웹 취약점 점검 어플리케이션 개발

이승찬*, 장원준*, 조남현*, 조현욱**
*백석대학교 정보보호학과
**중부대학교 정보보호학과
e-mail : toevas@naver.com

Development for Web Weakness Application

Seung-Chan Lee*, Won-June Jang*, Nam-Hyun Jo*,
Hyeon-Wook Jo**
*Dept of Information Security, Baek Seok University
**Dept of Information Security, Joong Bu University,

요 약

이 어플리케이션은 서버의 취약점을 보고하는 것을 목적으로 한다. 웹 취약점 점검을 위해서 Nikto와 Nmap을 이용했고, 취약점 분석 보고서를 시간 순으로 보기 위해 보고서에 순번을 정해 피드백을 생성하도록 하였다. 또한 웹 취약점 번호를 생성함으로써 사용자가 좀 더 효율적으로 웹 서버의 취약점을 확인할 수 있도록 개발하였다.

1.서 론

시장조사업체 가트너에 의하면 2016년에 약 64억 개의 IOT 기기가 있었지만, 2017년에는 84억 개의 IOT기기가 있을 것이라고 추정하고 있다. 그 수는 2016년도의 약 31% 증가한 것으로 나타났다.[1]

IOT기기들은 모두 인터넷에 연결되어있고 패치하기도 어렵다보니 IOT의 보안이 취약한 것으로 나타났다.[2]

본 연구에서는 별도의 장비 없이 스마트 폰의 어플리케이션만으로 취약점을 분석한다.

2. 사물인터넷 시장

2.1 사물인터넷 시장 현황

가트너(Gartner)의 통계자료에 따르면, 2014년에 비해 2020년 사물인터넷의 부가가치는 약 5배의 성장을 예측하고 있으며, 이 밖에도 국내·외 사물인터넷 시장 및 정책 동향을 분석한 자료인 [3]는 국내시장 규모를 그림 1과 그림 2와 같이 규모면에서 2022년까지 약 6배의 성장과 함께 서비스 및 애플리케이션과 디바이스의 비중이 점차 커질 것으로 전망했다.

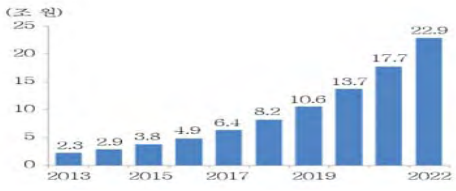

그림 1. 국내 사물 인터넷 시장 규모 전망[3]

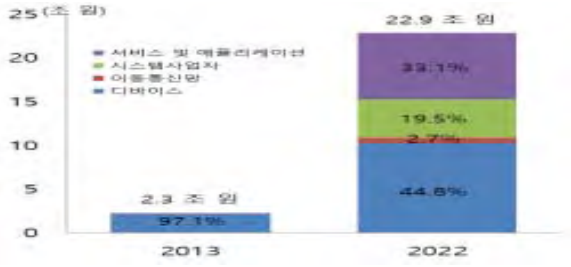

그림 2. 국내 사물 인터넷 시장 규모

2.2 웹 해킹 통계

씨디네트웍스의 2016년 4분기 통계자료에 따르면, SQL Injection, CSRF(Cross-site Request Forgery) 및 XSS (Cross-site scripting) 등 웹에 대한 공격 시도가 많은 부분을 차지하고 있다.[4]

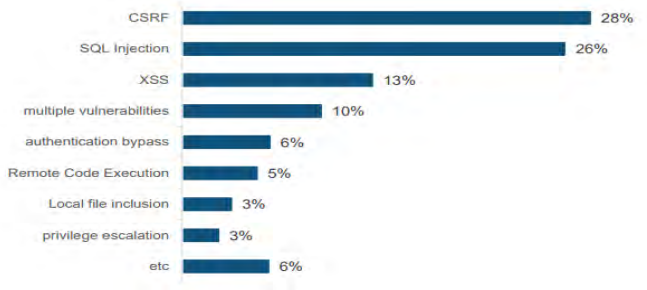

그림 3. 취약점 유형별 공격

그림 3은 SQL Injection, CSRF(Cross-site Request Forgery) 및 XSS (Cross-site scripting) 등 웹에 대한 공격 시도가 많은 부분을 차지하는 것을 나타낸다.

2.3 웹 해킹 사례

AhnLab에 따르면 2017년 5월에 영국을 시작으로 전 세계에 발생한 워너크라이(WannaCry) 랜섬웨어[5]는 SMB 원격 코드 실행 취약점을 이용한 공격이었다. 이를 막기 위해서는 열려 있는 Port를 막아 SMB의 원격 실행을 차단했어야 했다.

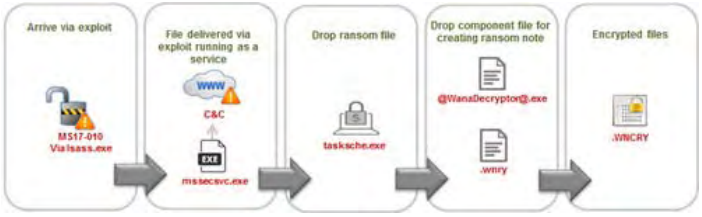

그림 4. 워너크라이 공격 방법

그림 4는 워너크라이 랜섬웨어의 침투 방식을 나타낸다.

또한 미래창조과학부와 방송통신위원회의 민·관합동조사단의 조사결과에 의하면 얼마 전 숙박 App인 '여기어때'의 사용자 개인정보가 유출되는 사건이 있었다. 약 99만 명의 개인정보가

유출되었고 웹사이트는 비정상적인 DB 질의 검증 절차가 없어 SQL 인젝션 공격에 취약한 웹페이지가 존재하였고 탈취된 관리자 세션 값을 통한 우회 접속(세션변조 공격)을 탐지·차단하는 체계도 없었던 것으로 확인했다.

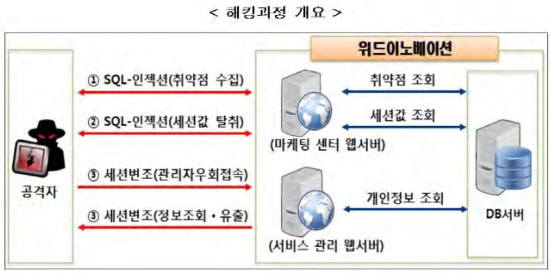

그림 5. '여기 어때' 해킹 과정

그림 5는 숙박 어플리케이션인 '여기어때'의 해킹 과정을 나타낸다. 이처럼 웹페이지의 공격만으로도 이렇게 큰 피해가 발생할 수 있다.

3. 관련연구

3.1 어플리케이션 구성도

웹 취약점 점검 어플리케이션은 클라이언트에서 점검대상주소와 옵션을 설정 후 점검을 시작하게 된다. 그 후 Client와 TCP Socket 통신을 이용하여 데이터를 송·수신한다.

서버에서 받은 옵션 인자를 토대로 Port Scan과 Web Scan 함수를 호출한다.

Port Scan 결과 값과 Web Scan 결과 값을 나누어 데이터베이스에 저장한 후 데이터베이스에 저장되어 있는 값을 보고서 형식으로 작성하여 작성된 보고서를 어플리케이션에서 순서에 맞춰서 열람할 수 있도록 하였다.

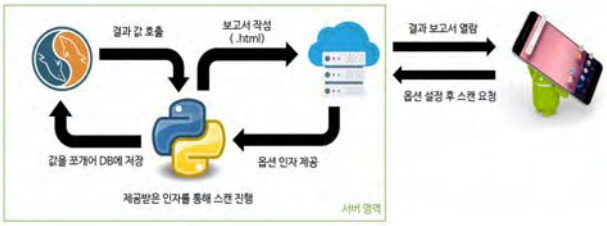

그림 6. 어플리케이션 구성도

그림 6은 웹 취약점 점검 어플리케이션의 자세한 구성도를 나타낸다.

3.2 주요 기능

Port Scan기능은 오픈 소스 툴인 Nmap을 사용하여 웹 서버의 열려 있는 포트 정보를 확인 가능하게 만들었다.

Web Scan의 경우 오픈 소스 툴인 Nikto를 사용하여 웹 서버에 존재하는 웹 취약점(Directory Indexing Attacks, XSS 등)을 확인 가능하며 각 취약점에 대한 정보를 제공했다.

두 기능 모두 HTML 형식의 보고서가 제공되며 고유번호인 작업번호를 기준으로 이전 스캔 정보를 확인할 수 있다.

그림 7. 어플리케이션 실행 화면

그림 7은 어플리케이션을 실행하여 얻은 결과 보고서를 확인하는 화면이다.

3.3 DB 파싱

Nmap의 경우 -sS옵션을 이용하여 출력되는 형식을 Output을 파일로 만들어 split("")를 이용하여 띄어쓰기 기준으로 자른 후, split("/") 로 / 기준으로 또 한 번 나누어 반복문을 사용하여 DB에 저장한다.

Nikto의 경우 Python에서 XML파서 라이브러리인 ElementTree를 사용하여 값을 변수에 담아서 파싱하였고 반복문으로 변수 값을 DB에 저장한다.

Nikto

```
mysql> desc opnikto;
+-------------+-------------+------+-----+---------+-------+
| Field       | Type        | Null | Key | Default | Extra |
+-------------+-------------+------+-----+---------+-------+
| idx         | varchar(6)  | YES  |     | NULL    |       |
| startTime   | datetime    | YES  |     | NULL    |       |
| endTime     | datetime    | YES  |     | NULL    |       |
| ip          | varchar(15) | YES  |     | NULL    |       |
| hostname    | varchar(100)| YES  |     | NULL    |       |
| port        | varchar(50) | YES  |     | NULL    |       |
| sitename    | varchar(100)| YES  |     | NULL    |       |
| banner      | varchar(200)| YES  |     | NULL    |       |
| total       | varchar(20) | YES  |     | NULL    |       |
| vulnetable  | varchar(20) | YES  |     | NULL    |       |
| second      | varchar(20) | YES  |     | NULL    |       |
| method      | varchar(50) | YES  |     | NULL    |       |
| osvdb       | varchar(50) | YES  |     | NULL    |       |
| description | text        | YES  |     | NULL    |       |
| uri         | text        | YES  |     | NULL    |       |
| namelink    | text        | YES  |     | NULL    |       |
| iplink      | text        | YES  |     | NULL    |       |
+-------------+-------------+------+-----+---------+-------+
```

그림 8. Nikto DB 테이블

nmap

```
mysql> desc opnmap;
+----------+-------------+------+-----+---------+-------+
| Field    | Type        | Null | Key | Default | Extra |
+----------+-------------+------+-----+---------+-------+
| idx      | varchar(6)  | NO   |     | NULL    |       |
| ID       | varchar(20) | NO   |     | NULL    |       |
| DATE     | varchar(30) | NO   |     | NULL    |       |
| TARGET   | varchar(30) | NO   |     | NULL    |       |
| PORT     | varchar(6)  | NO   |     | NULL    |       |
| PROTOCOL | varchar(10) | NO   |     | NULL    |       |
| STATE    | varchar(20) | NO   |     | NULL    |       |
| SERVICE  | varchar(20) | NO   |     | NULL    |       |
+----------+-------------+------+-----+---------+-------+
```

그림 9. Nmap DB 테이블

그림 8과 그림 9는 Nikto와 Nmap 결과 값을 각 필드에 맞게 나누어 정상적으로 DB에 저장한 것을 나타낸다.

4. 개발 결과 및 고찰

Namp과 Nikto를 이용하여 기본적인 Port스캔과 취약점 스캔을 완료 하였고 이 외에도 XSS 같은 취약점과 CSRF에 대해서는 아직 부족하다고 생각된다. 좀 더 다양한 툴을 이용하여 여러 기능을 좀 더 추가해야 한다. 또한 시큐어 코딩을 통해 어플리케이션에 대한 보안도 추가해야 한다.

5. 결론 및 향후 연구

결론적으로 Port Scan기능과 Web Scan기능을 장착한 어플리케이션을 만드는데 성공하였고 좀 더 다양한 기능과 시큐어 코딩이 앞으로의 연구과제이다.

참고문헌

[1] 전정훈, “사물인터넷 기술동향과 전망에 관한 연구,” 융합보안학회, vol.14, no.7, 2014.12

[2] 진정훈, “사물 인터넷의 보안 위협 요인들에 대한 분석”, 융합보안 논문지 제 15권 제7호, p. 5~6, 2015.12

[3] 이현지, 김광석, “사물인터넷의 국내외 시장 및정책 동향,” 한국정보통신기술진흥센터, 주간기술동향, 2015.9.16

[4] 씨디네트웍스 보안서비스팀, “2016년 4분기 웹 공격 분석 보고서”, 씨디네트웍스, 2017,2

[5] 한국랜섬웨어침해대응센터, “[긴급] Windows SMB 취약점을 이용한 WanaCry 랜섬웨어 전 세계 감염 확산”, 2017.5.14

[6] 이유지, ‘여기어때’ 개인정보 99만건 유출…‘SQL인젝션’ 공격이 원인”, https://www.bloter.net/archives/278144 , 2017.4.26

본 논문은 미래창조과학부의 지원을 통해 수행한 ICT 멘토링 사업의 프로젝트 결과물입니다.