















## <sick xss - web>





우선 파일을 다운 받아서 압축을 풀었다. 풀자마자 나온 화면은 다음과 같다.

 app		2024-07-21 오후 10:05	파일 폴더	
 docker-compose		2024-07-21 오후 10:04	Yaml 원본 파일	1KB
 Dockerfile		2024-07-21 오후 5:12	파일	1KB











app 폴더에 들어가보니 다음과 같은 화면이 떴다.

 views		2024-07-21 오후 10:05	파일 폴더	
 app.js		2024-08-17 오전 10:58	JSFile	3KB
 package.json		2024-07-21 오후 10:04	JSON 파일	1KB
 package-lock.json		2024-07-21 오후 9:28	JSON 파일	80KB

views 폴더까지 들어가보니 다음과 같은 화면이 떴다.

 bot.ejs		2024-07-21 오후 9:20	EJS 파일	1KB
 echo.ejs		2024-07-21 오후 9:20	EJS 파일	1KB
 head.ejs		2023-06-26 오전 3:03	EJS 파일	1KB
 header.ejs		2024-07-21 오후 5:13	EJS 파일	1KB
 index.ejs		2023-06-26 오후 3:21	EJS 파일	1KB

구루1을 수강하면서 위와 같은 파일에 html 확장자를 붙이면 웹으로 바뀐다고 배웠던 게 생각나서 이름 변경을 통해 html 확장자를 붙여보았더니 다음과 같이 변했다.

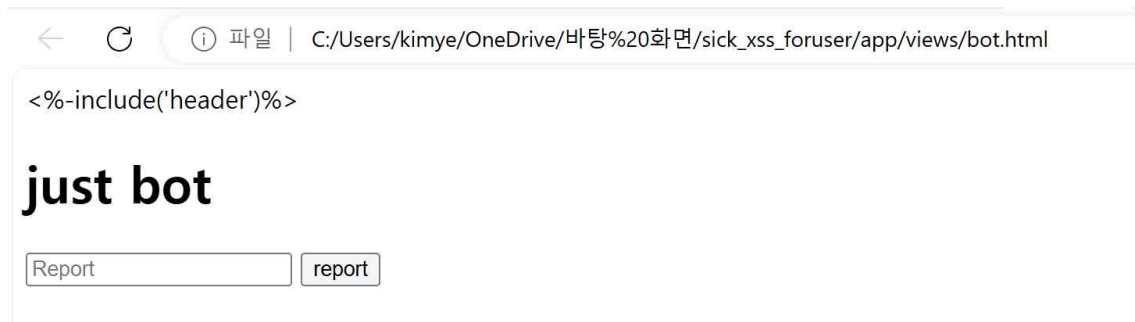
 bot		2024-07-21 오후 9:20	Microsoft Edge HTM...	1KB
 echo		2024-07-21 오후 9:20	Microsoft Edge HTM...	1KB
 head		2023-06-26 오전 3:03	Microsoft Edge HTM...	1KB
 header		2024-07-21 오후 5:13	Microsoft Edge HTM...	1KB
 index		2023-06-26 오후 3:21	Microsoft Edge HTM...	1KB

생각했던대로 마이크로소프트 로고가 나타나면서 웹으로 바뀌었다.

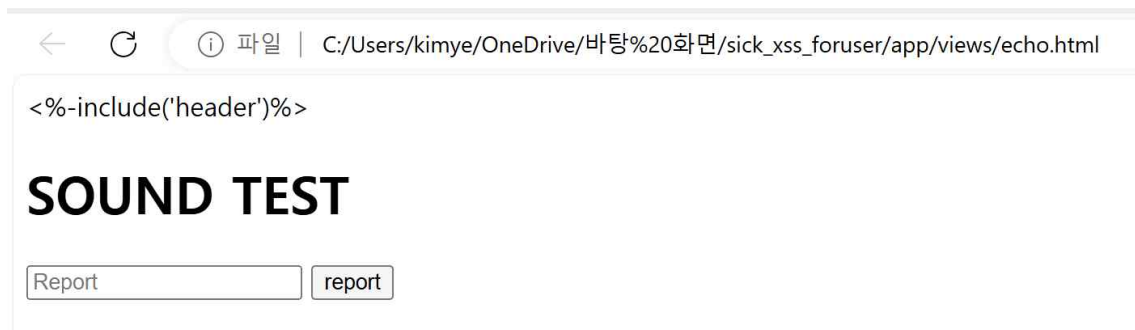
하나하나 눌러서 들어가보니 다음과 같은 화면이 나타났다.

우선 bot를 눌렀을 때는 just bot라는 문구가 뜨면서 무언가를 입력할 수 있는 버튼이 생겼다. 어떻게 사용해야 하는건지, bot의 뜻이 뭔지는 아직 잘 모르겠다.

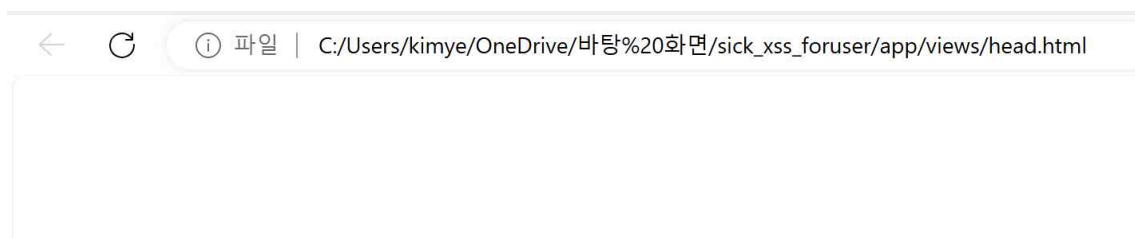
입력하는 칸에 <%-include('header')%> 양식으로 무언가를 입력하라는 뜻인가 싶다.



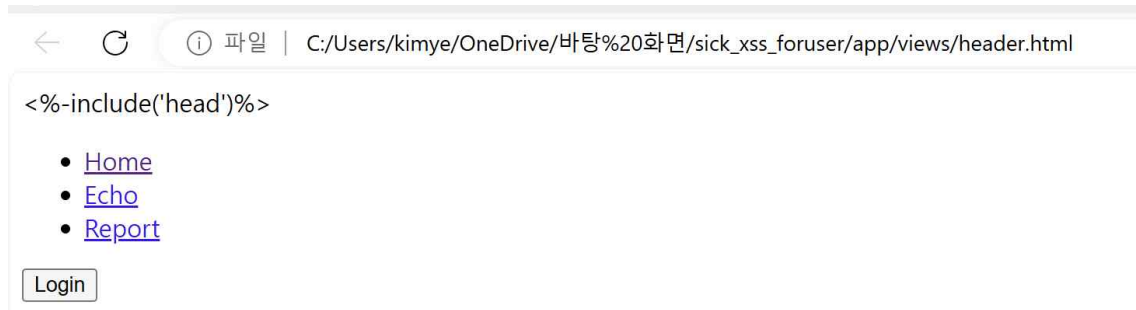
다른 웹들도 동일하게 열어보았다. echo를 눌렀더니 sound test라는 문구가 뜨면서 무언가를 report 할 수 있는 입력창이 떴다. 형태를 bot와 동일하고 문구만 다르다는 차이점을 가진다.



head를 눌렀을 때에는 페이지에 아무것도 뜨지 않았다.































header를 누르니 다음과 같은 화면이 떴다. 뭔가 header라고 하니까 의미가 담긴 페이지일 것 같아서 버튼들을 눌러보았다.



Login이랑 Echo랑 Report를 눌렀을 때는 페이지 오류가 뜨고 Home을 누르면 다음과 같은 디렉토리들이 뜬다.

## C:\의 인덱스

이름	크기	수정한 날짜
 \$RECYCLE.BIN/		24. 8. 18. 오전 12:18:09
 \$WINDOWS.BT/		24. 5. 16. 오후 4:40:01
 \$Windows.WS/		24. 5. 16. 오후 4:40:00
 Documents and Settings/		24. 1. 16. 오후 2:48:43
 ESD/		24. 5. 16. 오후 5:34:11
 MSOCache/		24. 2. 18. 오후 2:58:01
 OneDriveTemp/		24. 5. 11. 오후 11:24:38
 PerfLogs/		22. 5. 7. 오후 2:24:50
 PrivacyPolicy/		23. 12. 14. 오전 8:32:32
 Program Files/		24. 7. 30. 오전 10:33:20
 Program Files (x86)/		24. 8. 6. 오후 10:40:38
 ProgramData/		24. 8. 6. 오후 10:40:50
 Recovery/		23. 12. 14. 오전 8:40:23
 System Volume Information/		24. 2. 21. 오후 12:51:43
 Temp/		24. 2. 18. 오후 2:23:55
 User_manual/		23. 12. 14. 오전 8:34:13
 Users/		24. 3. 14. 오후 1:16:19
 Wallpaper/		24. 7. 18. 오후 2:48:03
 Windows/		24. 7. 13. 오전 8:52:18
 appverifUI.dll	110 kB	24. 2. 22. 오전 1:33:48
 bootTel.dat	112 B	23. 12. 14. 오전 8:57:09
 DumpStack.log	12.0 kB	24. 7. 27. 오후 5:46:16
 DumpStack.log.tmp	12.0 kB	24. 8. 13. 오후 4:26:32
 hiberfil.sys	6.2 GB	24. 8. 18. 오전 12:17:17
 nsispromotion_log.txt	264 B	24. 8. 6. 오후 10:38:59
 pagefile.sys	5.8 GB	24. 8. 13. 오후 4:26:32
 RHDSetup.log	3.3 kB	23. 12. 14. 오전 8:08:58
 Setup.log	212 B	23. 12. 14. 오전 8:11:30

만약 눌렀을 때 페이지 오류가 뜨는거라면, 해당하는 부분의 html 코드를 올바르게 수정해서 제대로 연결되도록 할 수 있지 않을까?라는 생각이 들었다.

그래서 해당 파일들의 html 코드를 읽기 위해서 visual code로 열어보았다.

bot 파일을 여니 다음과 같은 코드가 나온다 구글링을 좀 해보니 봇을 우회하거나 트래픽 로 그를 분석해서 플래그 값을 찾아야 하는 경우가 있다고 한다.

```
JS app.js {} package.json {} package-lock.json <> bot.html X <> echo.html <> head.html <> header.html
C: > Users > kimye > OneDrive > 바탕 화면 > sick_xss_foruser > app > views > <> bot.html > ...
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Document</title>
7 </head>
8 <body>
9   <%-include('header')%>
10  <h1>just bot</h1>
11  <div class="card w-50 position-absolute top-50 start-50 translate-middle">
12    <div class="card-body">
13      <form action="/bot" method="POST">
14        <input type="text" placeholder="Report" name="report" required class="form-control">
15        <input type="submit" value="report" class="float-end mt-1 btn btn-dark" id="submit">
16      </form>
17    </div>
18  </div>
19
20 </body>
21 </html>
22
```

echo 파일의 코드는 다음과 같다.

```
JS app.js {} package.json X {} package-lock.json <> bot.html <> echo.html X <> head.html <> header.html <> in
C: > Users > kimye > OneDrive > 바탕 화면 > sick_xss_foruser > app > views > <> echo.html > ...
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Document</title>
7 </head>
8 <body>
9   <%-include('header')%>
10  <h1>SOUND TEST</h1>
11  <div class="card w-50 position-absolute top-50 start-50 translate-middle">
12    <div class="card-body">
13      <form action="/echo" method="POST">
14        <input type="text" placeholder="Report" name="echo" id="echo" required class="form-control">
15        <input type="submit" value="report" class="float-end mt-1 btn btn-dark" id="submit">
16      </form>
17    </div>
18  </div>
19
20 </body>
21 </html>
22
```

head 파일 코드는 다음과 같다.

```
JS app.js package.json X package-lock.json bot.html echo.html head.html X header.html index.html
C: > Users > kimye > OneDrive > 바탕 화면 > sick_xss_foruser > app > views > head.html > link
1 <meta charset="UTF-8">
2 <meta http-equiv="X-UA-Compatible" content="IE=edge">
3 <meta name="viewport" content="width=device-width, initial-scale=1.0">
4 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/css/bootstrap.min.css" rel="stylesheet"
5 | integrity="sha384-18mE4kWBq781YhF1dvKuhfTAU6auU8tT94WrHftjDbrCEXSU1oBoqyl2QvZ6jIW3" crossorigin="anonymous">
6
7
```

header 파일 코드는 다음과 같다. echo랑 report랑 login 부분 코드를 수정하면 되지 않을까 싶은 생각이 들긴 하는데 어떻게 해야 하는지 아직 감이 잡히지 않는다.

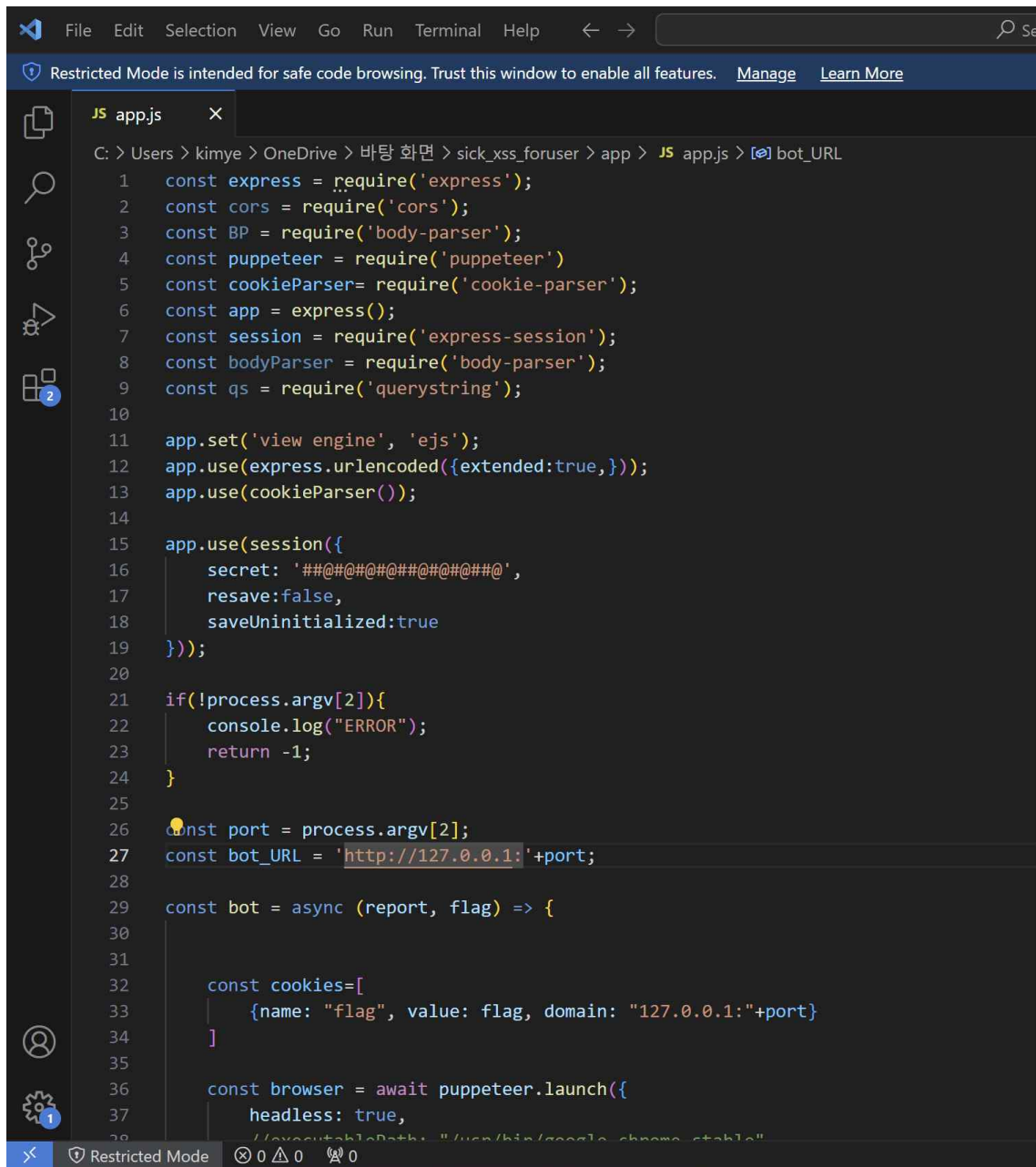
```
JS app.js X package.json package-lock.json bot.html echo.html head.html header.html X index.html
C: > Users > kimye > OneDrive > 바탕 화면 > sick_xss_foruser > app > views > header.html > ?
1 <%-include('head')%>
2 <header class="p-3 bg-dark text-white mb-4">
3 <div class="container">
4 <div class="d-flex flex-wrap align-items-center justify-content-center justify-content-lg-start">
5 <ul class="nav col-12 col-lg-auto me-lg-auto mb-2 justify-content-center mb-md-0">
6 <li><a href="/" class="nav-link px-2 text-white">Home</a></li>
7 <li><a href="/echo" class="nav-link px-2 text-white">Echo</a></li>
8 <li><a href="/bot" class="nav-link px-2 text-white">Report</a></li>
9 </ul>
10 <div class="text-end">
11 <button type="button" class="btn btn-outline-light me-2" onclick="location.href='/login'">Login</button>
12 </div>
13 </div>
14 </div>
15 </header>
```

echo 파일 코드는 다음과 같다.

```
JS app.js package.json package-lock.json bot.html echo.html head.html header.html index.html X
C: > Users > kimye > OneDrive > 바탕 화면 > sick_xss_foruser > app > views > index.html > ...
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4 <meta charset="UTF-8">
5 <meta name="viewport" content="width=device-width, initial-scale=1.0">
6 <title>Document</title>
7 </head>
8 <body>
9 <%-include('header')%>
10 <div class="card w-50 position-absolute top-50 start-50 translate-middle">
11 <div class="card-body">
12 <h1>Hello guys</h1>
13 </div>
14 </div>
15
16 </body>
17 </html>
18
```

코드도 분석해보고 링크로 연결되는 페이지들을 다 열어봤는데 어떻게 해야 할지 모르겠다,

일단 다른 파일들도 visual studio를 통해서 열어보았다.



```
JS app.js
C: > Users > kimye > OneDrive > 바탕 화면 > sick_xss_foruser > app > JS app.js > bot_URL

1  const express = require('express');
2  const cors = require('cors');
3  const BP = require('body-parser');
4  const puppeteer = require('puppeteer')
5  const cookieParser= require('cookie-parser');
6  const app = express();
7  const session = require('express-session');
8  const bodyParser = require('body-parser');
9  const qs = require('querystring');
10
11 app.set('view engine', 'ejs');
12 app.use(express.urlencoded({extended:true}));
13 app.use(cookieParser());
14
15 app.use(session({
16   secret: '#####',
17   resave:false,
18   saveUninitialized:true
19 }));
20
21 if(!process.argv[2]){
22   console.log("ERROR");
23   return -1;
24 }
25
26 const port = process.argv[2];
27 const bot_URL = 'http://127.0.0.1:'+port;
28
29 const bot = async (report, flag) => {
30
31
32   const cookies=[
33     {name: "flag", value: flag, domain: "127.0.0.1:"+port}
34   ]
35
36   const browser = await puppeteer.launch({
37     headless: true,
38     //executablePath: "/usr/bin/google-chrome-stable"
```

파일 링크들을 타고 들어가면 다 지원되지 않는 페이지라고 뜬다.

단계가 최하라고 해서 도전해보려고 했는데 접근법을 모르겠어서 허무하다.