



گزارش انجام حمله ی 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

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

فهرست مطالب

<u>صفحه</u>	<u>عنوان</u>
۱	فصل ۱: نصب و راه اندازی
۲	۱-۱- مقدمه
۲	۲-۱- نصب DVWA
۶	۳-۱- نصب Burp Suite
۷	فصل ۲: حمله Brute Force
۸	۱-۲- مقدمه
۸	۲-۲- تغییر Proxy
۹	۳-۲- انجام حمله Brute Force

فهرست شکل‌ها

<u>صفحه</u>	<u>عنوان</u>
۲.....	شکل (۱-۱) راه اندازی سرویسهای Apache و MySQL در xampp
۳.....	شکل (۲-۱) شکل صحیح اجرای سرویسهای Apache و MySQL در xampp
۳.....	شکل (۳-۱) نحوه‌ی ویرایش فایل config در DVWA
۴.....	شکل (۴-۱) ساخت پایگاه داده در DVWA
۴.....	شکل (۵-۱) ویرایش فایل config در DVWA
۵.....	شکل (۶-۱) صفحه‌ی Login در DVWA
۵.....	شکل (۷-۱) صفحه‌ی ابتدایی ابزار DVWA
۶.....	شکل (۸-۱) محیط ابزار BurpSuite در اجرای اول
۸.....	شکل (۱-۲) تنظیم Proxy در FireFox
۹.....	شکل (۲-۲) تغییر Proxy در BurpSuite
۹.....	شکل (۳-۲) خاموش کردن Intercept
۱۰.....	شکل (۴-۲) صفحه‌ی حمله BruteForce در DVWA
۱۰.....	شکل (۵-۲) روشن کردن Intercept
۱۰.....	شکل (۶-۲) فرم Login در حمله‌ی BruteForce در DVWA
۱۱.....	شکل (۷-۲) ارسال یک درخواست Login به Intruder در BurpSuite
۱۱.....	شکل (۸-۲) تعریف متغیرها برای حمله BruteForce در BurpSuite
۱۲.....	شکل (۹-۲) شکل نهایی متغیرها برای حمله BruteForce در BurpSuite
۱۲.....	شکل (۱۰-۲) افزودن مقادیر برای متغیر Username
۱۳.....	شکل (۱۱-۲) افزودن مقادیر برای متغیر Password
۱۳.....	شکل (۱۲-۲) تعیین عبارت welcome برای شناسایی Login های موفق
۱۴.....	شکل (۱۳-۲) انتخاب گزینه‌ی Start Attack برای شروع حمله
۱۴.....	شکل (۱۴-۲) نتیجه‌ی حمله‌ی BruteForce

فصل ۱:

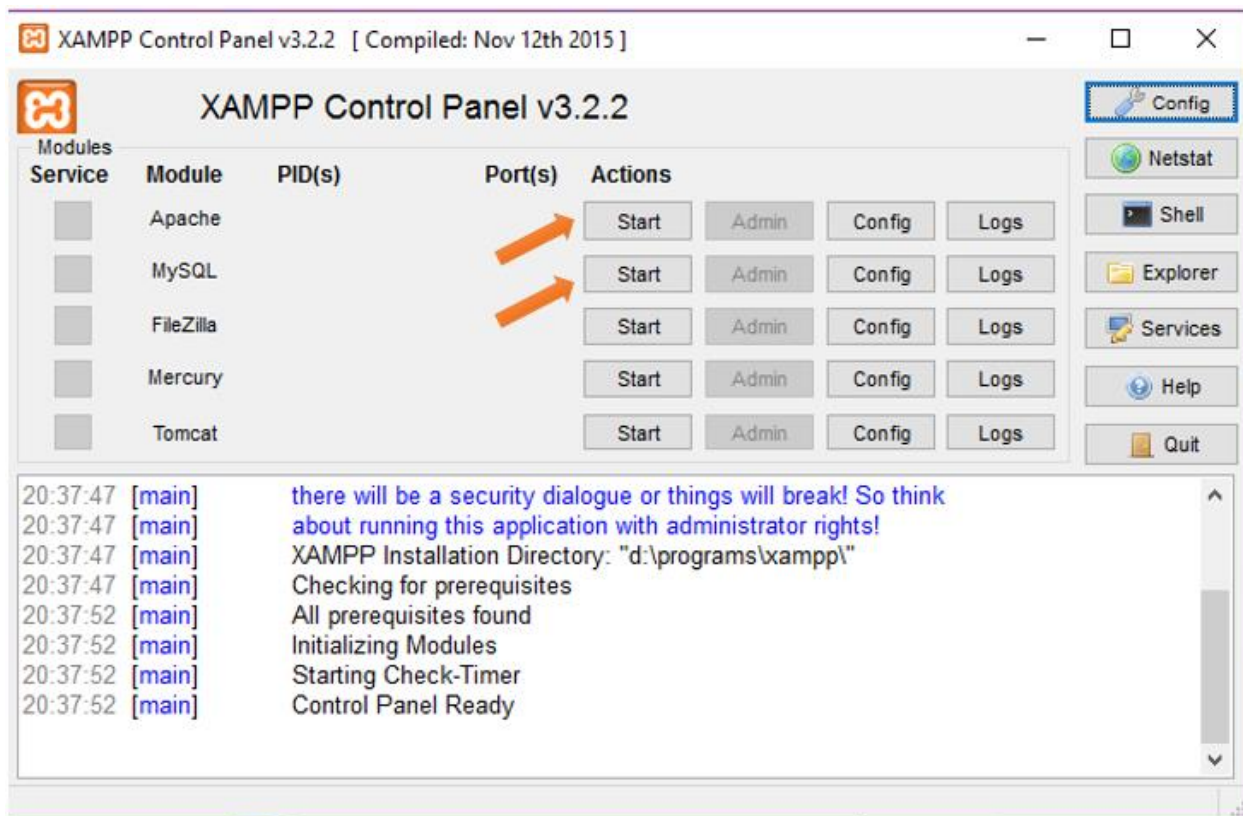
نصب و راه اندازی

۱-۱- مقدمه

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

۲-۱- نصب DVWA

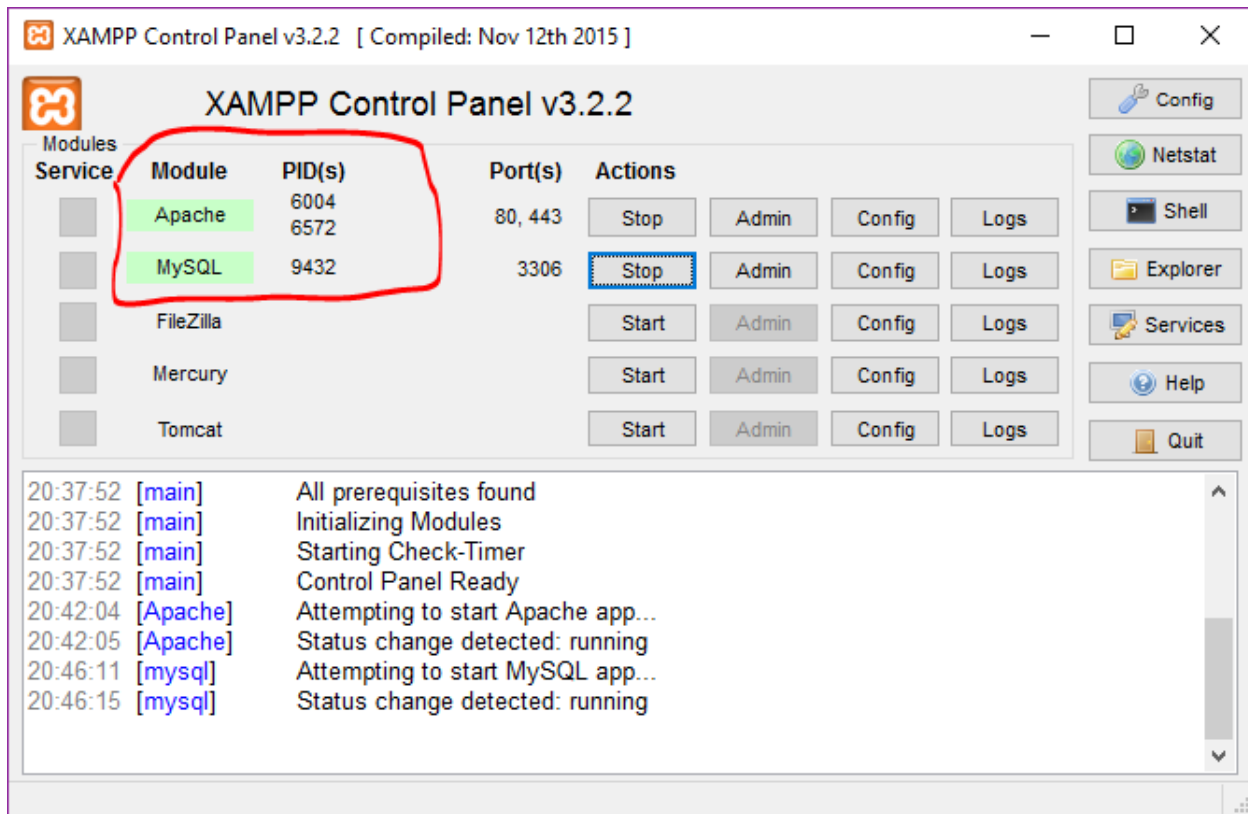
برای این کار لازم است ابتدا نرم افزار xampp را از قبل نصب کرده باشیم. این نرم افزار را اجرا کرده و سرویس های Apache و MySQL را اجرا کنید.



شکل (۱-۱) 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 (۲-۱) 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 پوشه ی config را به config.inc.php تغییر می‌دهیم.

	config.inc	06/16/2017 13:25	PHP File	2 KB
	config.inc.php.dist	06/16/2017 13:25	DIST File	2 KB

شکل (۳-۱) نحوه ی 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 صفحه ی باز شده گزینه ی Create را انتخاب می‌کنیم:

Setup Check

Operating system: **Windows**
Backend database: **MySQL**
PHP version: **7.1.1**

Web Server SERVER_NAME: localhost


PHP function display_errors: **Enabled (Easy Mode!)**
PHP function safe_mode: **Disabled**
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: **Enabled**
PHP function magic_quotes_gpc: **Disabled**
PHP module gd: **Installed**
PHP module mysql: **Installed**
PHP module pdo_mysql: **Installed**

MySQL username: root
MySQL password: *****
MySQL database: dvwa
MySQL host: 127.0.0.1

reCAPTCHA key: **Missing**

[User: Amirian] Writable folder D:\Programs\xampp\htdocs\DVWA\hackable\uploads: **Yes**
[User: Amirian] Writable file D:\Programs\xampp\htdocs\DVWA\external\phpids\0.6\lib\IDS\tmp\phpids_log.txt:
Yes

Status in red, indicate there will be an issue when trying to complete some modules.

 Create / Reset Database

شکل (۴-۱) 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 کنیم:

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

شکل (۵-۱) ویرایش فایل config در DVWA

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



Username

Password

Login

شکل (۶-۱) صفحه‌ی Login در DVWA

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

The screenshot shows the DVWA homepage. At the top is the DVWA logo. Below it is a navigation menu with links: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), DVWA Security, PHP Info, About, and Logout. The main content area has a heading "Welcome to Damn Vulnerable Web Application!" followed by a paragraph describing DVWA as a PHP/MySQL web application for security testing. Below this is a section titled "General Instructions" with a paragraph explaining the user's goal and a "WARNING!" section with a paragraph advising against uploading DVWA to public servers.

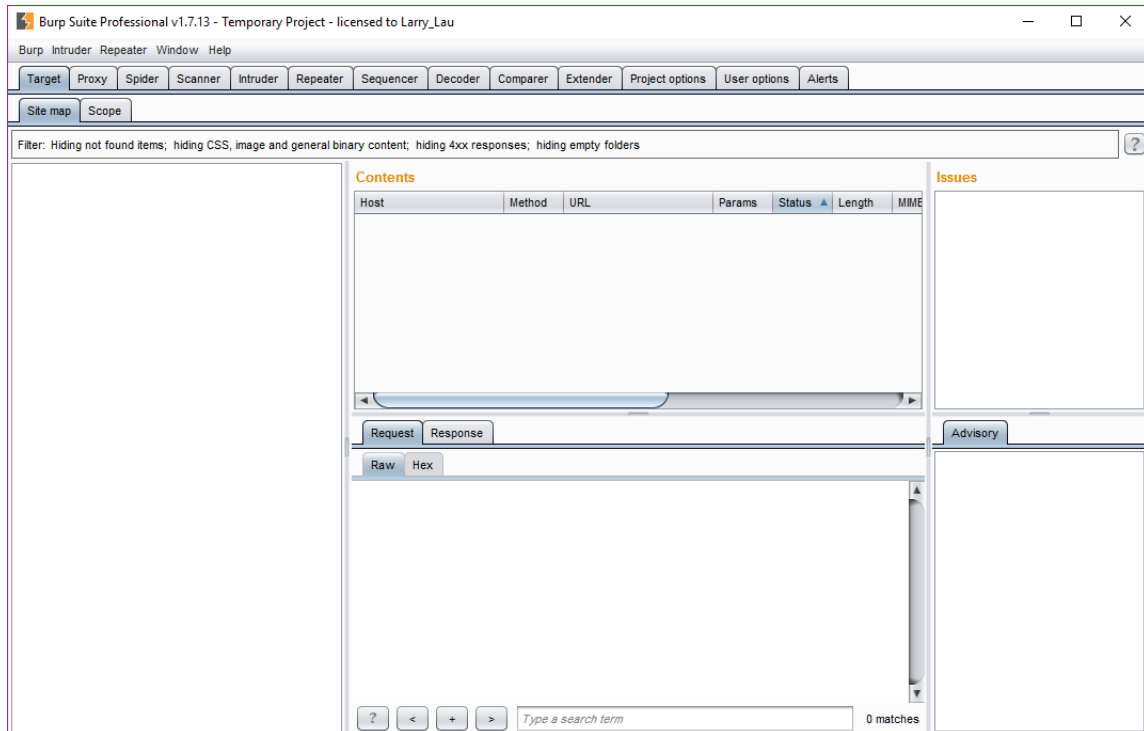
شکل (۷-۱) صفحه‌ی ابتدایی ابزار DVWA

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 (۸-۱) محیط ابزار BurpSuite در اجرای اول

فصل ٢:

حمله Brute Force

۱-۲- مقدمه

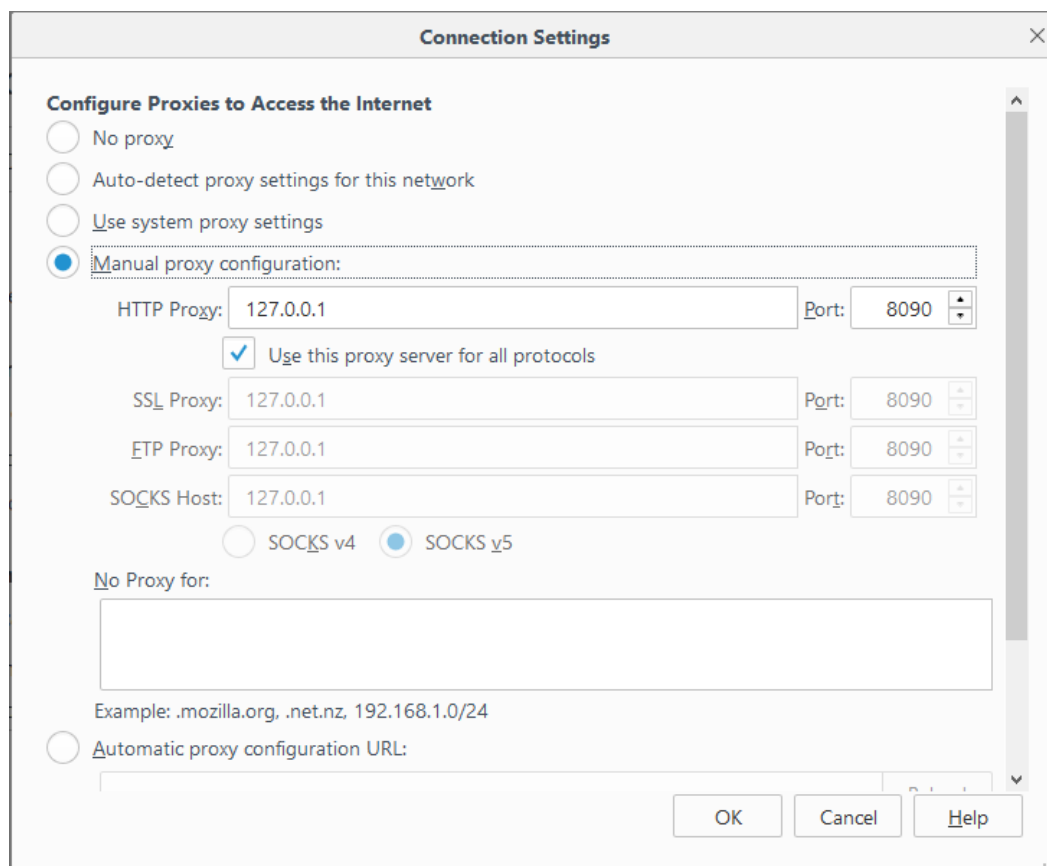
در این فصل نحوه‌ی استفاده از ابزار BurpSuite را برای انجام حمله‌ی Brute Force شرح خواهیم داد. سپس یک نمونه از اینگونه حملات را بر روی ابزار DVWA آزمایش خواهیم کرد.

۲-۲- تغییر Proxy

ابتدا وارد تنظیمات proxy در مرورگر Firefox می‌شویم:

Options => Advanced => Network => Setting...

و تنظیمات زیر را انجام می‌دهیم:



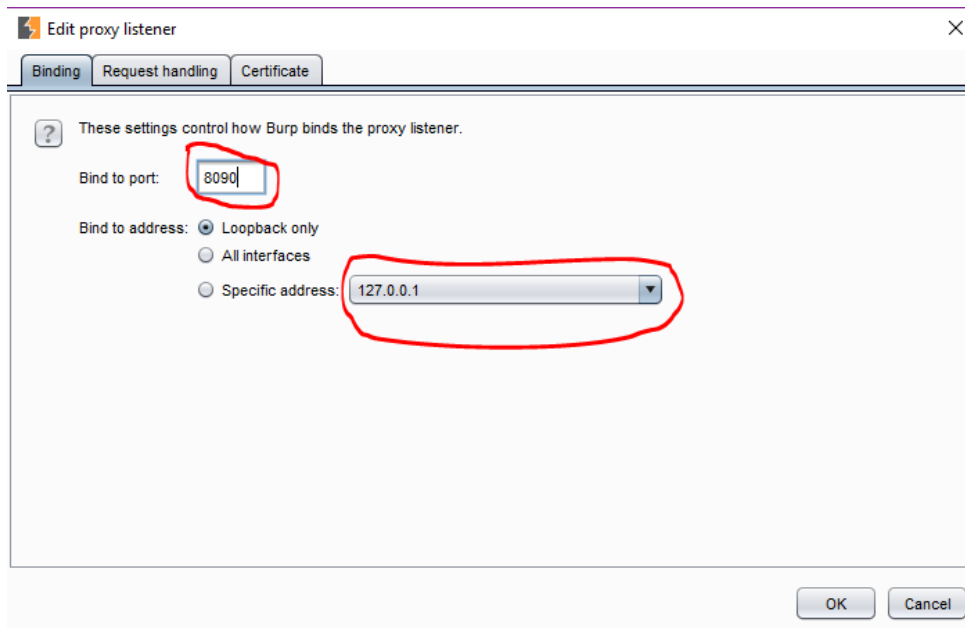
شکل (۱-۲) تنظیم Proxy در Firefox

سپس باید Proxy را در BurpSuite تغییر دهیم (مطابق با همان ip و port در Firefox). برای این

منظور در محیط BurpSuite وارد این مسیر می‌شویم:

Proxy => Options => Edit

و Proxy را به شکل زیر تغییر می‌دهیم:



شکل (۲-۲) تغییر Proxy در BurpSuite

با انجام این کار، اتصال مرور گر Firefox به اینترنت تنها از طریق BurpSuite امکان پذیر است (عمل شنود انجام می گیرد).

۳-۲- انجام حمله Brute Force

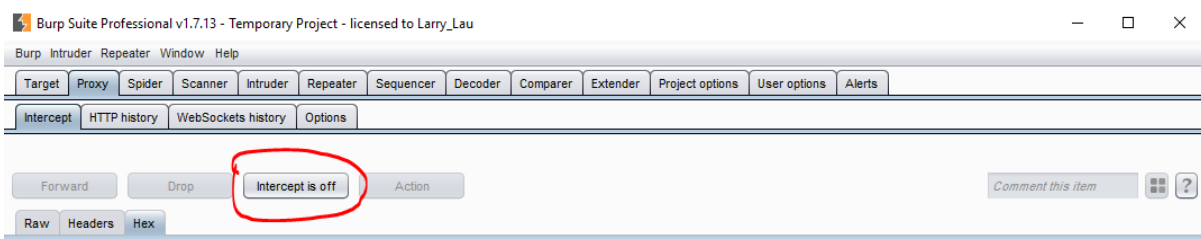
در بخش‌های قبل تمامی تنظیمات لازم برای انجام این حمله را انجام دادیم. در این بخش نحوه‌ی انجام این حمله را شرح می‌دهیم.

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 امنیت آن را تعیین کنیم. بعنوان مثال low بودن یعنی وبسایت مد نظر از نظر امنیتی در سطح بسیار ضعیفی می‌باشد.

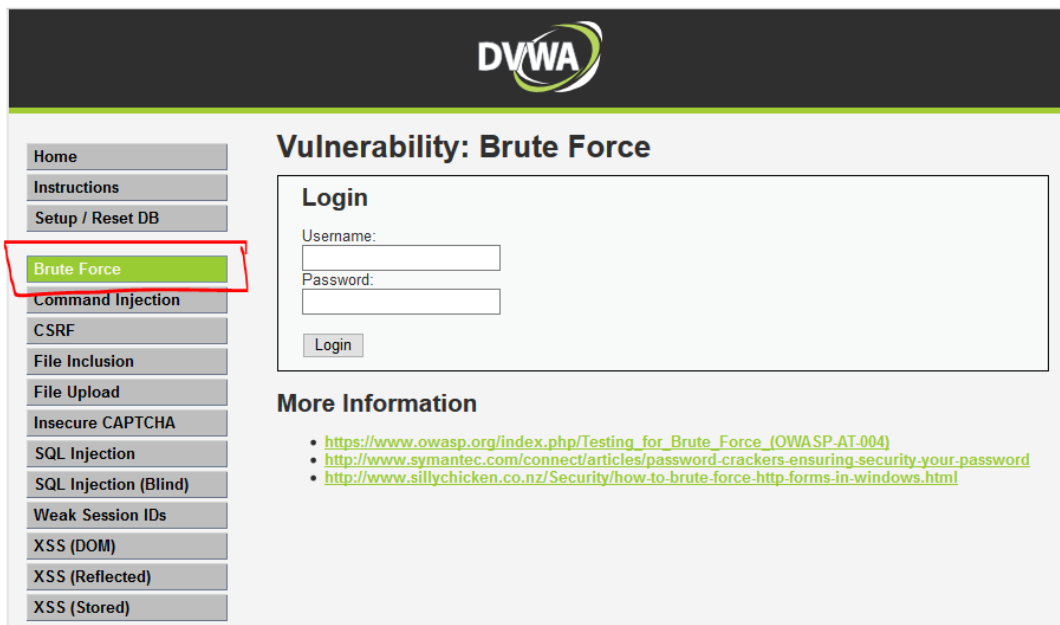
ابتدا در BurpSuite به مسیر زیر رفته و عمل شنود را متوقف می‌کنیم:

Proxy => Intercept



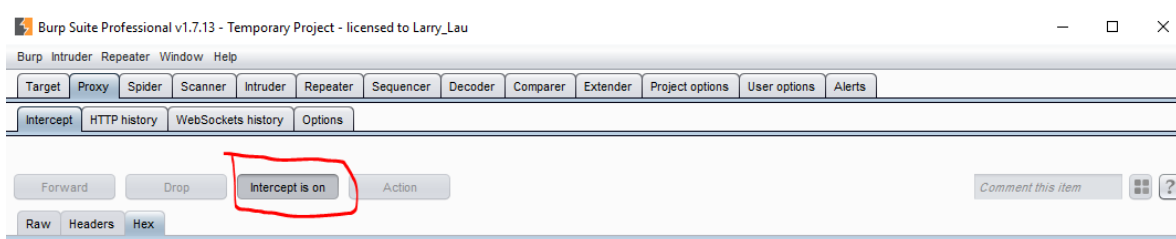
شکل (۳-۲) خاموش کردن Intercept

سپس در FireFox وارد ابزار DVWA می شویم و حمله ی BruteForce را انتخاب می کنیم:



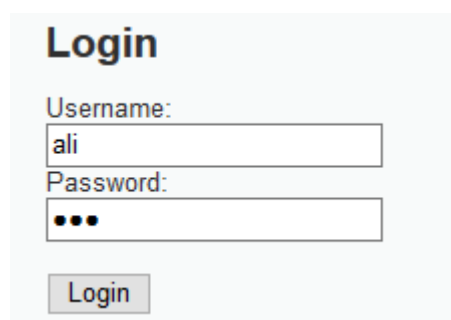
شکل (۴-۲) صفحه ی حمله BruteForce در DVWA

سپس دوباره به ابزار BurpSuite بازگشته و شنود را فعال می کنیم:



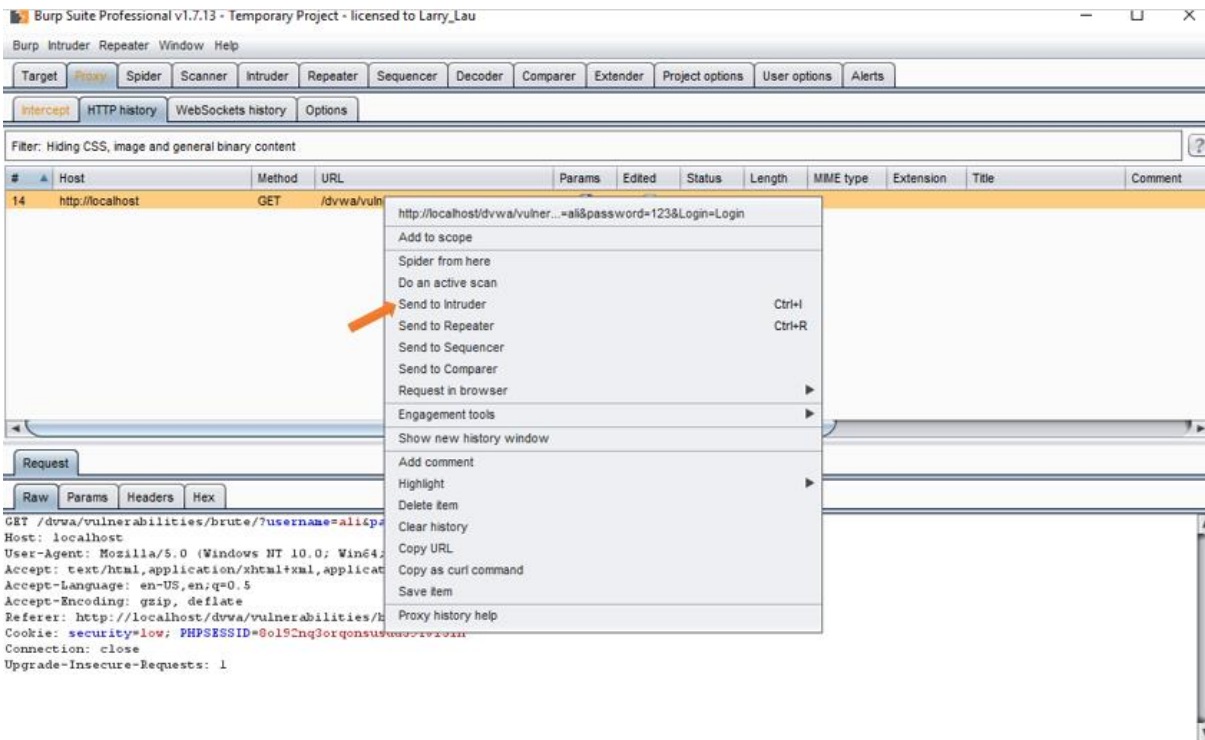
شکل (۵-۲) روشن کردن Intercept

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



شکل (۶-۲) فرم Login در حمله ی 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 گزینه ی Send To Intruder را انتخاب می کنیم:

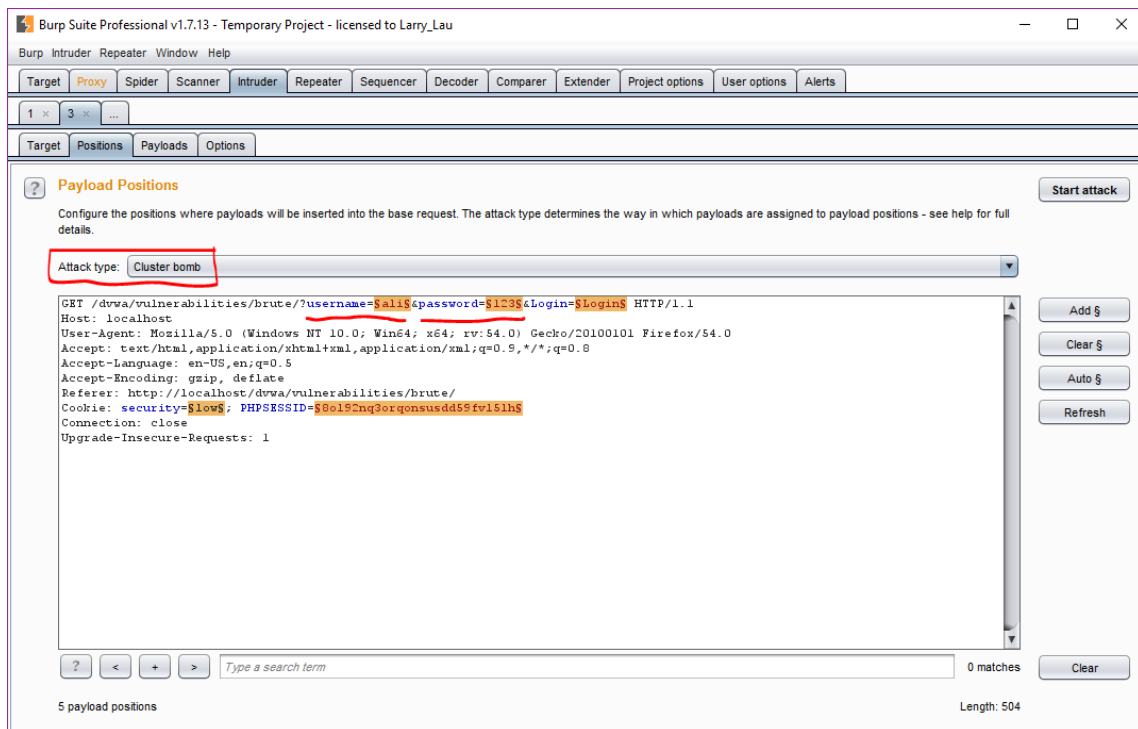


شکل (۷-۲) ارسال یک درخواست Login به Intruder در BurpSuite

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 (۸-۲) تعریف متغیرها برای حمله BruteForce در BurpSuite

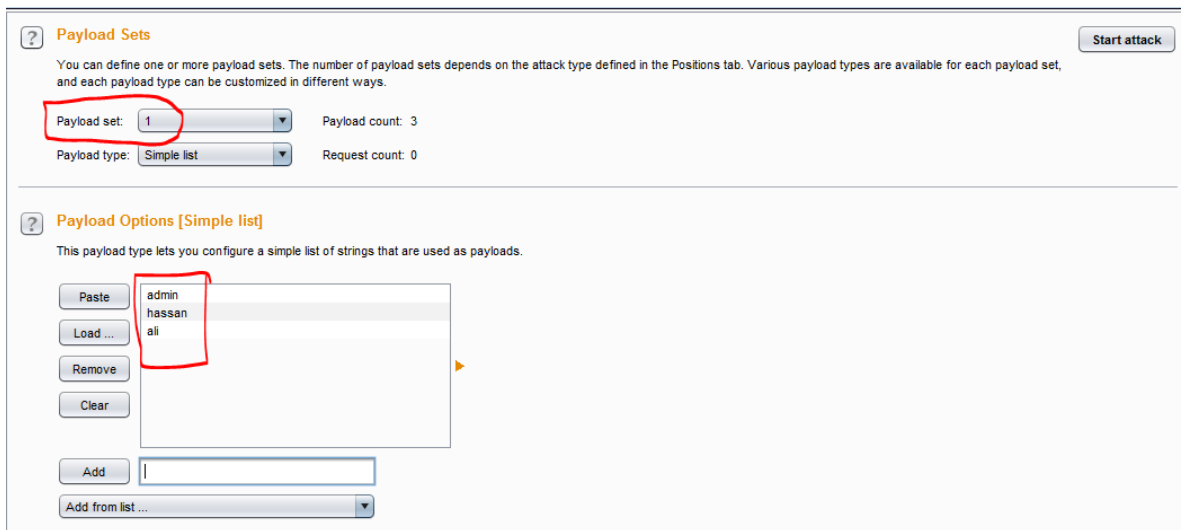
مطابق شکل بالا میباید Attack Type را بر روی حالت Cluster Bomb قرار دهیم. همچنین مشاهده میکنیم که به طور پیش فرض ۵ متغیر در نظر گرفته شده اند. ما تنها به دو متغیر نیاز داریم. تعریف و حذف متغیر به کمک گزینه های Add و Clear انجام می شوند. در نهایت این صفحه پس از تعریف متغیرها به شکل زیر در می آید:

```
Attack type: Cluster bomb
GET /dvwa/vulnerabilities/brute/?username=$ali&password=$123&Login=Login HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/dvwa/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=80192nq3orqonsusdd59fv151h
Connection: close
Upgrade-Insecure-Requests: 1
```

شکل (۹-۲) شکل نهایی متغیرها برای حمله BruteForce در BurpSuite

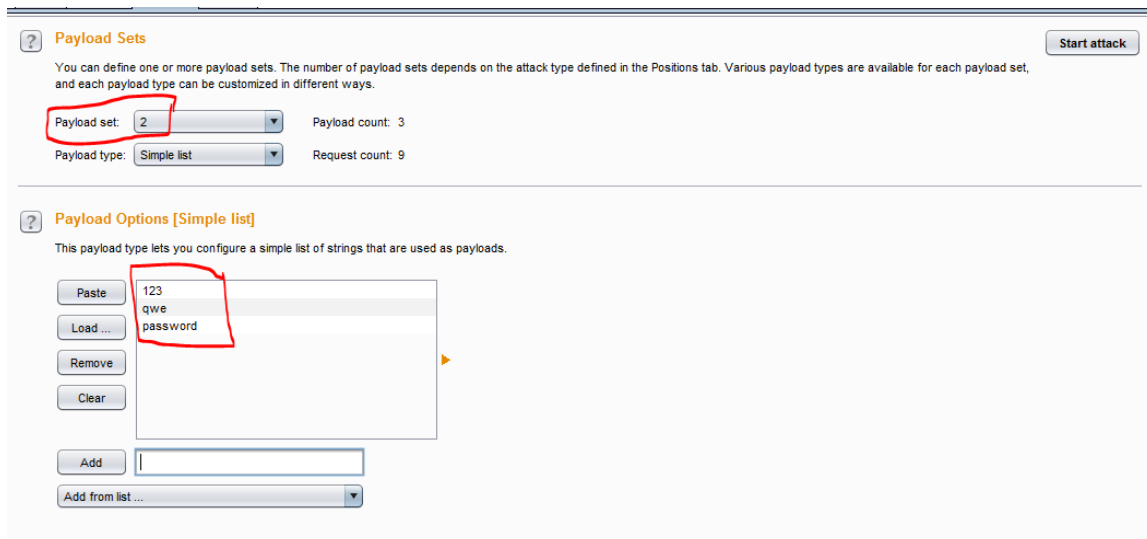
اکنون وارد سربرگ Payloads می شویم. در این صفحه، تعیین خواهیم کرد چه عباراتی برای هر متغیر استفاده شوند.

ابتدا Payload Set را روی ۱ قرار می دهیم و برای متغیر اول (Username) مقادیر admin, hassan و ali را در بخش Payload Options قرار می دهیم:



شکل (۱۰-۲) افزودن مقادیر برای متغیر Username

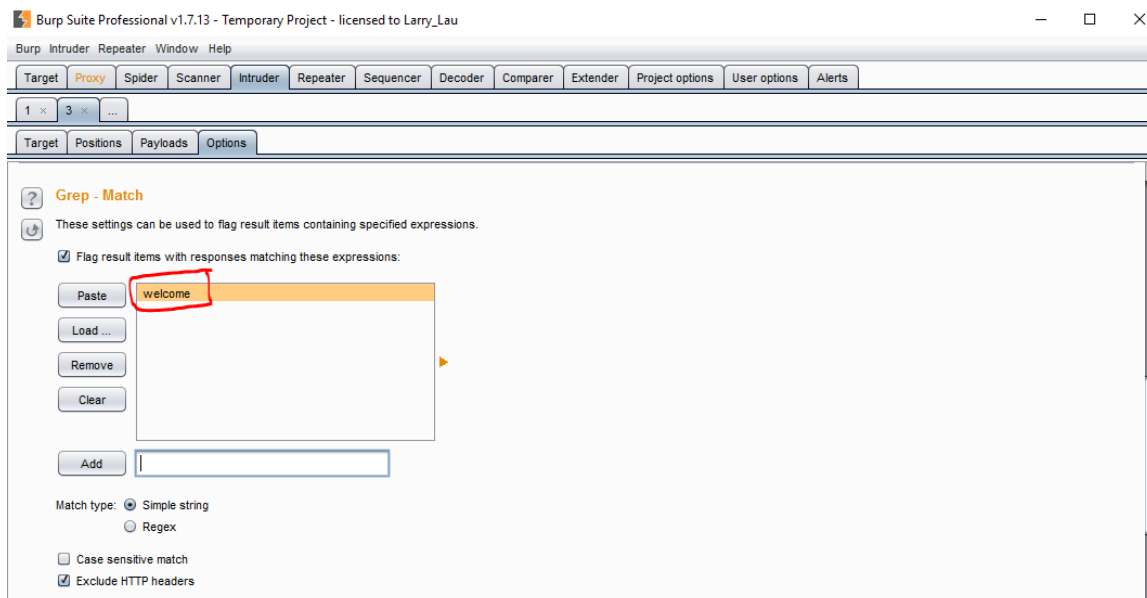
و همین کار را برای متغیر دوم (Password) با کلمات 123، qwe و password انجام می دهیم:



شکل (۱۱-۲) 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.

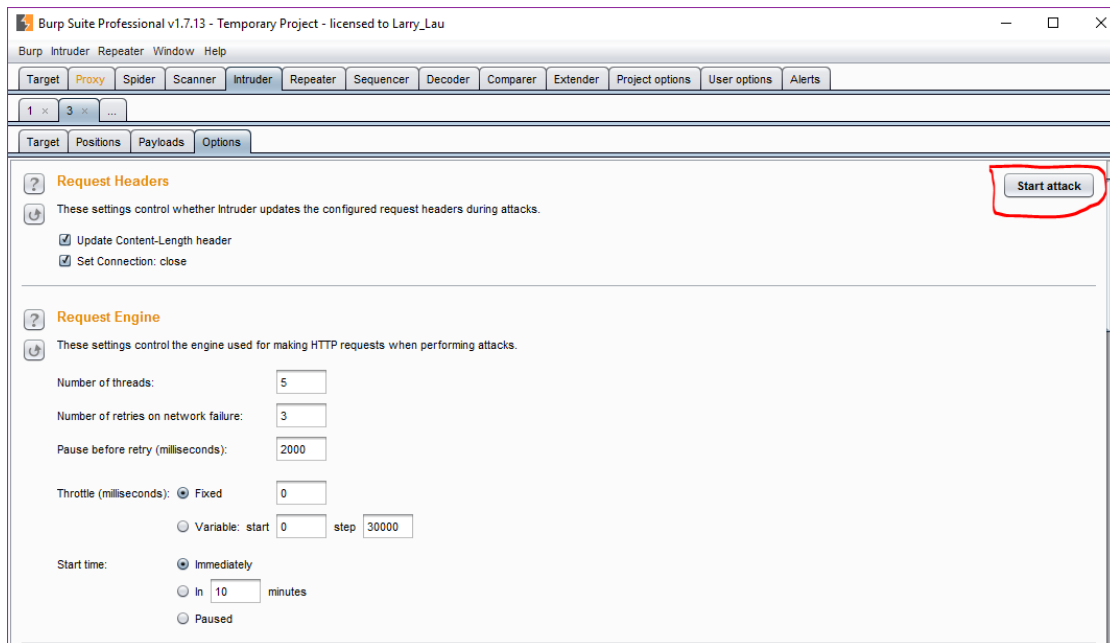
در ادامه به سربرگ Options از همین بخش می‌رویم. در این صفحه در قسمت Grep - Match کلماتی یا عباراتی را تعیین می‌کنیم که انتظار داریم در صورت ورود موفق به وبسایت، آن را مشاهده کنیم. به عنوان مثال عبارت welcome می‌تواند گزینه‌ی خوبی برای انتخاب باشد. آن را به لیست اضافه می‌کنیم. (عبارات اضافی را حذف می‌کنیم):



شکل (۱۲-۲) تعیین عبارت welcome برای شناسایی Login های موفق

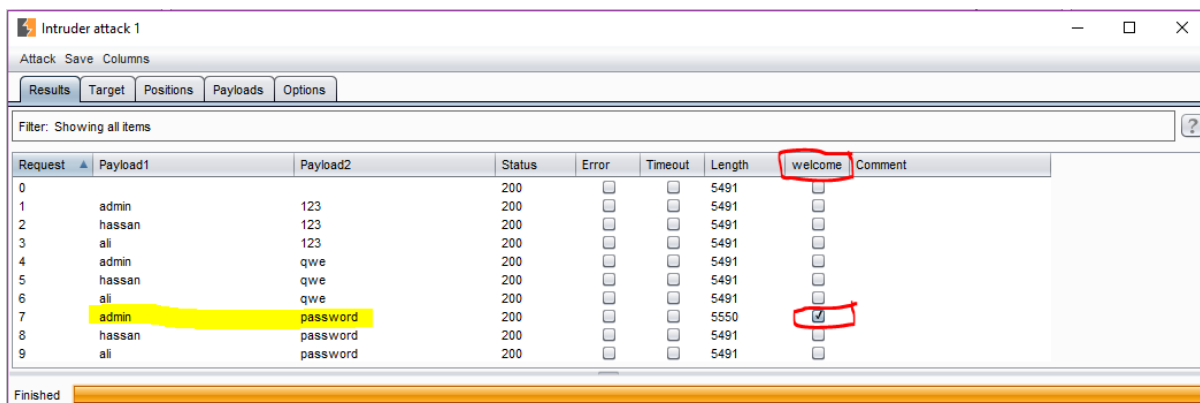
پس اگر یکی از تلاش‌های ورود با پاسخی شامل این عبارت همراه شود، آن حمله موفق بوده است.

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



شکل (۱۳-۲) انتخاب گزینهی Start Attack برای شروع حمله

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



شکل (۱۴-۲) نتیجهی حملهی BruteForce

همانطور که در شکل 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.