**Burp Suite**

**0. HTTP Proxy**

- 사용자와 웹 서버 가운데 위치

- 서로 간의 HTTP 요청과 응답을 중간에서 전달하는 역할

- 메시지 내용 조회, 수정, 취소 가능

- 웹 모의해킹에서는 사용자 호스트에서 동작하는 경우 많음

**1. Set Burp Suite**

**1-0) 처음 접속 화면**

텍스트, 스크린샷, 소프트웨어, 번호이(가) 표시된 사진

자동 생성된 설명

**<프로젝트 불러오기 화면>**

유료 버전: 프로젝트 저장, 불러오기 기능 제공

무료 버전: 프로젝트 저장, 불러오기 기능 제공 X

“Next 클릭”

텍스트, 스크린샷, 소프트웨어, 웹 페이지이(가) 표시된 사진

자동 생성된 설명

**<프로젝트 설정 불러오기 화면>**

기본 설정대로 진행, “Start Burp” 클릭

텍스트, 스크린샷, 소프트웨어, 웹 페이지이(가) 표시된 사진

자동 생성된 설명

**<Settings 화면>**

- 처음 실행시, 127.0.0.1:8080으로 설정되어 있음

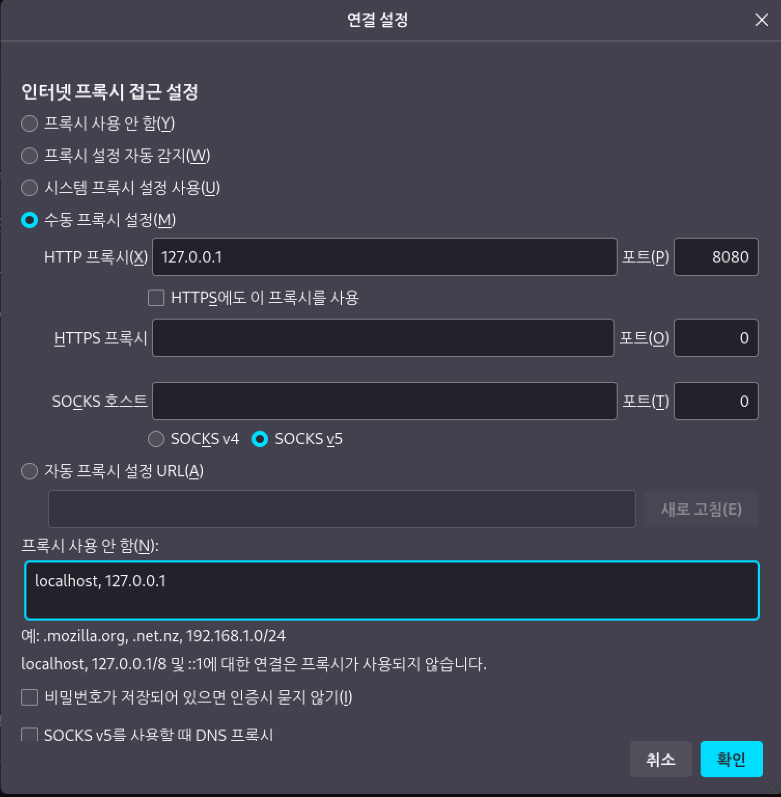
- Running 항목은 실행 여부 (다른 프로그램이 해당 포트 사용 중일 경우, 체크 해제될 수 있음)

- Edit 버튼을 통해 IP주소와 포트 변경 가능

**1-1) Set Web Browser Proxy**

웹 브라우저에서 웹 서버에 접속할 때 발생하는 요청을 Burp Suite로 전달하기 위해 설정

Firefox 브라우저 – 설정 – 네트워크 설정 – 설정 버튼



Manual Proxy Configuration 선택 - 127.0.0.1:8080 입력 – OK 버튼

(만약, Burp Suite에서 IP 주소 또는 포트를 변경했다면 변경된 정보로 입력)

텍스트, 스크린샷, 소프트웨어, 번호이(가) 표시된 사진

자동 생성된 설명

**<실습 가상 머신의 dvwa로 접속 시도했을 때, Burp Suite 화면>**

Firefox를 통해 웹 해킹 실습 가상 머신으로 접속을 시도하면 접속이 되지 않음

Burp Suite에서 Proxy - Intercept에서 요청을 캡처한 것을 볼 수 있음

사용자의 조작을 기다리는 상태

텍스트, 스크린샷, 소프트웨어, 컴퓨터 아이콘이(가) 표시된 사진

자동 생성된 설명

**<옵션 변경 후, Firefox 화면>**

이제 “Intercept is on”을 off로 변경하면 캡처되지 않고 이전처럼 접속 가능

텍스트, 스크린샷, 번호, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

**<Proxy – HTTP History 화면>**

인터셉트 기능 off 후에도 Firefox에 proxy 설정이 되어 있으면, 모든 HTTP 요청과 응답이 Burp Suite에 기록

**1-2) FoxyProxy Add-ons**

위의 설정을 한 경우, Burp Suite 종료시, Firefox의 Proxy 설정을 원래의 상태로 되돌려야 정상적인 통신 가능

Proxy 설정을 간편하게 할 필요가 있음

텍스트, 스크린샷, 멀티미디어 소프트웨어, 소프트웨어이(가) 표시된 사진

자동 생성된 설명



텍스트, 스크린샷, 소프트웨어, 웹사이트이(가) 표시된 사진

자동 생성된 설명

Firefox에서 Add-ons (확장 기능)에서 FoxyProxy 검색 후 추가 (버전 상관 X)

텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명

**<정상적으로 추가된 모습>**

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

**<FoxyProxy 클릭 후, Option - Proxies 화면>**

FoxyProxy의 설정에서 Proxies 화면으로 이동하면 Proxy를 추가할 수 있다.

텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명

**<Proxy 추가 화면>**

127.0.0.1:8080을 입력해주고, 저장을 누른다.

텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명

**<Proxy가 추가된 모습>**

이후, FoxyProxy의 화면을 보면 정상적으로 추가된 모습을 볼 수 있다.

**텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명**

**<Firefox의 Proxy 설정 화면>**

이전에 수정했던 Firefox의 Proxy는 다시 “Use System Proxy settings”로 변경한다.

이제부터는 FoxyProxy를 통해 Proxy를 자유롭게 변경할 수 있다.

- Burp Suite 사용시: 127.0.0.1:8080 (loopback) 사용

- Burp Suite 미사용시: Disable 사용

**1-3) HTTPS Sites Connection Problems**

- Burp Suite의 Proxy 사용시, HTTPS를 사용하는 사이트에서 에러가 발생할 수 있음

- 해당 사이트 접속시, 인증서 신뢰하지 못해 발생하는 문제

(웹 브라우저가 HTTPS를 사용하는 사이트에 접속할 때는 해당 사이트의 인증서를 거치는 작업.

확인 후에 제대로 된 사이트일 경우, 신뢰하고 접속.

But, Burp Suite를 거치면 Burp Suite가 인증서를 서버 인증서 대신 웹 브라우저에게 전달.

웹 브라우저는 신뢰하지 못하는 인증서이므로 에러 발생.)

- 일반적으로 에러 표시와 함께 표시되는 “Advanced – Add exception”을 통해 예외 처리 가능

- 웹 서버에서 HSTS (HTTP Strict Transport Security) 사용시, 보안 강화로 예외 처리 불가

- Burp Suite가 보내는 인증서가 신뢰할만한 인증서라는 것을 웹 브라우저가 알게 해줘야 함.

텍스트, 소프트웨어, 컴퓨터 아이콘, 번호이(가) 표시된 사진

자동 생성된 설명

**<Burp Suite – Proxy – Settings 화면>**

Burp Suite에서 Setting으로 들어와 “Import/export CA certificate” 클릭

텍스트, 전자제품, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

“Certificate in DER format” 클릭 후, “Next” 클릭

텍스트, 스크린샷, 소프트웨어, 운영 체제이(가) 표시된 사진

자동 생성된 설명

원하는 위치 선택 후, 파일 이름을 “bs.der”로 설정한 후 “Next” 클릭하면 해당 위치에 파일 저장됨

텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명

**<Firefox – Preferences - Privacy & Security 화면>**

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

아래쪽 Certificate에서 “View Certificate” 클릭

텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 소프트웨어, 디스플레이이(가) 표시된 사진

자동 생성된 설명

“Import” 클릭 후, 저장했던 “bs.der” 파일 가져오기

“Trust this CA to identify websites” 체크 후 “OK” 버튼 클릭

텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명

PortSwigger에서 PortSwigger CA가 추가된 것 확인