**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

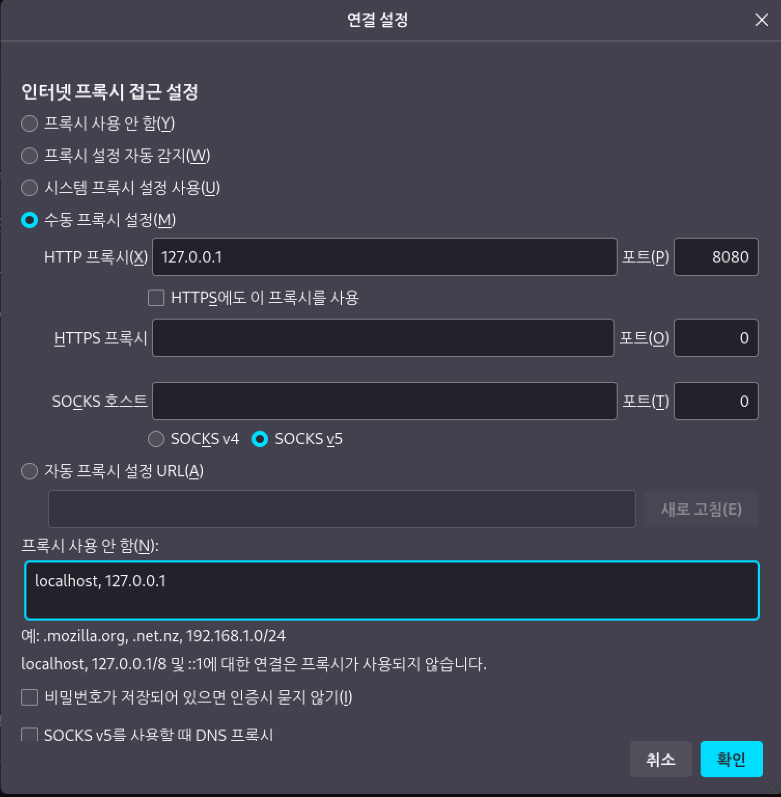
- Running 항목은 실행 여부 (다른 프로그램이 해당 포트 사용 중일 경우, 체크 해제될 수 있음)

- 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

**2. Burp Suite’s Function**

**2-1) Target**

**a) Site Map**

**텍스트, 스크린샷, 디스플레이, 소프트웨어이(가) 표시된 사진

자동 생성된 설명**

- 접속한 모든 호스트와 URL 구조 파악

- 좌측: 접속했던 호스트들의 목록

(선명하게 표시된 호스트: 직접 접속한 호스트

흐릿하게 표시된 호스트: Burp Suite가 HTTP 메시지 분석 -> 메시지가 포함된 링크를 찾은 호스트)

- 우측 상단: 좌측에서 선택된 호스트 대상 간략화된 보낸 요청과 응답 정보 표시

(메소드, URL, 파라미터 존재 여부, 응답 코드, 응답 메시지 길이 등)

- 우측 하단(Request): 우측 상단에서 선택한 항목의 요청 메시지 내용

- 우측 하단(Response): 우측 상단에서 선택한 항목의 응답 메시지 내용

다음은 필터 항목들이다.

텍스트, 스크린샷, 소프트웨어, 번호이(가) 표시된 사진

자동 생성된 설명

Show only in-scope items: 바로 다음에 설명할 스코프에 설정된 항목만 표시

Show only requested items: 직접 요청한 항목들만 표시

Show only parameterized requests: 파라미터가 포함된 요청만 표시

Hide not-found items: 웹 사이트에 존재하는 않는 항목 표시 X

Filter by MIME type: 응답 데이터의 종류로 필터링

Filter by status code: 응답 코드로 필터링

Filter by file extension: 파일 확장자로 필터링

Filter by annotation: 코멘트를 남겼거나, 하이라이트된 항목만 표시

Show all, Hide all: 모든 요청 표시 또는 숨김

**b) Scope**

텍스트, 스크린샷, 소프트웨어, 디스플레이이(가) 표시된 사진

자동 생성된 설명

- Burp Suite를 거쳐간 특정 대상의 내용만 표시

- 스코프에 등록 후, 사이트맵에서 Show only in-scope item 이용시, 스코프에 등록된 항목만 표시

- Include in scope: 스코프 리스트에 대상 추가, 수정 ,삭제

- Exclude from scope: 특정 파일(또는 URL)에 대한 요청 제외

- 사이트맵에서 바로 스코프에 추가 가능

(Proxy History Logging: 스코프에 등록되지 않은 항목들을 Proxy 히스토리나 다른 기능으로 전달할지 여부

Yes – 스코프에 등록되지 않은 항목들에 대해서 데이터 수집 중단

No – 데이터 계속 수집, 스코프에 있는 항목만 표시하도록 설정 가능)

**2-2) Proxy**

**a) Intercept**

텍스트, 스크린샷, 소프트웨어, 컴퓨터 아이콘이(가) 표시된 사진

자동 생성된 설명

- 웹 브라우저와 웹 서버가 주고받는 HTTP 요청 메시지와 응답 메시지 내용 변경 가능

- 인터셉트된 요청 메시지는 Forward 버튼을 눌러야 웹 서버에 전송

- 인터셉트된 응답 메시지는 Forward 버튼을 눌러야 웹 브라우저로 전송

- HTTP는 자체적으로 타임아웃 처리 X -> 장시간 인터셉트하고 있어도 통신 문제 X

(But, 세션 타임아웃이 있는 웹 사이트의 경우, 로그인이 끊어지는 일 발생 가능)

**b) HTTP History**

텍스트, 스크린샷, 소프트웨어, 번호이(가) 표시된 사진

자동 생성된 설명

- 사이트맵의 우측과 비슷

- 접속 기록을 시간 순으로 정렬, 사이트맵보다 더 많은 정보

- 상단: 각 요청의 핵심적인 정보 요약

- 하단: 선택한 항목의 요청 메시지와 응답 메시지 확인

다음은 필터 항목들이다.

텍스트, 스크린샷, 번호, 폰트이(가) 표시된 사진

자동 생성된 설명

- 사이트 맵의 항목들과 비슷

- Hide items without responses: 응답이 없는 항목 표시 X

- Filter by listener: 포트 번호로 필터링

**c) Proxy settings**

**텍스트, 스크린샷, 소프트웨어, 디스플레이이(가) 표시된 사진

자동 생성된 설명**

- Proxy와 관련된 옵션 설정

- 아래는 자주 사용하는 설정

- Proxy Listeners: Proxy와 인터페이스 주소와 상태 설정

- Intercept Client Requests: 어떤 요청을 인터셉트할지 설정

- Intercept Server Responses: 어떤 응답을 인터셉트할지 설정

- Response Modification: 응답 메시지를 자동으로 수정

- Match and Replace: 요청/응답 메시지의 특정 부분을 패턴 매칭 및 자동 변경

**2-3) Spider – 현재 X**

- 웹 사이트의 링크를 자동으로 찾아 웹 사이트의 전체 구조 파악 (크롤링)

- Control: 요청 전송 횟수, 바이트 등의 통계 정보 확인

**2-4) Intruder**

- 요청 메시지의 특정 위치를 지정하여 여러 개의 데이터를 자동으로 반복해서 전송하는 기능

(보내는 데이터 = 페이로드, 이와 같은 테스트 방법 = 퍼징)

**a) Positions**

텍스트, 스크린샷, 소프트웨어, 디스플레이이(가) 표시된 사진

자동 생성된 설명

- Tartget: 공격 대상 (호스트 주소와 포트 지정)

- 공격 종류 선택

- 요청 메시지 임의 생성 및 페이로드 삽입 위치 지정

- 페이로드 입력 위치: 주로 파라미터나 쿠키 등과 같이 동적으로 변경될 수 있는 부분

- 공격 유형에 따라 위치마다 페이로드 하나씩 전송 또는 모든 위치 동일한 페이로드 전송 가능

- 사이트 맵 또는 Proxy 히스토리 항목의 우클릭 메뉴에서 “Send to Intruder” 메뉴 이용시 요청 메시지 쉽게 생성 가능

**b) Payloads**

텍스트, 스크린샷, 소프트웨어, 디스플레이이(가) 표시된 사진

자동 생성된 설명

- 어떤 페이로드를 입력하여 테스트할지 지정

- 페이로드 타입: 패스워드와 같은 문자열 리스트 또는 숫자나 문자의 범위 등으로 랜덤 값. 대소문자 구분 또는 비정상적인 값 입력 가능

**2-5) Repeater**

텍스트, 스크린샷, 소프트웨어, 컴퓨터 아이콘이(가) 표시된 사진

자동 생성된 설명

- 인트루더와 비슷한 기능, 수동으로 메시지 조작 및 반복적인 테스트

- 사이트 맵 또는 Proxy 히스토리 항목의 우클릭 메뉴에서 “Send to repeater” 메뉴 이용시 요청 메시지 쉽게 생성 가능

- 좌측 화면 (Request): 메시지 임의 변경 가능, “Send” 버튼으로 전송

- 우측 화면 (Response): 요청에 대한 응답, 값이 어떻게 변하는지 쉽게 확인 가능

**2-6) Scanner – Professional Version**

- 웹 애플리케이션의 보안 취약점 자동 찾기

- Issue Definition: 스캐너를 통해 찾을 수 있는 취약점 목록 확인 가능

**2-7) Sequencer**

텍스트, 스크린샷, 소프트웨어, 디스플레이이(가) 표시된 사진

자동 생성된 설명

- 세션 값 추측 또는 세션 값이 얼마나 랜덤하게 생성되는지 테스트

- 세션 값 추측시, 세션 하이재킹 공격에 노출 가능성

**2-8) Decoder**

텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

- 각종 문자열의 인코딩, 디코딩 값 확인

- URL 인코딩, HTML 인코딩, Hex 값 및 Base64 인코딩 값 -> 디코딩

**2-9) Comparer**

텍스트, 스크린샷, 소프트웨어, 디스플레이이(가) 표시된 사진

자동 생성된 설명

- 두 개의 요청 메시지나 응답 메시지 1대1 비교 -> 두 메시지 간 차이점 확인

- Proxy 히스토리에서 컨트롤 키를 이용하여 동시에 두개 항목 선택 후 “Send to Comparer” 메뉴를 통해 이용 가능

- Words: 두 메시지 내용 중 어떤 내용이 다른지 확인

**2-10) Extensions**

**텍스트, 스크린샷, 소프트웨어, 디스플레이이(가) 표시된 사진

자동 생성된 설명**

- 자신이 개발한 코드나 서드 파티에서 개발한 확장 기능 추가 설치 가능

- Bapp Store: 기본 제공 확장 기능 목록