|  |
| --- |
| **Praise the Blanket Writeup** |

Writer : Sakuya Izayoi

1. **문제 개요**Secuincide에서 나온 발표주제인 Sniff Sql query를 사용한 문제이다. Diary 부분에서 SQL injection 취약점이 발생하며, 이를 통해 secret 페이지에 있는 쿼리를 Sniffing하여 인증하면 되는 문제이다.
2. **문제 구성환경**

|  |  |
| --- | --- |
| OS | Ubuntu16.04.3 LTS |
| KERNEL | 4.13.0-37-generic |
| APACHE | Apache/2.4.18 (Ubuntu) |
| PHP | PHP 7.0.28-0ubuntu0.16.04.1 (cli) |

1. **풀이**웹 페이지에서 제공하는 기능을 사용하기 위해서 우선 Register를 통해 ID를   
   생성한다. 해당 페이지는 Prestatement SQL 을 사용하여 제작하였고, 해당 페이지는 공격대상이 아니다. 로그인 또한 같은 사유로 공격대상이 아니며, 통상적인 로그인/회원가입 기능만 제공한다. 해당 기능을 통해 로그인하면 새로운 메뉴가 활성화 되는 것을 볼 수 있다.

|  |
| --- |
|  |
| [그림1] Diary와 Logout 기능의 활성화 |

우선 소스코드를 보면 주석으로 secret 페이지가 숨겨져 있음을 알 수 있다. 해당 페이지를 들어가 보면 C,T,F 3개의 값을 요구하고 있고 이 페이지의 주석 또한 show 변수를 세팅하면 해당 페이지의 소스코드를 볼 수 있게 되어있다.

|  |  |
| --- | --- |
|  |  |
| [그림2] secret 페이지 | [그림3] secret 페이지의 소스코드 |

해당 소스코드를 분석해 보면 mt\_rand와 uniqid를 합쳐서 해쉬를 만들고, 해당 해쉬를 Table명(T), Column명(C), Flag명(F)로 지정하는 것을 볼 수 있다.

그리고 이 값들을 제대로 입력한다면 쿼리가 동작하게 되고 그 결과와 Flag값이 일치한다면 플래그 파일을 던져주는 것을 볼 수 있다.  
임시테이블의 경우 INNODB에서 확인이 가능하지만 이는 사용자가 지정한 문자열이 아닌, 것으로 정확한 테이블 이름을 알 수 없다.

|  |
| --- |
|  |
| [그림 4] 임시 테이블의 정보와 존재유무 |

이렇기 때문에 information\_schema에 접근하더라도 테이블 이름을 얻을 수 없다.

|  |
| --- |
|  |
|  |

SQL 취약점이 일어나는 곳은 Diary의 게시판 부분으로, content를 입력하는 부분에서 일어난다. 해당 Diary는 타인이 쓴 글은 읽어볼 수 없으며, 자신이 쓴 글 최근 10개만 열람 가능하도록 되어 있다. 이곳에 SQL 취약점을 통해 secret 페이지의 SQL 쿼리를 Sniffing 하도록 하자.

|  |
| --- |
|  |
| [그림 5] SQL 취약점을 통한 쿼리sniff 시도 |

SQL 쿼리 sniff의 중요한 점은, 2가지를 들 수 있는데, 첫째는 benchmark를 통해 반복문처럼 여러 번의 구문을 돌려야 한다는 것, 둘째는 의도적으로 시간을 지연시킬 수 있는 구문을 넣어야 한다는 것이다. 이외에 sleep(0)을 줌으로써 다중 쓰레드에서 변수에 대한 Race Condition 문제를 조금 손봐주어야 한다는 것을 추가하면 쿼리는 얼마든 변형 할 수 있다. [그림5]에 content로 적은 부분이 SQL 쿼리 sniff 부분이다. 변수를 선언하고 benchmark를 통해 변수에 해당 쿼리는 제외하며 새로 추가되는 쿼리만을 더해서 출력하게 만드는 쿼리이다.

이 상태로 글을 쓰게 되면 일정 시간동안 쿼리가 동작하며 processlist의 info 부분을 계속 요청하게 되고, 이 때 secret 페이지를 요청하면 임시 테이블을 만드는 쿼리를 가져올 수 있다. 위의 쿼리를 실행시키면 2개의 글이 써지는데, 하나는 정상적으로 요청한 글이고 다른 하나는 인젝션 공격을 통해 써진 answere라는 제목의 글이다.

|  |  |
| --- | --- |
|  |  |
| [그림 6] 공격성공 | [그림 7] Query sniff에 성공한 모습 |

그렇게 얻어낸 값을 secret 페이지의 C,T,F 값에 넣어주게 되면 FLAG를 획득 할 수 있다.

|  |
| --- |
|  |
| [그림 8] Flag 획득 |

끝으로, secuinside에서 좋은 발표 해준 Rubiya 에게 감사의 뜻을 전한다.

FLAG: C4T\_HA5\_9L!V3S