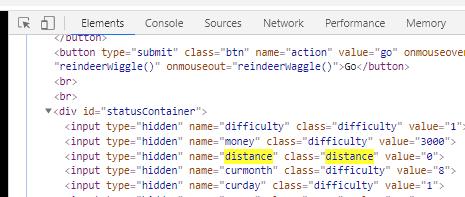
1. How did you change the request so that you won the game?  
     
   The simplest way is to click distance in the URL and change it to 8000. Note that the top left of the web page displays the distance left to go and the browser sends distance traveled to the site. Distance left to go plus distance traveled = 8000
2. What could the web designer do to prevent you from cheating this way?  
     
   They can make tricky algorithms in the browser to make changes easy to detect. When we get to Hard mode, the developer has implemented an algorithm to detect changes. The problem is that any algorithms in the browser are available to the attacker as well and can be broken. The best way is to keep the official copy of the data on the server.
3. What was the request method the browser used?  
     
   The challenge designer has crafted the site to look like it is using the GET method.   
   However, if you look behind the scenes, he is using POST. The correct answer for the students is GET.

## Medium Difficulty Mode

### Questions

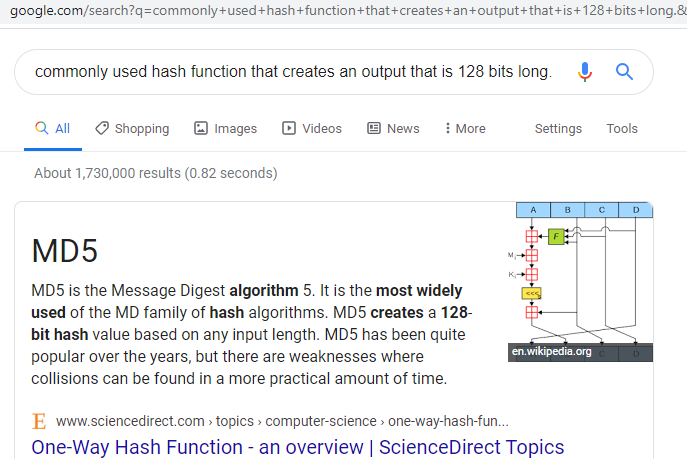
1. What was the HTTP Request Method the browser used? (GET, HEAD, POST, CONNECT, and TRACE are possible answers.)  
   POST  
   
2. What status code did the server return?  
     
   200 OK. It means everything is fine, here’s your data.
3. What is the IP address of the web server?  
   35.222.178.2

### Questions

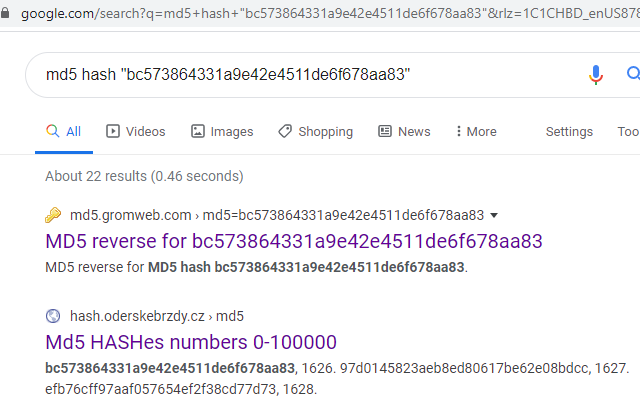
1. What did you do to win the game?  
   Change distance to 8000 and click GO.  
     
   Distance before and after change—0 before and 8000 after.

## HARD Mode

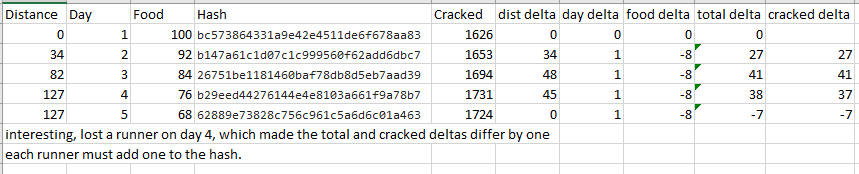
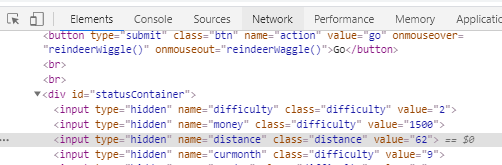
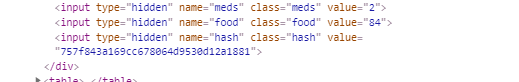
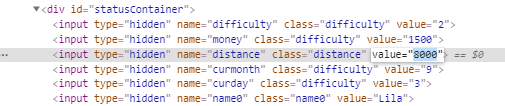
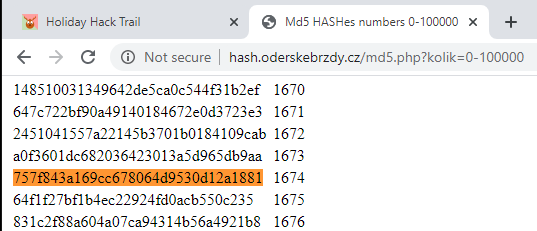
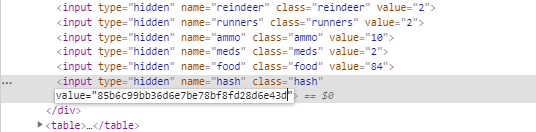
### Question

1. What is, most likely, the hash function that created the hash in the image above?  
     
     
   MD5 is the hash algorithm

### Question

1. What was the input to the hash function, so that "bc573864331a9e42e4511de6f678aa83" was the output?  
     
     
   1626 was the input to the hash.

### Questions

1. What is the relationship between the change in distance and the change in number that is hashed?  
     
   After clicking GO several times at the beginning of the game, I noticed that Distance, Day, and Food were usually the only parameters that changed. That prompted me to make this spreadsheet.  
     
   change in hashed number = change in distance (as long as nothing else changes)
2. How did you beat the game?  
     
   To make it more interesting, I clicked GO a couple of times to get a distance to go that was not 8000.  
     
   Original Distance = 62  
     
     
   The hash right now is 757f843a169cc678064d9530d12a1881  
     
     
   Change distance to 8000  
     
     
   The original hash was 757f843a169cc678064d9530d12a1881. Cracked, that’s 1674.  
     
     
   Distance changed by 8000 – 62 = 7938  
   Distance increased by 7938, so hashed number needs to increase by 7938  
   1674 + 7938 = 9612  
   Hash 9612 to get new hash  
     
     
   Put 85b6c99bb36d6e7be78bf8fd28d6e43d in for the new hash.  
     
     
   Click GO  
   
3. Can you think of a way that this vulnerability could be fixed? Remember that any code on the browser can be studied or changed by the attacker.  
     
   Keep the official copy of the data on the server. Don’t trust the user or the browser!!