دانشکده مهندسی کامپیوتر

گزارش انجام حمله‌ی Brute Force به کمک ابزارهای BurpSuite و DVWA

تمرین درس مهندسی نرم افزار پیشرفته

در رشته مهندسی کامپیوتر - گرایش نرم افزار

دانشجویان:

محسن امیریان – مرتضی ذاکری

استاد راهنما:

دکتر سعید پارسا

تیر ماه ۱۳۹۶


بسم الله الرحمن الرحيم

فهرست مطالب

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فصل ۱:

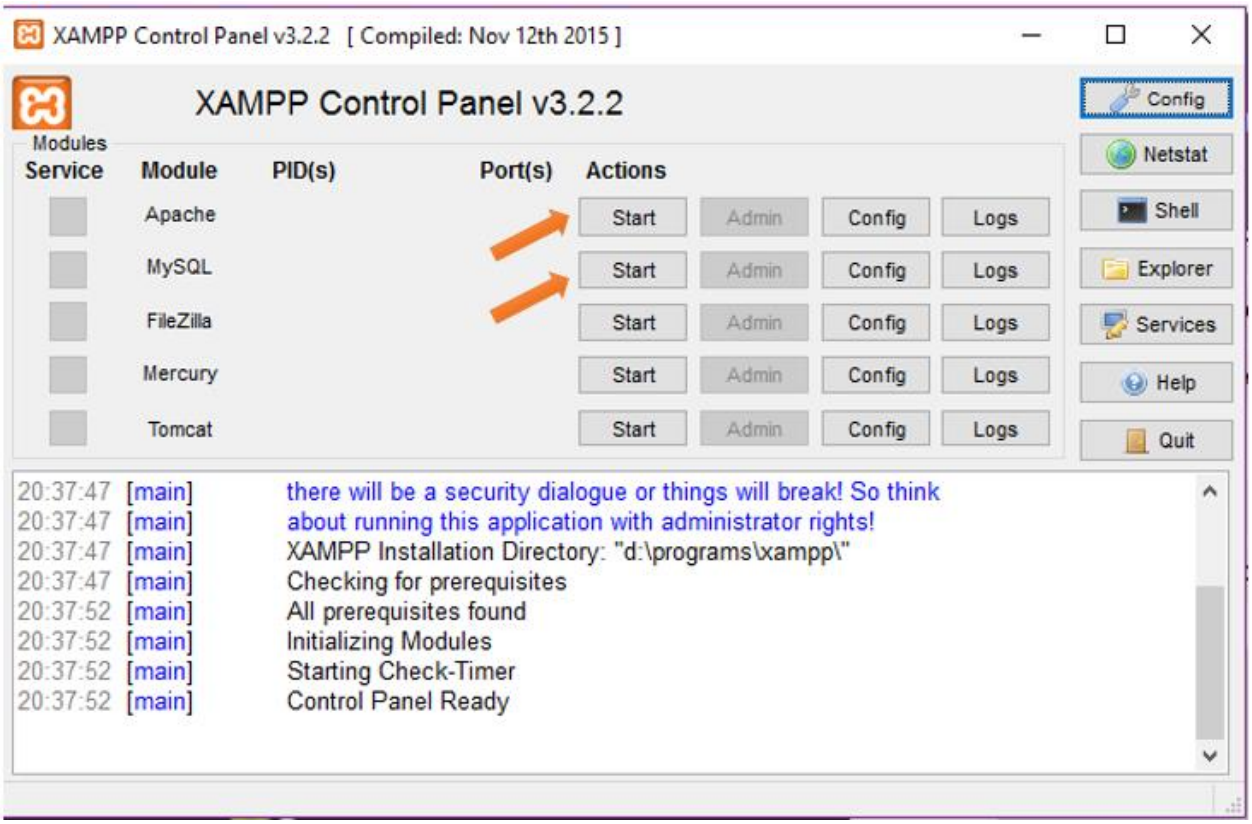
نصب و راه اندازی

۱-۱- مقدمه

در این فصل شیوه‌ی نصب و راه اندازی دو ابزار DVWA و BurpSuite را در محیط ویندوز شرح می‌دهیم.

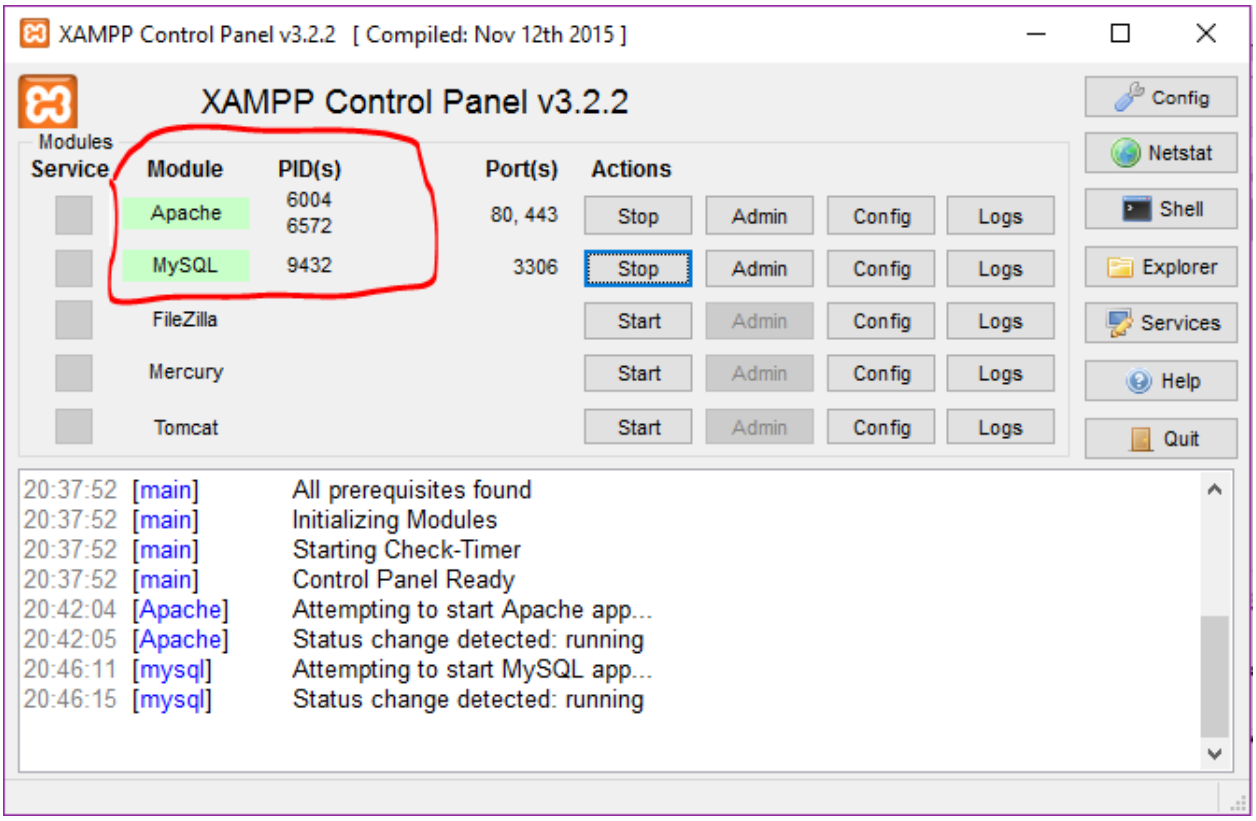
۱-۲- نصب DVWA

برای این کار لازم است ابتدا نرم افزار xampp را از قبل نصب کرده باشیم. این نرم افزار را اجرا کرده و سرویس های Apache و MySql را اجرا کنید.



شکل (۱ـ۱) راه اندازی سرویس‌های Apache و MySql در xampp

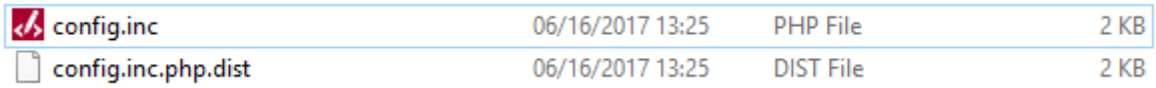
بعد از اجرای این سرویس ها، می بایست این بخش ها به رنگ سبز رنگ در بیایند. در غیر این صورت مشکلی در اجرای سرویس ها بوده و می بایست پورت های مربوط به آن ها را رفع اشکال کنیم.



شکل (۱ـ۲) شکل صحیح اجرای سرویس‌های Apache و MySql در xampp

سپس باید DVWA را از سایت مربوط به آن دانلود کرده و محتویات آن را در پوشه ی htdocs کپی کنیم (...\xampp\htdocs).

در مرحله بعد نام فایل config.inc.php.dist موجود در پو شه ی config را به config.inc.php تغییر می‌دهیم.

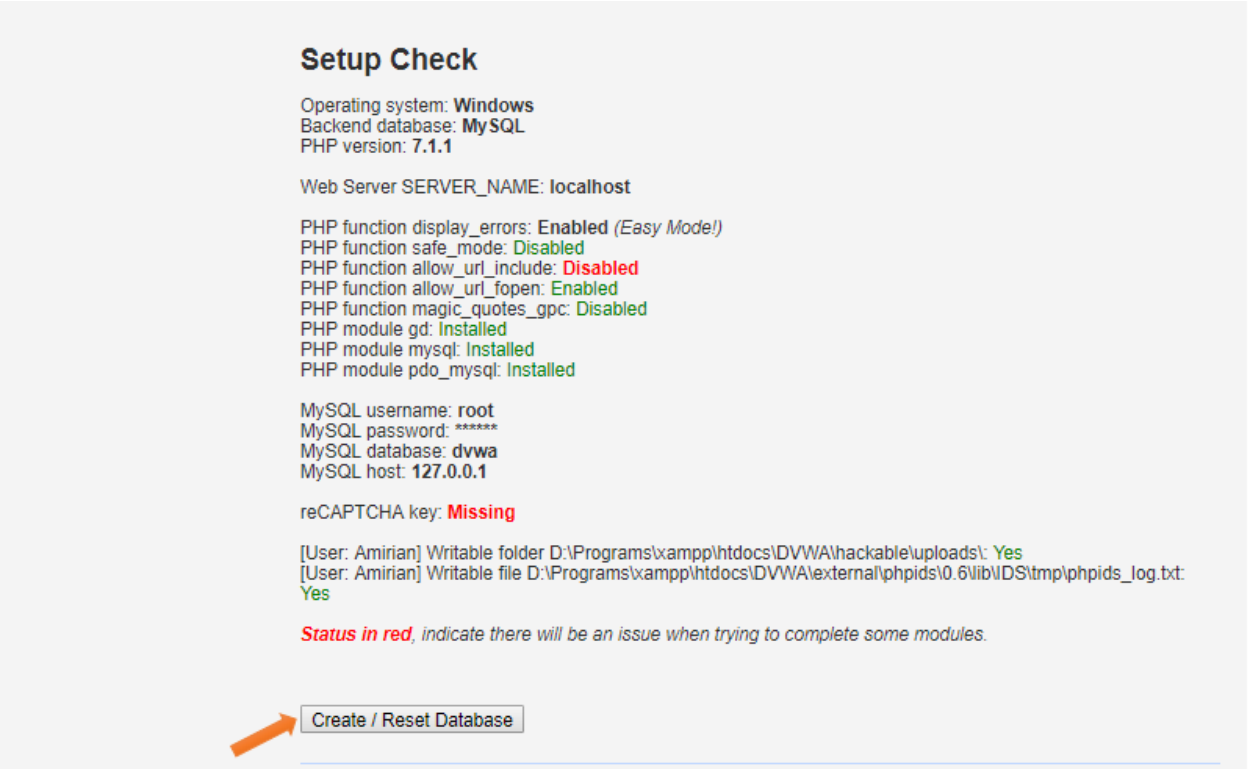


شکل (۱ـ۳) نحوه‌ی ویرایش فایل config در DVWA

پس از انجام مراحل گفته شده، مروگر را باز کرده و آدرس زیر را وارد می‌کنیم:

http://localhost/dvwa/setup.php

در صفحه‌ی باز شده گزینه‌ی Create را انتخاب می‌کنیم:



شکل (۱ـ۴) ساخت پایگاه داده در DVWA

اگر در این مرحله با مشکل مواجه شدیم، می‌بایست فایل config.inc.php را که به آن اشاره شد، به شکل زیر ویرایش کینم:

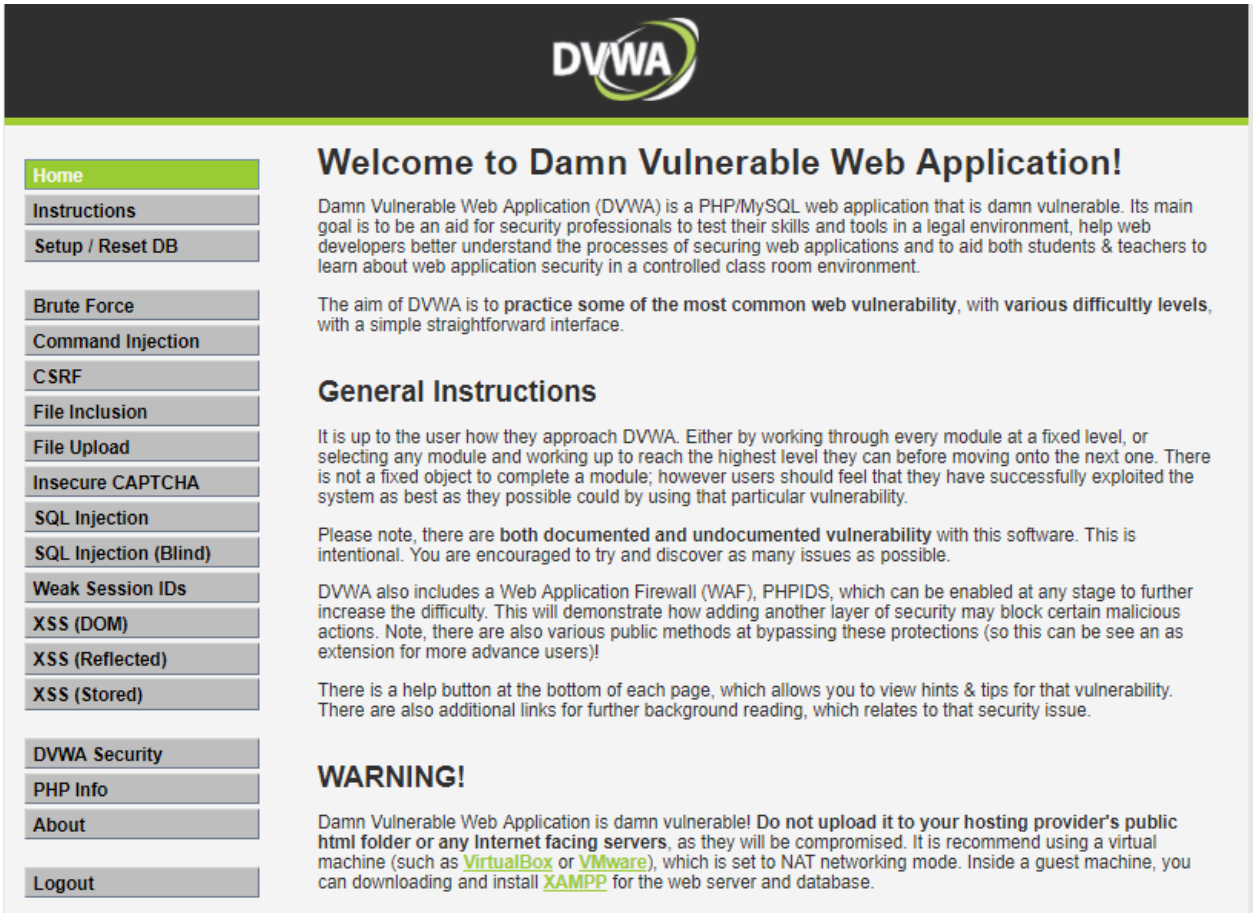
```
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = '';
```

شکل (۱ـ۵) ویرایش فایل config در DVWA

سپس دوباره گزینه‌ی Create را انتخاب می‌کنیم. پس از ساخته شدن پایگاه داده، به صفحه‌ی زیر منتقل می‌شویم:

شکل (۱ـ۶) صفحه‌ی Login در DVWA

در صـــفحه‌ی Login می‌توانید برای Username عبارت admin و برای Password عبارت password را نوشته و وارد نرم افزار شوید:



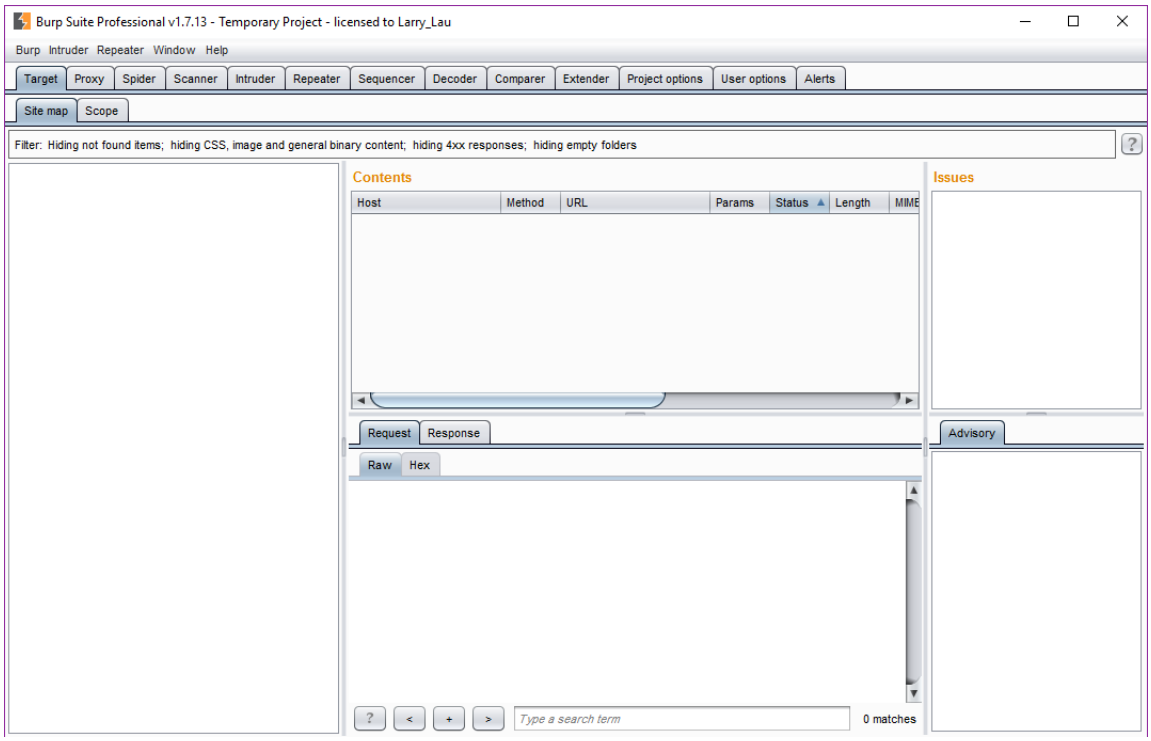
شکل (۱ـ۷) صفحه‌ی ابتدایی ابزار DVWA

مشاهده‌ی صفحه‌ی بالا به منزله‌ی نصب کامل و صحیح DVWA می‌باشد.

۱-۳-نصب Burp Suite

این ابزار به زبان جاوا نوشته شده است. برای اجرای آن می‌بایست ابتدا Java SE Runtime را بر روی کامپیوتر خود نصب کرده باشیم.

سپس این ابزار را دانلود کرده و فایل BurpLoader را اجرا می‌کنیم:



شکل (۱ـ۸) محیط ابزار BurpSuite در اجرای اول

فصل ۲:

حمله Brute Force

۲-۱- مقدمه

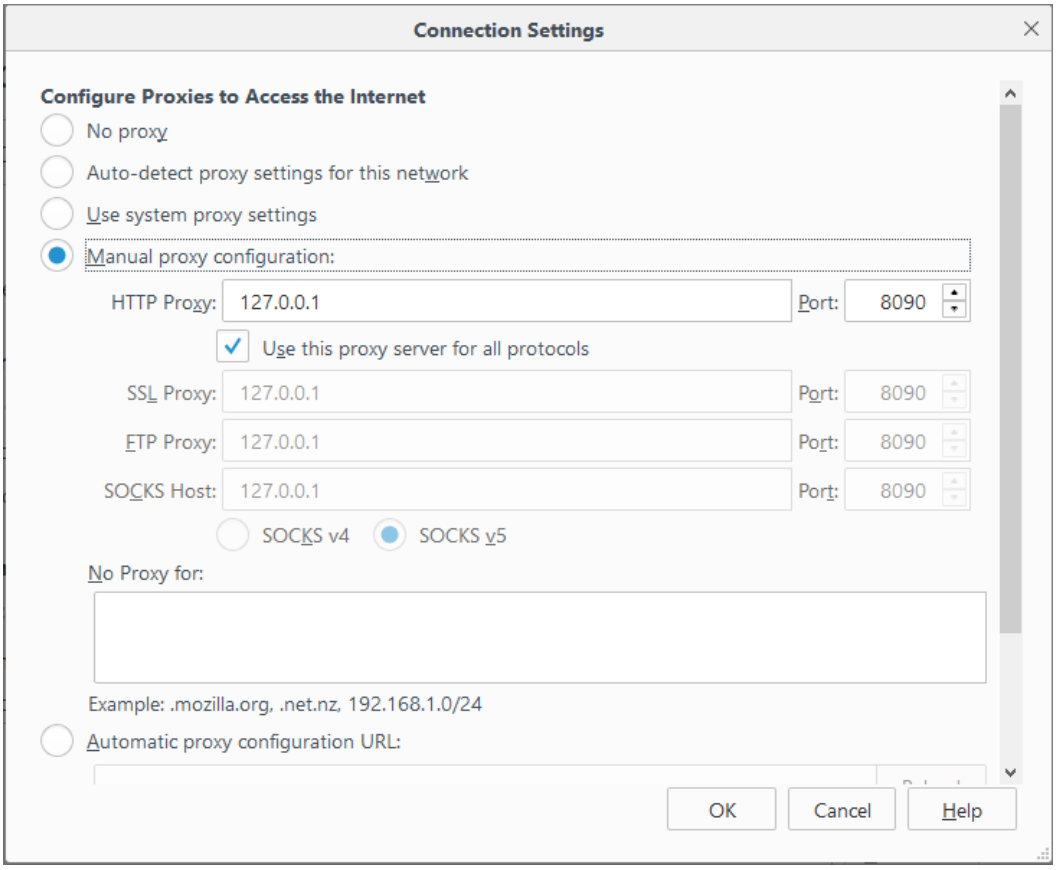
در این فصل نحوه‌ی استفاده از ابزار BurpSuite را برای انجام حمله‌ی Brute Force شرح خواهیم داد. سپس یک نمونه از اینگونه حملات را بر روی ابزار DVWA آزمایش خواهیم کرد.

۲-۲- تغییر Proxy

ابتدا وارد تنظیمات proxy در مرورگر FireFox می‌شویم:

Options => Advanced => Network => Setting…

و تنظیمات زیر را انجام می‌دهیم:

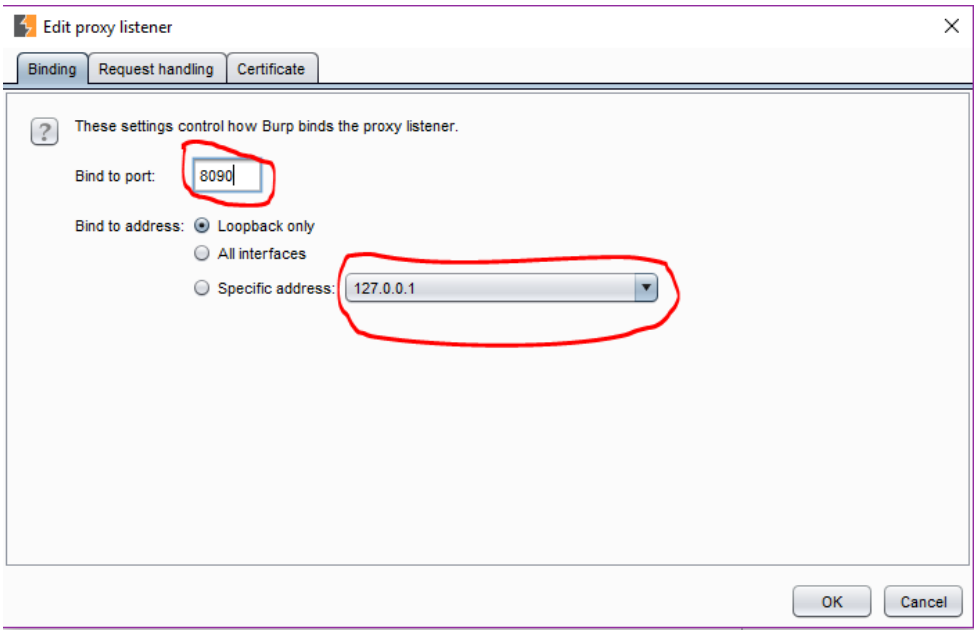


شکل (۲ـ۱) تنظیم Proxy در FireFox

سپس باید Proxy را در BurpSuite تغییر دهیم (مطابق با همان ip وport در FireFox). برای این منظور در محیط BurpSuite وارد این مسیر می‌شویم:

Proxy => Options => Edit

و Proxy را به شکل زیر تغییر می‌دهیم:



شکل (۲ـ۲) تغییر Proxy در BurpSuite

با انجام این کار، اتصـــال مرور گر FireFox به اینترنت تنها از طریق BurpSuite امکان پذیر اســـت (عمل شنود انجام می‌گیرد).

۲-۳-انجام حمله Brute Force

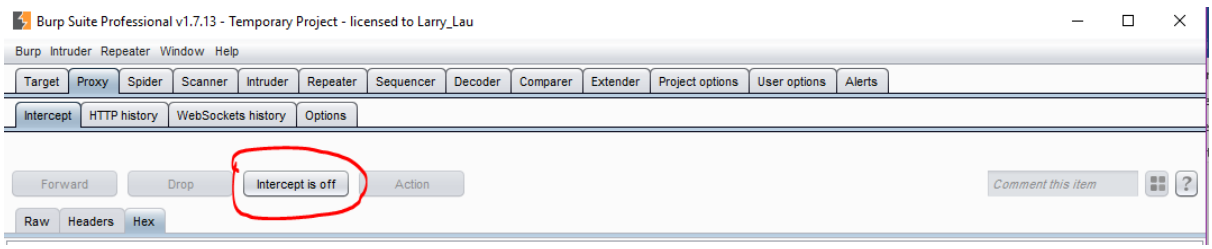
در بخش‌های قبل تمامی تنظیمات لازم برای انجـــام این حمله را انجام دادیم. در این بخش نحوه‌ی انجام این حمله را شرح می‌دهیم.

ما قصد داریم با ابزار BurpSuite حمله BruteForce را بر روی یک وبسایت انجام دهیم.

DVWA این امکان را برای ما فراهم می‌کند که بعنوان وبسایت مورد هجوم از آن استفاده کنیم. همچنین این ابزار این قابلیت را دارد که میزان امینت آن را تعیین کنیم. بعنوان مثال low بودن یعنی وبسایت مد نظر از نظر امنیتی در سطح بسیار ضعیفی می‌باشد.

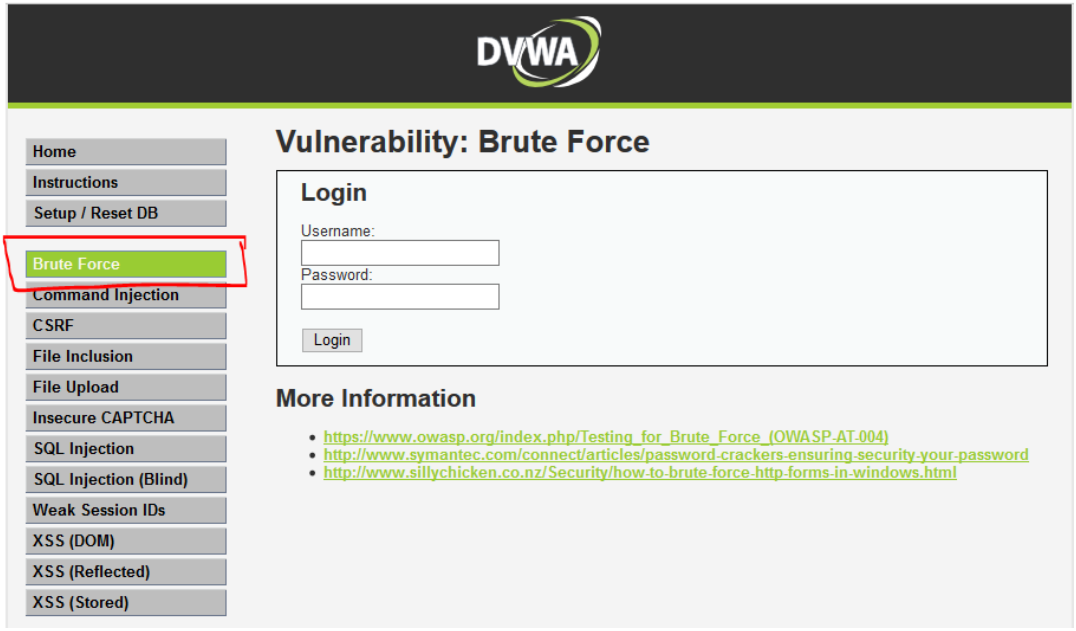
ابتدا در BurpSuite به مسیر زیر رفته و عمل شنود را متوقف می‌کنیم:

Proxy => Intercept



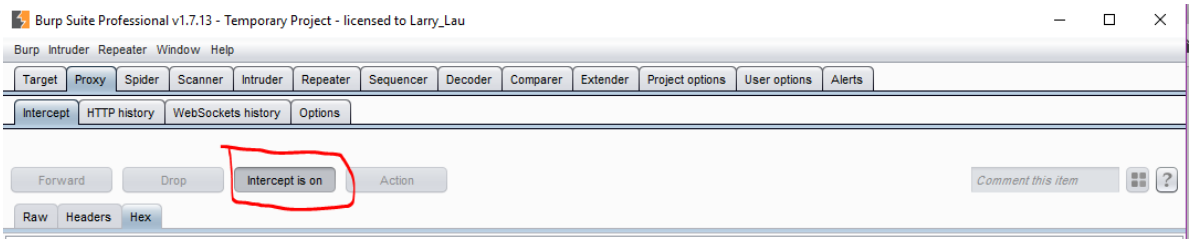
شکل (۲ـ۳) خاموش کردن Intercept

سپس در FireFox وارد ابزار DVWA می‌شویم و حمله‌ی BruteForce را انتخاب می‌کنیم:



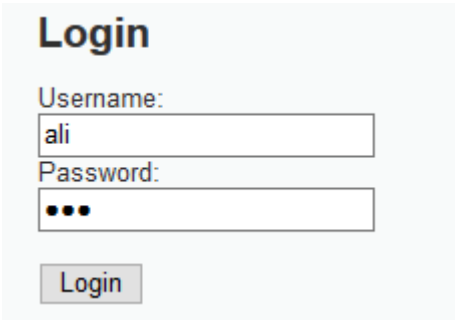
شکل (۲ـ۴) صفحه‌ی حمله BruteForce در DVWA

سپس دوباره به ابزار BurpSuite بازگشته و شنود را فعال می‌کنیم:



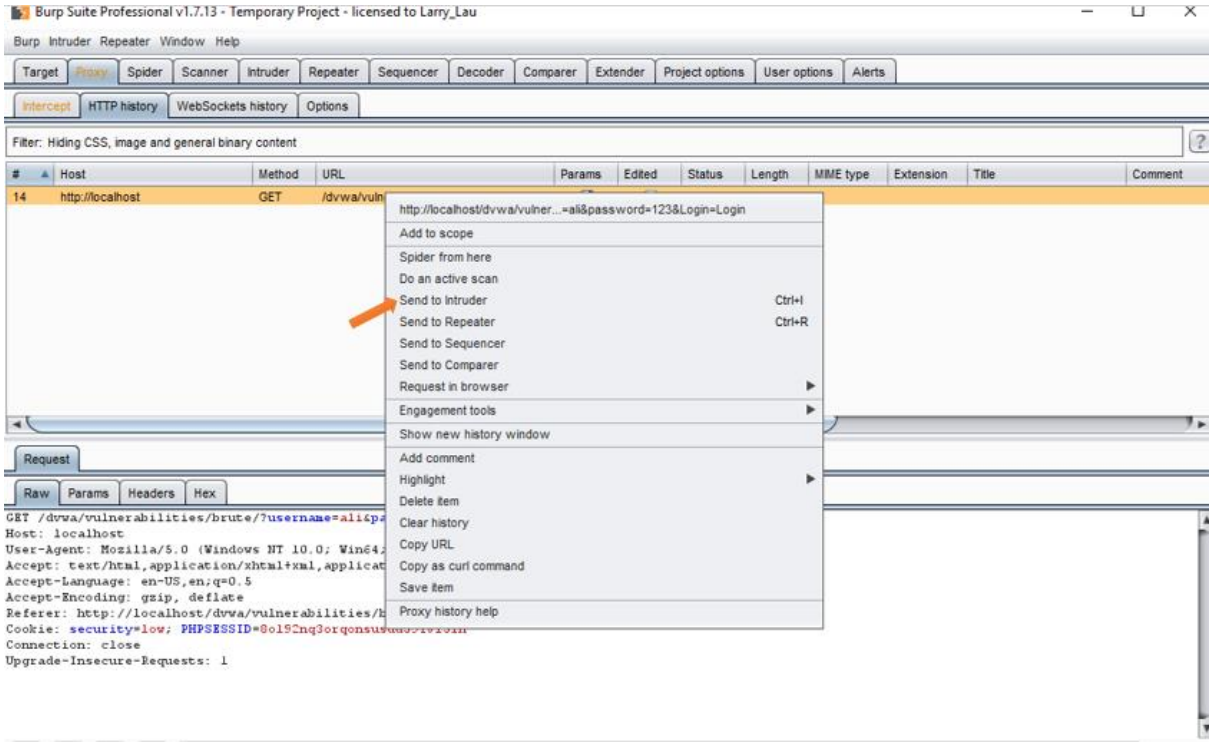
شکل (۲ـ۵) روشن کردن Intercept

به DVWA بازگشته و در همان صفحه‌ی نمایش داده شده در شکل ۲-۴، عمل Login را انجام می‌دهیم (به عنوان مثال Username را ali و Password را 123 قرار می‌دهیم).



شکل (۲ـ۶) فرم Login در حمله‌ی BruteForce در DVWA

پس از زدن دکمه Login وارد BurpSuite شده و درخواست ارسال شده را مشاهده خواهیم کرد. بر روی آن کلیک راست کرده و گزینه‌ی Send To Intruder را انتخاب می‌کنیم:

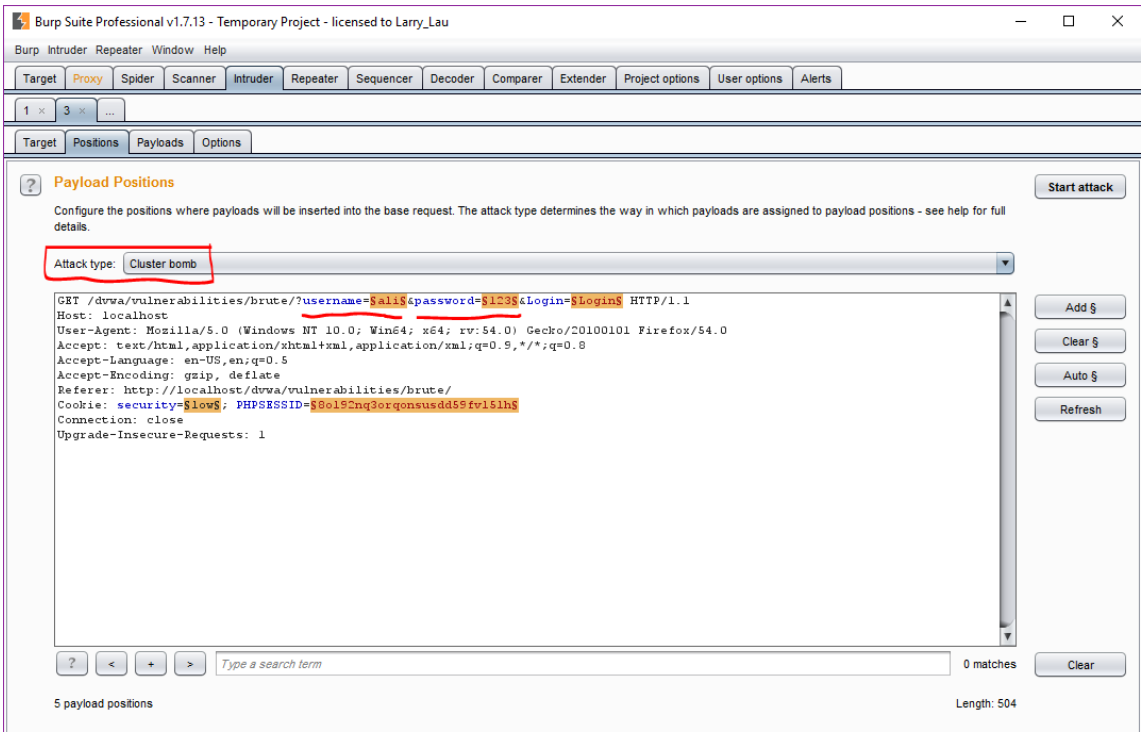


شکل (۲ـ۷) ارسال یک درخواست Login به Intruder در BurpSuite

سپس به مسیر زیر می‌رویم:

Intruder => Positions

در این صفحه تعیین می‌کنیم کدام مقادیر در این حمله به عنوان متغیر هستند. در این مثال، Username و Password را به عنوان متغیر معرفی می‌کنیم:

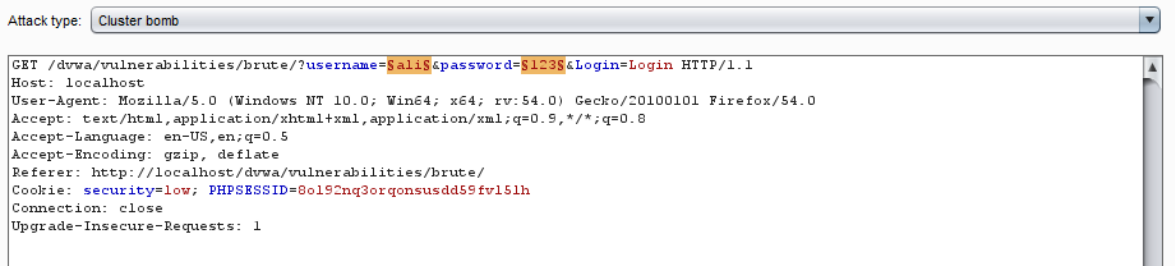


شکل (۲ـ۸) تعریف متغیرها برای حمله BruteForce در BurpSuite

مطابق شکل بالا میباید Attack Type را بر روی حالت Cluster Bomb قرار دهیم.

همچنین م شاهده میکنیم که به طور پی شفرض ۵ متغیر در نظر گرفته شده اند. ما تنها به دو متغیر نیاز داریم. تعریف و حذف متغیر به کمک گزینه های Add و Clear انجام می‌شوند.

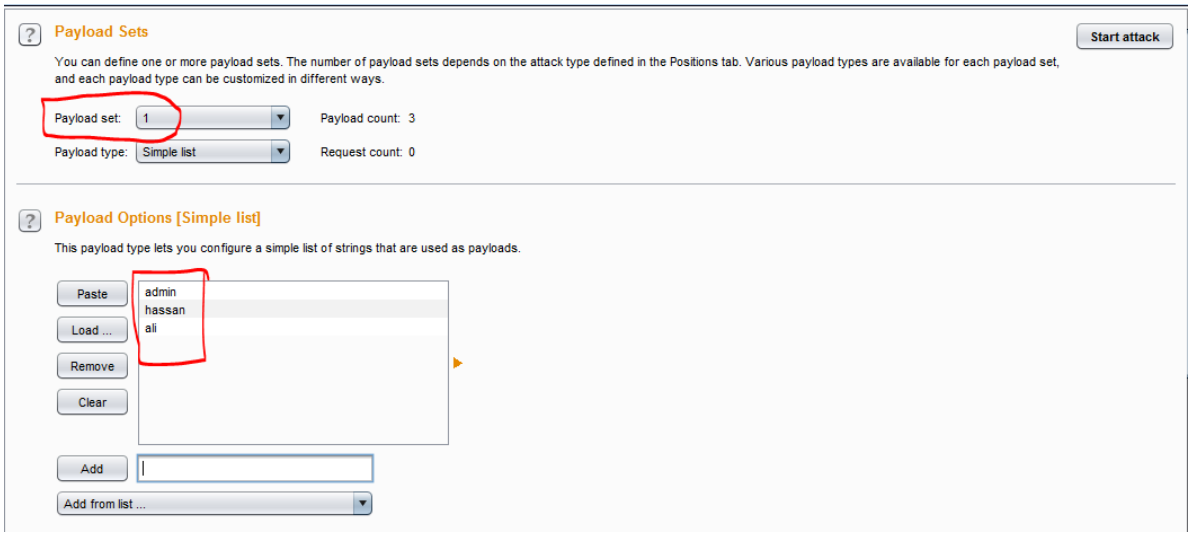
در نهایت این صفحه پس از تعریف متغیر ها به شکل زیر در می‌آید:



شکل (۲ـ۹) شکل نهایی متغیر ها برای حمله BruteForce در BurpSuite

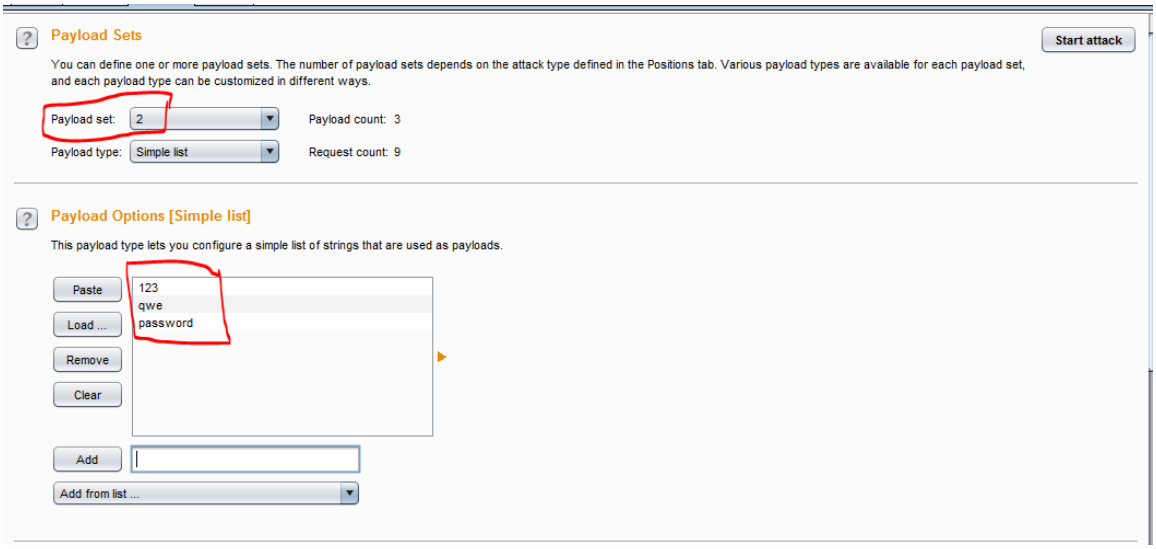
اکنون وارد سربرگ Playloads می شویم. در این صفحه، تعیین خواهیم کرد چه عباراتی برای هر متغیر استفاده شوند.

ابتدا Playload Set را روی ۱ قرار می‌دهیم و برای متغیر اول (Username) مقادیر admin، hassan و ali را در بخش Playload Options قرار می‌دهیم:



شکل (۲ـ۱۰) افزودن مقادیر برای متغیر Username

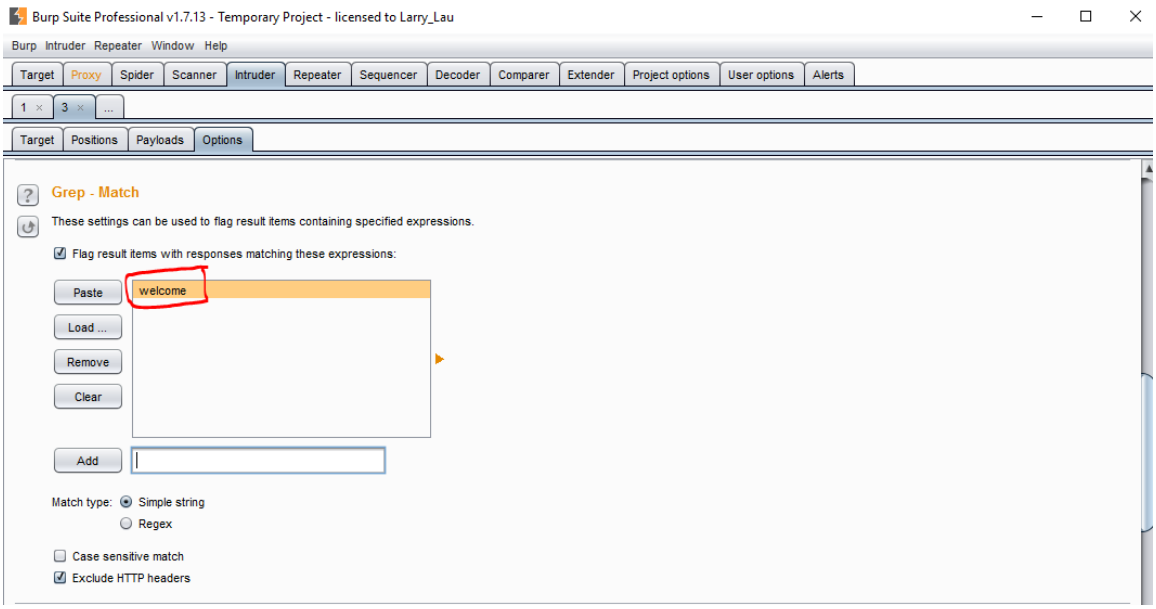
و همین کار را برای متغیر دوم (Password) با کلمات 123، qwe و password انجام می‌دهیم:



شکل (۲ـ۱۱) افزودن مقادیر برای متغیر Password

در ضمن اگر از قبل لیستی از مقادیر در اختیار داشته باشیم، میتوانیم از بخش ..Add from list آن را انتخاب کنیم.

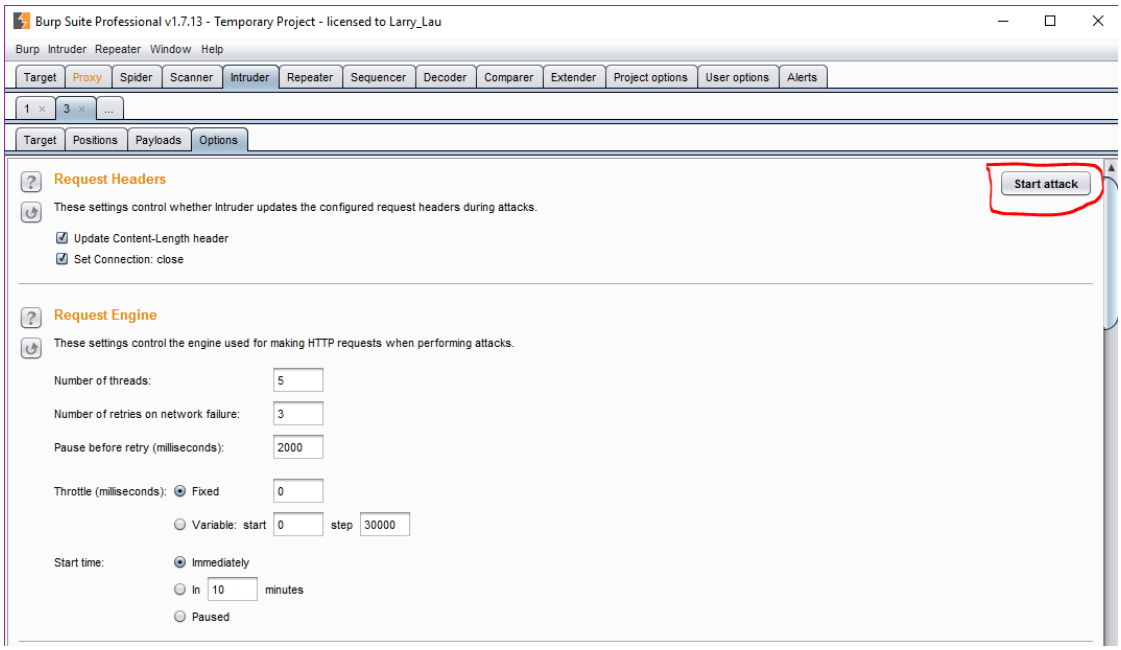
در ادامه به سربرگ Options از همین بخش می‌رویم. در این صفحه در قسمت Grap – Match کلماتی یا عباراتی را تعیین می‌کنیم که انتظار داریم در صورت ورود موفق به وبسایت، آن را مشاهده کنیم. به عنوان مثال عبارت welcome می‌تواند گزینه‌ی خوبی برای انتخاب باشد. آن را به لیست اضافه می‌کنیم. (عبارات اضافی را حذف می‌کنیم):



شکل (۲ـ۱۲) تعیین عبارت welcome برای شناسایی Login های موفق

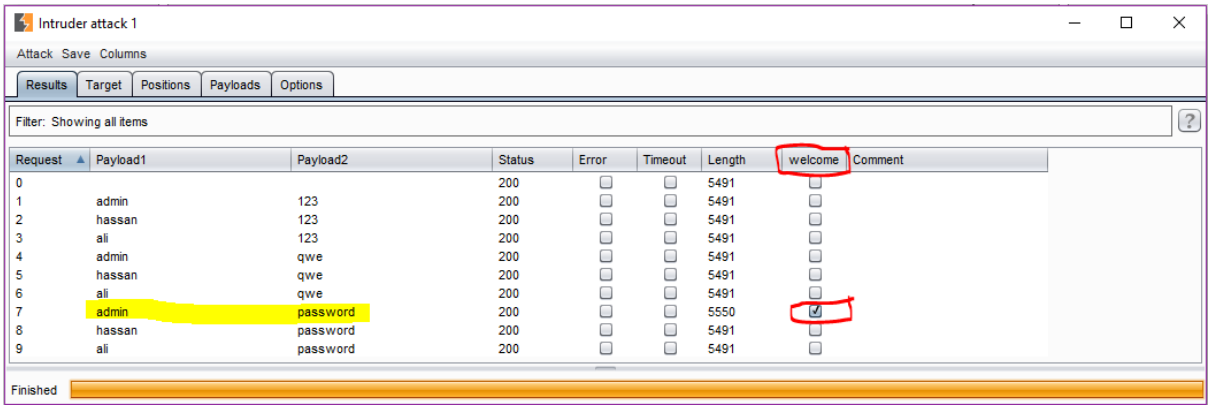
پس اگر یکی از تلاش های ورود با پاسخی شامل این عبارت همراه شود، آن حمله موفق بوده است.

در آخر برای انجام حمله گزینه‌ی Start Attack را از بالای صفحه انتخاب می‌کنیم:



شکل (۲ـ۱۳) انتخاب گزینه‌ی Start Attack برای شروع حمله

پس از انجام این حمله، نتیجه آن نمایش داده می‌شود:



شکل (۲ـ۱۴) نتیجه‌ی حمله‌ی BruteForce

همانطور که در شـکل می‌بینیم، تمامی حالات ممکن با مقادیری که برای متغیرها در نظر گرفتیم امتحان شده و نتایج آن‌ها نمایش داده شده است. تنها در یکی از حالات، عبارت welcome در پاسخ به درخواست ما برای Login ظاهر شده است.

در نتیجه ما به کمک حمله‌ی BruteForce، توانستیم Username و Password وبسایت مدنظر را بشکنیم.