Tryhackme - Learning Cybersecurity

<https://tryhackme.com/room/beginnerpathintro>

Room Description: Get a short introduction to a few of the security topics you'll be learning about.

***Task 1: Web Application Security***

**Why understanding how the web works is important**

To attack web applications, you need to understand how they work. Hacking websites isn't some magical process but does come down to knowing how a part of a website functions and being able to identify weaknesses to take advantage of. Once you have a good understanding of the fundamentals, you'll learn about the techniques and tools used in hacking sites.

If something is vulnerable, it means there is the possibility of it being attacked or harmed. If an application or system has a vulnerability, there is something that can be attacked or taken advantage of (a weakness).

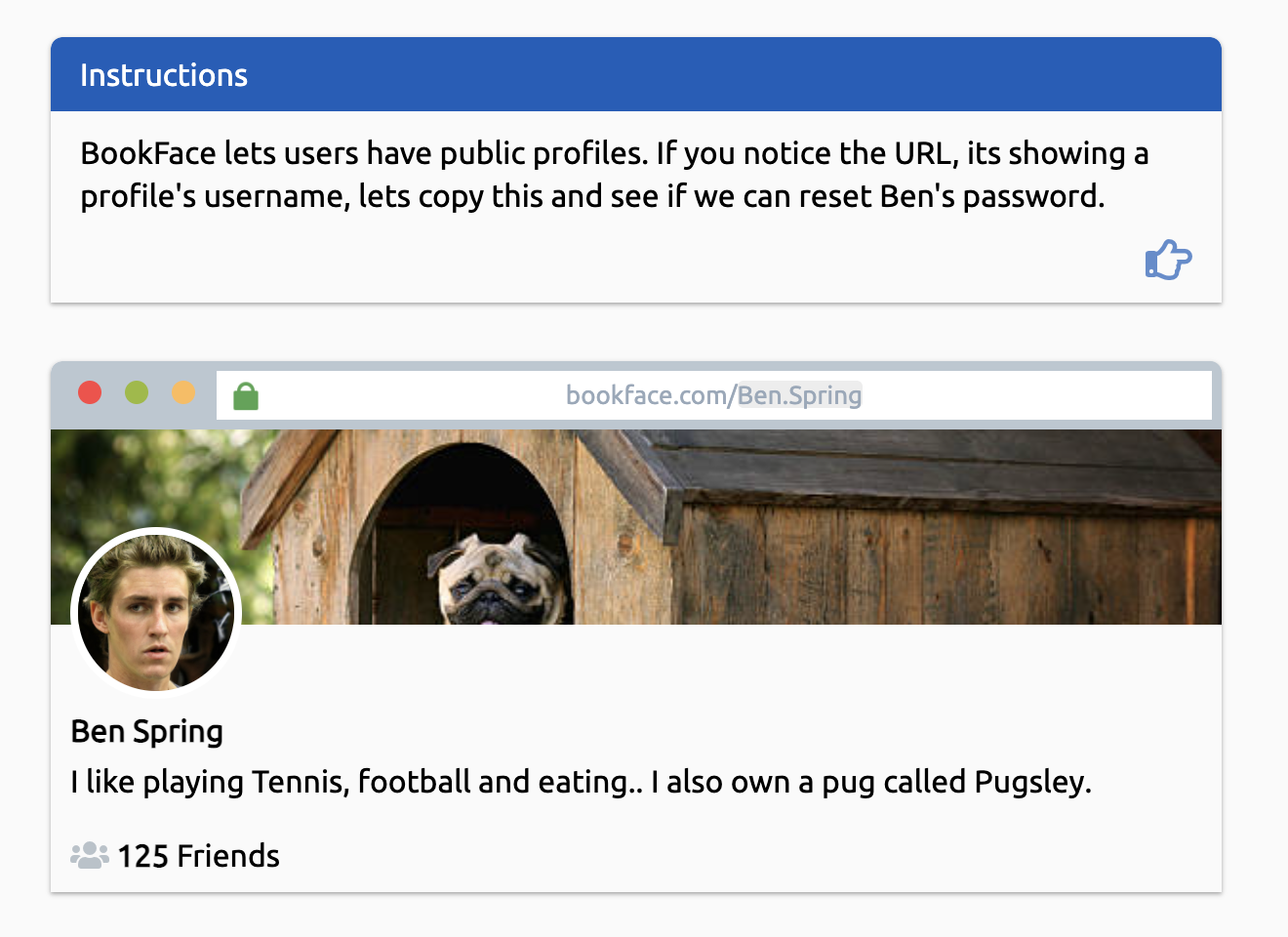


**Question 1**: Read the above and learn how to hack BookFace, TryHackMe's vulnerable social media site. ***|| No answer needed. ||***

**Question 2**: What is the username of the BookFace account you will be taking over?

**How to get the answer:**

From the beginning Bookface page, click the next arrow and you will get to the page shown below:

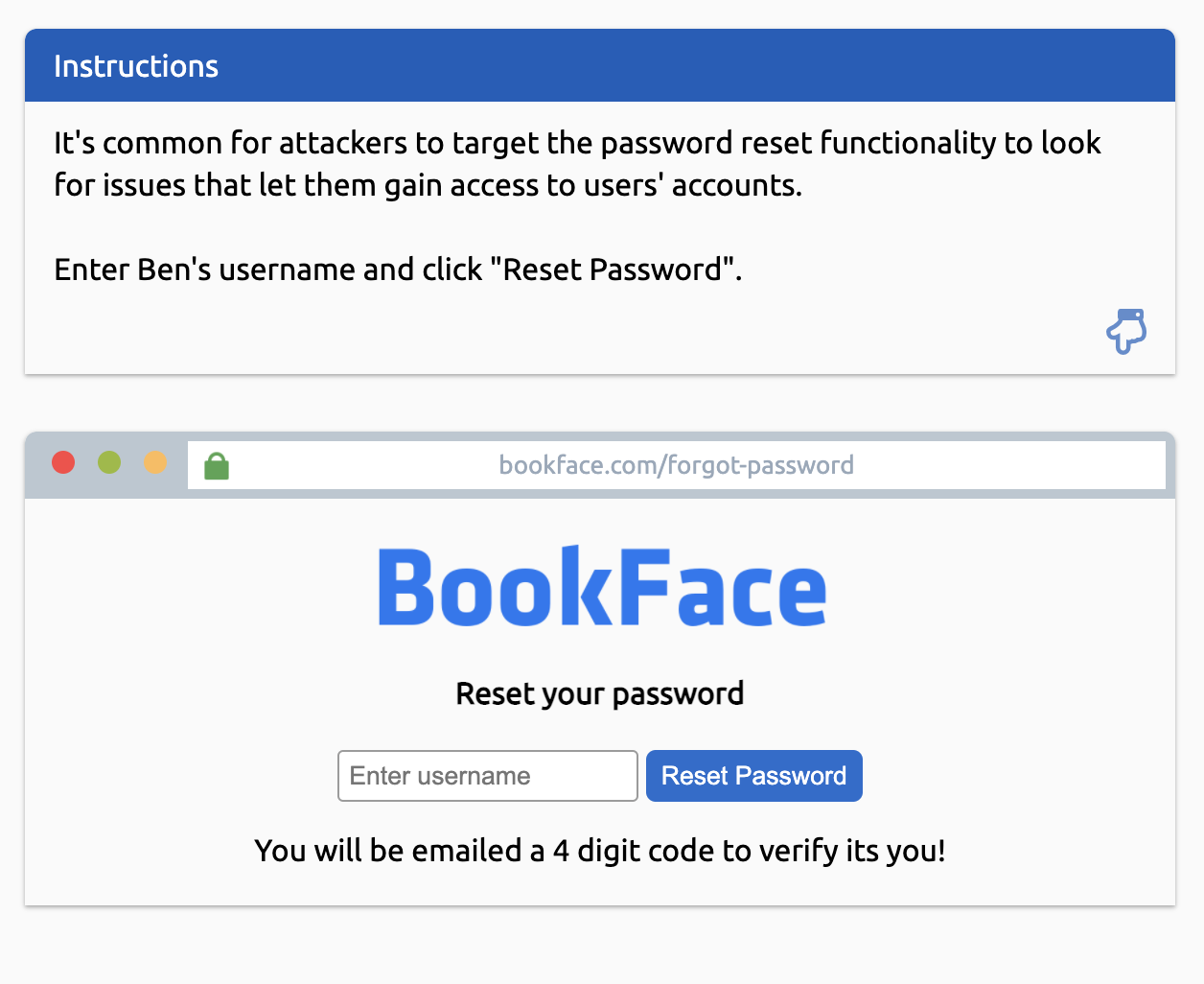


As you can tell in the screenshot above, we are directed to a user page of a “Ben Spring”, with the end of the url containing the username of this user, which is “Ben.Spring”. Therefore, giving you the answer to the second question.

**Question 3**: Hack the BookFace account to reveal the task’s answer!

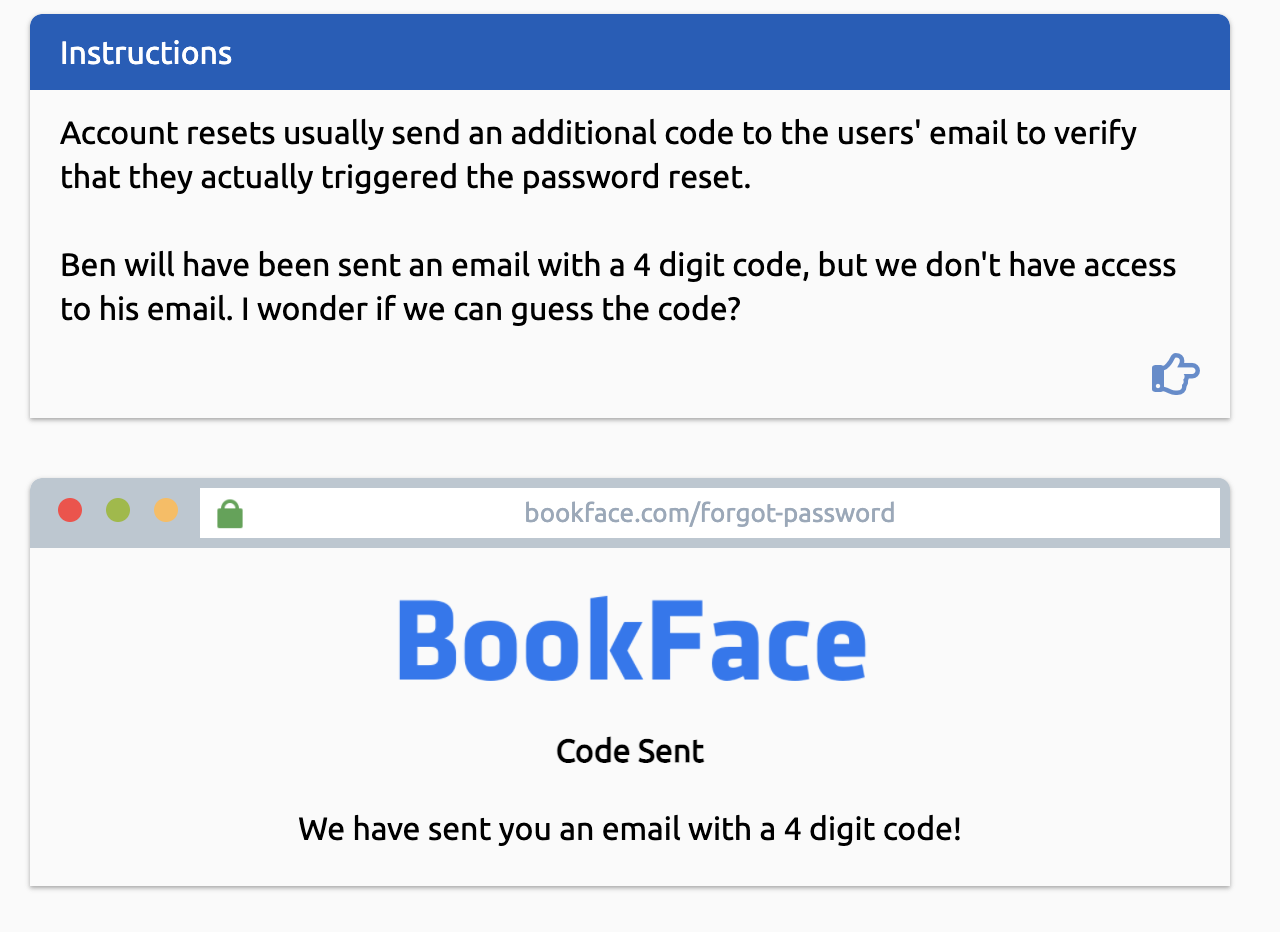
**How to solve for Question 3:**

Go to the next page in the webpage:

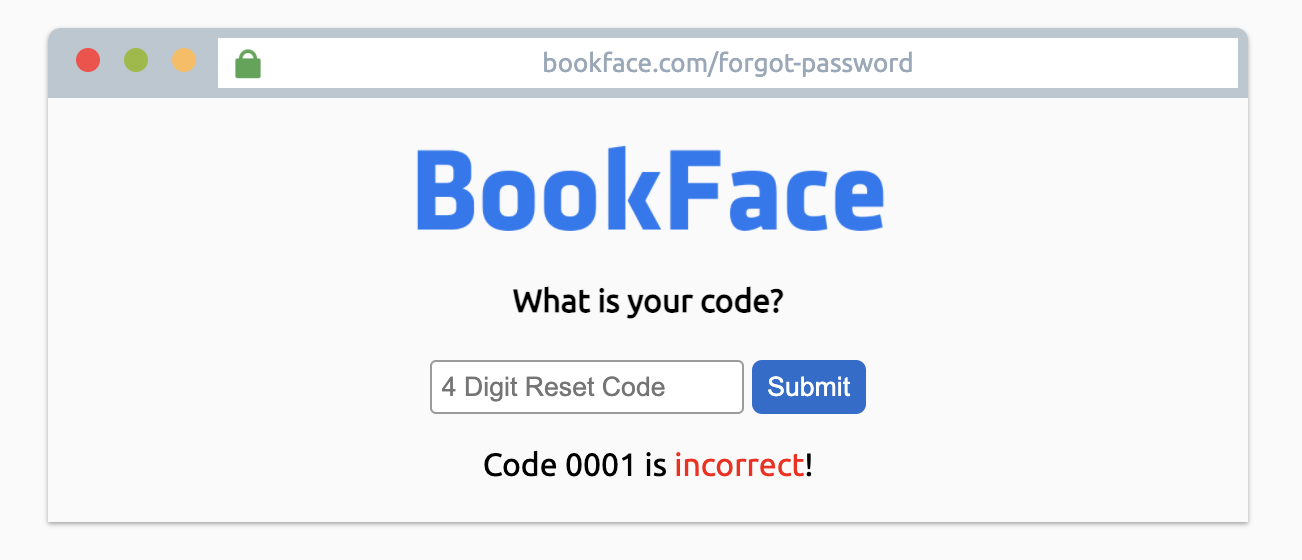


Here, you will enter the username that you found for Question 2 and enter it into the box and reset the password.

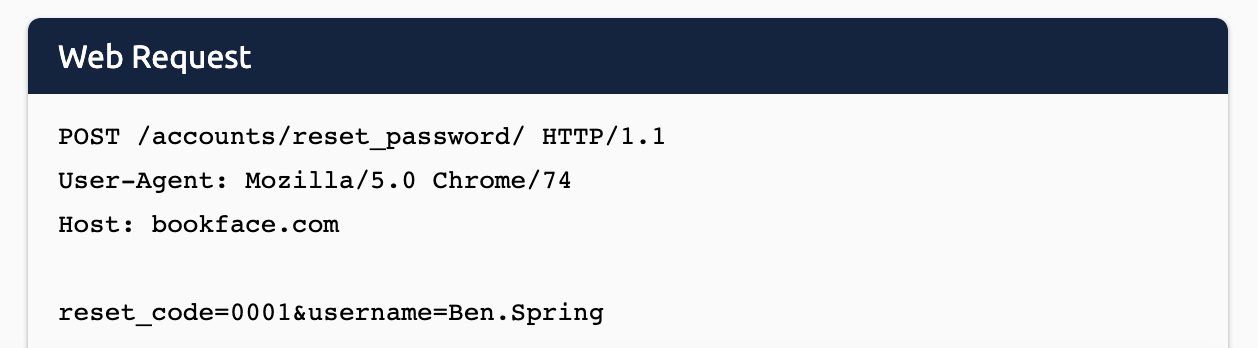
You will then be sent the the following page:



As stated, you do not have access to this user’s email, so you’re probably wondering… how will I get the code? On the following page, you receive information stating that there are 10,000 different combinations that it could be, but let’s start with just entering a random number like 0001.



We see that this code is incorrect, but we are given the web request below to investigate.



The first line of the web request is the type of web request (options can include GET, POST, DELETE) and location to send data to.

*GET: An HTTP command used to request a file from a Web server. GET is widely implemented in HTML files (Web pages) for making database queries that do not involve any updating at the server side.*

*POST: An HTTP command used to send text to a Web server for processing. The POST method is widely implemented in HTML files (Web pages) for sending filled-in forms to the server, updating databases and sending email. In certain cases, POST is used to retrieve data in a similar manner to the HTTP GET command.*

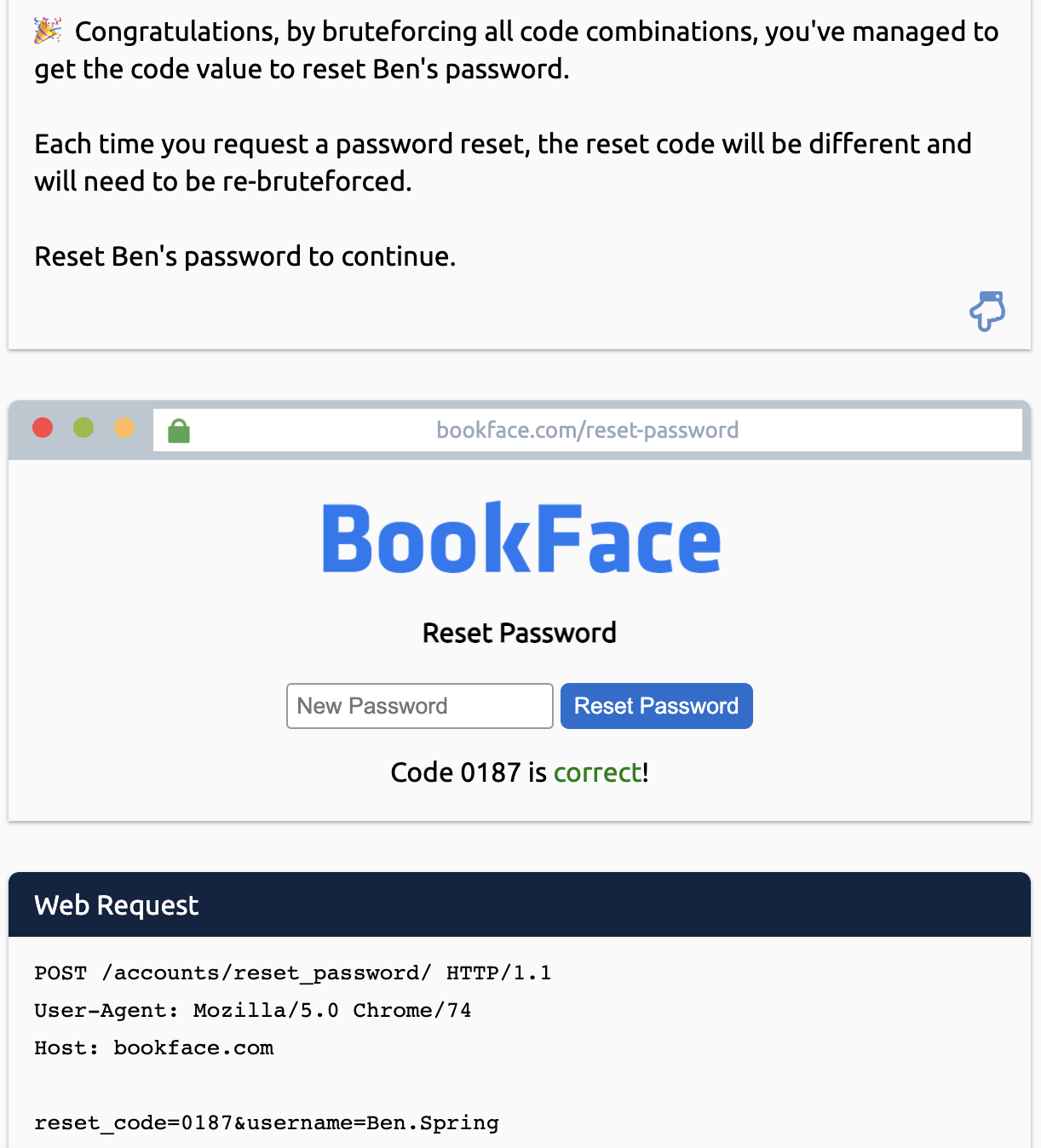
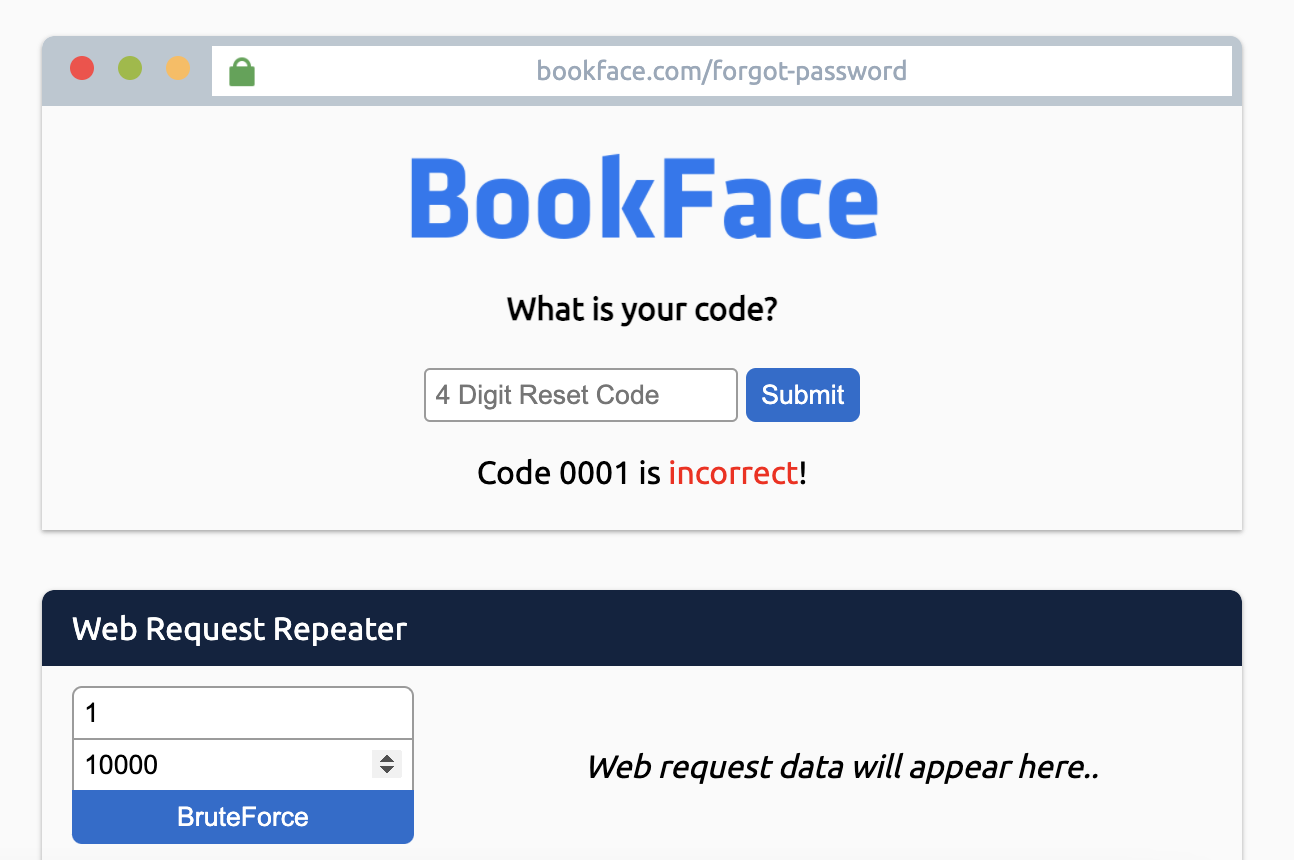
*DELETE: The HTTP DELETE request method deletes the specified resource.*

The second line of the web request is part of the request that tells the web server we are using a Google Chrome (version 74) browser.

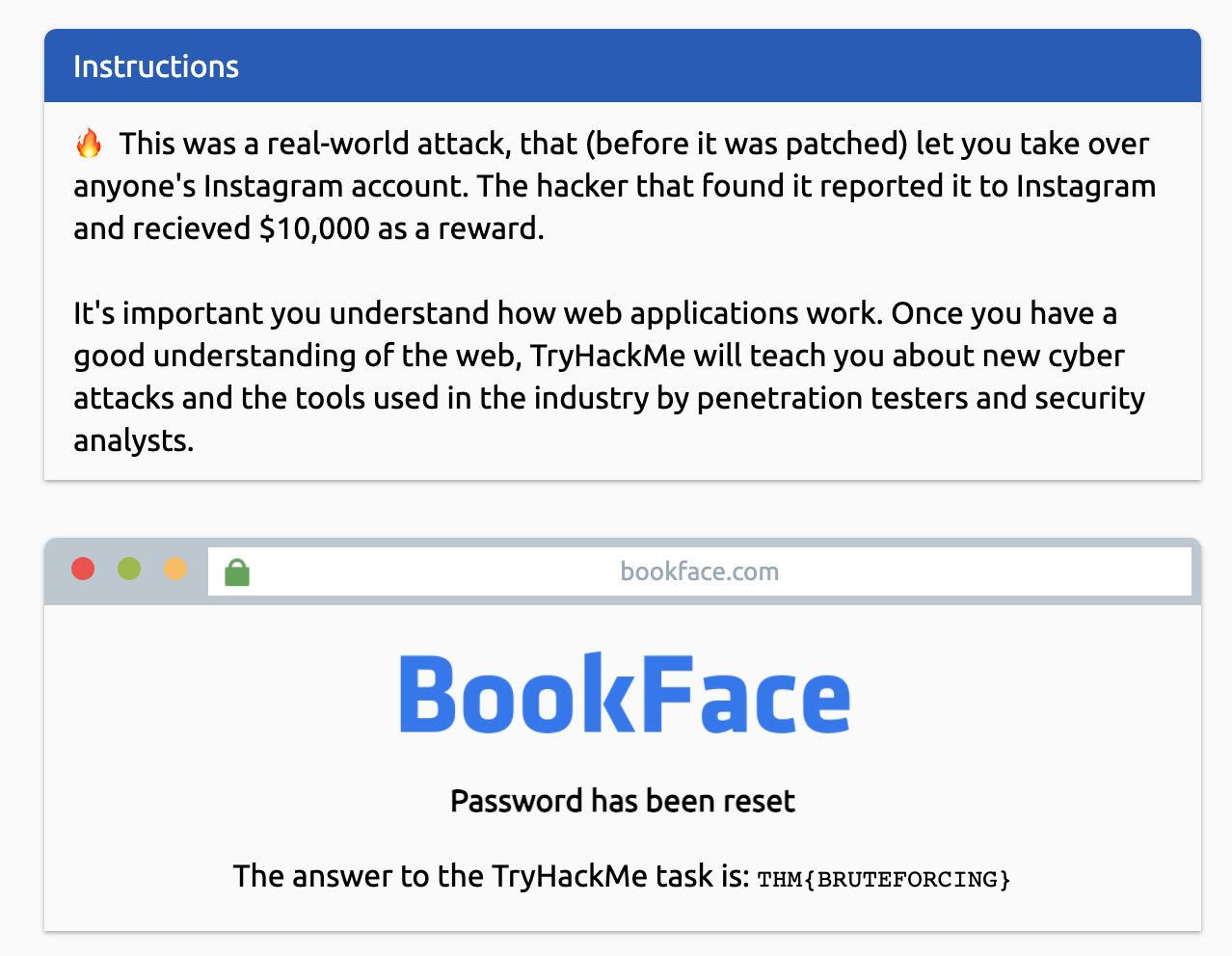
The third line of the web request is telling the web server we want the website bookface.com.

The fourth, and final, line of the web request is the data we are sending to the web server, separated by the & symbol. The “0001” for example is the code you entered in earlier.

In the next step, we are going to “brute force” the code to reset Ben’s Bookface account password. We’re going to do this by using the “Request Repeater” located at the bottom of the page. We will do this by entering ‘1’ for the minimum value and ‘10000’ for the maximum. As shown below:



After brute forcing, you will get the correct code as shown above. After this success notification, we will now reset the password for Ben. Once we hit ‘Reset Password’, we have successfully completed the task and gotten the answer for the third question.



***Task 2: Network Security***

**Why networking is important**

Networking is really important to understand in cyber security. From scanning and identifying who and what is on a network, to reviewing network logs to monitor and track what users have been up to will require you to have an understanding of how networks work.

TryHackMe's Complete Beginner learning path will walk you through the networking concepts and give you enough knowledge to get started in your cyber security journey.

Question 1: Read the above, and see how Target was hacked on the right hand side.

***|| No Answer Needed ||***

******

**Question 2:** How much did the data breach cost Target?

**How to get the answer:**

In order to solve for the answer for question two, click the “see the hack in action” button on the right hand side. While scrolling through the hack, the answer will be located on one of the pages.

***This concludes the Learning Cybersecurity room, although this room was beginner, I hope you enjoyed this write up on it and hopefully it helped!***

I hope you continue your journey throughout cybersecurity and the TryHackMe world.