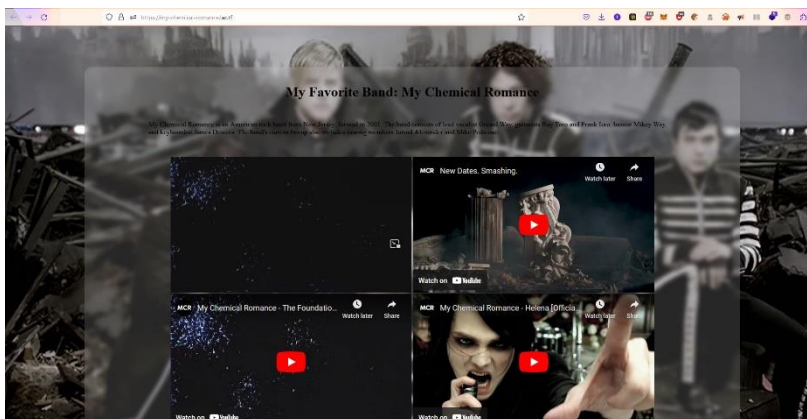
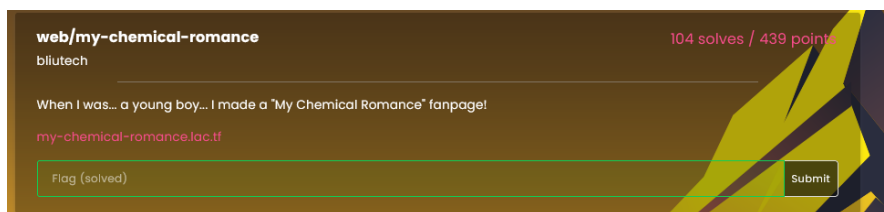


This web challenge comes from LACTF 2023:

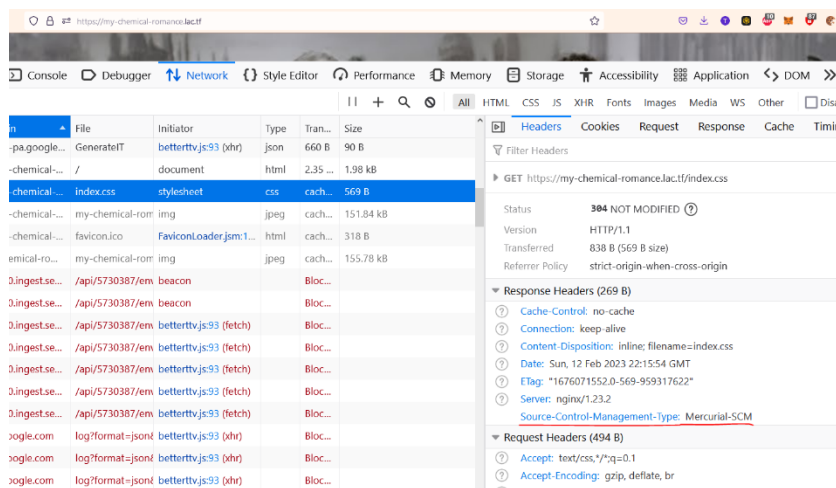
As a my chemical romance fan, I was obliged to do this challenge. We get a description that this is a MCR fanpage, let's go check it out.



Wow, what a beautiful website. Okay so we have a bunch of music videos from Youtube, nothing too interesting here. Looking at the source we can see it's just a basic website, nothing of interest jumps out at me.

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title>My Favorite Band: My Chemical Romance</title>
5     <link rel="stylesheet" href="index.css">
6   </head>
7   <body>
8     <div class="content">
9       <div>My Favorite Band: My Chemical Romance</div>
10      <p>My Chemical Romance is an American rock band from New Jersey, formed in 2001. The band consists of lead vocalist Gerard Way, guitarists Ray Toro and Frank Iero, bassist Mikey Way, and keyboardist James Dewees. The band's sound is a mix of post-hardcore, alternative rock, and emo. They have released four studio albums and one live album. The band's music has been described as "a mix of post-hardcore, alternative rock, and emo".</p>
11      <iframe width="560" height="315" src="https://www.youtube.com/embed/V2kM0J3vVg" title="YouTube video player" frameborder="0" allow="accelerometer; autoplay; clipboard-write; encrypted-media; gyroscope; picture-in-picture" allowfullscreen></iframe>
12      <iframe width="560" height="315" src="https://www.youtube.com/embed/8M49Tf-46Ls" title="YouTube video player" frameborder="0" allow="accelerometer; autoplay; clipboard-write; encrypted-media; gyroscope; picture-in-picture" allowfullscreen></iframe>
13      <iframe width="560" height="315" src="https://www.youtube.com/embed/V2kM0J3vVg" title="YouTube video player" frameborder="0" allow="accelerometer; autoplay; clipboard-write; encrypted-media; gyroscope; picture-in-picture" allowfullscreen></iframe>
14      <iframe width="560" height="315" src="https://www.youtube.com/embed/UCyocDv8A" title="YouTube video player" frameborder="0" allow="accelerometer; autoplay; clipboard-write; encrypted-media; gyroscope; picture-in-picture" allowfullscreen></iframe>
15      <iframe width="560" height="315" src="https://www.youtube.com/embed/py187fu1Iu" title="YouTube video player" frameborder="0" allow="accelerometer; autoplay; clipboard-write; encrypted-media; gyroscope; picture-in-picture" allowfullscreen></iframe>
16    </div>
17  </body>
18 </html>
```

Next let's check out the network tab, maybe something fishy is happening in the cookies or something like that?



Hmm, the website is telling us it is using Mercurial source control management.

I had no idea what Mercurial SCM was before this challenge, so I spent some time researching it and found out it's like Git. So, I went and downloaded Mercurial on Kali, and figured out you can just clone people's public websites and see their control history.

```
(kali@kali)-[~/Desktop]
$ hg clone https://my-chemical-romance.lac.tf/ mcr
requesting all changes
malformed line in .hg/bookmarks: '<!DOCTYPE html>'
malformed line in .hg/bookmarks: '<html>'
malformed line in .hg/bookmarks: '<head>'
malformed line in .hg/bookmarks: '<title>My Favorite Band: My Chemical Romance</title>'
malformed line in .hg/bookmarks: '<link rel="stylesheet" href="/index.css">'
malformed line in .hg/bookmarks: '</head>'
malformed line in .hg/bookmarks: '<body>'
malformed line in .hg/bookmarks: '<div class="content">'
malformed line in .hg/bookmarks: '<h1>Error 404: Page Not Found</h1>'
malformed line in .hg/bookmarks: ''
malformed line in .hg/bookmarks: '</div>'
malformed line in .hg/bookmarks: '</body>'
malformed line in .hg/bookmarks: '</html>'
adding changesets
adding manifests
adding file changes
added 2 changesets with 8 changes to 6 files
new changesets 2445227b04cd:3ecb3a79e255
updating to branch default
6 files updated, 0 files merged, 0 files unresolved

(kali@kali)-[~/Desktop]
$ ls mcr
gerard_way2001.py  static

(kali@kali)-[~/Desktop]
$ cd mcr

(kali@kali)-[~/Desktop/mcr]
$
```

Notice how it says, “requesting all changes”, that could be bad. Let's check out the change logs in mercurial.

```
(kali@kali)-[~/Desktop/mcr]
$ hg log
changeset: 1:3ecb3a79e255
tag: tip
user: bliutech <bensonhliu@gmail.com>
date: Fri Feb 10 06:50:48 2023 -0800
summary: Decided to keep my favorite song a secret :D

changeset: 0:2445227b04cd
user: bliutech <bensonhliu@gmail.com>
date: Fri Feb 10 06:49:48 2023 -0800
summary: I love 'My Chemical Romance'
```

Hmmm, well well well what do we have here? Let's check what changed from revision 0 to revision 1.

```
(kali@kali)-[~/Desktop/mcr]
$ hg diff -r 0 --to 1
diff -r 2445227b04cd -r 3ecb3a79e255 gerard_way2001.py
--- a/gerard_way2001.py Fri Feb 10 06:49:48 2023 -0800
+++ b/gerard_way2001.py Fri Feb 10 06:50:48 2023 -0800
@@ -2,7 +2,6 @@
 app = Flask(__name__)

-# FLAG: lactf{d0nT_6rInk_m3rCurial_fr0m_0_fl4Sk}
@app.route('/')
@app.route('/<path:path>')
def index(path='index.html'):
diff -r 2445227b04cd -r 3ecb3a79e255 static/index.html
--- a/static/index.html Fri Feb 10 06:49:48 2023 -0800
+++ b/static/index.html Fri Feb 10 06:50:48 2023 -0800
@@ -8,8 +8,6 @@
 <div class="content">
 <h1>My Favorite Band: My Chemical Romance</h1>
 <p>My Chemical Romance is an American rock band from New Jersey, formed in 2001. The band consists of lead vocalist Gerard Way, guitarists Ray Toro and Frank Iero, bassist Mikey Way, and keyboardist James Dewees. The band's current lineup also includes touring members Jarrod Alexander and Mike Pedicone.</p>
-
- <iframe width="560" height="315" src="https://www.youtube.com/embed/RRKJ1M9Njr8" title="YouTube video player" frameborder="0" allow="accelerometer; autoplay; clipboard-write; encrypted-media; gyroscope; picture-in-picture; web-share" allowfullscreen></iframe>
-
- <iframe width="560" height="315" src="https://www.youtube.com/embed/V2kWUJkRvVs" title="YouTube video player" frameborder="0" allow="accelerometer; autoplay; clipboard-write; encrypted-media; gyroscope; picture-in-picture; web-share" allowfullscreen></iframe>
```

Ah ha! Flag was deleted in last revision.