

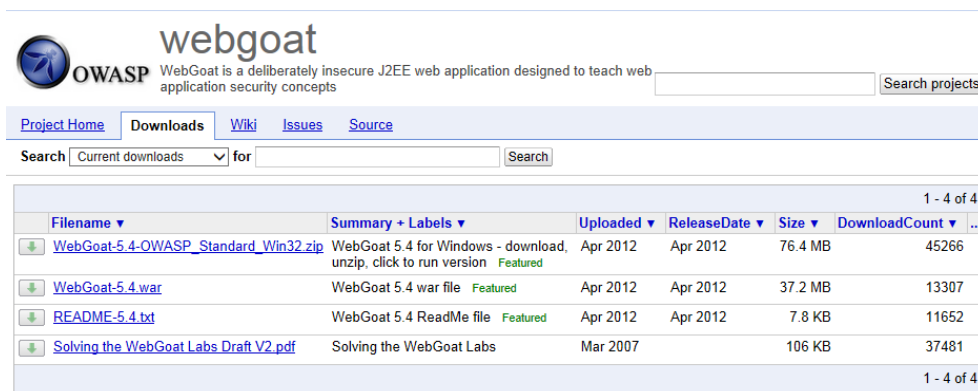
## WebGoat

WebGoat란 OWASP에서 발표한 10대 웹 애플리케이션의 취약점(OWASP TOP 10)을 기반으로 웹 취약점을 테스트하며, 웹 취약점의 기술적인 이해를 돕기 위해 만들어진 웹 취약점을 내포한 웹 애플리케이션을 말한다. WebGoat는 12개의 웹 취약점을 다루고 있어, 교육용으로 많이 사용된다.

### 4.1 설치

웹 사이트 취약점 분석의 기술적인 이해 자료로 활용되는 WebGoat의 설치 방법에 대해서 알아보자. WebGoat는 구글(google) 검색 엔진에서 'WebGoat download' 키워드를 입력하여 검색 후 내려받을 수 있다.

<http://code.google.com/p/webgoat/downloads/list>



| Filename                              | Summary + Labels  | Uploaded | ReleaseDate | Size    | DownloadCount |
|---------------------------------------|---|----------|-------------|---------|---------------|
| WebGoat-5.4-OWASP_Standard_Win32.zip  | WebGoat 5.4 for Windows - download, unzip, click to run version | Apr 2012 | Apr 2012    | 76.4 MB | 45266         |
| WebGoat-5.4.war                       | WebGoat 5.4 war file  | Apr 2012 | Apr 2012    | 37.2 MB | 13307         |
| README-5.4.txt                        | WebGoat 5.4 ReadMe file   | Apr 2012 | Apr 2012    | 7.8 KB  | 11652         |
| Solving the WebGoat Labs Draft V2.pdf | Solving the WebGoat Labs  | Mar 2007 |             | 106 KB  | 37481         |

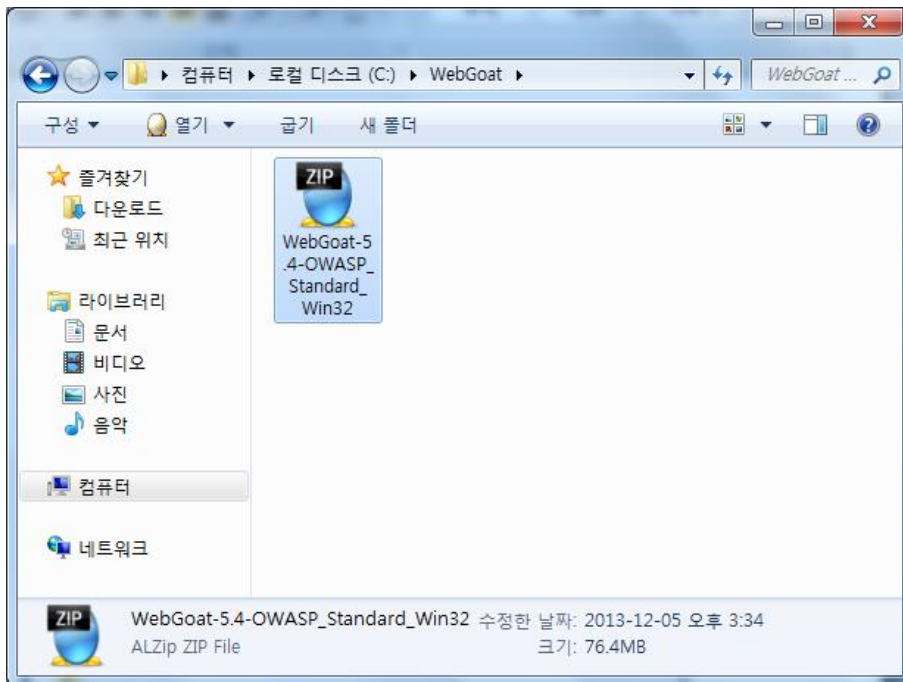
WebGoat를 설치하기 전에 확인할 사항이 있다. WebGoat는 JSP 기반의 웹 애플리케이션이므로 자바가 사전 설치되어 있어야 운영할 수 있다. 혹시 설치가 이미 된 독자들도 아래에서 설명한 절차를 따라가면서 WebGoat를 정상적으로 운영할 수 있는 환경인지를 확인해 보도록 하자.

| 사전 요구 사항                  |
|---------------------------|
| ① 자바 1.4.1 이상 버전 설치       |
| ② 운영 환경을 위한 시스템 환경 변수 설정  |
| ③ 환경 변수 설정 적용을 위한 시스템 리부팅 |

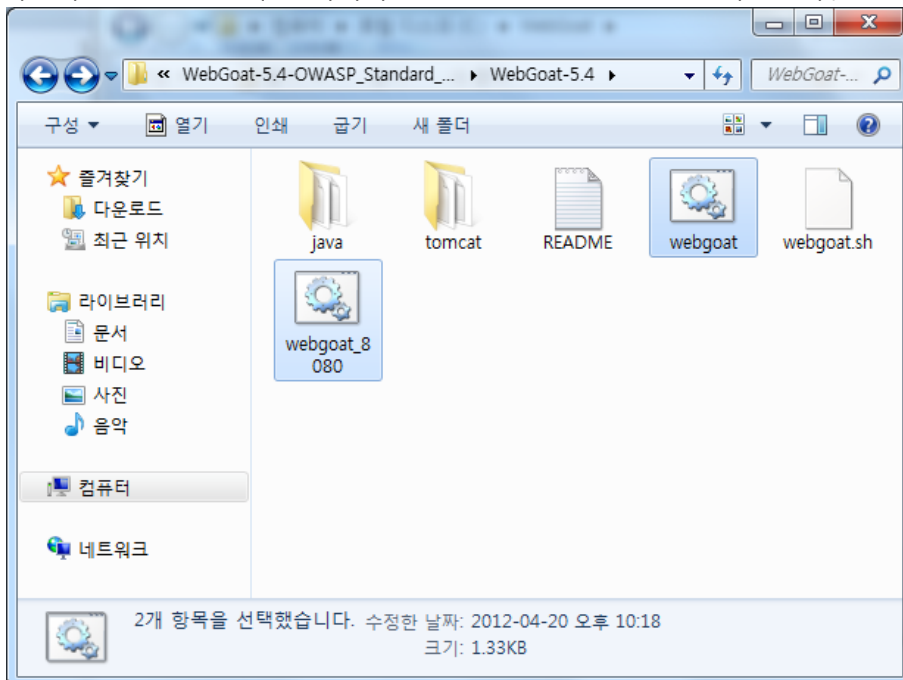
자바 설치에 앞서 소개한 파로스 부분에서 다뤘으므로 참고하길 바란다.

### [ WebGoat 설치 ]

1. 다운로드한 파일을 압축풀기 한다.

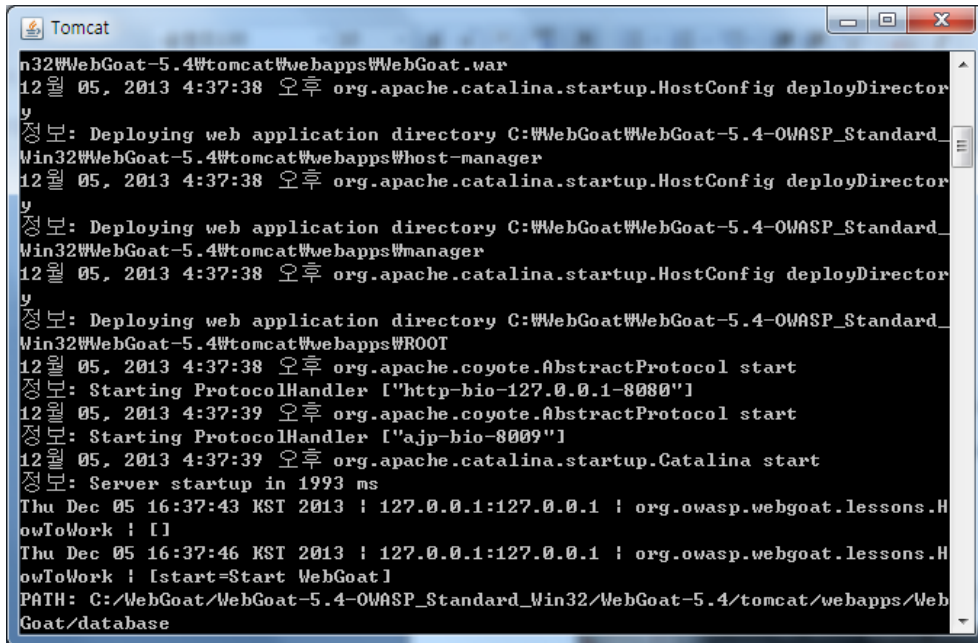


2. 압축을 푼 파일로 이동한다면 아래의 그림과 같이 여러 개의 폴더와 WebGoat 배치파일과 WebGoat\_8080 배치파일을 볼 수 있을 것이다. WebGoat 배치파일은 80번 포트를 사용하며, WebGoat\_8080은 8080 포트를 사용한다. (일반적으로 80번 포트는 윈도우에서 사용하므로 충돌 방지를 위해서 WebGoat는 8080 포트를 사용한다.)

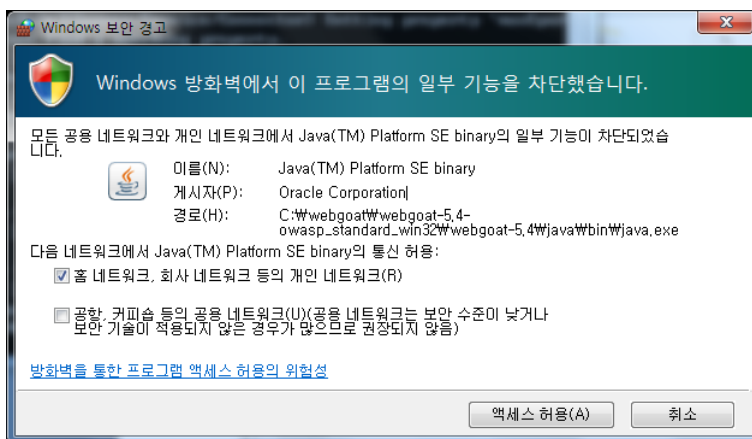


## 4.2 사용방법

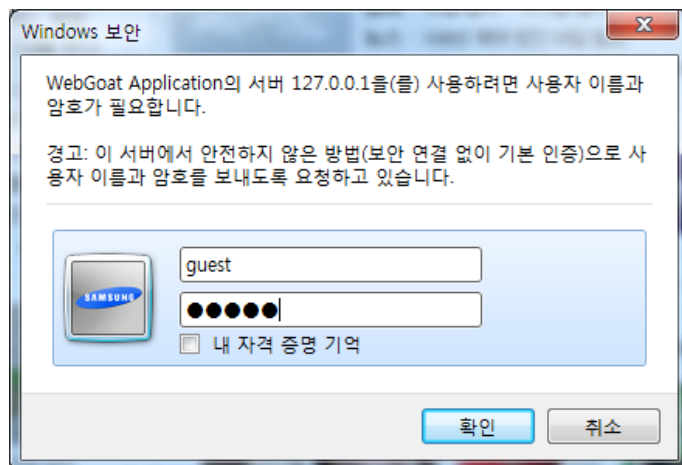
WebGoat를 사용하기 위해서 WebGoat\_8080 배치파일을 실행한다. 아래와 같이 WebGoat 실행 파일들이 실행된다.



또한 Windows 방화벽으로 인한 WebGoat 기능이 차단되므로 '엑세스 허용(A)'을 클릭한다.



웹 브라우저의 URL에 '<http://127.0.0.1:8080/WebGoat/attack>'을 입력한다.  
WebGoat를 실행하기 위해서 인증을 해야한다. (ID : guest, Pass : guest )

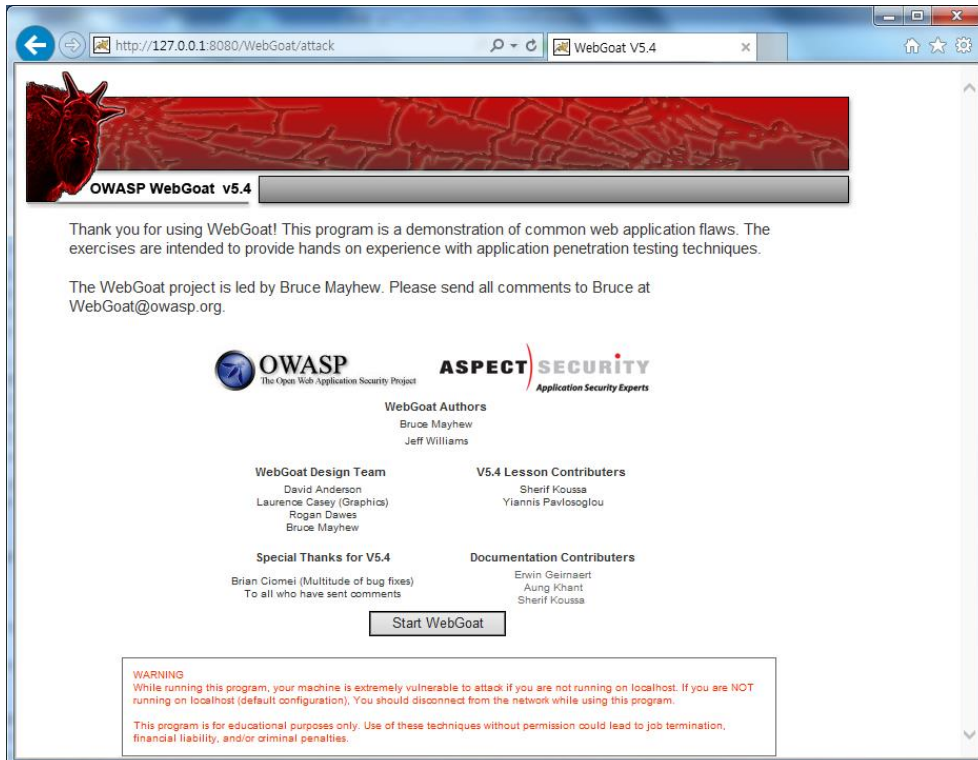


WebGoat를 실행하기 위해 입력하는 URL에 대한 설명은 아래의 표를 참고하길 바란다.

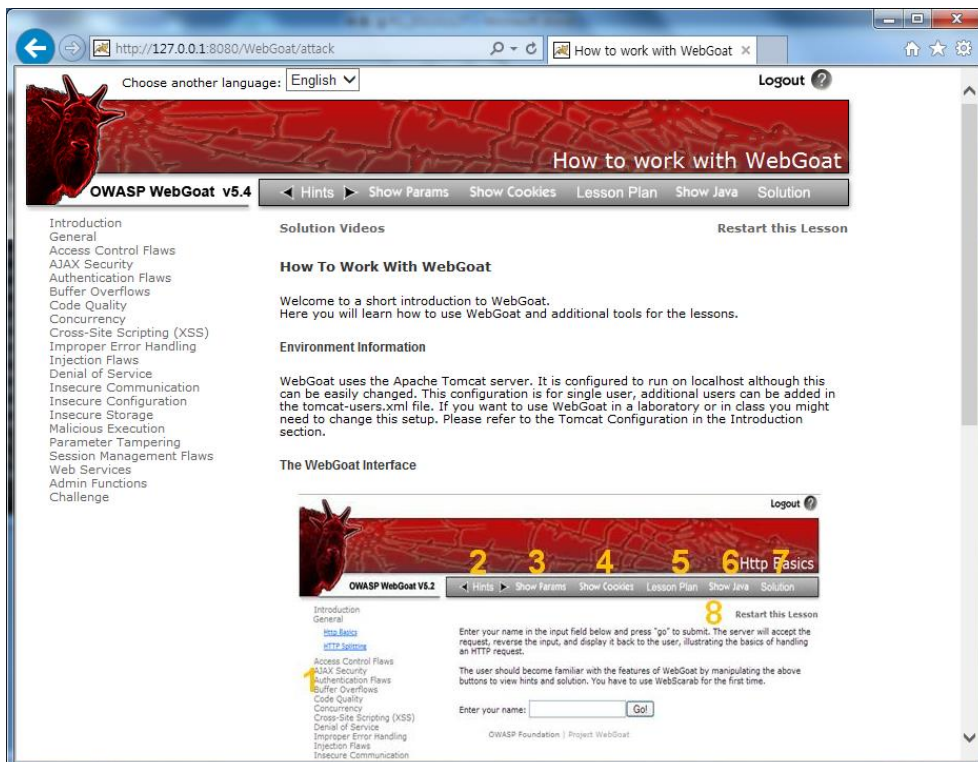
| WebGoat 실행 URL | 설명                    |
|----------------|-----------------------|
| http           | 프로토콜을 의미한다.           |
| 127.0.0.1      | 로컬 주소를 의미한다.          |
| 8080           | 포트번호를 의미한다.           |
| WebGoat/attack | WebGoat의 기본 경로를 의미한다. |

정상적으로 인증을 성공했다면 아래의 화면을 볼 수 있다. 만약 그렇지 않은 경우는 다시 한 번 절차대로 진행해보길 바란다.

본격적으로 WebGoat를 진행하기 위해서 'Start WebGoat'을 클릭한다.



왼쪽 상단을 보면 WebGoat의 다양한 취약점에 관해서 다뤄 볼 수 있다.



WebGoat에서 다루고 있는 취약점은 아래의 표를 참고하길 바란다.

| 취약점                        | 설명               |
|----------------------------|------------------|
| Access Control Flaws       | 접근 취약점           |
| AJAX Security              | AJAX 보안 취약점      |
| Authentication Flaws       | 인증 취약점           |
| Code Quality               | 코드 취약점           |
| Concurrency                | 동시성 처리의 취약점      |
| Cross-Site Scripting (XSS) | 크로스 사이트 스크립팅 취약점 |
| Improper Error Handling    | 부적절한 에러 처리 취약점   |
| Injection Flaws            | 인젝션 취약점          |
| Denial of service          | 서비스 거부 취약점       |
| Insecure Communication     | 안전하지 않은 통신 취약점   |
| Insecure Configuration     | 취약한 환경설정에 의한 취약점 |
| Insecure Storage           | 안전하지 않은 저장의 취약점  |
| Malicious Execution        | 악성(파일, 스크립트) 실행  |
| Parameter Tampering        | 부적절한 매개변수        |
| Session Management Flaws   | 세션 관리의 취약점       |
| Web Services               | 웹 서비스 취약점        |