

컴퓨터보안 실습

1주차

참고문헌 : 프리렉 (www.freelec.com) - 웹해킹과 방어

1. 프록시 툴을 이용한 HTTP분석(1)

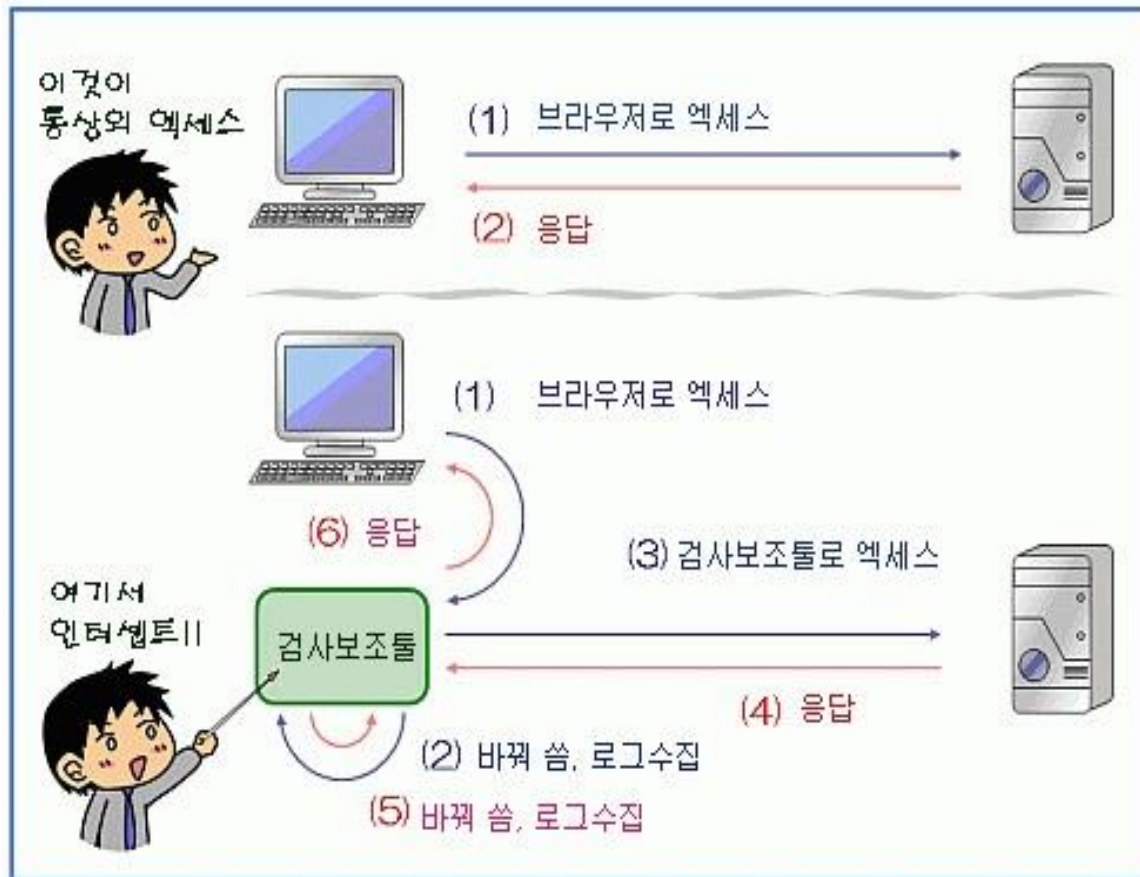


그림. HTTP분석 및 테스트

1. 프록시 툴을 이용한 HTTP분석(2)

파로스는 HTTP분석 (프록시 기능) 및 취약점 분석을 보유

* 파로스 운영 요구 사항

- ① 자바 1.4 이상 버전 설치 (파로스는 자바 어플리케이션)
- ② ant(자바 컴파일러) 설치 (파로스 소스 수정 및 컴파일)
- ③ 운영 환경을 위한 시스템 환경 변수 설정
- ④ 환경 변수 설정 적용을 위한 시스템 리부팅

1. 프록시 툴을 이용한 HTTP분석(3)

① 자바 설치 여부 확인

```
C:\W>java -version
```

```
java version "1.4.2_03"  
Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2_03-b02)  
Java HotSpot(TM) Client VM (build 1.4.2_03-b02, mixed mode)
```

[주의] 위와 같은 메시지가 없는 경우, java 설치되지 않음

자바설치는 “프리렉 본 강의 게시판” 혹은 “인터넷 검색을 통한 다운로드”

1. 프록시 툴을 이용한 HTTP분석(4)

② ant 설치 여부 확인

```
C:\W>ant
```

```
Buildfile: build.xml does not exist!  
Build failed
```

[주의] 위와 같은 메시지가 없는 경우, ant 설치

“프리렉 본 강의 게시판” 혹은 “인터넷 검색을 통한 다운로드”

1. 프록시 툴을 이용한 HTTP분석(5)

③ 시스템 환경 설정 - 자바 설정

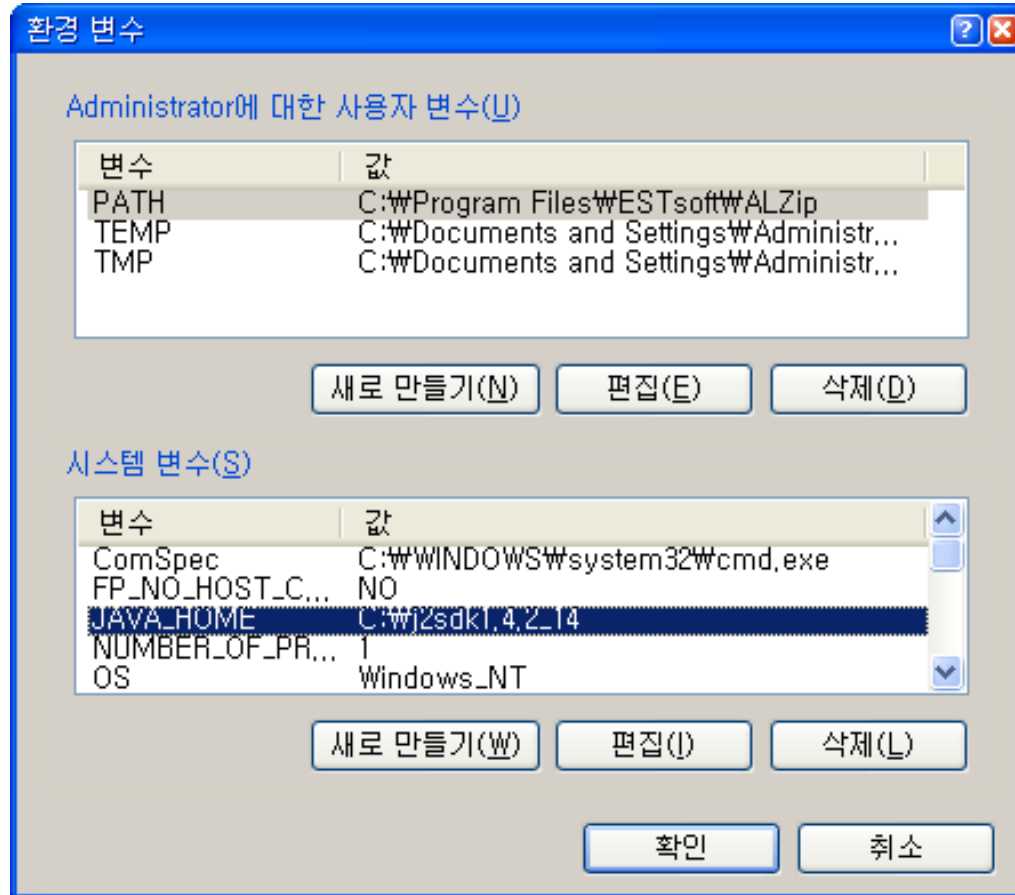


그림. 자바 설정

1. 프록시 툴을 이용한 HTTP분석(6)

③ 시스템 환경 설정(2)

2) ant 위치 지정 - "프리렉 본 강의 게시판"을 통한 다운로드

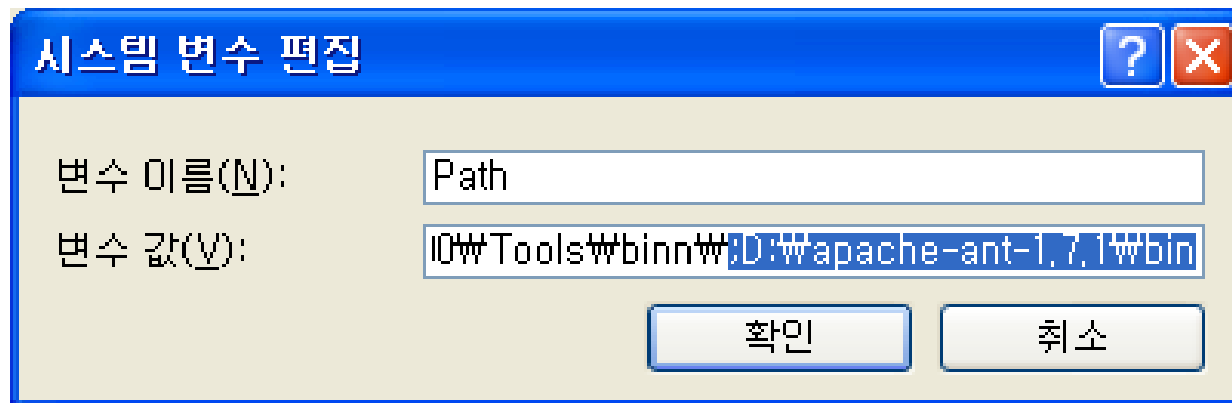


그림. ANT 설정

1. 프록시 툴을 이용한 HTTP분석(7)

④ 시스템 리부팅 후, 재 확인

```
C:\W>java -version
```

```
java version "1.4.2_03"
```

```
Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2_03-b02)
```

```
Java HotSpot(TM) Client VM (build 1.4.2_03-b02, mixed mode)
```

```
C:\W>ant
```

```
Buildfile: build.xml does not exist!
```

```
Build failed
```

1. 프록시 툴을 이용한 HTTP분석(8)

○ 파로스 설치 - 소스 및 실행파일 다운로드 및 설치

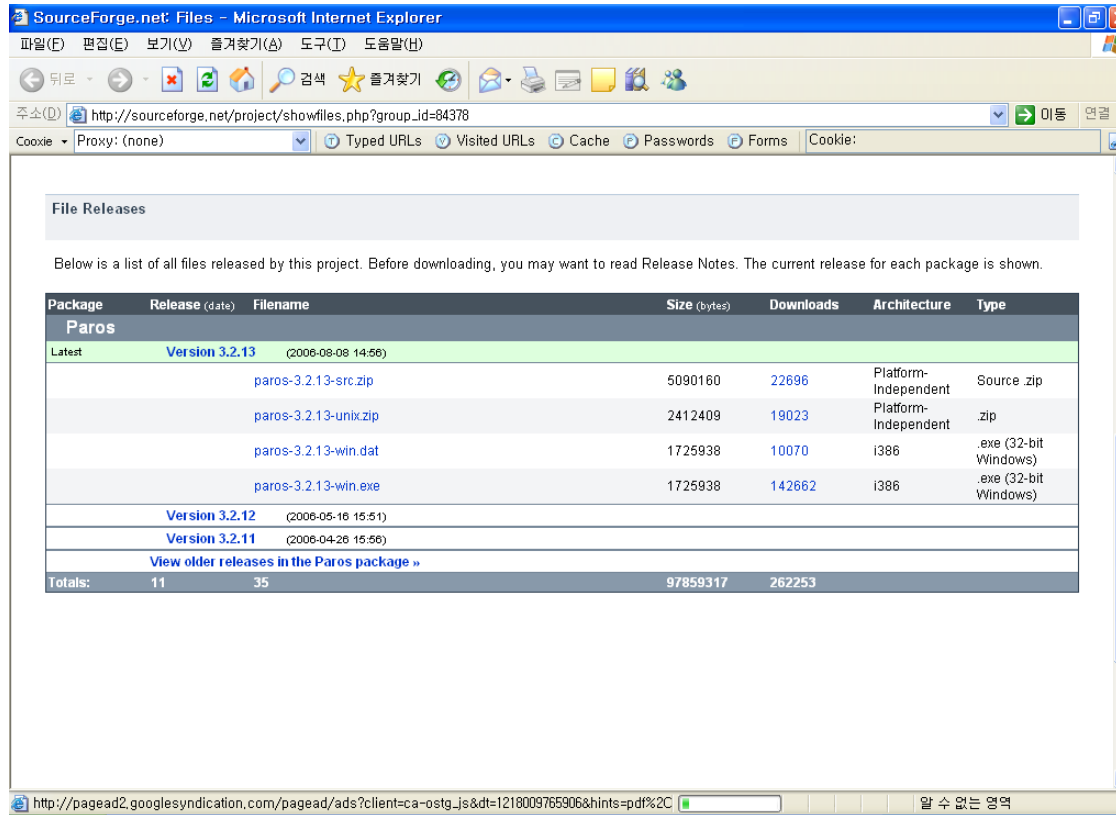


그림. 파로스 다운로드

1. 프록시 툴을 이용한 HTTP분석(9)

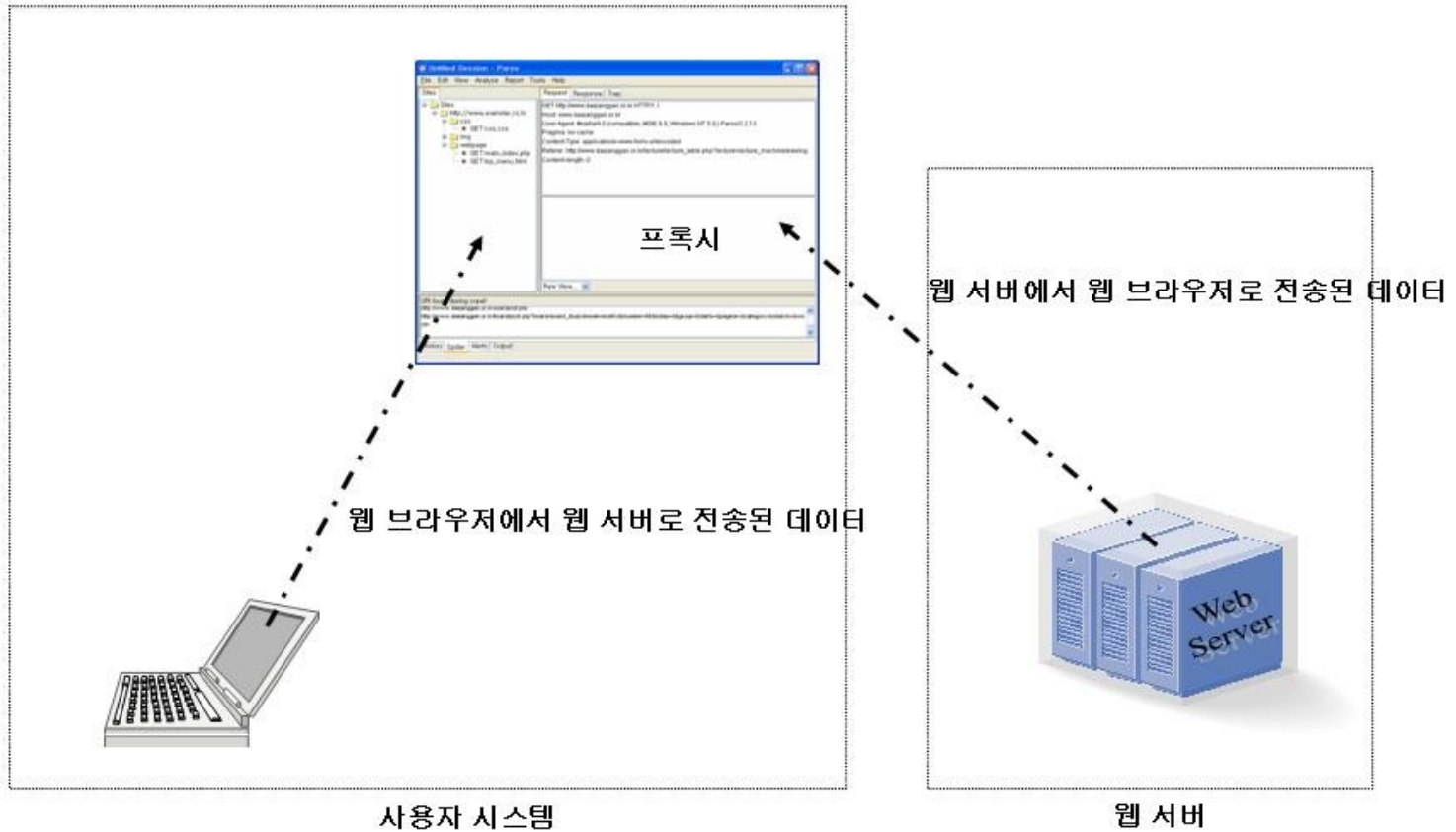


그림. 파로스의 운영(프록시)구조

1. 프록시 툴을 이용한 HTTP분석(10)

○ 파로스의 중요 모듈

- **Crawl** : URL구조를 파악하고 페이지 정보를 수집하는 단계
-
- **Scan** : 수집된 정보를 바탕으로 취약점 패턴을 전송하는 단계
- **Report** : 취약점 결과를 제공하는 단계
- **Proxy** : HTTP 프록시 구조 제공

1. 프록시 툴을 이용한 HTTP분석(11)

○ 파로스 프록시 설정

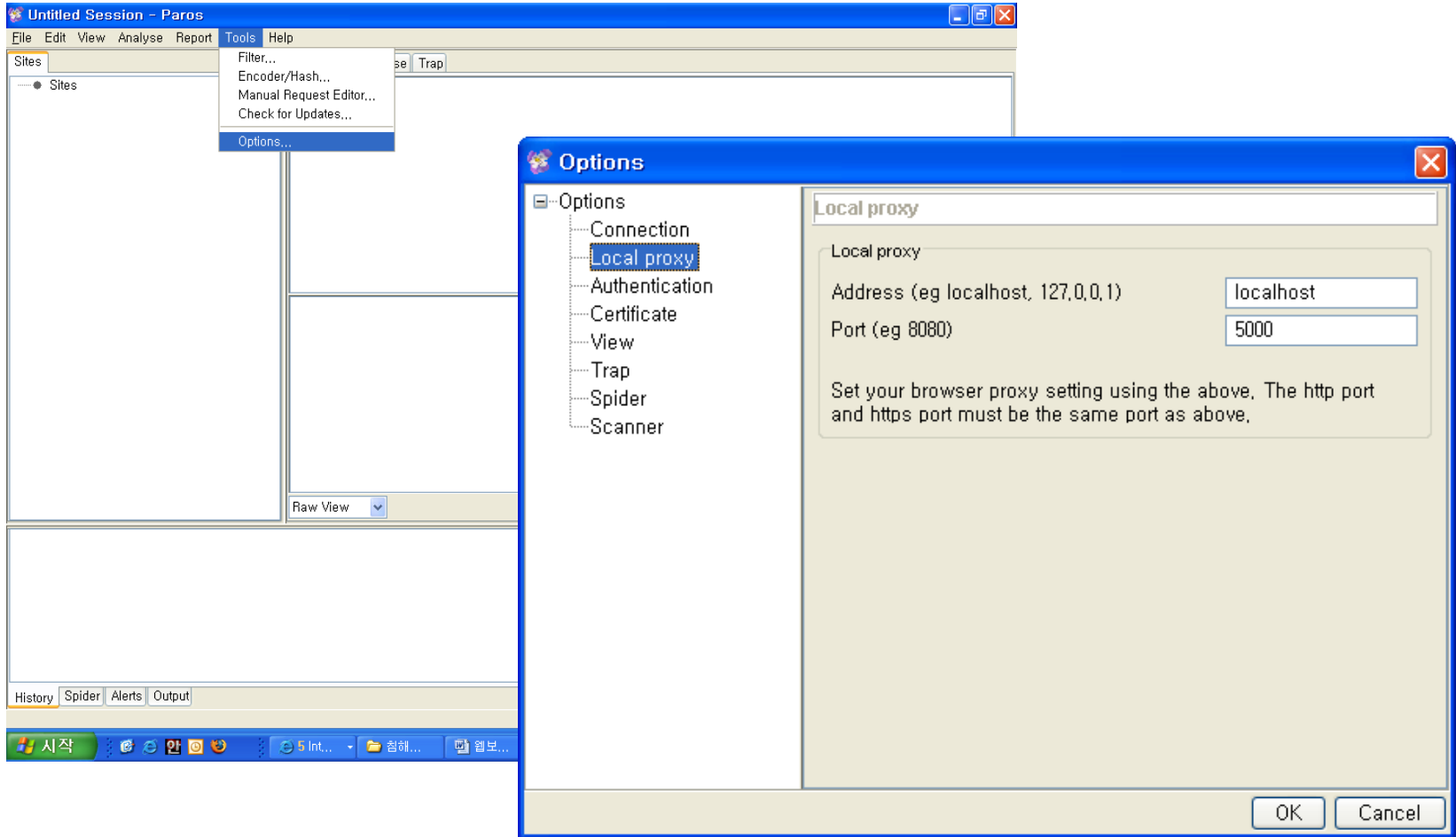


그림. 파로스 포트 설정

1. 프록시 툴을 이용한 HTTP분석(12)

- 웹 브라우저 프록시 설정
주의할 점은 파로스의 프록시 포트와 동일해야 한다.

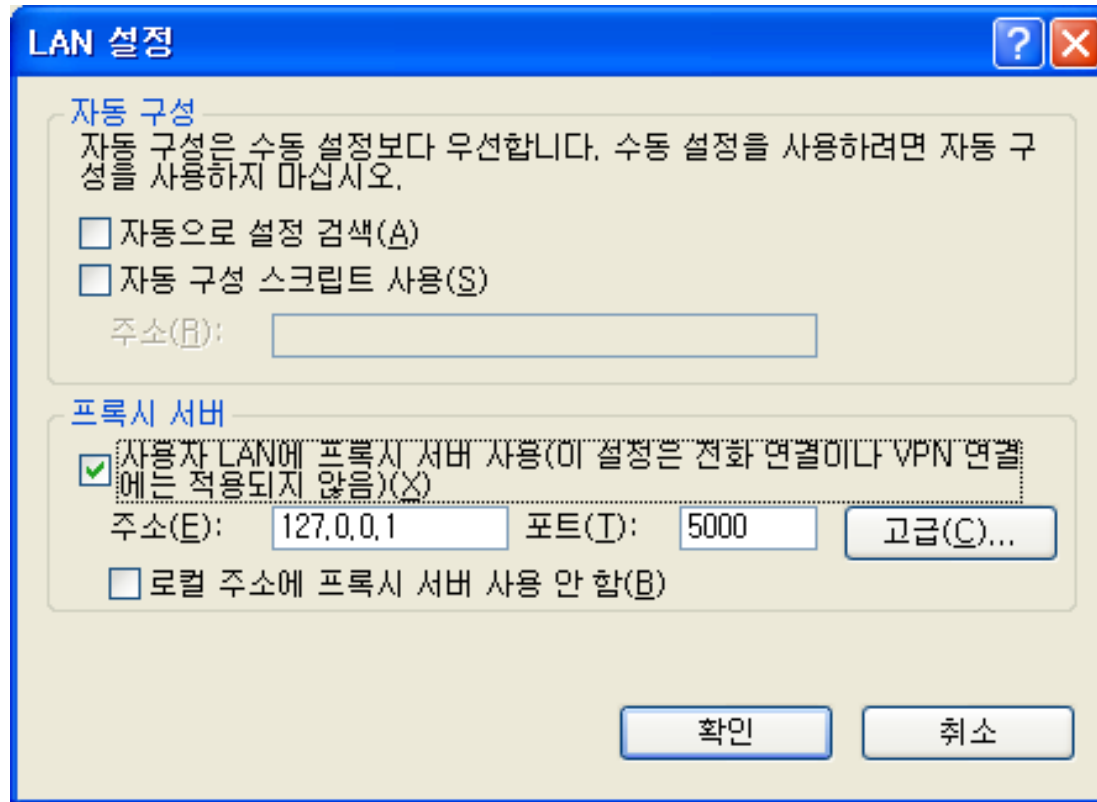


그림. 웹 브라우저 프록시 설정

1. 프록시 툴을 이용한 HTTP분석(13)

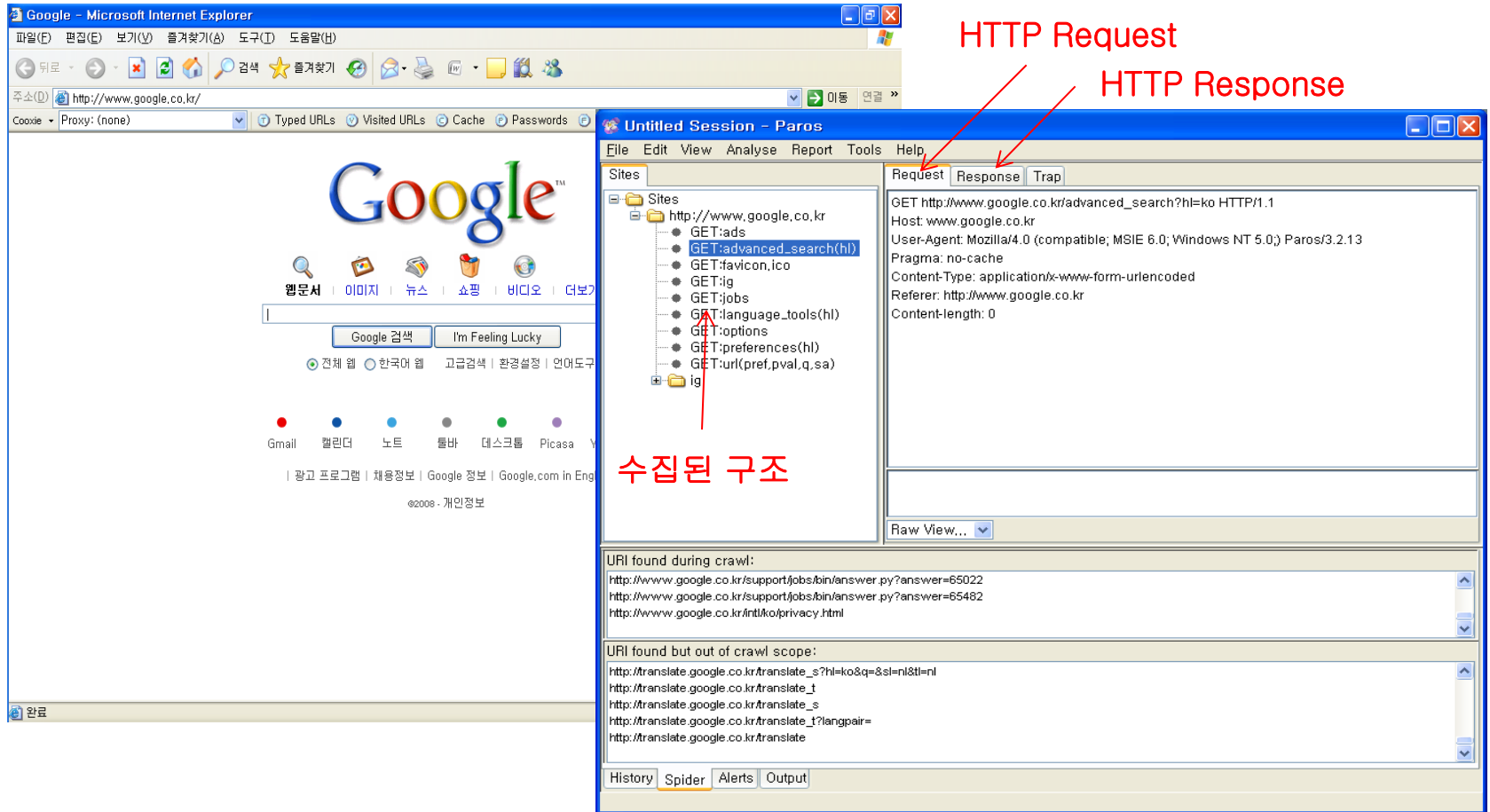


그림. 파로스 운영 설정 테스트

1. 프록시 툴을 이용한 HTTP분석(14)

○ 파로스 프록시를 이용한 데이터 변조 방법(1)

http://www.elated.com/res/File/articles/development/javascript/form-validation-with-javascript/simple_form.html

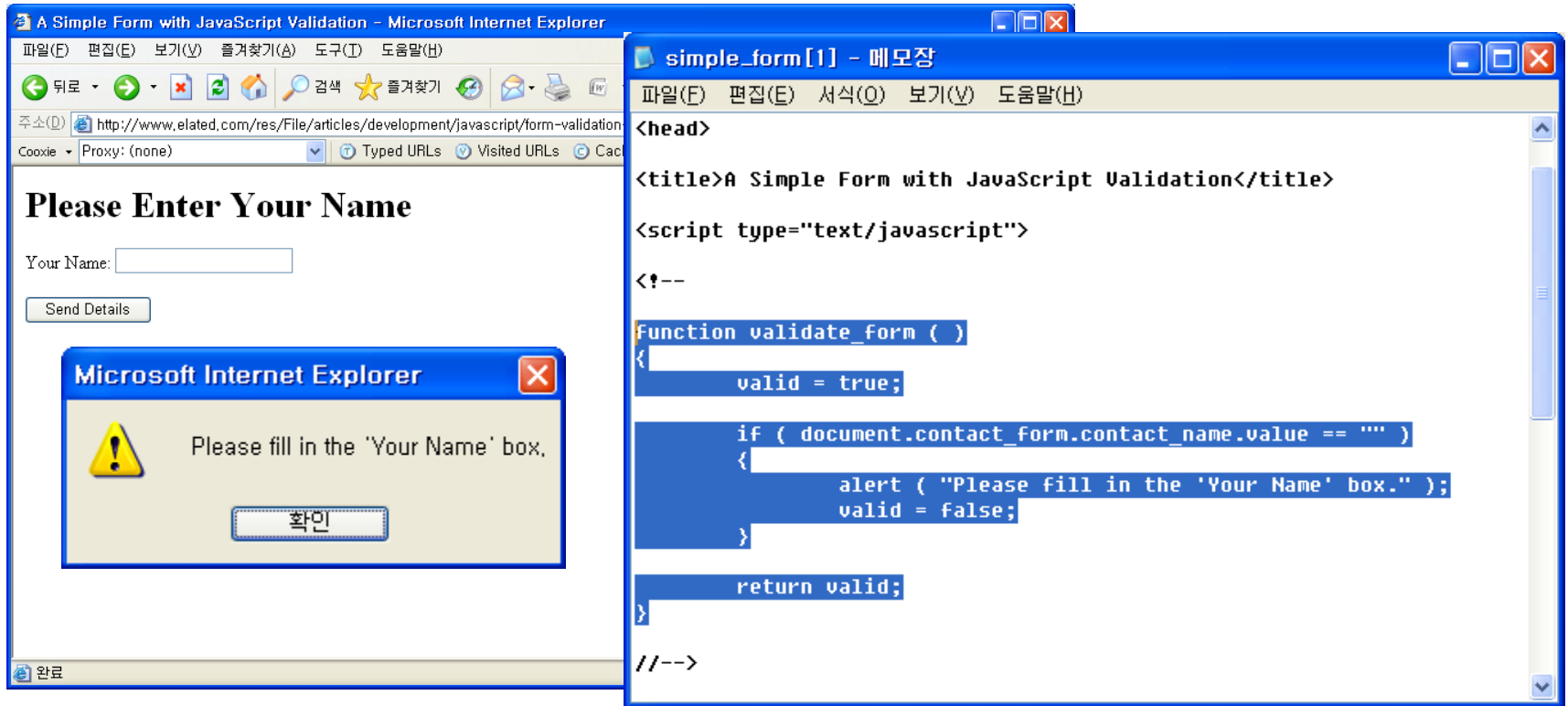


그림. 파로스를 이용한 데이터 변조(1)

1. 프록시 툴을 이용한 HTTP분석(15)

○ 파로스 프록시를 이용한 데이터 변조 방법(1)

- Trap Request : 웹 브라우저에서 웹 서버로 전송되는 데이터 가로채기
- Trap Response : 웹 서버에서 웹 브라우저로 전송되는 데이터 가로채기

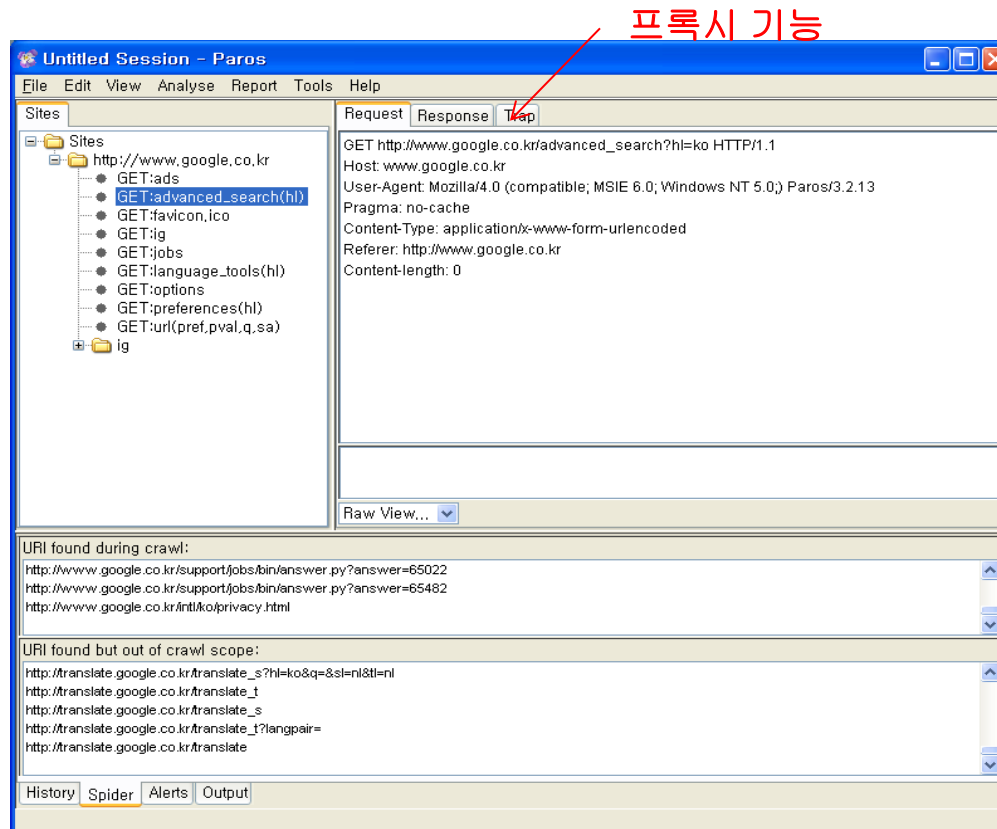


그림. 파로스를 이용한 데이터 변조(2)

Q & A