



웹 해킹이란 무엇인가?

Web Hacking Tutorial

프로토콜 보안(Helmet)

[BOSS] 손 우 규

<https://github.com/swk3169/web-hacking>

목차

1. 프로토콜 보안(Helmet)	3
1.1 정의	
1.2 방어법	
1.3 문제점	
1.4 해결방안	
2. 실습	7
2.1 [Node.js] Helmet 모듈을 이용한 프로토콜 보안	
3. 참조	19

1. 프로토콜 보안(Helmet)

1.1 정의

Helmet은 다양한 HTTP 헤더를 설정하여 Express 응용 프로그램의 보안을 유지하도록 도와준다.

1.2 방어법

1.2.1 Helmet

Helmet을 이용하면 HTTP 헤더를 적절히 설정하여 몇 가지 잘 알려진 웹 취약성으로부터 앱을 보호할 수 있다.

사실 Helmet은 보안 관련 HTTP 헤더를 설정하는 다음과 같은 더 작은 크기의 미들웨어 함수 9개의 모음이다.

- csp는 Content-Security-Policy 헤더를 설정하여 XSS(Cross-site scripting) 공격 및 기타 교차 사이트 인젝션을 예방한다.
- hidePoweredBy는 X-Powered-By 헤더를 제거한다.
- hpkp는 Public Key Pinning 헤더를 추가하여, 위조된 인증서를 이용한 중간자 공격을 방지한다.
- hsts는 서버에 대한 안전한(SSL/TLS를 통한 HTTP) 연결을 적용하는 Strict-Transport-Security 헤더를 설정한다.
- ieNoOpen은 IE8 이상에 대해 X-Download-Options를 설정한다.
- noCache는 Cache-Control 및 Pragma 헤더를 설정하여 클라이언트 측에서 캐싱을 사용하지 않도록 한다.
- noSniff는 X-Content-Type-Options 를 설정하여, 선언된 콘텐츠 유형으로부터 벗어난 응답에 대한 브라우저의 MIME 가로채기를 방지한다.
- frameguard는 X-Frame-Options 헤더를 설정하여 clickjacking에 대한 보호를 제공한다.
- xssFilter는 X-XSS-Protection을 설정하여 대부분의 최신 웹 브라우저에서 XSS(Cross-site scripting) 필터를 사용하도록 한다.

다른 모든 npm 모듈처럼 Helmet은 다음과 같이 설치할 수 있습니다.

```
$ npm install --save helmet
```

이후 코드에서 Helmet을 사용하는 방법은 다음과 같다.

```
...  
var helmet = require('helmet');  
app.use(helmet());  
...
```

적어도 X-Powered-By 헤더는 사용하지 않도록 설정

Helmet의 사용을 원치 않는 경우에는 적어도 X-Powered-By 헤더를 사용하면 안된다. 공격자는 이 헤더(기본적으로 사용하도록 설정되어 있음)를 이용해 Express를 실행하는 앱을 발견한 후 특정한 대상에 대한 공격을 실행할 수 있다.

따라서 우수 사례는 다음과 같이 app.disable() 메소드를 이용해 이 헤더를 끄는 것이다.

```
...  
app.disable('x-powered-by');  
...
```

1.3 문제점

모듈을 사용한다고 하더라도, 다른 모든 웹 앱과 마찬가지로 Express 앱은 다양한 웹 기반 공격에 취약할 수 있다. 알려져 있는 웹 취약성을 숙지한 후 이러한 취약성을 피하기 위한 예방 조치가 최선이다.

1.4 해결방안

HTTP 헤더를 설정하여 최소한의 취약성으로부터 앱을 보호한다. 때문에 HTTPS와 같은 안전한 프로토콜을 쓰는 것이 하나의 방법이다.

1.4.1 HTTPS

HTTPS에서 마지막의 S는 Over Secure Socket Layer의 약자로 Secure라는 말을 통해서 알 수 있듯이 보안이 강화된 HTTP라는 것을 짐작할 수 있다. HTTP는 암호화되지 않은 방법으로 데이터를 전송하기 때문에 서버와 클라이언트가 주고 받는 메시지를 감청하는 것이 매우 쉽다. 예를들어 로그인을 위해서 서버로 비밀번호를 전송하거나, 또는 중요한 기밀 문서를 열람하는 과정에서 악의적인 감청이나 데이터의 변조등이 일어날 수 있다는 것이다. 이를 보안한 것이 HTTPS다. HTTPS는 소켓 통신에서 일반 텍스트를 이용하는 대신에, SSL이나 TLS 프로토콜을 통해 세션 데이터를 암호화한다. 따라서 데이터의 적절한 보호를 보장한다. HTTPS의 기본 TCP/IP 포트는 443이다.

1.4.2 추가적인 고려사항

- 속도 제한(rate-limiting)을 구현하여 인증에 대한 무차별 대입 공격을 방지해야 한다. 이를 실행하는 한 가지 방법은 StrongLoop API Gateway를 이용하여 속도 제한 정책을 적용하는 것이다. 대안적으로, express-limiter와 같은 미들웨어를 사용할 수 있지만, 그러한 경우에는 코드를 어느 정도 수정하여야 한다.
- csrf 미들웨어를 이용하여 교차 사이트 요청 위조(CSRF)로부터 보호하여야 한다.
- 항상 사용자 입력을 필터링하고 사용자 입력에서 민감한 데이터를 제거하여 XSS(Cross-site scripting) 및 명령 인젝션 공격으로부터 보호하여야 한다.
- 매개변수화된 조회 또는 준비된 명령문을 이용하여 SQL 인젝션 공격으로부터 방어하여야 한다.
- 오픈 소스 방식의 sqlmap 도구를 이용하여 앱 내의 SQL 인젝션 취약성을 발견하여야 한다.
- nmap 및 sslyze 도구를 이용하여 SSL 암호, 키 및 재협상의 구성, 그리고 인증서의 유효성을 테스트하여야 한다.
- safe-regex를 이용하여 정규식이 정규식 서비스 거부 공격을 쉽게 받지 않도록

록 하여야 한다.

2. 실습

2.1 [Node.js] md5, sha256 모듈을 이용한 비밀번호 보안

Security Headers
Sponsored by **SOPHOS**

Home About

Scan your site now

Scan

☐ Hide results ☒ Follow redirects

Grand Totals

A+	486,244
A	3,731,238
B	1,152,083
C	496,904
D	1,671,541
E	1,122,898
F	4,692,565
R	1,406,596
Total	14,760,069

Recent Scans

kml.inegi.up.pt	F
www.instagram.com	D
cp74.webserver.pt	F
stagingsupport.dat...	F
coral.cilmar.up.pt	F
chariscrete.blogs...	D
cdn.mwam.com	F
easyline-se.com.br	D
centenario.up.pt	F

Hall of Fame




www.izzi.co.il	A
llumarmgm.yeahc.co...	A
dev.eos.arista.com	A
stageten-charity-d...	A
www.halodoc.com	A
apiutilidadestest...	A
foxtrot.secne.site	A+
hosted.directid.co	A
fated.org	A

Hall of Shame

kml.inegi.up.pt	F
cp74.webserver.pt	F
stagingsupport.dat...	F
coral.cilmar.up.pt	F
cdn.mwam.com	F
centenario.up.pt	F
www.book4groups.co...	F
14.63.171.152	F
remoteaccess.i3s.u...	F

A [scotthelme.co.uk](#) project - [CC-BY-SA 4.0](#)

Sponsored by [Sophos](#)



Security Report Summary



Site: <https://www.facebook.com/>

IP Address: 2a03:2880:f131:83:face:b00c:0:25de

Report Time: 17 Oct 2018 14:38:44 UTC

Headers:

✓ X-XSS-Protection ✓ Content-Security-Policy ✓ X-Frame-Options ✓ Strict-Transport-Security
✓ X-Content-Type-Options ✗ Referrer-Policy ✗ Feature-Policy

Warning: Grade capped at A, please see warnings below.

Raw Headers

HTTP/1.1	200 OK
X-XSS-Protection	0
Pragma	no-cache
content-security-policy	default-src * data: blob:;script-src *.facebook.com *.fbcdn.net *.google-analytics.com *.virtualearth.net *.google.com 127.0.0.1:* *.spotilocal.com: * 'unsafe-inline' 'unsafe-eval' *.atlassolutions.com blob: data: 'self';style-src data: blob: 'unsafe-inline' *;connect-src *.facebook.com *.fbcdn.net *.facebook.net *.spotilocal.com: * ws://*.facebook.com: * https://fb.scanandcleanlocal.com: * *.atlassolutions.com attachment.fbsbx.com ws://localhost: * blob: *.cdninstagram.com 'self' chrome-extension://boadgeojelhngndaghljhdicfkmllpatfd chrome-extension://dllochdbjfkdbacpmhlcplmaeejdimm;
Cache-Control	private, no-cache, no-store, must-revalidate
X-Frame-Options	DENY
Strict-Transport-Security	max-age=15552000; preload
X-Content-Type-Options	nosniff
Expires	Sat, 01 Jan 2000 00:00:00 GMT
Set-Cookie	fr=1i0GpXdigK9bws8xY..Bbx0i0.es.AAA.0.0.8bx0i0.AWUPK3LR; expires=Tue, 15-Jan-2019 14:38:44 GMT; Max-Age=7776000; path=/;
Set-Cookie	sb=dEnHW3ZOozxdvFG1QCEU9j8B; expires=Fri, 16-Oct-2020 14:38:44 GMT; Max-Age=63072000; path=/; domain=.facebook.com; secure; httponly
Vary	Accept-Encoding
Content-Type	text/html; charset="utf-8"
X-FB-Debug	6kcb6VacIDipYSL0FjwfrPxiOnTeU/UrsEMA3h5BaRC6TN81Uj8XEHQ0U6t4840004XwGMZ37JPDmV7dlc1BJQ==
Date	Wed, 17 Oct 2018 14:38:44 GMT
Transfer-Encoding	chunked
Connection	keep-alive

Missing Headers

Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Feature-Policy	Feature Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Security Report Summary



Site: <https://www.naver.com/>

IP Address: 104.92.116.145

Report Time: 17 Oct 2018 14:39:22 UTC

Headers:

✔ **X-Frame-Options** ✔ **Strict-Transport-Security** ✔ **Referrer-Policy** ✖ **Content-Security-Policy**
✖ **X-XSS-Protection** ✖ **X-Content-Type-Options** ✖ **Feature-Policy**

Warning: Grade capped at A, please see warnings below.

Raw Headers

HTTP/1.1	200 OK
Server	NWS
Content-Type	text/html; charset=UTF-8
Cache-Control	no-cache, no-store, must-revalidate
Pragma	no-cache
P3P	CP="CAO DSP CURa ADMa TAIa PSAa OUR LAW STP PHY ONL UNI PUR FIN COM NAV INT DEM STA PRE"
X-Frame-Options	SAMEORIGIN
Strict-Transport-Security	max-age=31536000; preload
Referrer-Policy	unsafe-url
X-EdgeConnect-MidMile-RTT	3
X-EdgeConnect-Origin-MEX-Latency	7
X-EdgeConnect-MidMile-RTT	146
X-EdgeConnect-Origin-MEX-Latency	7
X-EdgeConnect-Cache-Status	0
Date	Wed, 17 Oct 2018 14:39:22 GMT
Transfer-Encoding	chunked
Connection	keep-alive
Connection	Transfer-Encoding

Missing Headers

Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-XSS-Protection	X-XSS-Protection sets the configuration for the cross-site scripting filter built into most browsers. Recommended value "X-XSS-Protection: 1; mode=block".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Feature-Policy	Feature Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Helmet 사용

Helmet을 이용하면 HTTP 헤더를 적절히 설정하여 몇 가지 잘 알려진 웹 취약성으로부터 앱을 보호할 수 있습니다.

사실 Helmet은 보안 관련 HTTP 헤더를 설정하는 다음과 같은 더 작은 크기의 모듈웨어 함수 9개의 모음입니다.

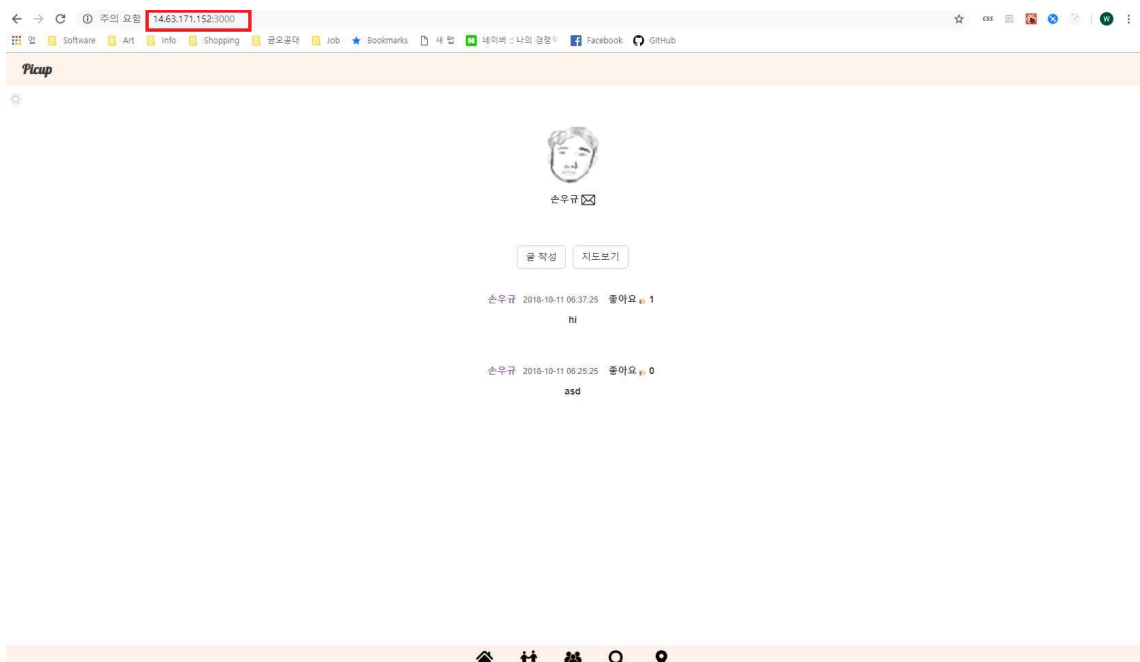
- **csp**는 Content-Security-Policy 헤더를 설정하여 XSS(Cross-site scripting) 공격 및 기타 교차 사이트 인젝션을 예방합니다.
- **hidePoweredBy**는 X-Powered-By 헤더를 제거합니다.
- **hpkp**는 Public Key Pinning 헤더를 추가하여, 위조된 인증서를 이용한 중간자 공격을 방지합니다.
- **hsts**는 서버에 대한 안전한(SSL/TLS를 통한 HTTP) 연결을 적용하는 Strict-Transport-Security 헤더를 설정합니다.
- **ieNoOpen**은 IE8 이상에 대해 X-Download-Options를 설정합니다.
- **noCache**는 Cache-Control 및 Pragma 헤더를 설정하여 클라이언트 측에서 캐싱을 사용하지 않도록 합니다.
- **noSniff**는 X-Content-Type-Options를 설정하여, 선언된 콘텐츠 유형으로부터 벗어난 응답에 대한 브라우저의 MIME 가로채기를 방지합니다.
- **frameguard**는 X-Frame-Options 헤더를 설정하여 clickjacking에 대한 보호를 제공합니다.
- **xssFilter**는 X-XSS-Protection을 설정하여 대부분의 최신 웹 브라우저에서 XSS(Cross-site scripting) 필터를 사용하도록 합니다.

다른 모든 모듈처럼 Helmet은 다음과 같이 설치할 수 있습니다.

```
$ npm install --save helmet
```

이후 코드에서 Helmet을 사용하는 방법은 다음과 같습니다.

```
...  
var helmet = require('helmet');  
app.use(helmet());  
...
```



```

28 import axios from 'axios';
29
30 import './App.css';
31
32 import MemberContainer from './containers/MemberContainer'; // 멤버
33 //import MyFriend from './components/MyFriend'; // 내 친구
34 import FriendContainer from './containers/FriendContainer'; // 내 친구
35
36 //import FacebookLogin from './components/FacebookLogin';
37
38
39 //console.log(localStorage)
40 class App extends Component {
41   render() {
42     return (
43       <Router>
44         <div className="App">
45           <Header/>
46           <Navbar/>
47           {}
48           <Route exact path="/" component={ Home } />
49           <Route exact path="/login" component={ Login } />
50           <Route exact path="/member/new" component={ Register } />
51           <Route exact path="/group/new" component={ GroupRegister } />
52           <Route exact path="/post/new" component={ PostForm } />
53           <Route exact path="/post/detail" component={ DetailPost } />
54           <Route exact path="/post/location" component={ PicupMap } />
55           <Route exact path="/map" component={ PicupPostListMap } />
56           <Route exact path="/group" component={ MyGroup } />
57           <Route exact path="/board/group" component={ GroupBoard } />
58           <Route exact path="/search" component={ Search } />
59           <Route exact path="/around" component={ SearchPicupMap } />
60           <Route exact path="/member" component={ MemberContainer } />
61           <Route exact path="/friend" component={ Friend } />
62           <Route exact path="/board" component={ Board } />
63           <Route exact path="/friend/recommend" component={ FriendRecommend } />
64           <Route exact path="/colorfulmap" component={ PicupColorfulMap } />
65         </div>
66       </Router>
67     );
68   }
69 }
70
71 export default App;

```

```
JS app.js {} package.json x
1 {
2   "name": "frontend",
3   "version": "0.1.0",
4   "private": true,
5   "dependencies": {
6     "axios": "^0.18.0",
7     "bootstrap": "^4.1.3",
8     "classnames": "^2.2.6",
9     "jimp": "^0.5.3",
10    "jwt-decode": "^2.2.0",
11    "npm": "^6.3.0",
12    "passport-facebook": "^2.1.1",
13    "passport-kakao": "0.0.5",
14    "react": "^16.4.2",
15    "react-avatar-edit": "^0.6.0",
16    "react-bootstrap": "^0.32.4",
17    "react-checkbox-group": "^4.0.1",
18    "react-dom": "^16.4.2",
19    "react-facebook-login": "^4.0.1",
20    "react-google-maps": "^9.4.5",
21    "react-passport-auth": "^1.2.1",
22    "react-redux": "^5.0.7",
23    "react-router-dom": "^4.3.1",
24    "react-scripts": "^1.1.4",
25    "redux": "^4.0.0",
26    "redux-thunk": "^2.3.0"
27  },
28  "scripts": {
29    "start": "react-scripts start",
30    "build": "react-scripts build",
31    "test": "react-scripts test --env=jsdom",
32    "eject": "react-scripts eject"
33  },
34  "proxy": {
35    "/api/*": {
36      "target": "http://localhost:4000/",
37      "secure": "false"
38    },
39    "/auth/*": {
40      "target": "http://localhost:4000/",
41      "secure": "false"
42    }
43  }
44 }
45
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 168

No.	Time	Source	Destination	Protocol	Length	Info
8193	358.936740	14.63.171.152	192.168.0.2	TCP	66	3000 → 2647 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=128
8194	358.936817	192.168.0.2	14.63.171.152	TCP	54	2647 → 3000 [ACK] Seq=1 Ack=1 Win=65536 Len=0
8195	358.937129	192.168.0.2	14.63.171.152	HTTP	780	GET /api/board/5bbe1331d0b3c168ef95ebf0/post/5bbeefaf5ce6f7c7c003e2a0b1f2a000 HTTP/1.1
8196	358.946681	14.63.171.152	192.168.0.2	TCP	54	3000 → 2647 [ACK] Seq=1 Ack=727 Win=16128 Len=0
8197	358.955350	14.63.171.152	192.168.0.2	TCP	1514	3000 → 2647 [ACK] Seq=1 Ack=727 Win=16128 Len=1460 [TCP SACK] Win=65536 Len=0
8198	358.955459	14.63.171.152	192.168.0.2	TCP	179	3000 → 2647 [PSH, ACK] Seq=1461 Ack=727 Win=16128 Len=125
8199	358.955479	192.168.0.2	14.63.171.152	TCP	54	2647 → 3000 [ACK] Seq=727 Ack=1586 Win=65536 Len=0
8200	358.956066	14.63.171.152	192.168.0.2	HTTP	55	HTTP/1.1 200 OK (application/json)
8201	358.956125	192.168.0.2	14.63.171.152	TCP	54	2647 → 3000 [ACK] Seq=727 Ack=1588 Win=65536 Len=0
8202	358.956361	192.168.0.2	14.63.171.152	TCP	54	2647 → 3000 [FIN, ACK] Seq=727 Ack=1588 Win=65536 Len=0
8204	358.965236	14.63.171.152	192.168.0.2	TCP	54	3000 → 2647 [ACK] Seq=1588 Ack=728 Win=16128 Len=0

Frame 8195: 780 bytes on wire (6240 bits), 780 bytes captured (6240 bits) on interface 0

Ethernet II, Src: RivetNet_e0:8b:93 (9c:b6:d0:e0:8b:93), Dst: EFWNetwo_d5:c1:2c (90:9f:33:d5:c1:2c)

Internet Protocol Version 4, Src: 192.168.0.2, Dst: 14.63.171.152

Transmission Control Protocol, Src Port: 2647, Dst Port: 3000, Seq: 1, Ack: 1, Len: 726

Hypertext Transfer Protocol

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCIP
Follow TCP Stream
Copy UDP Stream
Protocol Preferences SSL Stream
Decode As... HTTP Stream
Show Packet in New Window

```

0000  90 9f 33 d5 c1 2c 9c b6 d0 e0 8b 93 08 00 45 00  ...3....E.
0010  02 fe 0e 4a 40 00 00 06 f7 2e c0 a8 00 02 0e 3f  ...30...0....?
0020  ab 98 0a 57 0b 0d d7 14 30 b4 65 9f 76 cf 50 18  ...w....0-e.v.P.
0030  01 00 68 75 00 00 47 45 54 20 2f 61 70 69 2f 62  ..hu..GE T /api/b
0040  6f 61 72 64 2f 35 62 62 65 31 33 33 31 64 30 62  oard/5bb e1331d0b
0050  33 63 31 36 38 65 66 39 35 65 62 66 30 2f 70 6f  3c168ef9 5ebf0/po
0060  73 74 2f 35 62 62 65 65 66 61 35 63 65 36 66 65  st/5bbeefaf5ce6fe
0070  37 35 32 39 38 61 62 36 34 30 62 2f 63 6f 6d 6d  75298ab0 40b/comm
0080  65 66 74 20 48 54 54 50 2f 31 2e 31 0d 0a 40 6f  ent HTTP /1.1..ho
0090  73 74 3a 20 31 34 2e 36 33 2e 31 37 31 2e 31 35  st: 14.6 3.171.15
00a0  32 3a 33 30 30 30 0d 0a 43 6f 6e 6e 65 63 74 69  2:3000.. Connecti
00b0  6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a  on: keep -alive..
00c0  41 63 63 65 70 74 3a 20 61 70 70 6c 69 63 61 74  Accept: applicat
  
```

wreshark_C3D666DB-3F53-4D2B-9DB9-8113FEE943B8_20181018014858_a11740

Packets: 12821 Displayed: 12 (0.1%) Profile: Default

Wireshark · Follow TCP Stream (tcp.stream eq 166) · wireshark_C3D656DB-3F53-4D2B...

GET /api/board/5bbe1331d0b3c168ef95ebf0/post/5bbeefa5ce6fe75298ab640b/
comment HTTP/1.1

Host: 14.63.171.152:3000

Connection: keep-alive
Accept: application/json, text/plain, */*
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfawQiOiJmYWNLm9vazEyMzI5MDUzNTI3O
DUxMyIsImhhdCI6MTUzOTMxMzQ0MX0.23S0HkCf_q_ElF00QNxD1YA7i2Q8ePErRKj5OT_uRQ
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36
Referer: http://14.63.171.152:3000/post/detail
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7

Cookie: connect.sid=s%3ATELNxm3SztTrgbpA6ac11WU5SM8w_6g0.j7%2FR1kbwYSY
%2B13c0sltNB0EkCK2Hx690P%2BFcdGFjHXk

HTTP/1.1 200 OK
X-Powered-By: Express
x-dns-prefetch-control: off
x-frame-options: SAMEORIGIN
strict-transport-security: max-age=15552000; includeSubDomains
x-download-options: noopen
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
surrogate-control: no-store
cache-control: no-store, no-cache, must-revalidate, proxy-revalidate
pragma: no-cache
expires: 0
access-control-allow-origin: *
access-control-allow-methods: GET, POST, PUT, DELETE
access-control-allow-headers: content-type, authorization
content-type: application/json; charset=utf-8


3 client pkt(s), 5 server pkt(s), 3 turn(s).

Entire conversation (2312 bytes) Show and save data as ASCII Stream 166

Find: Find Next

Filter Out This Stream Print Save as... Back 닫기 도움말

Security Report Summary



Site: <http://14.63.171.152:3000/> [\(Scan again over https\)](#)

IP Address: 14.63.171.152

Report Time: 17 Oct 2018 14:34:51 UTC

Headers:

✖ Content-Security-Policy

✖ X-Frame-Options

✖ X-XSS-Protection

✖ X-Content-Type-Options

✖ Referrer-Policy

✖ Feature-Policy

Warning: Grade capped at A, please see warnings below.

Raw Headers

HTTP/1.1	200 OK
X-Powered-By	Express
Accept-Ranges	bytes
Content-Type	text/html; charset=UTF-8
Content-Length	2281
ETag	W/"8e9-iK7AYtotV3j/IZ6KGn50s+IeVM"
Vary	Accept-Encoding
Date	Wed, 17 Oct 2018 14:34:50 GMT
Connection	keep-alive

Missing Headers

Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "x-frame-options: SAMEORIGIN".
X-XSS-Protection	X-XSS-Protection sets the configuration for the cross-site scripting filter built into most browsers. Recommended value "X-XSS-Protection: 1; mode=block".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Feature-Policy	Feature Policy is a new header that allows a site to control which features and APIs can be used in the browser.

← → ↺

주요 정보

14.63.171.152:3000

☆ CSS

🔍

🌐

🔒

🔑

🔧

🔗

📁

Software

Art

Info

Shopping

공공데이터

Job

Bookmarks

새 탭

내이버 : 나의 길잡이

Facebook

GitHub

hello world!!!!!!!

```

23 var helmet = require('helmet'); // HTTP 헤더를 설정하여 웹 취약성으로부터 정보를 보호하는 모듈
24
25 DB_URL = db.config.url;
26 SESSION_KEY = session_config.secret;
27
28 mongoose.Promise = global.Promise;
29 mongodb = DB_URL;
30 mongoose.connect(mongodb);
31
32 var db = mongoose.connection;
33
34 db.once('open', function () {
35   console.log('DB connected!');
36 });
37
38 db.on('error', function (err) {
39   console.log('DB ERROR:', err);
40 });
41
42 var app = express();
43
44 app.use(express.static('upload'));
45
46 app.use(bodyParser.urlencoded({ extended: true })); // content-type header를 보고 unencoded body를 parse해줌. extended로 string, array외의 type을 받을수 있도록함.
47 app.use(bodyParser.json());
48
49 app.use(session({
50   secret: SESSION_KEY, //keyboard cat (랜덤한 값)
51   resave: false, // 세션을 언제나 저장할 지 (변경되지 않아도) 저장하는 것
52   saveUninitialized: true, // 세션이 저장되기 전에 uninitialized 상태로 미리 만들어서 저장
53   store: new FileStore(),
54 }));
55
56 app.use(helmet()); // 헤더 보안
57 app.use(helmet.noCache());
58 app.use(helmet.xssFilter());
59 app.use(helmet.noSniff());
60 app.disable('x-powered-by');
61
62 app.use(function (req, res, next) {
63
64   res.header('Access-Control-Allow-Origin', '*');
65   res.header('Access-Control-Allow-Methods', 'GET, POST, PUT, DELETE');
66   res.header('Access-Control-Allow-Headers', 'Content-type, authorization');
67
68   next();
69 });

```

The image shows a Wireshark packet capture analysis. The top pane displays a list of captured packets. Packet 15312 is highlighted, showing an HTTP GET request from 192.168.0.2 to 14.63.171.152. The bottom pane shows the details of this packet, including the Ethernet II header, Internet Protocol Version 4 header, and Hypertext Transfer Protocol details. The packet is a GET request for the root path (/) with a user-agent of 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36'.

No.	Time	Source	Destination	Protocol	Length	Info
15302	1342.519942	192.168.0.2	14.63.171.152	TCP	66	2809 → 4000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
15310	1342.548242	14.63.171.152	192.168.0.2	TCP	66	4000 → 2809 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=128
15311	1342.548275	192.168.0.2	14.63.171.152	TCP	54	2809 → 4000 [ACK] Seq=1 Ack=1 Win=65536 Len=0
15312	1342.548453	192.168.0.2	14.63.171.152	HTTP	570	GET / HTTP/1.1
15323	1342.571775	14.63.171.152	192.168.0.2	TCP	54	4000 → 2809 [ACK] Seq=1 Ack=517 Win=15744 Len=0
15324	1342.571775	14.63.171.152	192.168.0.2	TCP	745	4000 → 2809 [PSH, ACK] Seq=1 Ack=517 Win=15744 Len=0
15335	1342.618505	192.168.0.2	14.63.171.152	TCP	54	2809 → 4000 [ACK] Seq=517 Ack=692 Win=64768 Len=0
15336	1342.628105	14.63.171.152	192.168.0.2	HTTP	55	HTTP/1.1 200 OK (text/html)
15337	1342.670355	192.168.0.2	14.63.171.152	TCP	54	2809 → 4000 [ACK] Seq=517 Ack=693 Win=64768 Len=0
15382	1347.573756	14.63.171.152	192.168.0.2	TCP	54	4000 → 2809 [FIN, ACK] Seq=693 Ack=517 Win=15744 Len=0
15383	1347.573809	192.168.0.2	14.63.171.152	TCP	54	2809 → 4000 [ACK] Seq=517 Ack=694 Win=64768 Len=0

Details of packet 15312:

- Ethernet II, Src: RivetNet 08:8b:93 (9c:b6:d0:e0:8b:93), Dst: EfwNetwo_d5:c1:2c (90:9f:33:d5:c1:2c)
- Internet Protocol Version 4, Src: 192.168.0.2, Dst: 14.63.171.152
- Transmission Control Protocol, Src Port: 2809, Dst Port: 4000, Seq: 1, Ack: 1, Len: 516
- Hypertext Transfer Protocol
 - GET / HTTP/1.1
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36

GET / HTTP/1.1

Host: 14.63.171.152:4000

Connection: keep-alive

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8

Accept-Encoding: gzip, deflate

Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7

Cookie: connect.sid=s%3ATELNxm3SztTrgbpA6ac11WU5SM8w_6g0.j7%2FR1kbwYSY%2B13c0sltNB0EkCK2Hx690P%2BFcdGFjHXk

HTTP/1.1 200 OK

X-DNS-Prefetch-Control: off

X-Frame-Options: SAMEORIGIN

Strict-Transport-Security: max-age=15552000; includeSubDomains

X-Download-Options: noopen

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

Surrogate-Control: no-store

Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate

Pragma: no-cache

Expires: 0

Access-Control-Allow-Origin: *

Access-Control-Allow-Methods: GET, POST, PUT, DELETE

Access-Control-Allow-Headers: content-type, authroization

Content-Type: text/html; charset=utf-8


Content-Length: 20

ETag: W/"14-4YUWBmO2gRgBaRxNsovh9kucpgg"

Date: Wed, 17 Oct 2018 17:11:21 GMT

Connection: keep-alive

SECURITY REPORT



Site:

IP Address:

Report Time:

Headers:

Warning:

<http://14.63.171.152:4000/> (Scan again over https)

14.63.171.152

17 Oct 2018 14:35:38 UTC

✓ X-Frame-Options

✓ X-Content-Type-Options

✓ X-XSS-Protection

✗ Content-Security-Policy

✗ Referrer-Policy

✗ Feature-Policy

Grade capped at A, please see warnings below.

Raw Headers

HTTP/1.1	200 OK
X-DNS-Prefetch-Control	off
X-Frame-Options	SAMEORIGIN
Strict-Transport-Security	max-age=15552000; includeSubDomains
X-Download-Options	noopen
X-Content-Type-Options	nosniff
X-XSS-Protection	1; mode=block
Surrogate-Control	no-store
Cache-Control	no-store, no-cache, must-revalidate, proxy-revalidate
Pragma	no-cache
Expires	0
Access-Control-Allow-Origin	*
Access-Control-Allow-Methods	GET, POST, PUT, DELETE
Access-Control-Allow-Headers	content-type, authorization
Content-Type	text/html; charset=utf-8
Content-Length	20
ETag	W/"14-4YUW8mO2gRgBaRxNsovH9kucpgg"
set-cookie	connect.sid=s%3A4WIAy7jpvatO8juYBEILLxNtsByxtFzc.GAJbKhmj5L9kCPL7zDFQ8h%2B5xs2A%2FX66w0oUn3wpnFA; Path=/; HttpOnly
Date	Wed, 17 Oct 2018 14:35:38 GMT
Connection	keep-alive

Missing Headers

Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Feature-Policy	Feature Policy is a new header that allows a site to control which features and APIs can be used in the browser.

3. 참조

- <http://expressjs.com/ko/advanced/best-practice-security.html>