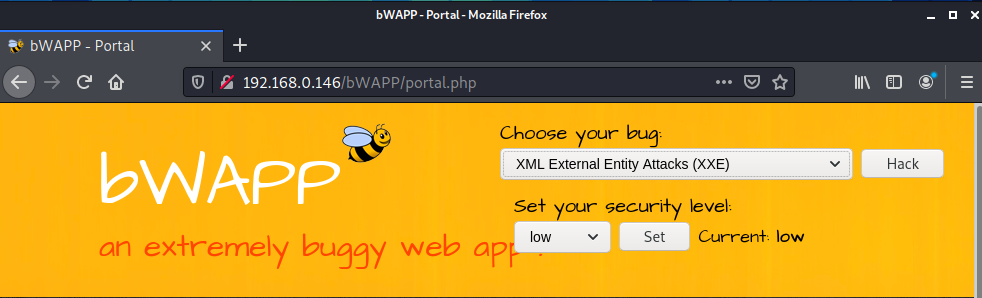
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | **작성: 신세은** | | |  | |
|  | **XEE** | | | | | | |  |
|  | | **-XML External Entity Attaks-** | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

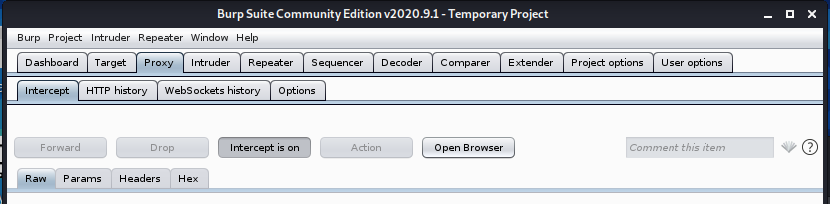
|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
|  |
|  |
| 1. **XML 외부 개체 (XXE)** |
| * 1. **XXE는 악의적인 자바스크립트를 막기 위한 필터장치를 우회하는 취약점으로 XML 문서에서 동적으로 외부 URL의 리소스를 포함시킬 수 있는 외부 엔티티(ENTITY)를 사용할 때 발생**   2. **오래되고 설정이 엉망인, 많은 XML 프로세서들은 XML 문서 내에서 외부 개체 참조를 평가**   3. **외부 개체는 파일 URL 처리기, 내부 파일 공유, 내부 포트 스캔, 원격 코드 실행과 서비스 거부 공격을 사용하여 내부 파일을 공개하는데 사용 할 수 있음** |
|  |

|  |
| --- |
|  |
| 2. 공격과정 (필요시 가정이나 예상 시나리오 포함) |
|  |
| 1. **실습환경** |
| |  |  |  | | --- | --- | --- | |  | OS | IP | | 공격 호스트 | Kali Linux | 192.168.0.150/24 | | 타겟 호스트 | Ubuntu(Bee-box) | 192.168.0.146/24 | |
| 1. **XXE 공격과정** |

1. **보안 레벨 선택 및 시나리오 선택**
2. **XML External Entity Attacks (XXE)**
3. **low 선택 후, set 클릭**



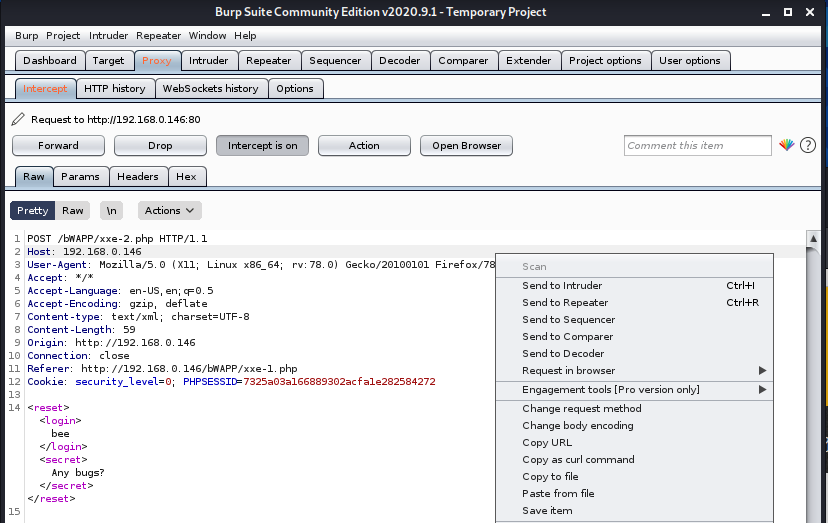
1. **Burp Suite 사용**
   * 1. **[proxy] -> [Intercept] -> [Intercept is on]**



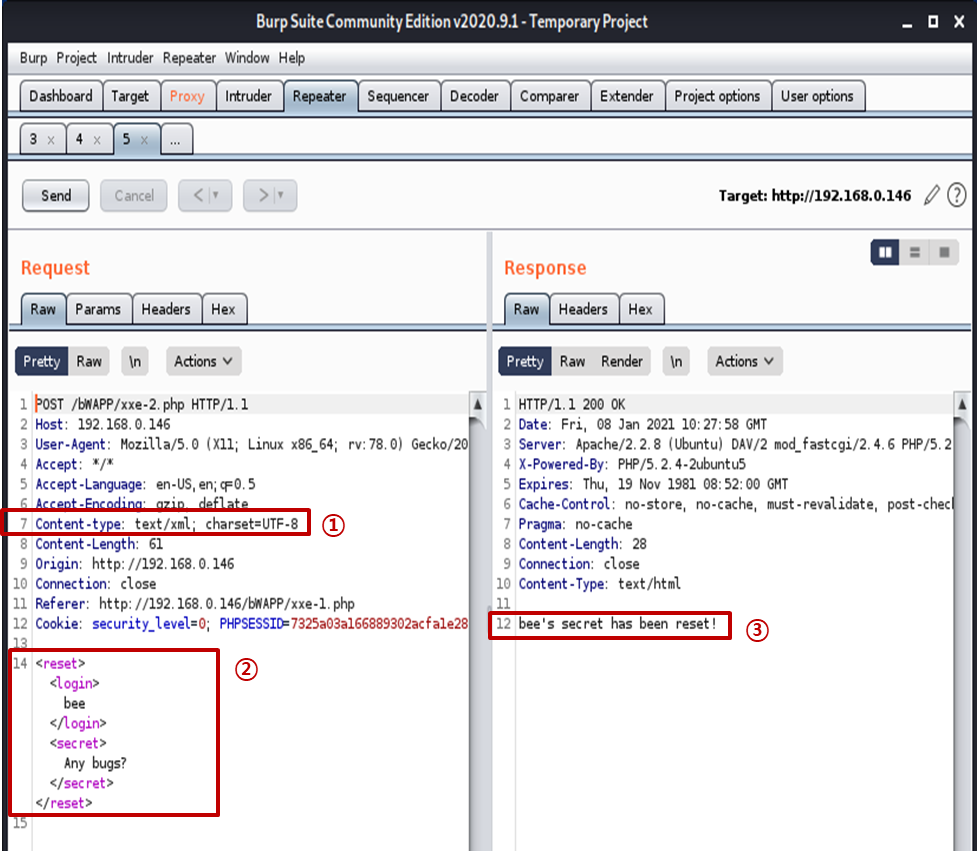
* + 1. **Any bug? 선택**



* + 1. **Burp suite로 웹 요청 메시지 확인 후, Send to Repeater 클릭**

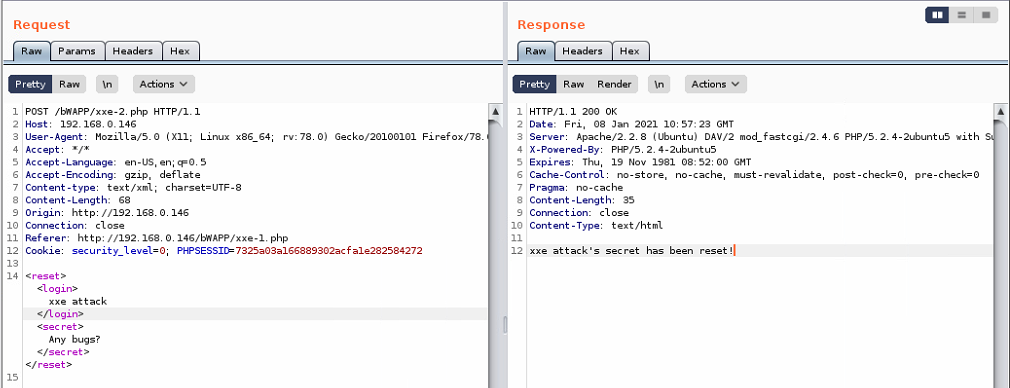
****

1. **[Repeater] 요청, 응답 확인**
2. **Content-type: textl/xml: XEE 취약점 공격은 XML 이 전송되는 부분을 통해 이루어짐**
3. **바디 부분에 XML 형태의 데이터로 전송되어짐을 확인 가능**
4. **요청 메시지 XML 데이터 중 <login></login> 사이에 전송된 bee 문자열이 bee’s secret has been rest! 형태로 응답하는 것을 확인 가능**

****

1. **bee 문자열을 임의로 변경해본 결과 응답 메시지도 bee 부분이 임의의 문자로 바뀐 것을 확인 가능**

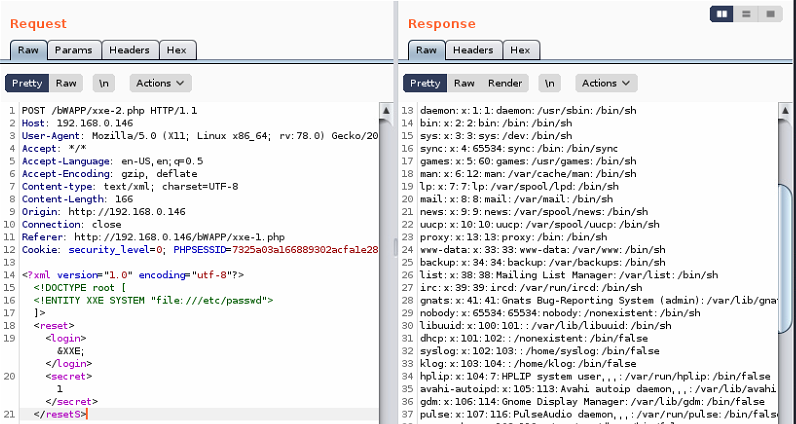
* **즉, <login> 태그로 전달된 값이 응답 메시지에 나타내고 있으며, 이를 통해 서버가 XML 처리되고 있다는 것을 추측 가능**

****

|  |
| --- |
| 1. **공격 시도** |

1. **외부 엔티티 선언**
   * 1. **‘&XXE;’ 이라는 외부 엔티티를 선언하여 서버의 passwd 파일 출력**

**- 웹 서버 내부의 /etc/passwd 파일을 지정하는 외부 엔티티를 선언하고, <login> 태그 값으로 해당 외부 엔티티를 참조함으로써, /etc/passwd 파일 내용 확인 가능**

****

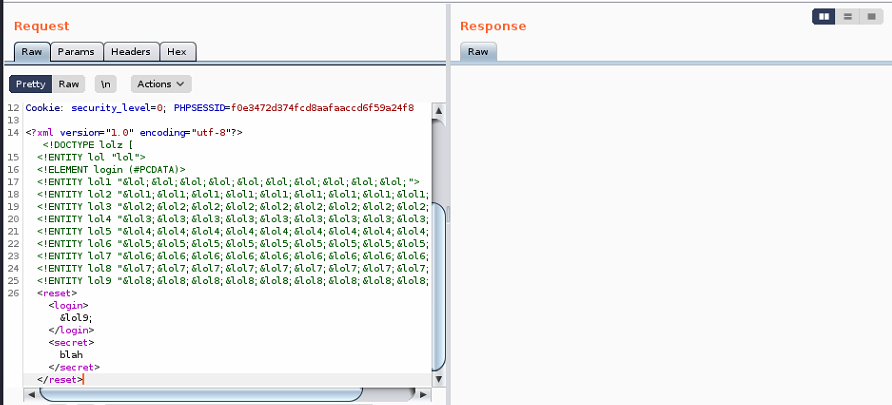
**2) DOS Attack**

1. **일종의 XML Bomb 공격으로** **하나의 ENTITY에 다른 ENTITY를 계속적으로 참조하여 관련 응용 프로그램의 부하를 일으키는 공격**

* **lol1~lol9까지 ENTITY를 생성하다가 마지막**

**<****reset><login>&lol9;</login><secret>blah</screst></reset> 에서 문제 발생**

* **각** **ENTITY에서 상위 lol을 호출하여 DOS 공격을 발생 시킴 -> 10^9 109번 호출**

****

1. **실행 결과**

**- 30초가 지나도 응답을 출력하지 않음**

**- 애플레키션 계층에서 일어나는 DoS 공격으로 웹 서비스 제공을 방해**

|  |
| --- |
|  |
| 3. 보안진단 및 적용결과 |
|  |
| 1. **‘XXE-1.php’ & ‘ XXE-2.php’ 파일 내용 확인** |
| 1. **파일 확인**    1. **cd /var/www/BWAPPS**      * 1. **xxe-1.php 파일 확인**      * **xxe-1.php 페이지는 [Any Bugs?] 버튼을 클릭하면 비밀번호 힌트를 초기화 하기 위하여**   **xxe-2.php 페이지를 호출한다.**   * 1. **xxe-2.php 파일 확인** |
| * **login 변수에 사용하는 아이디를 세션에서 받아 입력하기 때문에 버프 스위트에서 수정하여도 로그인한 사용자의 비밀번호 힌트 초기화** * **비밀번호 힌트를 mysqli\_real\_escape\_string 함수를 사용하여 우회** * **SQL 인젝션 공격에서 사용하는 특수 문자는 XXE 공격에도 사용되므로 NULL, \n, \r, \, ‘, “, ^Z 문자 앞에 백슬래시를 추가하여 XML 코드를 일반 문자로 변경** * **MySQL 의 업데이트 셋 구문은 secret 변수에 입력된 내용으로 비밀번호 힌트를 초기화 시킴** |
|  |
|  |
| 1. **적용 결과** |
| 1. **보안 레벨 선택 및 시나리오 선택**    1. **XML External Entity Attacks (XXE)**    2. **high 선택 후, set 클릭**      * 1. **XXE 인젝션 실패 확인** |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | | |  | | KITRI 모의해킹 28기 | | | | |  | | |  | |  | | | | |  | | |  | |  | | | | |  | | |  | |  | | | | |  | | |  | |  | | | | |  | | |  | |  | | | | |  | | |  | |  | | | | |  | | |  | |  | | | | |  | | |  | 작성:신세은 | | |  | | |  | **XXE** | | | | | | |  | |  | | **-XXE Bomb-** | | | |  | | | |  | |  | | | |  | | | |  | | |  | |  | | | | |  | | |  | |  | | | | |  | | |  | |  | | | |  |  | | --- | | 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) | |  | | 1. **Security Misconfiguration** | | * **잘못된 보안 구성** * **서버/ 시스템/ DB/ 네트워크 장비/ 웹 설정 오류로 인하여 발생하는 취약점이다.** | | 1. **Dos/DDos 공격** | | * **대량 패킷들을 전송하여 시스템/ 서버/ 네트워크 리소스를 고갈시켜 부하 발생, 요청 방해 및 연결거부를 발생하는 공격이다.** * **단, 정보 유출에 대한 취약점은 없지만, 서비스 마비되기 때문에 사용자 및 기업 입장에서 시간/ 비용 손실을 발생시킨다.** |  |  | | --- | |  | | 2. 공격과정 (필요시 가정이나 예상 시나리오 포함) | |  | | 1. **실습환경** | | |  |  |  | | --- | --- | --- | |  | OS | IP | | 공격 호스트 | Kali Linux | 192.168.0.150/24 | | 타겟 호스츠 | Ubuntu(Bee-box) | 192.168.0.146/24 | | | 1. **XEE 공격과정** |  1. **보안 레벨 선택 및 시나리오 선택**    1. **Denial-of-Service(XML Bomb)**    2. **low 선택 후, set 클릭**      * 1. **‘lol’ 버튼 클릭**      1. **wireshark 실행 및 eh0 Capture 실시**    1. **# wireshark &&**      * 1. **Filter: http**      * 1. **하나의 ENTITY에 다른 ENTITY를 계속적으로 참조하여 관련 응용 프로그램의 부하를 일으키는 공격**      + **lol1~lol9까지 ENTITY를 생성하다가 마지막**   **<reset><login>&lol9;</login><secret>blah</screst></reset> 에서 문제 발생**   * + - **각 ENTITY에서 상위 lol을 호출하여 DOS 공격을 발생 시킴 -> 10^9 109번 호출**      |  | | --- | |  | | 3. 보안진단 및 적용결과 | |  | | 1. **BWAPP 부하 발생 확인** | | 1. **CPU와 메모리 부하**    1. **BWAPP에서 시스템 모니터링 도구 실행**   **#gnome-system-monitor &**     * 1. **CPU와 메모리 부하** | | 1. **‘sm\_dos\_2.php’ 파일 내용 확인** | | 1. **‘sm\_dos\_2.php’ 파일 내용 확인**    1. **# vi sm\_dos\_2.php**        * **소스코드에서 XML Bomb가 설정이 되어있음을 확인 가능** | |