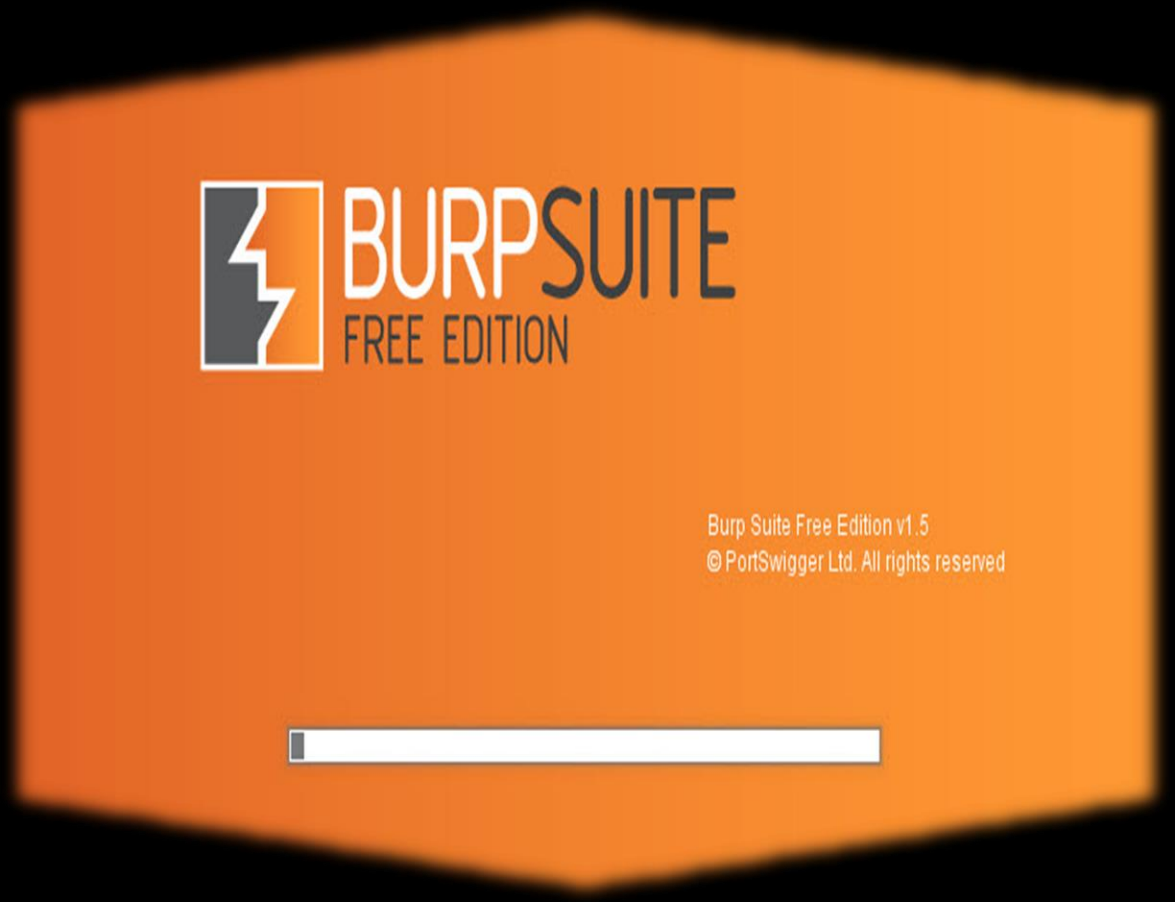


Yellow Way; Burp Suite, Web Penetration Testers Guide

By Milad Kahsari Alhadi(C3phalex1n)

Www.miladkahsari.iR

What is Burp Suite?, Intercepting web requests, Inspecting web requests, Tampering web requests, Target site map functionality, Crawling a web application with Burp Spider, Launching an automatic scan with Burp Scanner, Automating customized attacks with Burp Intruder

بِسْمِ اللّهِ الرَّحْمنِ الرَّحيمِ

اللّـهـم عـجّـل لـولیـــک الـفَــرَج و العـافـیة و الـنّـصـر

و اجـعـلنـا من خَیرَ اَنـصاره و اعوانه و المُستشهَدین بَـینَ یَـدَیــه

درباره نویسنده کتاب

نام و نام خانوادگی: میلاد کهساری الهادی (c3phalex1n)

تاریخ تولد: 1373- اردیبهشت -14

میلاد کهساری الهادی؛ در حال حاضر دانشجوی دوره کاردانی نرم افزار در دانشگاه شهید چمران می باشد. او علاقمند به ارزیابی امنیت سیستم های رایانه ای، تحلیل بدافزارهای کامپیوتری و مهندسی معکوس است و از سابقه کاری او می توان به مدیریت تیم دانشجویی فناوری شبکه و الکترونیک دانشگاه چمران و چندین دوره تدریس در webamooz اشاره کرد. او همچنین در دوره فعالیت های خود کتاب هایی از جمله؛ راهنمای استفاده از فریمورک متاسپلویت، راهنمای راه اندازی آزمایشگاه امنیت، راهنمای استفاده از برنامه Wireshark، راهنمای عملی تجزیه و تحلیل بدافزارهای کامپیوتری به همراه مقالاتی به انتشار عموم رسانده است. همچنین شایان ذکر است، زمینه مورد علاقه تحقیقات ایشان فیزیک، سیستم های دفاعی نظامی و امنیت سیستم های کامپیوتری است. همچنین او در حال حاضر مشغول پژوهش بر روی تکنیک های هوشمند سازی سیستم های امنیتی است.

Twitter: https://twitter.com/C3phalex1n_0x

Facebook: https://facebook.com/Milad.kahsari

Linkedin : https://ir.linkedin.com/in/miladkahsari

Milad Kahsari Alhadi (0xc3phalex1n[AT]gmail.com)

پیشگفتار نویسنده

دقایقی از شب یلدا سال 92 سپری نشده بود که داشتم به موزیک گوش می کردم و با تبلت مستندات Burp Suite را مشاهده و بررسی می کردم. متاسفانه متوجه شدم، مدت زمان زیادی از ایجاد و انتشار برنامه Burp Suite توسط شرکت PortSwigger می گذرد. اما در عجب بودم، بعد از این همه مدت فعالیت این برنامه کاربردی، یک شخص در این کشور اسلامی وجود نداشته است که منبعی به زبان پارسی برای این برنامه تعریف کرده و آنرا انفاق در راه علم کند؟

متاسفانه این روز ها بعد از چند دوره تدریس دروس مختلف امنیت و اطلاعات در آموزشگاه ها منبعی نیافته بودم که برای آشنایی هنرآموزان با این برنامه مفید و مناسب باشد. این بود که دست به قلم بردم تا آنکه این کتاب کوچک که پیش روی شماست را به نگاشت در آورم.

در حالی که این متن را می نویسم، به لطف پروردگار بزرگ چندین کتاب نوشته ام که برخی از آنها به صورت اینترنتی به انتشار رسیده اند و برخی از آنها هم در صف چاپ قرار دارند. اما با این اوصاف خیلی مواقع از طرف برخی افراد مورد کنایه قرار می گیرم، لذا این موضوع را حیاتی می دانم در اینجا ذکر کنم، بنده در آنچه چاپ شده یا به انتشار اینترنتی رسیده است کوچکترین نفع مادی نبرده ام و به آنچه در این راه وجود دارد نیز طمع مادی ندارم. این متون را فقط زکات علم می دانستم و می دانم و خواهم دانست.

همچنین، با یک محاسبه سر انگشتی به این نتیجه رسیدم خرید کتاب چاپ شده از توان مالی خیلی از دانشجویان و هنر آموزان خارج است. از همین روی، دل به دریا زدم و تصمیم گرفتم این کتاب را به صورت الکترونیکی و رایگان به انتشار برسونم. البته بارها و بارها بنده مورد کم لطفی دوستان قرار گرفتم، و شاید از نظر برخی از افراد با این وجود حماقت می کنم که وقت می زارم و کتب انگلیسی را می خوانم و ترجمه می کنم و در آخر به رایگان به انتشار می رسانم. این حرف ها را نمی زنم که گویی دارم معنت بر سر خوانندگان این کتاب می گذارم، نه. فقط می خواهم این را بگویم، شخصی در کار های خود موفق است که در مسیری که گام برداشته است، ثابت قدم باشد. لذا این آتش هایی که هر لحظه وجود من را به جهنم تبدیل می کنند را با آغوشی گرم پذیرا هستم. قابل ذکر است، این کتاب رایگان می باشد و قیمتی برای آن در نظر نگرفته ام. اما اگر شخصی از شما قصد حمایت مالی به شخص نویسنده این کتاب داشت، می تواند هرچقدر که این کتاب برای او ثمر بخش بوده است، به شماره حساب 6037-9918-3626-8742 به نام میلاد کهساری الهادی مبلقی واریز کند. همچنین ادب حکم می کند اینجا از دوست عزیزم علی عباسی(Black IC3) بابت تمامی راهنمایی ها و کمک هایی که به بنده کرد تشکر کنم. امیدوارم این بزرگوار در طول زندگی خود همواره موفق و سربلند باشد.

میلاد کهساری الهادی

1392-11-06

داستان فوق العاده آهنگر:

آهنگری پس از گذراندن جوانی پرشر و شور، تصمیم گرفت روحش را وقف خدا کند. سال‌ها با علاقه کار کرد، به دیگران نیکی کرد، اما با تمام پرهیزگاری، در زندگی‌اش اوضاع درست به نظر نمی‌آمد. حتی مشکلاتش مدام بیش‌تر می‌شد. یک روز عصر، دوستی که به دیدنش آمده بود و از وضعیت دشوارش مطلع شد، گفت: «واقعا که عجبا. درست بعد از این که تصمیم گرفته‌ای مرد خداترسی بشوی، زندگی‌ات بدتر شده، نمی‌خواهم ایمانت را ضعیف کنم اما با وجود تمام رنجهایی که در مسیر معنویت به خود داده‌ای، زندگیت بهتر نشده.»

آهنگر مکث کرد و بلافاصله پاسخ نداد. سرانجام در سکوت، پاسخی را که می‌خواست یافت. این پاسخ آهنگر بود: در این کارگاه، فولاد خام برایم می‌آورند و باید از آن شمشیر بسازم. می‌دانی چه طور این کار را می‌کنم؟ اول تکه‌ی فولاد را به اندازه‌ی جهنم حرارت می‌دهم تا سرخ شود. بعد با بی‌رحمی، سنگین‌ترین پتک را بر می‌دارم و پشت سر هم به آن ضربه می‌زنم، تا این که فولاد، شکلی را بگیرد که می‌خواهم. بعد آن را در تشت آب سرد فرو می‌کنم، و تمام این کارگاه را بخار آب می‌گیرد، فولاد به خاطر این تغییر ناگهانی دما، ناله می‌کند و رنج می‌برد. باید این کار را آن قدر تکرار کنم تا به شمشیر مورد نظرم دست بیابم. یک بار کافی نیست.

آهنگر مدتی سکوت کرد و سپس ادامه داد: گاهی فولادی که به دستم می‌رسد، نمی‌تواند تاب این عملیات را بیاورد. حرارت، ضربات پتک و آب سرد تمامش را ترک می‌اندازد. می‌دانم که این فولاد، هرگز تیغه‌ی شمشیر مناسبی در نخواهد آمد. آنوقت است که آنرا به میان انبوه زباله‌های کارگاه می اندازم. باز مکث کرد و بعد ادامه داد: می‌دانم که در آتش رنج فرو می‌روم. ضربات پتکی را که زندگی بر من وارد کرده، پذیرفته‌ام، و گاهی به شدت احساس سرما می‌کنم. انگار فولادی باشم که از آبدیده شدن رنج می‌برد. اما تنها دعایی که به درگاه خداوند دارم این است : **«خدای من، از آنچه برای من خواسته ای صرف نظر نکن تا شکلی را که می‌خواهی، به خود بگیرم. به هر روشی که می‌پسندی ادامه بده ؛ هر مدت که لازم است، ادامه بده، اما هرگز، هرگز مرا به کوه زباله های فولادهای بی فایده پرتاب نکن»**

Burp Suite – Web Penetration Tester's Guide

به کتابچه راهنمای برنامه Brup Suite برای متخصصین امنیت برنامه های کاربردی وب خوش آمدید. این کتاب برای مستند سازی برنامه امنیتی Brup Suite ایجاد شده است و در حین خواندن آن شما خواهید آموخت چگونه آن را راه اندازی کنید و چگونه از آن برای آزمایش امنیت برنامه های کاربردی تحت وب استفاده کنید. همچنین در حین خواندن این کتاب با ویژگی های اصلی این برنامه هم آشنا خواهید شد.

این کتابچه شامل محتویات زیر می شود:

خب، برنامه Burp Suite چیست؟ در این قسمت که فصل اوب این کتاب است، شما متوجه خواهید شد برنامه Burp Suite واقعا چیست، چه کاری می توانید با آن انجام بدهید و چرا آن برای متخصصین وب یک ابزار بسیار کاربردی است.

نصب کردن برنامه -- در این قسمت شما خواهید آموخت چگونه این برنامه را دانلود و نصب کنید.

یک شروع سریع -- در این قسمت به شما برخی از ویژگی های اصلی برنامه Brup Suite مانند جداسازی درخواست های HTTP/S و انجام دادن دستکاری بر روی آن ها را نشان خواهیم داد و به دنبال آنها ویژگی های دیگر برنامه مانند جداسازی، بررسی و تغییر دادن ترافیک HTTP/S میان سرور و کلاینت را مورد بررسی قرار خواهیم داد.

هشت ویژگی مهم Brup Suite که شما باید آنها را بدانید -- در این قسمت، شما انجام دادن هشت ویژگی موجود در برنامه Brup Suite را خواهید آموخت. در پایان این فصل شما قادر خواهید بود از قابلیت Target site map برنامه Burp Suite استفاده کنید، در یک برنامه کاربردی تحت وب بخزید یا crawl کنید، یک عملیات پوش به منظور شناسایی ضعف های امنیتی موجود در برنامه کاربردی تحت وب هدفتان انجام بدهید، برخی حملات را خودکار سازی کنید، درخواست های تکراری وب ایجاد کنید و آنها را تغییر بدهید، داده های تصادفی برنامه را تجزیه و تحلیل کنید، داده ها را در قالب های مختلف رمزگزاری و رمزگشایی کنید، و نقش سایت را به منظور شناسایی باگ های احراز هویت مورد بررسی قرار بدهید.

خب، Burp Suite چیست؟!

برنامه Burp Suite یک چهارچوب مجتمع و ساده برای ارزیابی برنامه های کاربردی تحت وب است. برنامه Burp Suite شامل چندین ابزار می باشد که به صورت یکپارچه با هم در تعامل هستند و به شما اجازه می دهند تمامی مولفه ها و جنبه های یک برنامه کاربردی تحت وب مدرن را مورد بررسی و تجزیه و تحلیل قرار بدهید. برنامه Burp Suite مانند یک چاقوی همه کاره سوئیسی(Swis army Knife) برای تحلیلگران امنیتی برنامه های تخت وب است.

این برنامه نه تنها به شما اجازه می دهد برنامه های تحت وب را به صورت عمیق مورد تحلیل و تجزیه قرار بدهید، بلکه حتی به شما اجازه می دهد روش های جمع آوری اطلاعات خودکار و تجزیه تحلیل منابع از برنامه تحت وب هدفتان را مورد استفاده قرار بدهید. همچنین شایان ذکر است، برنامه Burp Suite توسط شرکت PortSwigger Ltd طراحی شده و در دو نسخه رایگان و حرفه ای انتشار داده شده است.

گرچه نسخه حرفه ای این برنامه شامل پویشگر خودکار برنامه های تحت وب و چندین ویژگی دیگر می شود، اما نسخه رایگان آن هم برای شروع کار بسیار مناسب و کامل می باشد و در آن شما می توانید ابزار های ابتدایی برای کارتان را پیدا کنید. با این حال اگر می خواهید در مورد تفاوت های بین این دو نسخه اطلاعات بیشتری به دست آورید، می توانید به لینک http://www.portswigger.net رجوع کنید.

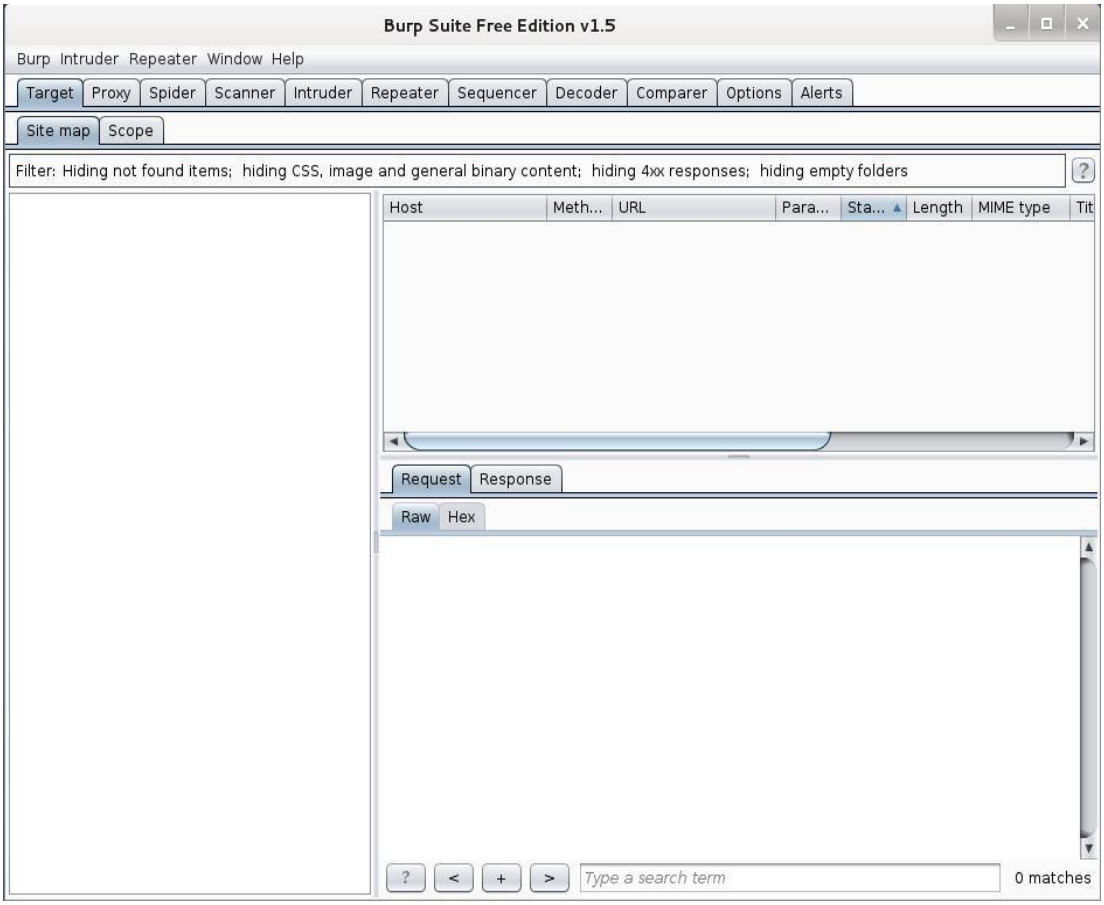
برنامه Burp Suite اگر بگوئیم ذاتا یک پراکسی وب محلی است، اشتباه نکرده ایم. این برنامه اجازه می دهد درخواست ها و پاسخگویی های Http و Https میان مرورگر کاربر و سرور وب سایت قربانی را مورد جلوگیری[1]، بازرسی[2] و اصلاح[3] قرار بدهید، که در ادامه نحوه انجام این کار را توزیح خواهم داد.

هنگامی که کاربر برنامه کاربردی تحت وبی را بررسی می کند، برنامه Burp Suite جزئیات موجود در تمامی صفحات مشاهده شده، اسکریپت ها، پارامتر ها و دیگر مولفه های برنامه وب هدفتان را جمع آوری خواهد کرد. همچنین ترافیک میان مرورگر کاربر و سرور می تواند، مورد تغییر قرار گیرد و حتی به صورت مصور در آید و چندین بار تکرار شود. ابزار های موجود در Burp Suite می توانند به راحتی با نوار ابزار بالای آن مورد تمییز قرار گیرند. شرح این ابزار ها در ادامه به صورت خلاصه آمده است.

[1] Intercept
[2] Inspect
[3] Modify

1. **Target :** این ابزار به شما اجازه می دهد تمامی منابع برنامه کاربردی تحت وب هدفتان را جمع آوری کنید که در نتیجه شخص کاربر یا متخصص می تواند از آن برای ارزیابی امنیت برنامه های تحت وب استفاده کند.
2. **Proxy :** به جرات می توان گفت این ابزار، مولفه اصلی برنامه Burp Suite است، چونکه اجازه می دهد تمامی ترافیک رد و بدل شده Http مرورگر و سرور را مورد اصلاح کردن و بازرسی قرار بدهید.
3. **Spider :** ابزار Spider را می توان یک خزنده خودکار نام برد. زیرا این ابزار می تواند برای پیدا کردن صفحات و پارامتر های جدید مورد استفاده قرار گیرد. قابل ذکر است همانند این ابزار، برنامه های زیادی وجود دارد که به صورت جداگانه ارائه می شوند.
4. **Scanner :** ابزار Scanner موجود در Burp Suite یک پویشگر امنیتی برنامه های تحت وب است که فقط در نسخه حرفه ای آن موجود می باشد.
5. **Intruder :** ابزار Intruder به شما اجازه می دهد درخواست های وب را خودکار و سفارسی سازی کنید. شایان ذکر است، تکرار کردن چندین بار درخواست های مشابه با محتوای متفاوت به شما اجازه می دهد عملیاتFuzzing را انجام بدهید. فازینگ برنامه های تحت وب معمولا شامل ارسال کردن ورودی های غیر منتظره به برنامه تحت وب می شود. این فرآیند می تواند به شما در پیدا کردن ضعف های امنیتی تحت وب کمک به سزایی کند، که اکثر متخصصین امنیت از آن بهره گیری می کنند.
6. **Repeater :** ابزار Repeater یک ابزار قدرتمند است که برای تغییر دادن یا اصلاح کردن درخواست های Http تحت وب مورد استفاده قرار می گیرد.
7. **Sequencer :** ابزار Sequencer موجود در برنامه Burp Suite یک ابزار عالی برای شناسایی و پیش بینی کردن توکن های امنیتی، کوکی ها و .... تکراری است.
8. **Decoder :** همانطور که از اسم این ابزار بر می آید، ابزار Decoder یا رمزگشا به شما اجازه می دهد داده های رمزنگاری شده توسط URLencode یا توابع هش کننده رایج مانند MD5 را رمزنگاری و رمزگشایی کنید.
9. **Comparer :** ابزار Comparer یک ابزار است که می تواند برای شناسایی و مقایسه کردن تغییرات صفحات وب مورد استفاده قرار گیرد.

تصویر آورده شده در زیر نمایش دهنده پنجره اصلی برنامه Burp Suite است.



نصب کردن Burp Suite

شما با چندین گام می توانید به راحتی این برنامه را بر روی سیستم های خود، خواه لینوکس باشد یا ویندوز نصب و راه اندازی کنید. الیته این ابزار به صورت پیش فرض بر روی Kali وجود دارد و می توانید از آن استفاده کنید.

گام اول؛ نیاز های سخت افزاری؟

قبل از شروع به نصب کردن برنامه Burp Suite؛ شما نیاز به بررسی کردن نیاز های سخت افزاری این برنامه دارید، گرچه ذکر کردن این نکته مضحک می باشد چونکه سیستم های امروزی آنقدر منابع سخت افزاری آنها بالاست که در خیلی از مواقع چنین مواردی اصلا مورد بحث و توجه قرار نمی گیرد. با این حال، منابع سخت افزاری مورد نیاز ابن برنامه در زیر لیست شده است.

1. **فضای دیسک:** برنامه Burp Suite حداقل 100 مگابایت فضا آزاد نیاز دارد. این برنامه از این فضا برای فایل های موقت خود، ذخیره سازی پیکربندی ها و... استفاده می کند.
2. **حافظه :** برنامه Burp Suite حداقل 2 گیگابایت حافظه رم نیاز دارد. این مقدار حافظه معمولا برای ارائه نهایت کارایی برنامه کافیست. اما اگر شما بخواهید یک برنامه بزرگ را مورد بررسی قرار بدهید نیاز به حافظه بیشتری دارید.
3. **سیستم عامل:** خوشبختانه برنامه Burp Suite را می توانید بر روی ویندوز، Mac OS X و لینوکس نصب و اجرا کنید.
4. **اجزاء های برنامه :** شایان ذکر است، برای اجرا شدن Burp Suite به نسخه جدید Java Runtime Environment و OpenJDK نیاز دارید. همچنین اطمینان حاصل کنید که آخرین نسخه مرورگر ها را نصب کرده اید. بنده پیشنهاد می کنم از Firefox استفاده کنید.

گام دوم؛ دانلود Burp Suite

نسخه رایگان برنامه Burp Suite را می توانید از وب سایت سازندگان آن http://www.portswigger.net/burp/download.html دانلود کنید. همچنین بنده پیشنهاد می کنم ابتدا نسخه رایگان آن را دانلود کرده و ویژگی های ساده و رایگان آن را مورد استفاده قرار بدهید، پس از اینکه متوجه شدید این برنامه می تواند برای شما مفید واقع شود، اقدام به خریدارینسخه حرفه ای آن کنید. پس از دانلود برنامه یک فایل با قالب Jar در پوشه دانلود مشاهده خواهید کرد که فایل اجرایی و اصلی برنامه Burp Suite است.

گام سوم؛ اجرا کردن Burp Suite

آخرین نسخه برنامه Burp که در لحظه نوشتن این کتاب در دسترس است burpsuite_v1.5.jar نام دارد. این برنامه یک فایل اجرایی جاوا است که می توانید آن را در سیستم عامل ویندوز به صورت زیر اجرا کنید.

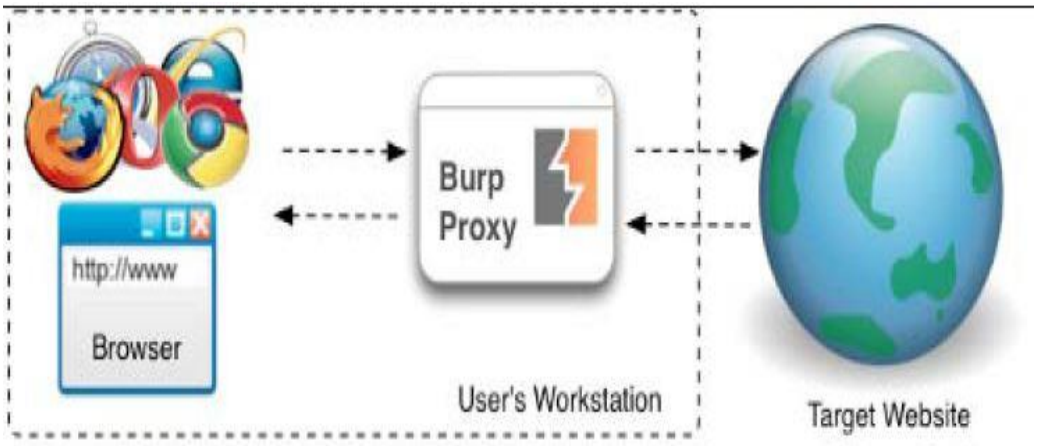
1. از منوی Start بر روی Run کلیک کنید و سپس cmd را وارد کرده و enter را بفشارید.
2. سپس به پوشه دانلود برنامه burpsuit بروید و با استفاده از فرمان آورده شده در زیر آن را اجرا کنید.

```
java -Xmx2g -jar burpsuite_v1.4.01.jar
```

ما در فرمان بالا از گزینه xmx2g- برای افزایش حداکثر حافظه اختصاص داده شده به جاوا، به 2 گیگابایت استفاده کرده ایم. با این حال، به این نکته توجه کنید، در برخی از چهارچوب ها(به عنوان مثال، ویندوز)، برنامه Burp Suite می تواند به سادگی با فشردن دو بار کلیک اجرا شود. اما، اجرا کردن برنامه Burp با این روش به شما اجازه نمی دهد حداکثر حافظه موجود برای این ابزار را سفارشی سازی کنید. با این حال، پس از اجرای دستور بالا، بعد از چند ثانیه، پنجره اصلی Burp در وسط صفحه مانیتور نمایش داده خواهد شد، اما اگر نمایش داده نشد و یا با خطایی رو به رو شدید، مقدار حافظه مشخص شده توسط گزینه را کاهش دهید یا با دو بار کلیک آن را اجرا کنید.

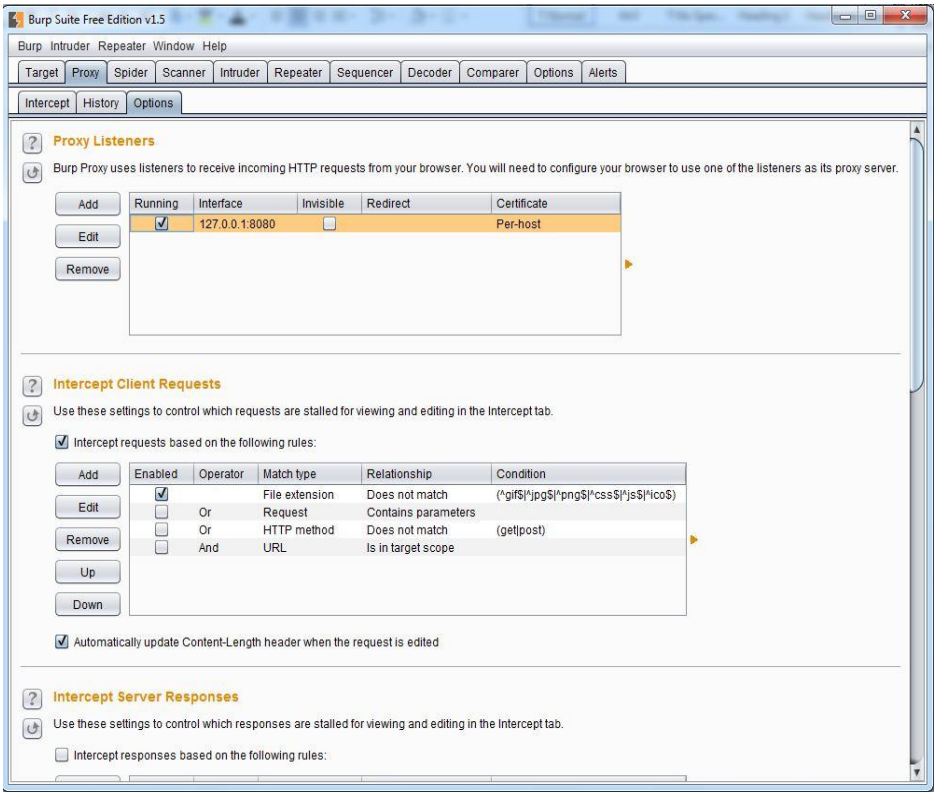
گام چهارم؛ پیکربندی پراکسی Burp

پراکسی Burp یا همان Burp Proxy برای درخواست ها ارسالی از طرف مرورگر به برنامه تحت وب به عنوان یک میانجی عمل می کند. اما به این نکته توجه داشته باشید، تا زمانیکه مروگر خود را به این برنامه متصل نسازید؛ پس از اجرای Burp Suite شما نمی توانید تحلیل برنامه های تحت وب را شروع کنید. پس در گام اول باید پراکسی Burp را در مرورگر تنظیم کنیم.



چگونگی تعامل پروکسی Burp با مرورگر و وب سایت هدف

در حالت پیش فرض، پراکسی Burp پیکربندی شده است تا بر روی درگاه Tcp با شماره 8080 در حالت شنود قرار گیرد. همچنین برای اطمینان حاصل کردن از اینکه هیچ برنامه ای بر روی سیستم با برنامه Burp Suite تداخل پیدا نکند، بهتر است از همان درگاه TCP پیش فرض استفاده کنید. همچنین شما می توانید شنونده پراکسی Burp را از قسمت Proxy و سپس Options مورد بررسی قرار بدهید. اگر تیک checkbox گزینه running را بزنید، پراکسی Burp آماده دریافت درخواست ها از مرورگر می شود. در صورت بروز خطا به استثناء های موجود در قسمت alerts توجه کنید. در بیشتر حالات، پراکسی نیاز دارد درگاه را تعویض کرده و شنونده را راه اندازی مجدد کنید.



پیکربندی پراکسی Burp

پیکربندی پراکسی می توانید با انتخاب آن و کلیک کردن بر روی گزینه Edit مورد ویرایش قرار گیرد. به عنوان مثال، شما می توانید درگاه مورد شنود پراکسی Burp را با تایپ کردن درگاه جدید در قسمت Bind to port و سپس کلیک کردن بر روی Ok آن درگاه پیش فرض را تغییر بدهید. در پایان، اگر از قبل شنونده انتخاب نشده بود، می توانید بر روی checkbox گزینه running را مجددا برای شروع شنونده تیک بزنید.

شایان ذکر است؛ در برخی موقعیت های خاص، به عنوان مثال هنگامی که یک برنامه کاربردی موبایل یا کلاینت های مستقل را با ارتباط برقرار کردن از طریق Http و یا Https بررسی می کنید، ممکن است نیاز داشته باشید تیک checkbox گزینه support invisible proxying for non-proxy-aware clients را بزنید و به صورت دستی آدرس میزبان قربانی و درگاه آنها را در فیلد های مناسب وارد کنید. در این روش، برنامه Burp از تمامی درخواست های بدون پراکسی مراقبت خواهد کرد و به شما اجازه خواهد داد تمامی ترافیک را به میزبان قربانی تغییر مسیر بدهید.

گام پنجم؛ پیکربندی مرورگر

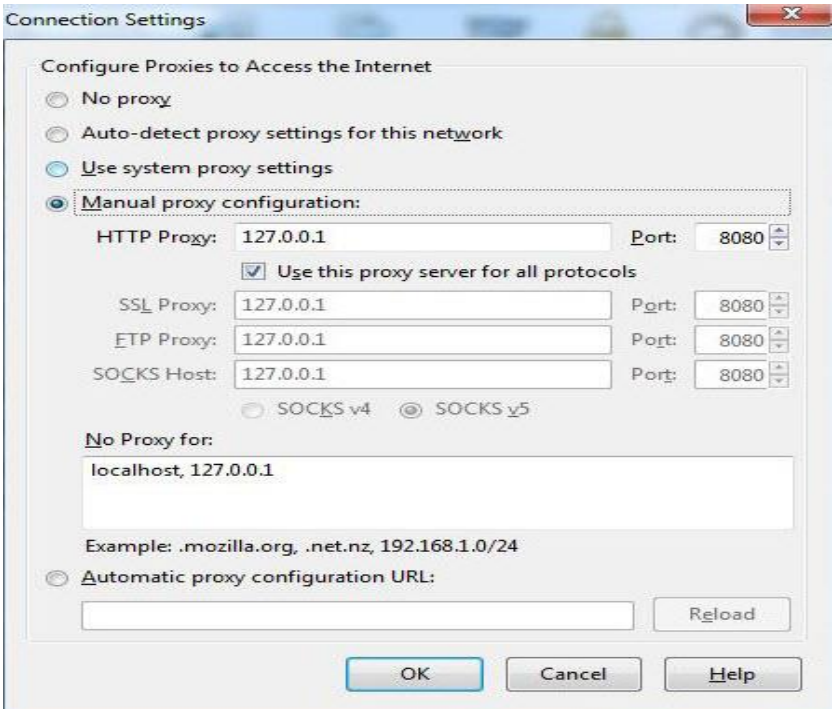
در این لحظه، شما فقط نیاز دارید مرورگر مورد استفاده خودتان را به منظور منتقل کردن ترافیک درخواست های Http/s آن به پراکسی Burp بجای وب سایت قربانی تنظیم و پیکربندی کنید. اگر شما در مرحله قبل پیکربندی پیش فرض Burp

را تغییر نداده اید، در این قسمت نیاز خواهید داشت آدرس میزبان پراکسی را با آدرس 127.0.0.1 و درگاه پراکسی را با 8080 برای Http و Https در مرورگر تنظیم کنید.

به هر حال، پیکربندی گام به گام در این قسمت برای دو مرورگر رایج یعنی Mozilla Firefox و Internet Explorer ارائه شده است. برای دیگر مرورگر ها از قبیل Safari، Chrome و Opera لطفا به مستندات وب سایت سازنده این برنامه رجوع کنید. من پیشنهاد می کنم شما از Mozila Firefox استفاده کنید، چونکه این مرورگر بسیار تطبیق پذیر است. همچنین، در زمان نوشتن این کتاب، مرورگر Mozila Firefox شامل هیچ فیلتر Anti-Cross-Site Scripting (XSS) شامل نشده است. اینگونه فیلتر ها ممکن است در بررسی و ارزیابی های شما تداخل ایجاد کنند.

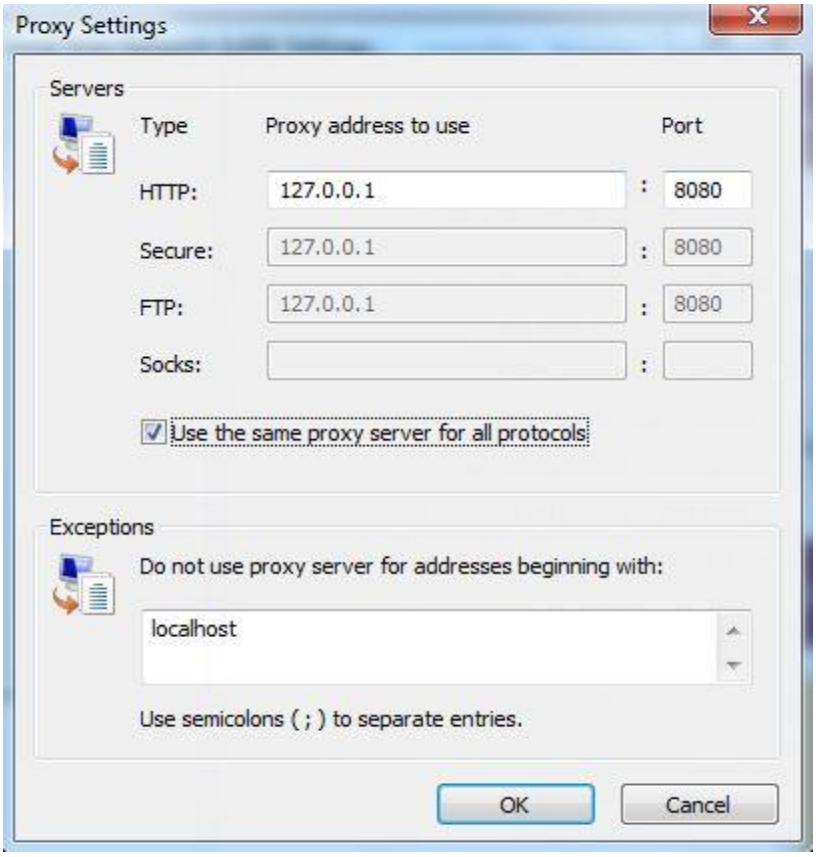
مرورگر Mozila Firefox

1. از منوی Tools مرورگر فایرفاکس بر روی Options کلیک کنید.
2. سپس در پنجره جدیدی که باز شد به منوی Advanced بروید و در تب Network بر روی Settings کلیک کنید.
3. گزینه Manual proxy configuration را انتخاب کنید.
4. سپس در پنجره پیکربندی پراکسی آدرس میزبان پراکسی (127.0.0.1) و سپس درگاه پراکسی (8080) را وارد کنید.
5. تیک گزینه Use this proxy server for all protocols را بزنید.
6. سپس بر روی Ok کلیک کنید و تمامی پنجره ها را ببندید.



مرورگر Internet Explorer

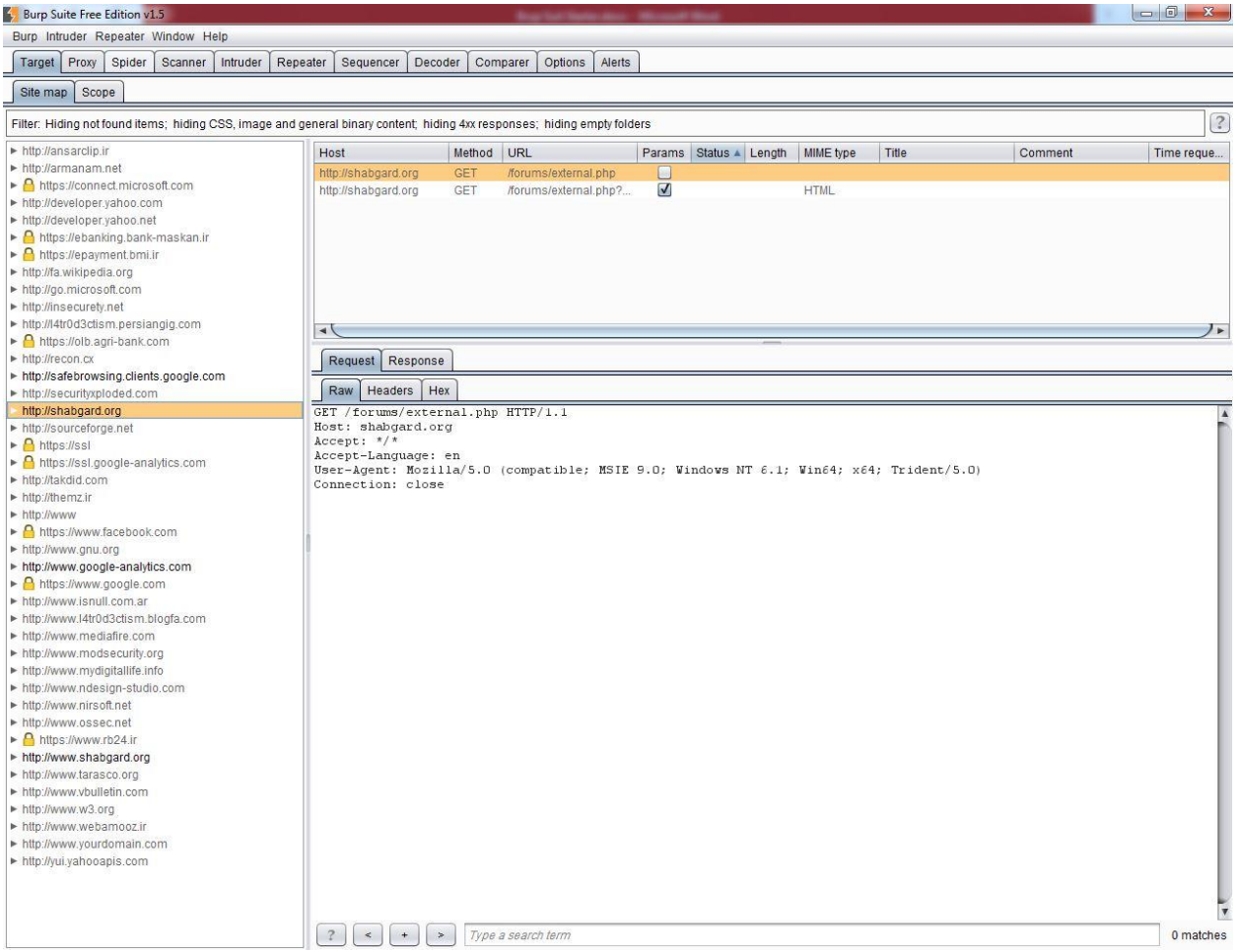
1. از منوی Tools بر روی گزینه Internet options کلیک کنید.
2. از منوی Connections بر روی LAN Settings کلیک کنید.
3. گزینه Use a proxy for your LAN را انتخاب کنید.
4. بر روی Advanced کلیک کنید.
5. در فیلد Http آدرس پراکسی میزبان را وارد کنید (به عنوان مثال 127.0.0.1) و در قسمت Port درگاه پراکسی را وارد کنید (به عنوان مثال 8080)
6. سپس گزینه Use the same proxy server for all protocols را انتخاب کنید.
7. و در نهایت بر روی OK کلیک کنید.



مجزا از اینکه از کدام مرورگر استفاده می کنید، تمامی افزونه ها و ویژگی های اضافی که در مرورگر وجود دارند و ممکن است با Brup Suite تداخل پیدا کنند را غیر فعال کنید. از جمله add-ons پراکسی ها و افزونه های امنیتی مانند Anti-XSS filters, NoScript و غیره.

مرور کلی

در این لحظه، اگر به درستی تمامی تنظیمات را اعمال کرده باشید Burp می تواند با موفقیت درخواست های ارسالی Http/s را متوقف سازد. برای بررسی این موضوع، بگذارید به مرورگر رفته و به عنوان مثال آدرس http://www.shabgard.org را در قسمت Address bar مرورگر وارد کرده و بر روی enter بفشارید. اگر همه چیز به درستی پیکربندی شده باشد، پراکسی Burp باید تمامی درخواست های مرورگر را متوقف کند. سپس در برنامه Burp Suite به منوی proxy و سپس به قسمت intercept بروید و درخواست های وب که منتظر تائید شما هستند را بررسی کنید. در قسمت بالا دکمه intercept on برجسته شده است؛ بر روی آن کلیک کنید و اجازه دهید درخواست ها از طریق پراکسی Burp منتقل شوند. در نهایت به مرورگر برگردید، شما باید پس از بازگشت به مرورگر باید صفحه وب سایت shabgard.org را مشاهده کنید. همچنین، شما می توانید از قسمت Target و سپس Site Map ساختار درختی منابع وب سایت هدف را مشاهده کنید. شایان ذکر است، در این قسمت shabgard.org مثال بود، شما می توانید هر سایتی را که می خواهید را در مروگر وارد کنید.



نکته، نویسنده میلاد کهساری الهادی : همانطور که می دانید، Burp Suite از پروتکل های Http و Https پشتیبانی می کند. در گذشته برای برقراری ارتباط ایمن میان مرورگر کلاینت و سرور از پروتکل های بسیاری استفاده می شد. اما امروزه Httpsیک پروتکل استاندارد برای محافظت کردن از فروشگاه های آنلاین، بانک های آنلاین و ... به شمار می رود. با استفاده از این پروتکل شما می توانید بسته های Http را در لایه SSL/TLS رمزنگاری کنید. پروتکل Https باعث می شود حمل و نقل اطلاعات به صورت ایمن صورت گیرد و در برابر حملاتی مانند(Man-in-the-Middle (MitM از اطلاعات محافظت شود.

با این حال، از آنجایی که برنامه Burp Suite در این آزمایش به درخواست های کلاینت و پاسخ های سرور شنود می کنند، می توانیم بگوئیم ما دقیقا Burp Suite را مانند یک مرد در میان یا همان حمله Man-in-the-Middle (MitM) پیکربندی کرده ایم. از همین روی، به عنوان یک اثر جانبی از پیکربندی Burp Suite مانند MitM، هنگامی که یک وب سایت را از طریق پروتکل Https مشاهده کنید (به عنوان مثال، https://facebook.com) متوجه خواهید شد که مرورگر یک اخطار امنیتی نمایش می دهد. به عنوان مثال، در فایرفاکس، شما صفحه This Connection is Untrusted را مشاهده خواهید کرد. در این مواقع، شما نیاز دارید به صورت دستی اتصال به وب سایت را با کلیک کردن بر روی Understand The Risks و سپس Add Exceptions و در پایان Confirm Security Exception تائید کنید تا بتوانید از فرآیند را ادامه بدهید.

یک شروع سریع؛ استفاده کردن از Burp Proxy

پراکسی Burp یک مولفه بسیار کاربردی از برنامه Burp Suite به شمار می رود. این ابزار به شما اجازه می دهد ترافیک وب میان مرورگر کلاینت و سرور برنامه تحت وب قربانی خود را متوقف کنید. حال در این قسمت ما با استفاده از این گزینه می توانیم کشف کنیم، چگونه برنامه های کاربردی تحت وب عمل می کنند و در پشت پرده آنها چه اتفاق هایی می افتد. در بالا Burp Proxy سه تب مستند شده در زیر را مشاهده می کنید.

1. **Intercept :** در این پنجره درخواست ها و پاسخگویی های Http می توانند متوقف گردند و مورد اصلاح قرار گیرند.
2. **Options :** در این پنجره می توانید پیکربندی پراکسی و تنظیمات پیشرفته را اعمال کنید.
3. **History :** تمامی ترافیک متوقف شده می توانند در این پنجره به سرعت مورد تحلیل قرار گیرند.

گام اول؛ متوقف ساختن درخواست های وب

پس از اجرا و پیکربندی کردن Burp و مرورگر، بگذارید اولین درخواست Http خودمان را متوقف سازیم. در طی این تمرین، ما یک درخواست ساده به وب سایت shabgard.org را متوقف خواهیم ساخت.

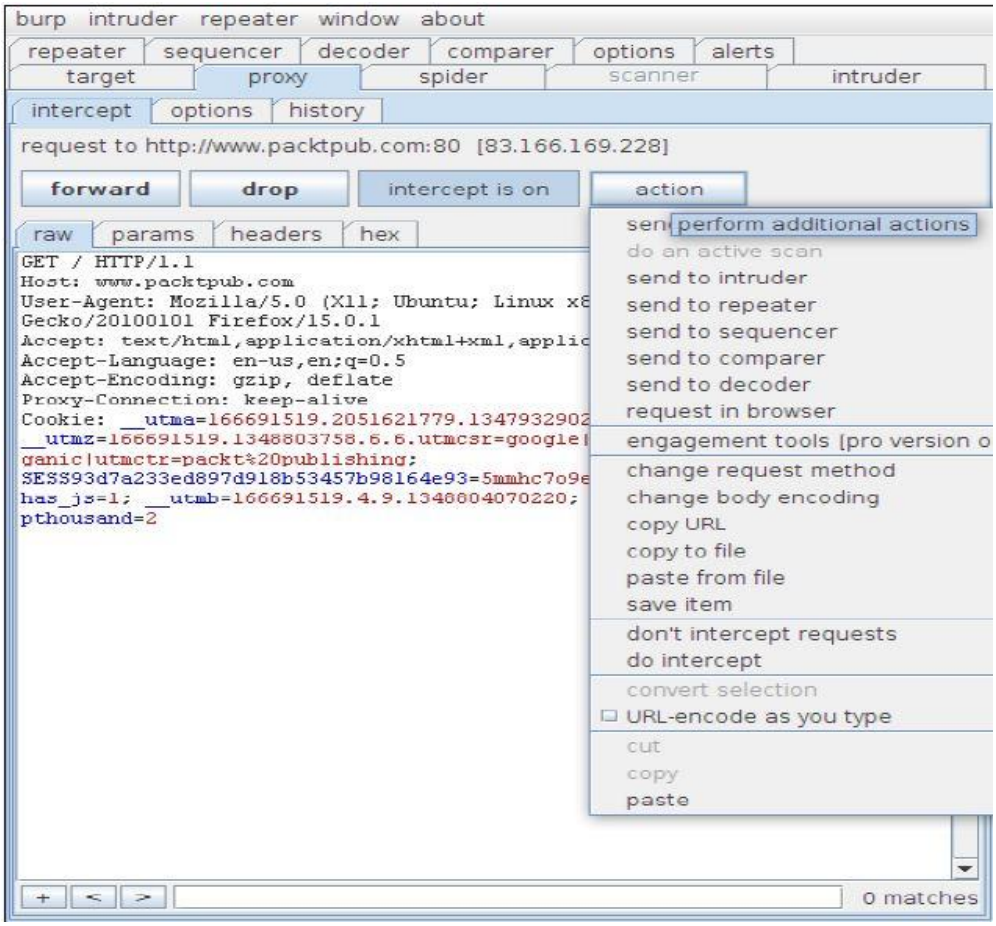
نکته، نویسنده، میلاد کسهاری الهادی : هنگامی که بنده از واژه **"متوقف ساختن[1] یک درخواست"** استفاده می کنم، منظورم این هست که از ارسال شدن یک بسته Http به سرور جلوگیری می کنم. شاید این مسئله کمی گنگ به نظر برسد. لذا بگذارید این مسئله را از دید دیگری نمایان سازم.

در حالت کلی اینترنت بر مبنای ارسال و دریافت بسته های اطلاعاتی کار می کند و تمامی پروتکل هایی که در لایه های TCP و OSI تعریف شده اند، وظیفه اشان این است که بسته های اطلاعاتی را به درستی و با دقت و سرعت به مقصد منتقل کنند. شایان ذکر است، شما در وب سایت های اینترنتی هم با همچین سناریوی رو به رو هستید. به عنوان مثال برای اینکه بتوانید وب سایت مدنظرتان را مشاهده کنید، ابتدا باید برای سرور آن یک درخواست از طریق پروتکل Http ارسال کنید، پس از اینکه شما درخواستتان را ارسال کردید، سرور آن درخواست را تحلیل کرده و به آن پاسخگویی می کند. این درخواست و پاسخ ها در قالب یک سری بسته های اطلاعاتی صورت می گیرد که اگر بتوانید آن بسته ها را دریافت کنید، به راحتی خودتان می توانید متوجه شوید که کلاینت به سرور چه چیزی را ارسال کرده است. لذا در این برنامه، برای اینکه بتوانیم درخواست های ارسالی مرورگر را مشاهده و تحلیل کنیم، لاجرم مجبور هستیم آن ها را از طریق پراکسی دریافت و متوقف کنیم. در این برنامه برای انجام این کار از intercept استفاده می شود که متوقف کننده درخواست های Http/s است.

[1] intercept

1. در تب intercept، با بررسی کردن دکمه intercept اطمینان حاصل کنید که پراکسی Burp تمامی درخواست ها Http را متوقف می کند. بدین منظور دکمه intercept باید با intercept is on مقداردهی شده باشد.
2. سپس در مرورگر، آدرس وب سایت هدف (به عنوان مثال shabgard.org) را تایپ کنید و Enter را بفشارید.
3. در گام بعد به پراکسی Burp بازگرید، در این لحظه شما باید بتوانید درخواست های Http ایجاد شده توسط مرورگر را مشاهده کنید. در این قسمت، در Burp درخواست ها موقتا متوقف خواهد شد و منتظر عملکرد کاربر خواهند ماند که آیا آنان را کاملا متوقف یا Forward کنند. به عنوان مثال اگر دکمه Forward را بفشارید و به مرورگر بازگردید مشاهده خواهید کرد که صفحه اصلی وب سایت Shabgard.org بارگزاری شده است. چون وقتی بر روی Forward کلیک می کنید، باعث می شوید درخواست Http به سرور برنامه تحت وب ارسال شود.
4. دوباره، آدرس shabgard.org را وارد کنید و Enter را بفشارید.
5. این بار بجای Forward بر روی Drop کلیک کنید.
6. حالا اگر به مرورگر خود باز گردید در صفحه پیام Burp proxy error: message was dropped by user را مشاهده خواهید کرد. در این قسمت ما درخواست Http ارسالی توسط مرورگر را drop کردیم، در نتیجه با این کار پراکسی Burp درخواست Http را به سرور سایت ارسال نخواهد کرد و یک صفحه Html موقت با پیام خطا تولید شده توسط خود را بجای صفحه اصلی وب سایت ارائه می کند.

همچنین شما می توانید از امکانات دیگری که در این برنامه یکپارچه به منظور دستکاری و تجزیه و تحلیل درخواست های وب وجود دارند به سادگی استفاده کنید. به عنوان مثال، اگر شما بخواهید یک درخواست رمز شده را رمزگشایی کنید، می توانید به راحتی با کلیک کردن بر روی آن و انتخاب گزینه send to decoder آن را رمزگشایی کنید.



شایان ذکر است در پراکسی Burp، ما می توانیم تصمیم بگیریم تمامی درخواست های Http را بدون اینکه منتظر اعمال دستور توسط کاربر بماند، به صورت خودکار Forward کند. بدین منظور شما می توانید با کلیک کردن بر روی دکمه intercept به راحتی بین حالت های فعال ساختن حالت متوقف سازی بسته ها (intercept is on) و حالت متوقف نساختن بسته ها (intercept is off) سویتچ کنید. با این وجود، پراکسی تمامی درخواست های ارسال شده را ظبط خواهد کرد. همچنین، پراکسی Burp به شما اجازه می دهد به صورت خودکار تمامی پاسخگویی هایی که با ویژگی های خاصی مطابقت دارند را متوقف سازید.

به چندین گزینه ای که در قسمت intercept server response وجود دارد از تب options پراکسی Burp نگاهی بیندازید. به عنوان مثال، شما می توانید پاسخ سرور را متوقف سازید، تنها اگر درخواست کلاینت متوقف شده باشد. این موضوع هنگامی که می خواهیم آسیب پذیری اعتبار سنجی ورودی[1] را بررسی کنیم بسیار مفید می باشد، چونکه در این حمله ما

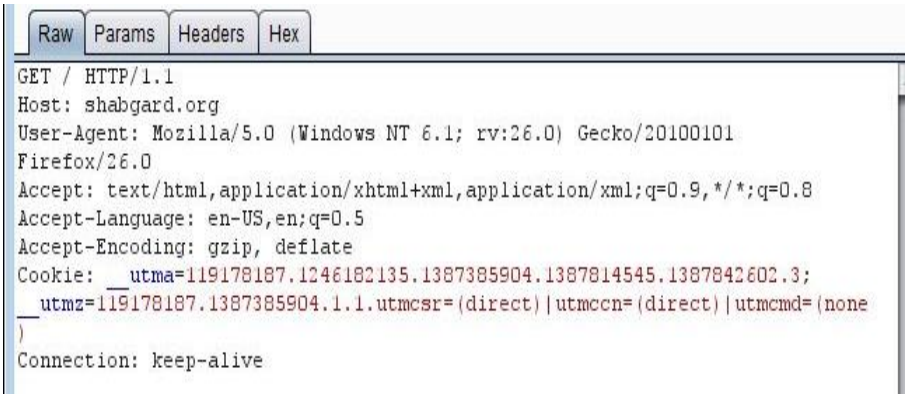
[1] Input Validation Vulnerabilities

عموما علاقمند هستیم پاسخ سرور برای تمامی درخواست های پنهانی را ارزیابی کنیم. یا شاید شما فقط بخواهید پاسخ هایی را متوقف ساخته و بررسی کنید که کد خاصی را باز می گرداند.

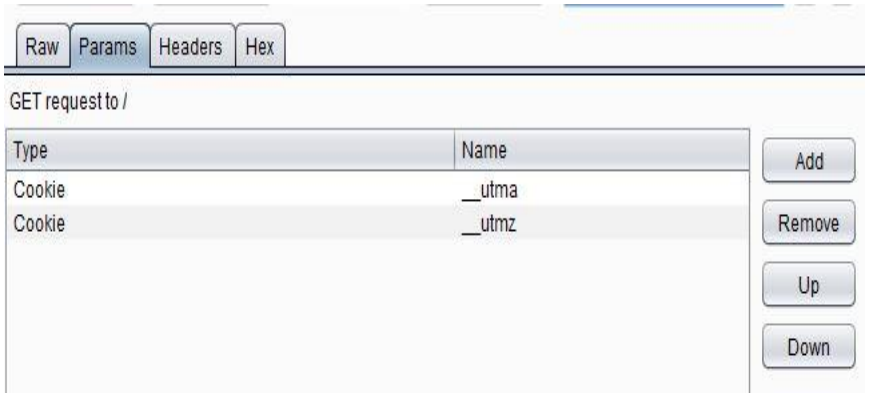
گام دوم؛ متوقف ساختن درخواست های وب

هنگامی که یک درخواست Http به خوبی متوقف شد، شما می توانید کل محتویات، هدر ها و پارامتر های آن درخواست را با یکی از چهار تب موجود در پراکسی Burp تحلیل کنید. این چهار تب در زیر مستند شده اند.

1. **Raw :** این پنجره به شما اجازه می دهد درخواست های وب را در قالب اولیه و خام که به صورت کد است درون یک ویرایشگر متن ساده مشاهده کنید. ارائه این اطلاعات در همچین قالبی بسیار مفید است و اجازه می دهد برای تحقیقات بیشتر محتویات آن را تغییر بدهید.

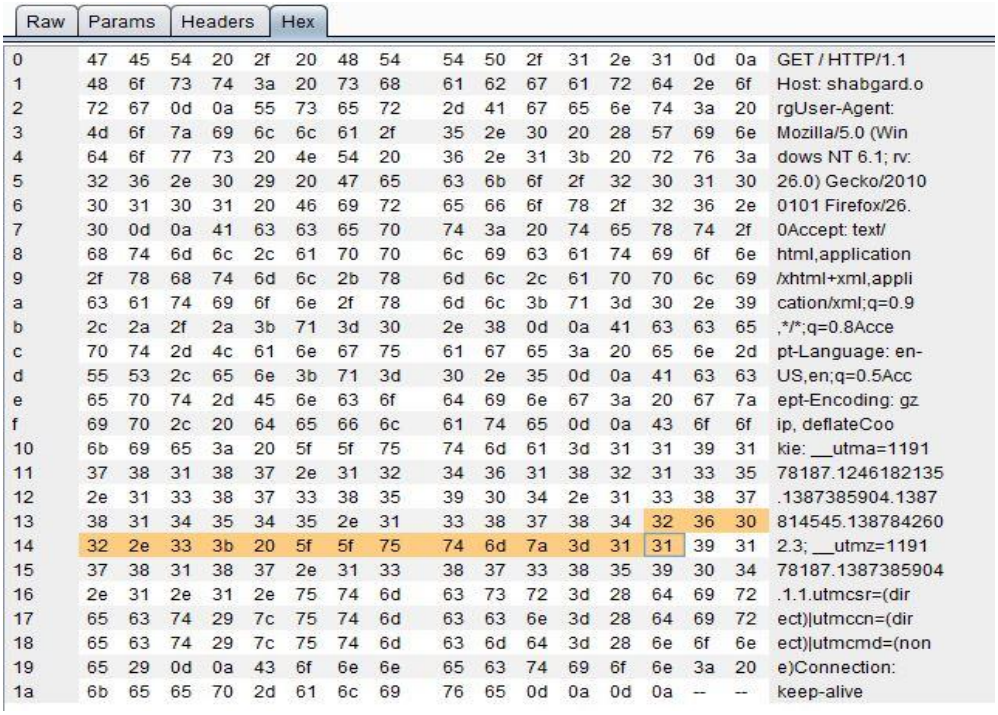


2. **Params :** این پنجره به شما اجازه می دهد، بر روی پارامتر های ارائه شده کاربر متمرکز شوید (پارامتر های GET/POST، کوکی ها) و آنها را در یک قالب جدول بندی شده مشاهده کنید. شایان ذکر است، این گزینه زمانی که درخواست های پیچیده اجازه می دهند نقاط ورودی به آسیب پذیری را در نظر بگیرید، بسیار مهم است. همچنین Burp Proxy به صورت خودکار URL را رمزگشایی خواهد کرد. علاوه بر این، Burp Proxy تلاش خواهد کرد قالب های استفاده شده رایج از قبیل JSON را هم تجزیه کند.



3. Headers : این پنجره نام سرآیند های Http و مقادیرشان را در یک جدول به صورت مرتب نمایش می دهد.

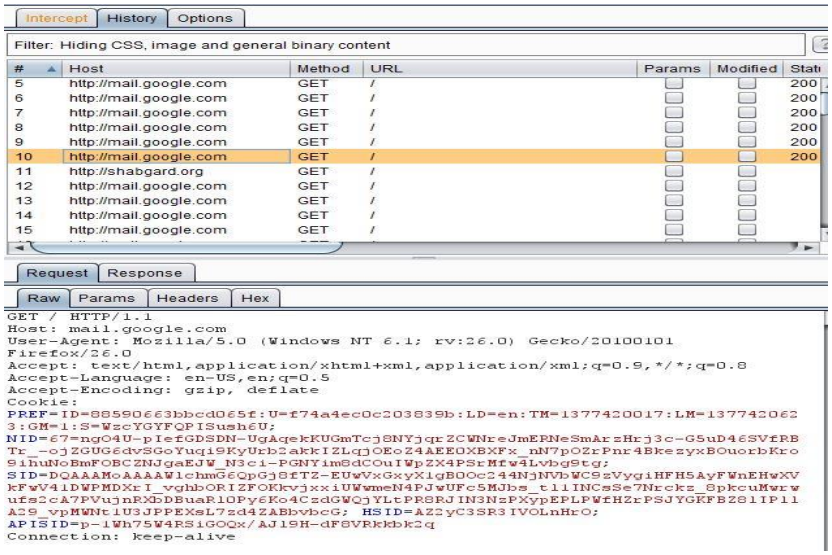
4. Hex : در این پنجره محتویات بسته های Http، به صورت هکسادسیمال نمایش داده می شود. این پنجره به شما اجازه می دهد درخواست های ارسال شده به سرور را در یک ویرایشگر ساده هکسادسیمال مشاهده و ویرایش کنید.



علاوه بر همه این ها، یک تب دیگر با نام history وجود دارد که به شما اجازه می دهد تمامی درخواست های ارسالی از طریق پراکسی تنظیم شده Burp را تجزیه و تحلیل کنید.

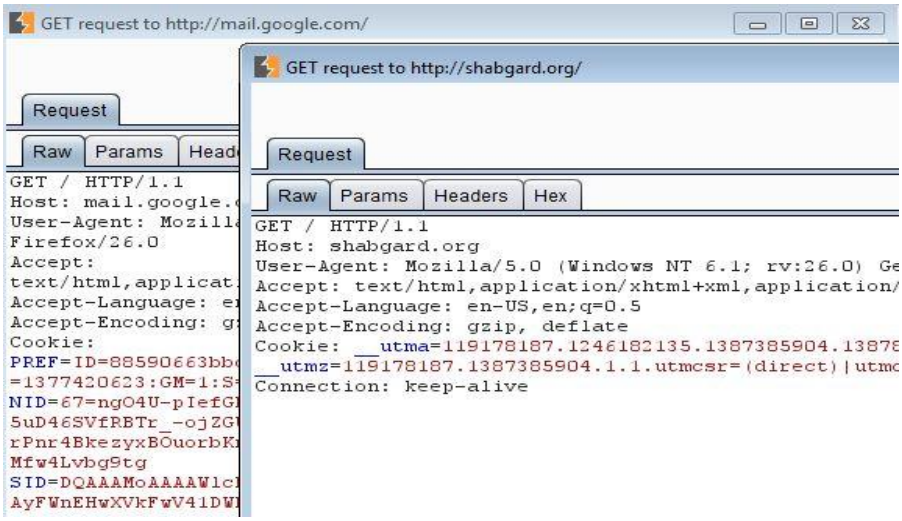
1. بر روی تب history کلیک کنید. پس از کلیک کردن بر روی این تب، در قسمت بالا پنجره Burp Proxy تمامی درخواست های ارسالی را به شما در یک قالب لیست شده نمایش می دهد، و در قسمت پایین Burp Suite محتویات آن درخواست و پاسخ را متناسب با انتخاب شما نمایش خواهد داد. همچنین، اگر شما در مراحل قبل درخواستی

را تغییر داده باشید، گزینه history موجود در burp proxy نسخه تغییر داده شده آن درخواست را نمایش خواهد داد.



نمایش درخواست و پاسخ های Http متوقف شده توسط Burp Proxy

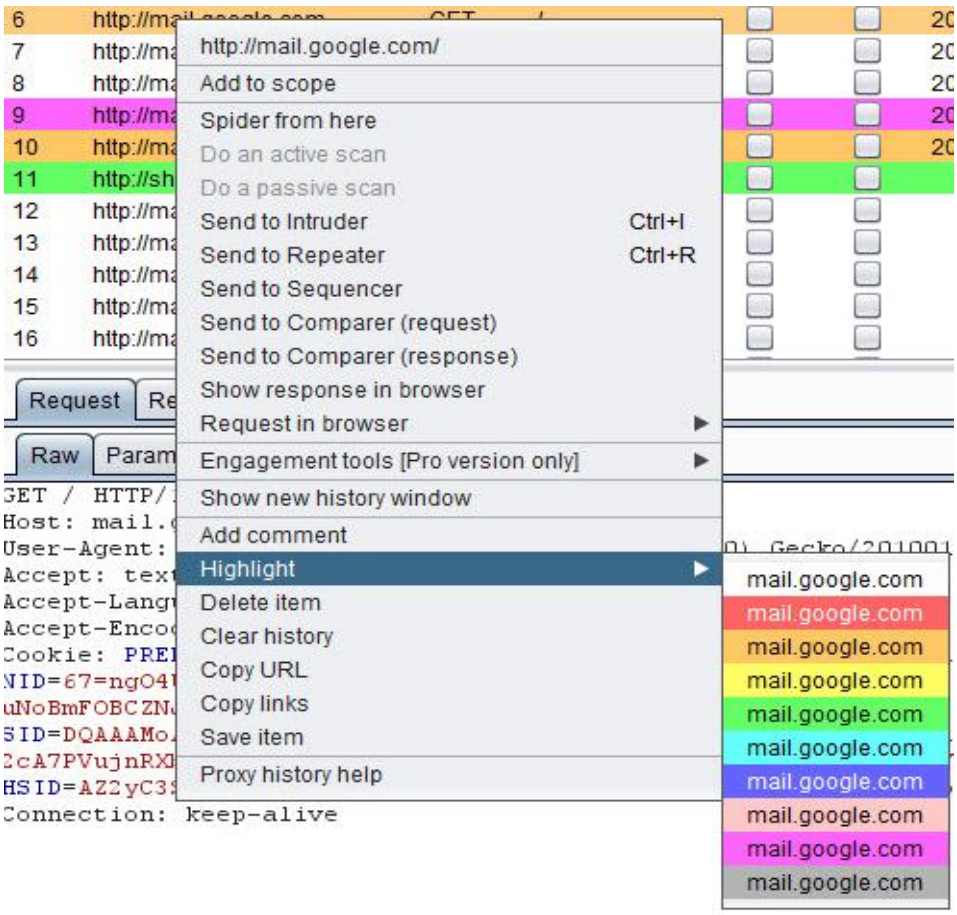
2. همچنین شما می توانید با دوبار کلیک کردن بر روی هر درخواست آن را در یک پنجره جدید باز کنید. با این ویژگی شما می توانید همزمان چندین درخواست را باز کرده و محتویات آن ها را با هم مقایسه کنید.



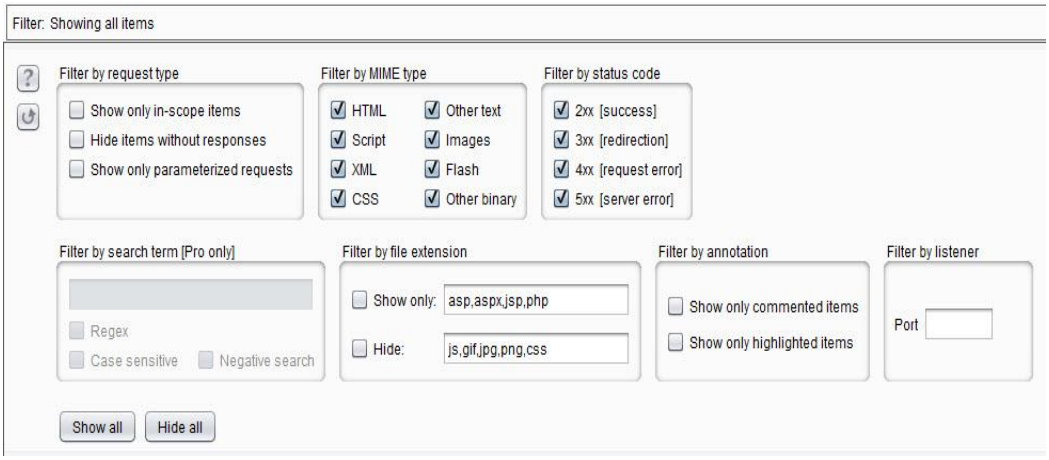
3. دوباره به تب history باز گردید. اگر به محتویات در این پنجره به دقت نگاه کنید، مشاهده خواهید کرد که این پنجره برای هر درخواست متوقف شده جزئیاتی از قبیل اندازه بسته(length)، url، روش درخواست(Method) و... ارائه کرده است. همچنین هر درخواست در سمت چپ با یک عدد شماره گذاری شده است.

#	Host	Method	URL	Params	Modified	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	Cookies	Time	Listener port
5	http://mail.google.com	GET	/			200	616	HTML					173.194.70.19		22:30:07 24...	8080

4. همچنین شما در این پنجره قادر هستید برخی از درخواست ها و یا پاسخ ها را با رنگ های مختلف نمایش دهید. این ویژگی به شما این امکان را می دهد برخی از درخواست ها یا پاسخ هایی که بسیار مهم هستند را از مابقی جدا بکنید. بدین منظور کافیه بر روی بسته مد نظرتان کلیک راست کرده و از منوی Highlight یک رنگ را برای آن مشخص سازید.



5. از قسمت بالا بر روی Filter کلیک کنید، پس از کلیک کردن بر روی نوار ابزار Filter یک پنجره در بالا نمایش داده خواهد شد. در این پنجره شما می توانید به راحتی بر روی بسته های متوقف شده اعمال فیلتر کنید. به عنوان مثال، اگر می خواهید تمامی درخواست های Http که دارای حداقل یک پارامتر هستند را مشاهده کنید، کافیست تیک گزینه show only parameterised را بزنید. پس از آن بر روی خارج از محیط فیلتر کلیک کنید تا فیلتر شما بر روی درخواست ها اعمال شود.

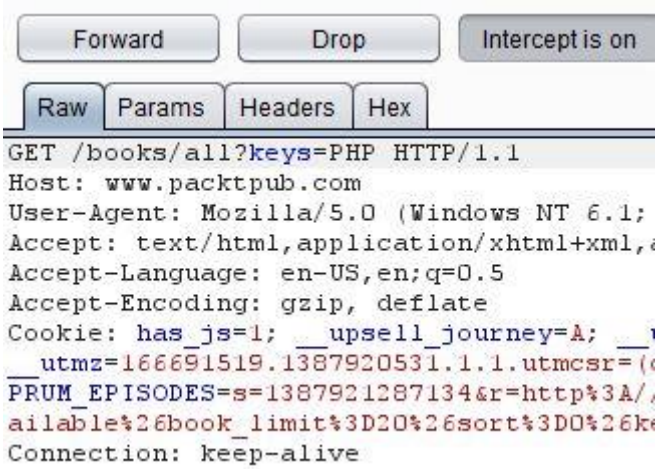


6. علاوه بر این، هنگامی که شما از Burp Suite نسخه Professional استفاده می کنید. قادر خواهید بود از گزینه filter by search term هم بهره مند شوید. این ویژگی به شما اجازه می دهد بر روی درخواست یا پاسخ ها با عبارت های رشته ای فیلتر گذاری کنید تا اگر بسته ای با آن رشته تطابق داشت در خروجی به شما نمایش داده شود. متاسفانه این گزینه در نسخه رایگان این برنامه وجود ندارد.

گام سوم؛ دستکاری درخواست های وب

دانستن این نکته بسیار مهم است، شما به عنوان قسمتی از ارزیابی امنیت برنامه های تحت وب، لاجرم نیاز دارید درخواست های Http را تغییر داده و پاسخگویی های وب سرور برنامه کاربردی تحت وب را تحلیل کنید. به عنوان مثال، برای شناسایی آسیب پذیری تزریق SQL یا همان حمله معروف SQL Injection، این موضوع بسیار مهم است که برخی از وکتورهای حمله (به عنوان مثال تک کوتیشن)در همه ورودی های ارائه شده کاربر از جمله سرآیند های Http، کوکی ها و پارامتر ها تزریق شود. با این حال دستکاری کردن درخواست های وب در Burp Suite بسیار ساده است. بدین منظور کافیست گام های زیر را دنبال کنید.

1. در اولین گام باید یک درخواست که حداقل یک پارامتر داشته باشد را متوقف کنید. به عنوان مثال شما می توانید به این آدرس http://www.packtpub.com/books/all?keys=ASP بروید.
2. سپس به Burp Proxy بازگردید و به تب Intercept بروید. در این قسمت، شما باید درخواست Http مناسب را مشاهده کنید.
3. از قسمت Raw شما می توانید هر کدام از جنبه های درخواست را که می خواهید ویرایش کنید. به عنوان مثال، شما می توانید مقدار پارامتر Keys که در Url آورده شده و با ASP مقداردهی گردیده است را در قسمت Raw آن را به PHP به شکل زیر تغییر بدهید. بدین منظور کافیست ویرایش پارامتر ها را به شکل زیر انجام بدهید.



4. سپس وقتی تغییرات خود را اعمال کردید بر روی دکمه Forward کلیک کنید و به مرورگر بازگردید. در صفحه باید مشاهده کنید که پارامتر Php بجای پارامتر Asp باید مورد استفاده قرار گرفته باشد. در حالت کلی ما در این قسمت مقدار پارامتر ارسالی را تعویض کردیم.

اگرچه ما از قسمت Raw برای عوض کردن درخواست Http قبلی استفاده کردیم، با این حال این ویژگی می تواند در هر کدام از قسمت های Burp Proxy اعمال شود. به عنوان مثال، در قسمت params، شما می توانید با استفاده از گام های زیر یک پارامتر جدید اضافه کنید.

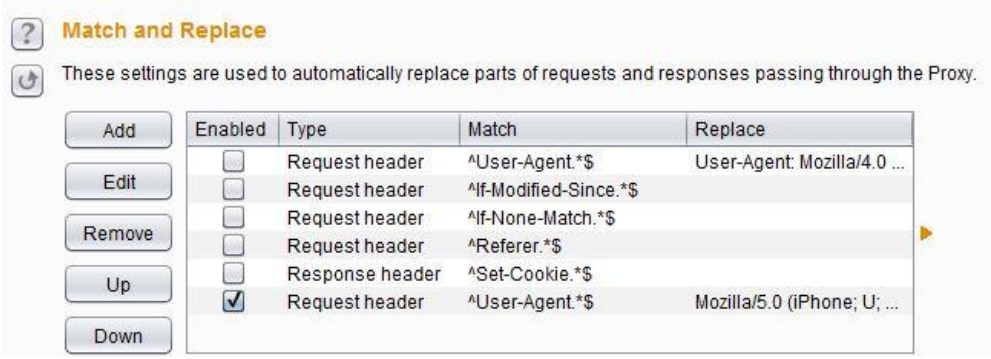
1. در پنجره Params از قسمت راست بر روی Add کلیک کنید.
2. در گام بعدی یک نوع پارامتر مناسب (URL، body یا cookie) را انتخاب کنید. در این قسمت از نوع URL برای پارامتر های GET و از نوع body برای پارامتر های POST استفاده می شود.
3. سپس نام و مقدار پارامتر جدیدی که می خواهید ایجاد کنید را تایپ کنید و بر روی enter بزنید.

گام چهارم؛ ویژگی های پیشرفته

بگذارید تصور کنیم که داریم یک برنامه که برای دستگاه های موبایل طراحی شده است را با استفاده از یک مرورگر در سیستم خود بررسی می کنیم. در بیشتر حالات، وب سرور user-agent ارسال شده از طرف مرورگر کاربر را برای شناسایی پلتفرمی مخصوص بررسی خواهد کرد تا به آن با منابع سفارشی سازی شده که برای موبایل و تبلت مناسب باشند پاسخگویی کند. تحت این شرایط، شما می توانید ویژگی match and replace را پیدا کنید که توسط Brup Proxy ارائه می شود. به هر حال بگذارید Burp Proxy را به منظور تغییر دادن سرآیند user-agent پروتکل http پیکربندی کنیم.

1. در تب options پنجره Burp Proxy به پایین بروید تا با قسمت match and replace رو به رو شوید.

2. سپس در قسمت match and replace، با کلیک کردن بر روی دکمه Add پنجره ای باز خواهد شد که به شما اجازه می دهد با استفاده از یک منوی کشویی و دو فیلد متنی یک rule سفارشی شده ایجاد کنید. از آنجایی که ما می خواهیم یک شرط تطبیق پذیر با درخواست Http ایجاد کنیم باید از منوی بازشو گزینه request header را انتخاب کنیم.
3. در گام بعد در اولین فیلد متنی واژه ^User-Agent.*$ را وارد کنید. این فیلد گزینه تطبیق (Match) را درون درخواست HTTP نمایش می دهد. ویژگی match and replace ابزار Burp Proxy به شما اجازه می دهد از رشته های ساده و همچنین عبارت های منظم پیچیده (complex regular expressions) استفاده کنید. اگر با عبارت های منظم آشنا نیستید، به این آدرس http://www.regular-expressions.info/quickstart.html بروید و در مورد آن مطالعه کنید.
4. در فیلد متنی دوم این متن را وارد کنید Mozilla/5.0 (iPhone; U; CPU like Mac OS X; en) AppleWebKit/4h20+ (KHTML, like Gecko) Version/3.0 Mobile/1C25 Safari/419.3 یا هر user-agent قلابی که می خواهید آن را جعل کنید. این گزینه باعث می شود سرآیند User-agent تمامی بسته های ارسالی با Mozila/5.0.... مقداردهی شود.
5. در پایان بر روی OK کلیک کنید که تطبیق دهنده جدید به لیست اضافه شود.



6. حال یک درخواست را متوقف سازید و به قسمت Raw ابزار Burp Proxy بروید. در آنجا مشاهده خواهید کرد که به صورت خودکار سرآیند درخواست اصلاح شده است.

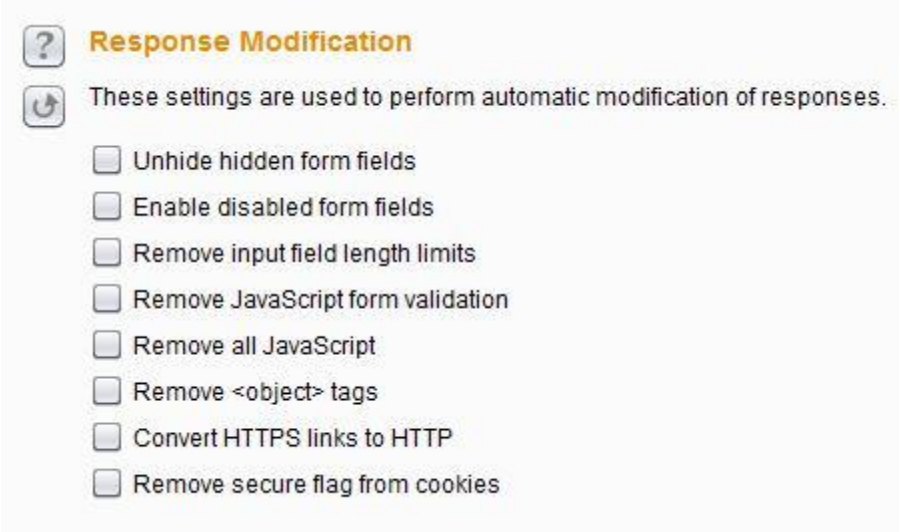
اصلاح کردن پاسخ ها[1]

یکی دیگر از ویژگی های جالب موجود در Burp Proxy اصلاح کردن خودکار پاسخ های Html است که می توانید آن را از قسمت Options درون Burp Proxy پیکربندی و فعال کنید. با استفاده از این ویژگی شما قادر خواهید بود که به صورت خودکار کد های جاوا اسکریپت را حذف کنید یا قالب تمامی پاسخ های دریافت شده HTML را تغییر بدهید.

بگذارید در عمل بررسی کنیم چگونه می توانید این ویژگی را فعال کنید.

1. در Burp Proxy ، به قسمت Options و سپس Responses Modification بروید.
2. چندین گزینه در این قسمت وجود دارد که هر کدام از آنها عملیات خاصی را انجام می دهند: گزینه unhide hidden form fields فیلدهای مخفی قالب Html را نمایش می دهد، گزینه enable disabled form fields تمامی ورودی ها به قالب های حاضر در صفحه را ثبت می کند، گزینه remove input field length limits اجازه می دهد رشته هایی با اندازه بزرگتر از حد استاندارد را به درون فیلد های متنی صفحه Html وارد کنید، گزینه remove JavaScript form validation موجب می شود Burp Proxy تمامی کنترل کننده های جاواسکریپت درون قالب های HTML را حذف کند، گزینه remove all JavaScript به صورت کامل تمامی اسکریپت های جاوا را حذف می کند و remove object tags شی های نهفته درون مستندات Html را حذف خواهد کرد.
3. گزینه مد نظر خودتان را انتخاب کنید تا به صورت خودکار برنامه Burp آن عملیات را انجام بدهد.

[1] Responses Modification



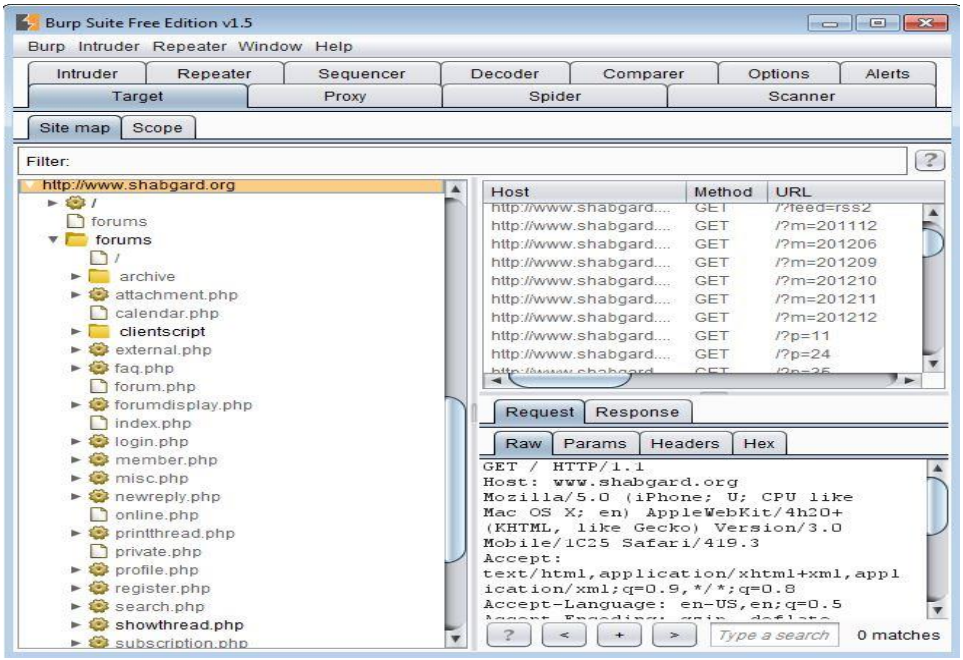
استفاده کردن از این گزینه، شما را قادر می سازد متوجه شوید که آیا برنامه کاربردی تحت وب هدف شما از اعتبار سنجی سمت سرور استفاده می کند یا خیر. به عنوان مثال، برخی از برنامه های کاربردی غیر ایمن از طریق توابع JavaScript تنها فقط از اعتبار سنجی سمت کلاینت استفاده می کنند، در این شرایط شما می توانید به راحتی با ویژگی اصلاح کننده خودکار درخواست ها و انتخاب کردن گزینه remove JavaScript form validation اعتبار سنجی را به صورت مستقیم از روی مرورگر خود انجام بدهید.

هشت ویژگی مهم Brup Suite که شما باید آنها را بدانید

زمانی که شما شروع به استفاده از Burp Suite بکنید، خیلی زود متوجه خواهید شد که با استفاده از این برنامه می توانید کارهای مختلفی انجام بدهید. در این قسمت به شما برخی از این ویژگی های رایج و سودمند آموزش داده خواهد شد.

ویژگی اول؛ استفاده از گزینه Site Map

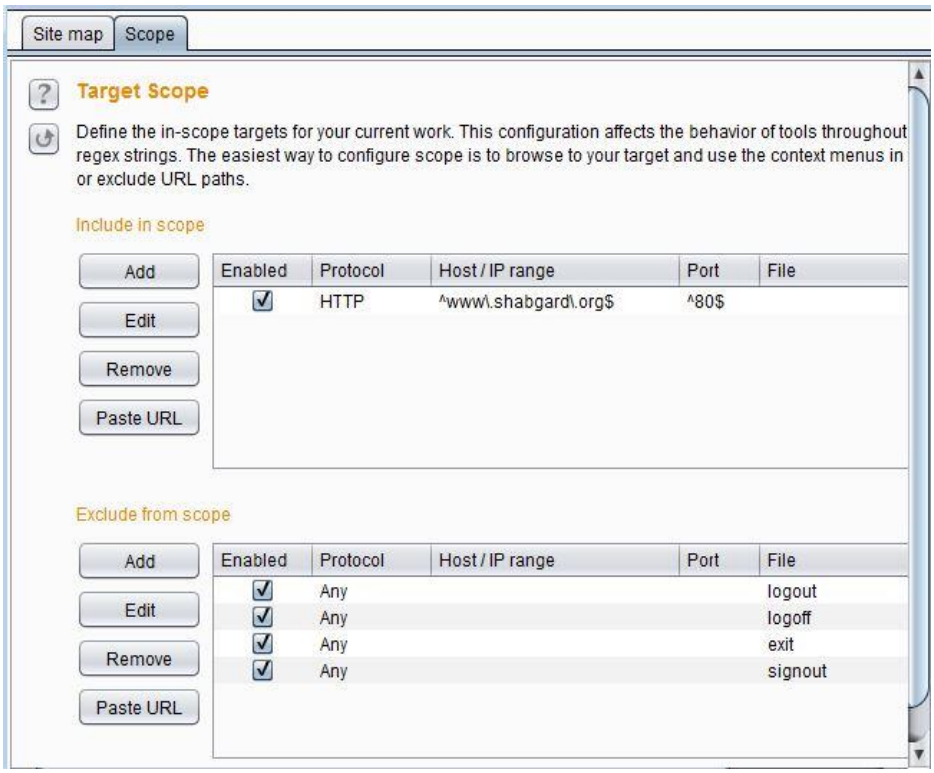
یکی از اولین کار هایی که در ارزیابی امنیت برنامه های تحت وب صورت می گیرد کاوش کردن وب سایت قربانی برای جمع آوری اطلاعات از منابع آن است. با استفاده از Burp Suite شما می توانید به سادگی برنامه تحت وب را مرور کرده و هر کاری که می خواهید به صورت معمول بر روری وب سایت انجام بدهید. با این حال، در حین مرورکردن وب سایت توسط شما، برنامه Burp Suite همه درخواست ها و پاسخ های Html را ردیابی و ضبط خواهد کرد و تمامی داده ها و اطلاعات را با استفاده از Site Map خود نمایش خواهد داد.



تب Target موجود در برنامه Burp تمامی نقاط پایانی و پارامتر های هدف را در یک قالب سلسله مراتبی نمایش می دهد. این پنجره به طور معمول به عنوان نمایش دهنده نقشه سایت عمل می کند. فرآیند مرور کردن تمامی منابع برنامه کاربردی تحت وب بسیار مهم است و Site Map برنامه Burp به شما اجازه می دهد به سرعت سطوح حمله به نرم افزار را تحلیل کنید.

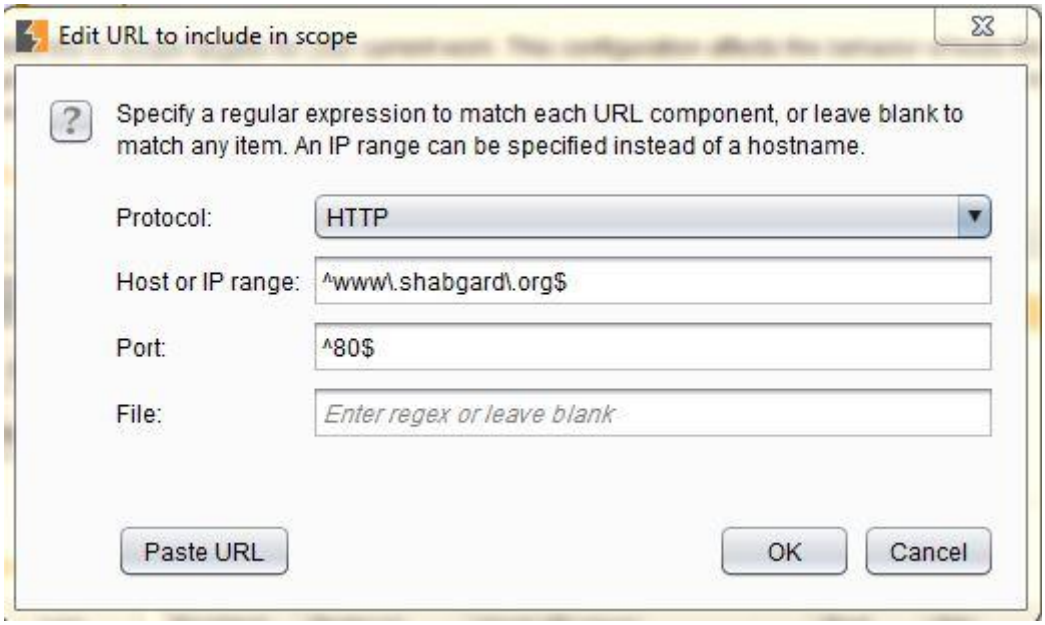
از ساختار درختی Site Map شما می توانید آدرس وب سایت هدف خودتان را انتخاب کنید و به سادگی تمامی منابع آن را مشاهده کنید. این یک ویژگی مهم است که اجازه می دهد کاربر Burp فقط بر روی منابع مربوطه متمرکز شود و از هرگونه تعامل با منابع دیگر برنامه جلوگیری شود. بگذارید ببینیم چگونه این کار را می توان انجام داد.

1. در قسمت Target تب Site Map هدف خود را با کلیک کردن بر روی نام دامنه آن انتخاب کنید. در اینجا من هدفم shabgard.org است.
2. بر روی هدف خود کلیک راست کنید و سپس Add item to scope را انتخاب کنید تا هدفتان به تب scope منتقل شود. در حالت پیش فرض، گزینه Scope برنامه Burp خالی است و همه دامنه ها به عنوان قسمتی از ارزیابی در نظر گرفته می شوند.
3. علاوه بر این، شما می توانید با کلیک کردن بر روی گزینه Filter موجود در تب Site Map و انتخاب کردن گزینه only in-scope items از قسمت filter by request type منابع مربوط به دیگر دامنه ها را فیلتر کنید. پس از اینکه این گزینه را انتخاب کنید، منابع دیگر وب سایت ها مخفی خواهد شد و فقط در پنجره محتویات و منابع وب سایت مورد نظر شما لیست می شود.
4. با این حال، در نهایت Site Map باید تنها منابعی را نمایش دهد که متعلق به دامنه انتخابی شما باشد. همچنین شما می توانید این تنظیمات را با بررسی کردن جدول include in scope درون تب scope بررسی کنید.



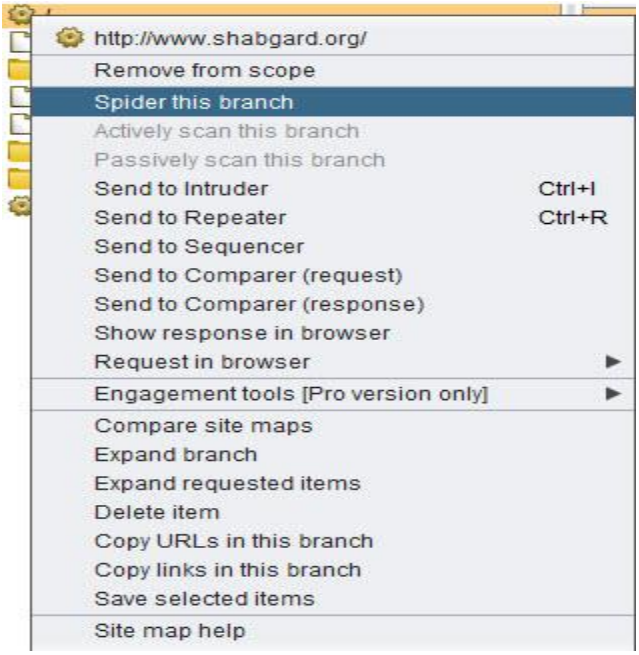
در این فرم شما می توانید به صورت دستی خود آیتم های موجود در Scope را تغییر بدهید. به عنوان مثال، اگر شما بخواهید دامنه جدیدی به Scope اضافه کنید، می توانید با دنبال کردن گام های آورده شده در زیر این کار را انجام بدهید.

1. ابتدا در قسمت include in scope بر روی Add کلیک کنید، سپس در پنجره جدیدی که باز می شود از منوی باز شو می توانید پروتکلی که هدف شما از آن استفاده می کند را انتخاب کنید.
2. سپس در فیلد متنی اول، یک عبارت منظم یا همان regular expression که شناسه دامنه و زیر دامنه ها را مشخص ساز را وارد کنید. (به عنوان مثال می توانید بدین شکل هدف را وارد کنید : $^www\.shabgard\.org$). شایان ذکر است عبارت های منظم استفاده شده در Burp بسیار شبیه عبارت های منظمی هست که در پرل وجود دارند.
3. سپس در فیلد متنی وسط، یک عبارت منظم را وارد کنید که شماره درگاه مناسبی را مشخص می سازد. (به عنوان مثال می توانید از این الگوی استفاده کنید $80^ برای پروتکل http و $443^ برای https)
4. همچنین می توانید به صورت اختیاری یک عبارت منظم برای فایل ها و پوشه های در فیلد متنی سوم مشخص سازید. با این حال اگر شما می خواهید کل برنامه کاربردی تحت وب را تحلیل کنید این فیلد را خالی بگذارید.
5. در نهایت، بر روی دکمه Add کلیک کنید تا به صورت خودکار به جدول include in scope وارد و اعمال شود.



همچنین به صورت مشابه می توانید با استفاده از جدول exclude from scope منابعی را مشخص سازید که نمی خواهید توسط برنامه بررسی شوند. این ویژگی به شما امکان ایجاد کردن یک لیست سیاه از نقاط پایانی خارج از محدوده برنامه کاربردی تحت وب را به شما می دهد. همچنین این ویژگی می تواند در جلوگیری کردن از خارج شدن توابع، دکمه های تنظیم مجدد یا دیگر عملیات های مخرب مفید واقع شود.

همچنین در قسمت Site Map از هر دامنه و آیتمی (نقاط پایانی یا پارامتر ها) شما می توانید با راست کلیک کردن بر روی آنها یک منوی متنی باز کنید که در آن هر گزینه یک عملیات خاصی را بر روی آیتمی توانند برای شما انجام بدهد.



این مکانیزم به شما اجازه می دهد به سرعت هر درخواست و پاسخ ورودی به برنامه را که می خواهید با کلیک کردن بر روی گزینه ها موجود در آن به ابزار های موجود در Burp Suite وارد کنید. این گزینه ها در زیر تشریح شده اند:

1. Spider this branch : این گزینه اسپایدر برنامه را به کار می اندازند.
2. Actively/Passively scan this branch : این گزینه یک پویش خودکار با Burp Scanner آغاز می کند.(البته این گزینه فقط در نسخه حرفه ای این برنامه وجود دارد.)
3. Send to intruder: این گزینه یک حمله سفارشی شده را اجرا می کند.
4. Send to repeater : این ابزار یک درخواست را اصلاح کرده و پشت سر هم ارسال می کند.
5. Send to sequencer : این ابزار داده های پیش بینی شده برنامه را تحلیل می کند.
6. Send to comparer (request/response) : این ابزار چندین تکرار و پاسخ را با هم مقایسه می کند.

عاملیت های بالا در ادامه این فصل تشریح خواهند. علاوه بر این، منوی متنی اجازه می دهد درخواست ها و پاسخ های Html را باز تولید کنید. این ویژگی در بررسی رفتار مرورگر در طی تجزیه و تحلیل حملات مبتنی بر کلاینت (به عنوان مثال، Cross-Site Scripting, UI redressing و ..) بسیار مفید است. بدین منظور کافیست گام های آورده شده در زیر را انجام بدهید.

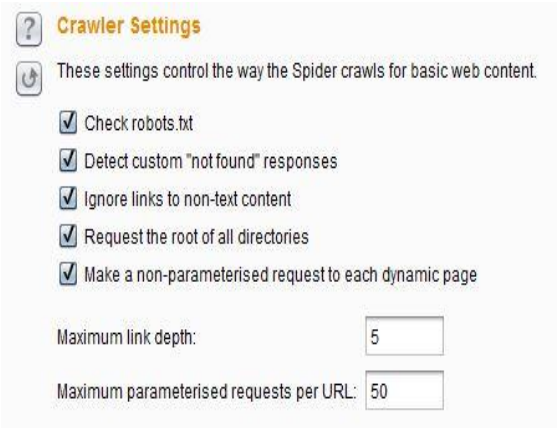
1. یک درخواست را از قسمت Map برنامه انتخاب کنید.
2. بر روی آن کلیک راست کرده و گزینه request in browser را انتخاب کنید.
3. سپس در گام بعد یا گزینه جلسه جاری مرورگر (current browser session) یا گزینه (original session) را انتخاب کنید که Burp را قادر می سازد از توکن جلسه که در درخواست موجود ذخیره شده است استفاده کند(البته اگر قابل اجرا باشد).
4. در گام بعد یک پنجره باز خواهد شد و یک URL مجازی (مانند http://burp/repeat/1) را نشان خواهد داد.
5. سپس در مرورگر، آن Url را با فشردن کلید هایCtrl+V قرار بدهید.
6. در گام آخر Enter را بفشارید تا درخواست درون مرورگر شبیه سازی شود.

ویژگی دوم؛ خزیدن در یک وب سایت با Burp Spider

ابزار Burp Spider به شما اجازه می دهد در یک وب سایت بخزید(Crawling) و تمامی منابع پنهان و آشکار آن را بدست آورید. این ابزار از روش های ترکیبی برای دریافت حداکثر نتیجه استفاده می کند.

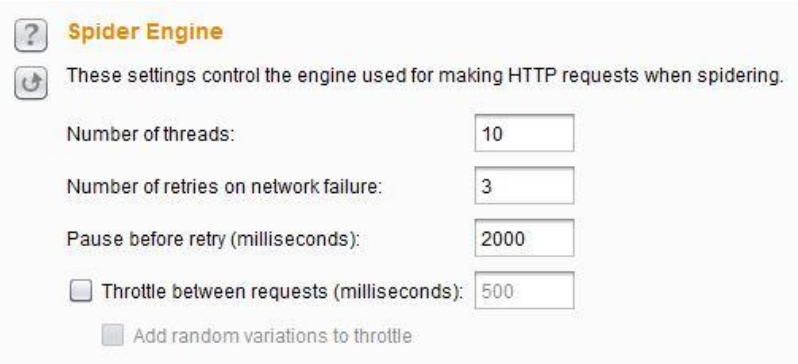
اولین گام نیازمند تنظیم کردن Sider با استفاده از تب Option در ابزار Burp است. گرچه در بیشتر حالات، تنظیم پیش فرض خود ابزار برای بدست آوردن یک نتیجه خوب کافی هستند. اما در برخی موارد ممکن است شما بخواهید تنظیمات Spider را شخصی سازی کنید.

1. برای وب سایت های بزرگ، ممکن است نیاز باشد maximum link depth تغییر یابد. این گزینه حداکثر ریدایکرت ها برای یک منبع را نمایش می دهد. این گزینه می تواند به سادگی تغییر یابد.



2. همچنین در حالت میزبان های آسیب پذیر با منابع سیستمی محدود، ممکن است شما بخواهید تعداد ترد های ارسالی را تغییر بدهید. بدین منظور می توانید با عوض کردن عدد موجود در Number of Thread درون قسمت

Spider Engine تعداد ترد ها را عوض کنید. همچنین، شما می توانید تعداد تلاش های مجدد در صورت قطع شدن شبکه و زمان توقف قبل از هر آزمایش را افزایش بدهید.

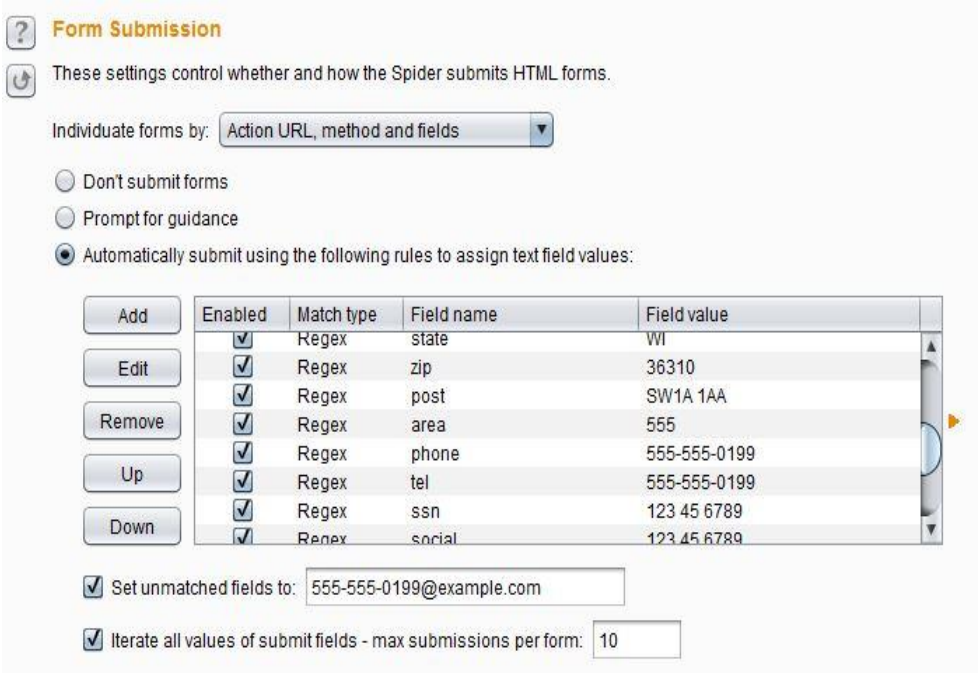


3. اگر شما می خواهید Burp Spider خودکار کلمه های عبور و نام های کاربردی را در قسمت ورود به برنامه به صورت خودکار وارد کند. می توانید کلمه عبور و نام کاربری را در قسمت Application login وارد کنید.

یکی از ویژگی های جالب Burp Spider تعریف نام و مقداردهی به آن است. این مقادیر توسط ابزار برای وارد کردن در فرم های Html استفاده می شود. در طی خزیدن در منابع وب سایت، ممکن است Spider با فرم های تحت وب رو به رو شود که با محتوای معنایی معتبری پر شده باشند. به عنوان مثال، بگذارید یک فرم ثبت نام با یک فیلد ایمیل را تصور کنیم؛ در این حالت، spider باید قادر به شناسایی کردن فیلد خاصی و یک ایمیل ثبت شده معتبر باشد. بدین منظور Burp Spider به شما اجازه می دهد یک عبارت منظم برای تطبیق دادن با نام های فیلد ها تعریف کنید.

1. در Burp Spider از منوی Options بر روی forms کلیک کنید.
2. فرض کنید می خواهید Burp Spider فرم های را مقداردهی کند، بدین منظور گزینه automatically submit using the following rules to assign parameter values انتخاب کنید .

3. جدول نمایش داده شده در قسمت پایین، تمامی نام ها و مقادیری که برنامه از آنها برای پر کردن فیلد ها استفاده می کند آورده شده است. مانند دیگر ابزار ها، شما می توانید در آن موجودیت اضافه کنید، حذف کنید و حتی موجودیت هایی که در لیست هستند را ویرایش کنید. به عنوان مثال، اگر شما می خواهید یک رول برای ثبت کردن یک ID که توسط کلمه کلیدی PacktUserID مشخص شده است شما می توانید از منوی باز شو گزینه regex را انتخاب کنید.
4. سپس PacktUserID در روی فیلد متنی اول وارد کنید. این فیلد نام برای رول سفارشی است و توسط برنامه متوقف می شود.
5. در قسمت field value مقدار مناسب برای پارامتر را وارد کنید. در این قسمت باید مقداری را وارد کنید که ما می خواهیم به پارامتر تخصیص پیدا کند .
6. در پایان، بر روی دکمه Add کلیک کنید و اطمینان حاصل کنید که تمامی checkbox ها به درستی انتخاب شده اند. همانند تصویری که در زیر آورده شده است.

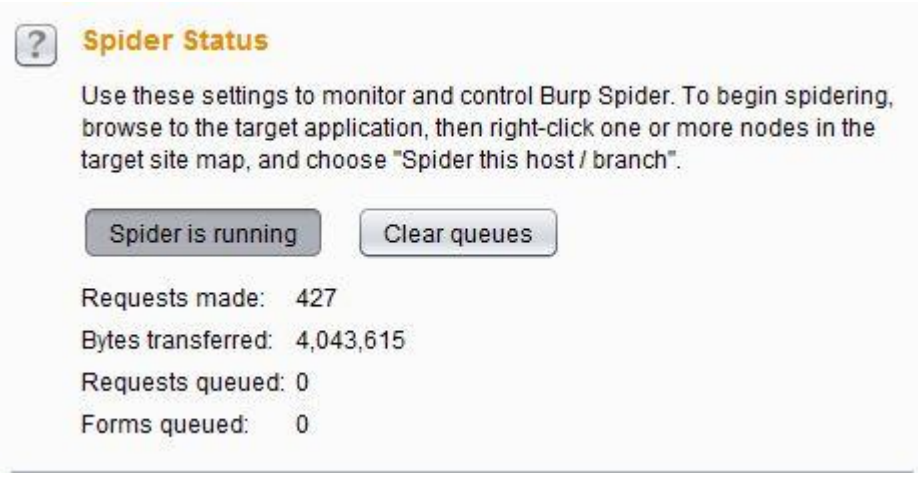


پیکربندی ثبت خودکار فرم ها در Burp Spider

در این نقطه؛ ابزار Burp Spider آماده فعال شدن است. شما می توانید ابزار Burp Spider را هم از قسمت منوی متنی در Burp Target فعال کنید و هم می توانید با زدن تیک checkbox گزینه Spider running در تب control ابزار Burp Spider آن را فعال کنید.

پیشنهاد بنده این است که از منوی Site Map Tree بر روی یک هدف کلیک راست کرده و گزینه Spider this host را انتخاب کنید. پس از انتخاب این گزینه Burp Spider به سادگی شروع به خزیدن در منابع وب سایت انتخاب شده می کند. همچنین شایان ذکر است، در حالت پیش فرض، Burp Spider از گزینه های تعریف شده در scope تب target استفاده می کند، که همین رفتار تضمین می کند، این ابزار به منابع خارج از دامنه های قربانی استناد نمی نماید.

همچنین از تب control در Burp Spider، شما می توانید پیشرفت ابزار را با مشاهده کردن اطلاعات نمایش داده شده در این قسمت بررسی کنید. این قسمت جزئیات تعداد کل درخواست های Http ارسال شده توسط Spider و تعداد منابع به کار گرفته شده را شامل می شود.



علاوه بر خودکار سازی خزیدن Burp Spider، این موضوع خیلی مهم است که بتوانید به صورت دستی تمامی منابع وب سایت را مرور کرده و تمامی منابع مهم آن برنامه را قبل از شروع پویش برنامه جمع آوری کنید.

ویژگی سوم؛ انجام یک پویش خودکار با پویشگر Burp

پویشگر Burp یا Burp Scanner یک پویشگر پویا برنامه های تحت وب است که در نسخه حرفه ای این برنامه وجود دارد. این ابزار به شما اجازه می دهد به صورت خودکار بتوانید وب سایت ها را پویش کرده و ضعف های امنیتی رایج را شناسایی کنید از قبیل ضعف هایی مانند SQL Injection، Cross-Site Scripting، XML Injection، missing cookie flags (به عنوان مثال HttpOnly و Secure) و غیره. همچنین این ابزار به شما اجازه می دهد در دو حالت برنامه هدف خود را پویش کنید، این دو روش در زیر تشریح شده اند.

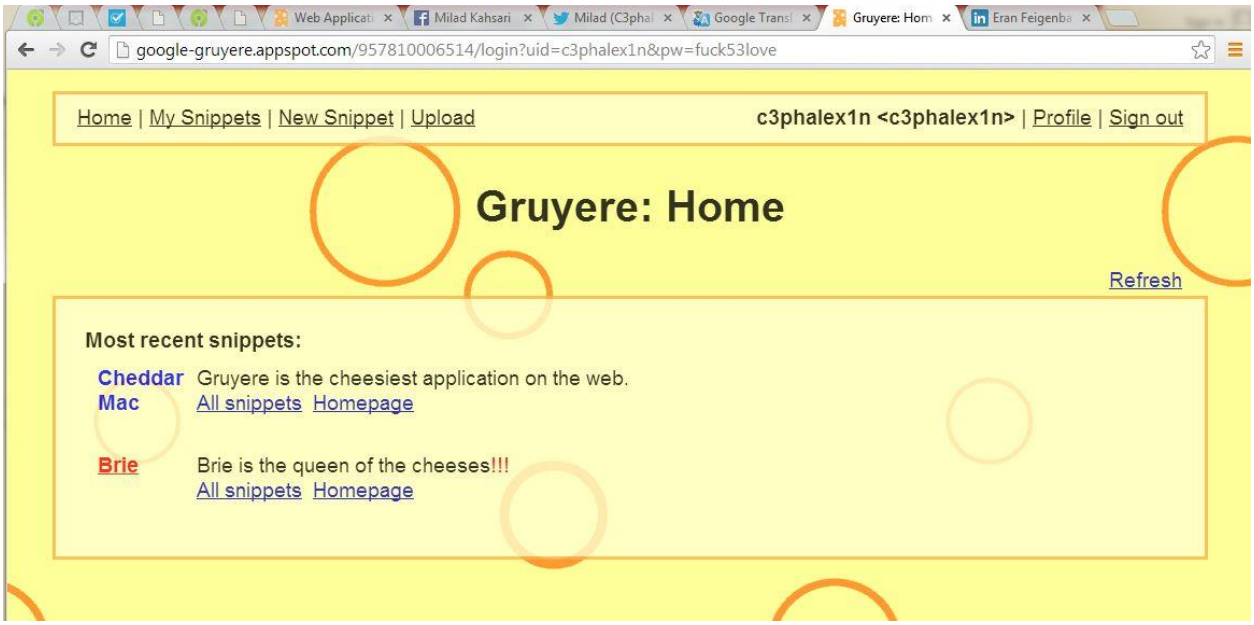
- ✓ **پویشگری مستقیم (Active Scanning) :** در این حالت، با ارسال بسته های درخواستی Http با الگوی های[1] تهاجمی خاص و تحلیل کردن پاسخ سرور به بسته درخواستی با روش تطبیق الگو هوشمند یا pattern-matching heuristics شناسایی ضعف های امنیتی صورت می گیرد.
- ✓ **پویشگری غیر مستقیم (Passive Scanning) :** با استفاده از این روش، پویشگر Burp از درخواست ها و پاسخ های ذخیره شده برای شناسایی ضعف های امنیتی استفاده می کند. در این روش تجزیه و تحلیل به صورت آفلاین صورت می گیرد و نیاز به پویش فعال نیست.

نویسنده، میلاد کهساری الهادی: همچنین در روش دوم می توان گفت که در این روش Burp Scanner از یک بانک اطلاعاتی برای کشف ضعف های امنیتی استفاده می کند. با این حال این نکته قابل ذکر است، چون بنده خودم از نسخه Free استفاده می کنم و به این ابزار دسترسی ندارم نمی توانم اطلاعات کامل به شما ارائه بدهم. با این حال با مستنداتی که در مورد این ابزار و این روش خوانده ام، فکر می کنم این روش همانند روش تطبیق با بانک اطلاعاتی عمل می کند.

برای بررسی ویژگی های این ابزار می توانید وب سایت http://google-gruyere.appspot.com/ را مورد بررسی و پویش قرار بدهید. این برنامه تحت وب دارای ضعف های امنیتی متنوع و بسیاری هست که می توانید از آن برای تمرین کشف ضعف های امنیتی تحت وب به صورت آنلاین استفاده کنید. شایان ذکر است یکی از افراد طراح این Code Lab خانوم Parisa Tabriz هست.

[1] Pattern

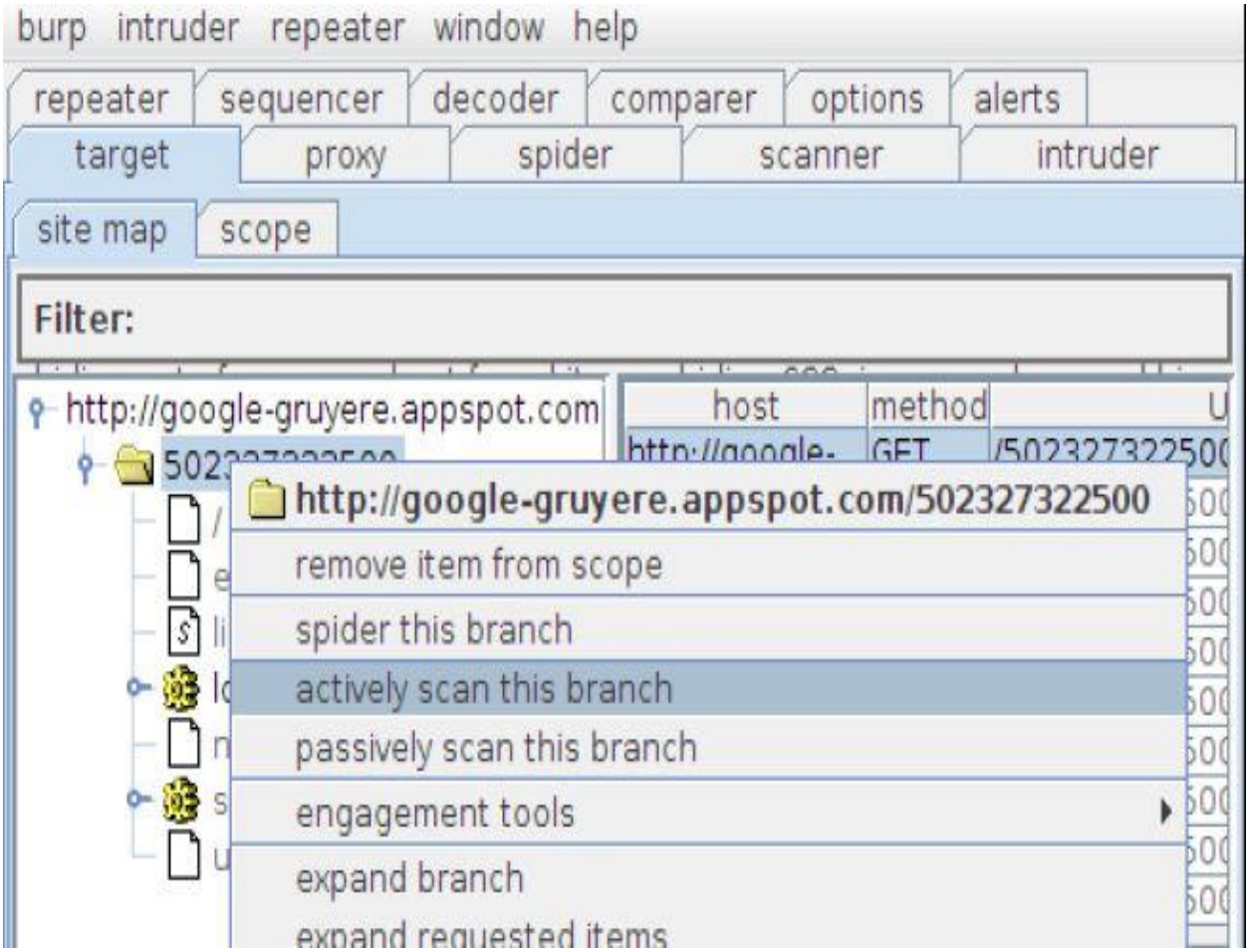
1. در گام اول لینک http://google-gruyere.appspot.com/part1 مشاهده کنید و با دقت دستورالعمل های آورده شده در آن را بخوانید .
2. در گام دوم به لینک http://google-gruyere.appspot.com/start بروید و بر روی Agree & Start کلیک کنید.
3. در گام سوم بر روی گزینه Sign Up کلیک کرده و یک حساب کاربری ایجاد کنید .
4. سپس در گام چهارم با مشخصات حساب کاربری که ایجاد کرده اید با کلیک کردن بر روی Sign In وارد سیستم شوید. در این لحظه، Burp را پیکربندی کنید که تمامی درخواست های ارسالی را متوقف سازد. مرورگر شما باید به شکل زیر در آید.



قابل ذکر است، پویشگر Burp می تواند هنگامی که شما وب سایت را مرور می کنید به صورت خودکار تمامی منابع وب سایت هدف را پویش کند، همچنین می توانید از قسمت Site map با کلیک کردن بر روی گزینه Actively Scan یا Passive Scan آنرا فعال کنید.

در حالت پیش فرض، هنگامیکه Active Scanning غیر فعال می باشد، پویشگر Burp بگونه ای پیکربندی شده است که تمامی دامنه ها را با روش Passive پویش کند. با این حال، در تب Scanner برنامه Burp گزینه Live Scanning را انتخاب کرده و سپس در هر دو قسمت یعنی Active Scanning و Passive Scanning گزینه Use suite scope را انتخاب کنید تا تمامی منابع برنامه تحت تحلیل که از Burp Proxy عبور داده می شوند، مورد پویش قرار گیرند. این روش عمدتا به عنوان پویشگری On the fly خطاب می شود. علاوه بر این روش، شما می توانید بجای آن، یک شاخه مشخص از هدف را در قسمت تب Site

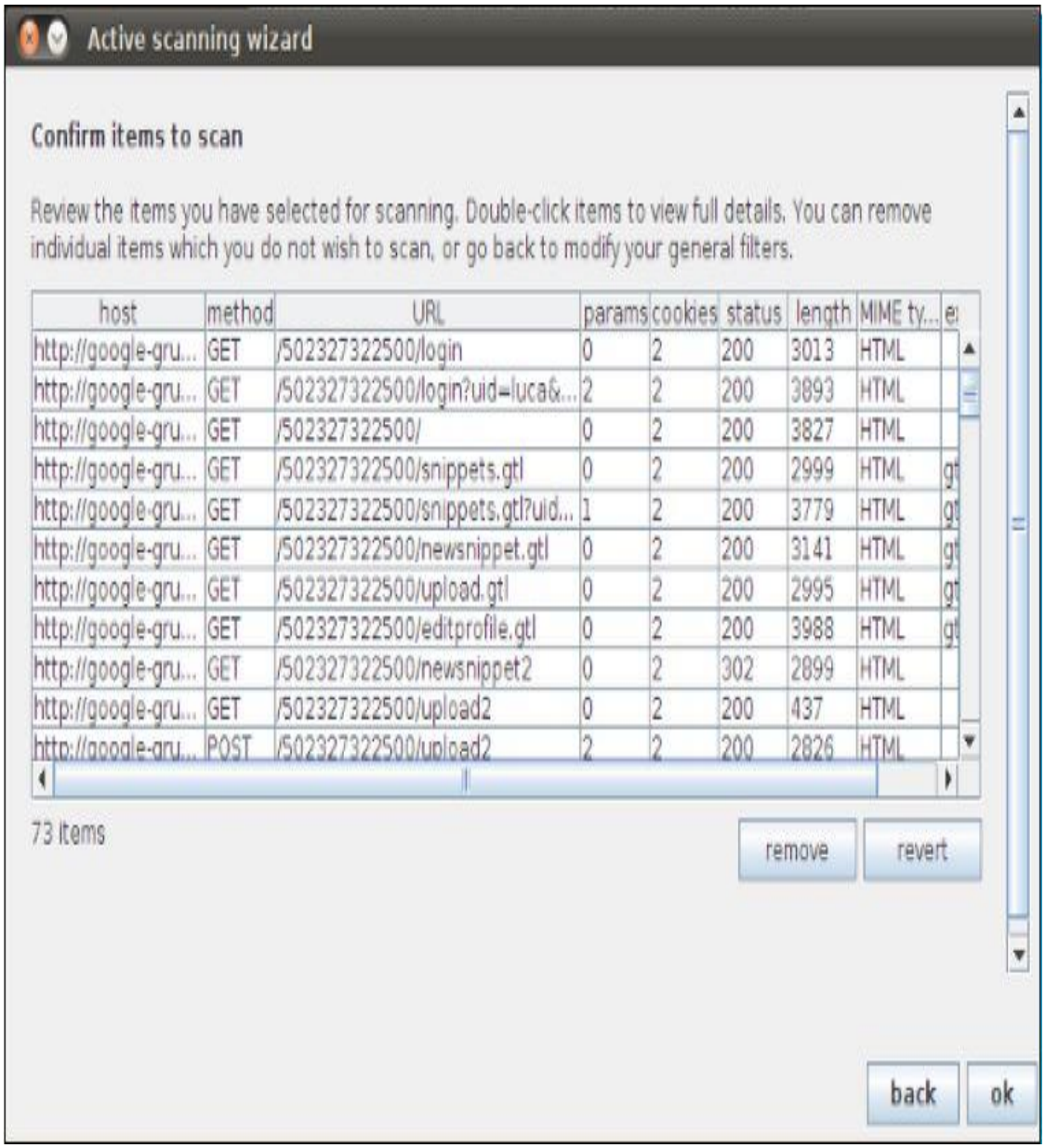
Map انتخاب کنید و با کلیک بر روی actively scan this host یا passively scan this host هدف خود را مطابق با خواسته های خود مورد پویش قرار بدهید. به نظر بنده این روش بهتر است.



اگر شما برای آغاز پویش active scan را انتخاب کنید، Burp Suite یک پنجره جدید با نام Active scanning wizard نمایش خواهد داد که یک ابزار بسیار ساده برای پیکربندی فرآیند پویش است.

1. در اولین گام فرآیند پیکربندی پویش، شما می توانید برخی از انواع منابع برنامه را به منظور پویش کردن مانند تصاویر، کدهای جاوا اسکریپت یا stylesheet ها را حذف کنید. در بیشتر حالات، تنظیمات پیش فرض برای پویش کردن اهداف کافی است و شما فقط باید در این قسمت بر روی Next کلیک کنید تا به مرحله بعد بروید.
2. در گام دوم، برنامه یک جدول از لیست تمامی پارامتر ها و نقطه های پایانی قربانی که Burp Scanner در طی پویش کردن شامل شده است را نمایش می دهد. در این قسمت شما باید با دقت لیست را مرور کرده و تمامی نقطه های پایانی که به هدف مرتبط نیستند را حذف کنید. همچنین در پایین جدول این ابزار تعداد آیتم های

موجود در لیست را هم می توانید مشاهده کنید. با این حال پس از انتخاب کردن آیتم های مناسب بر روی ok کلیک کنید تا فرآیند پویش آغاز شود.



ویزارد پویشگری مستقیم ابزار Burp Scanner

در بیشتر حالت های پویشگری، تنظیمات پیش فرض برنامه برای انجام پویشگری کافی است. با این حال، اگر شما می خواهید عملیات پویشگری را با تنظیمات مد نظر خود پیکربندی کنید، می توانید بدین منظور در ابزار Burp Scanner به

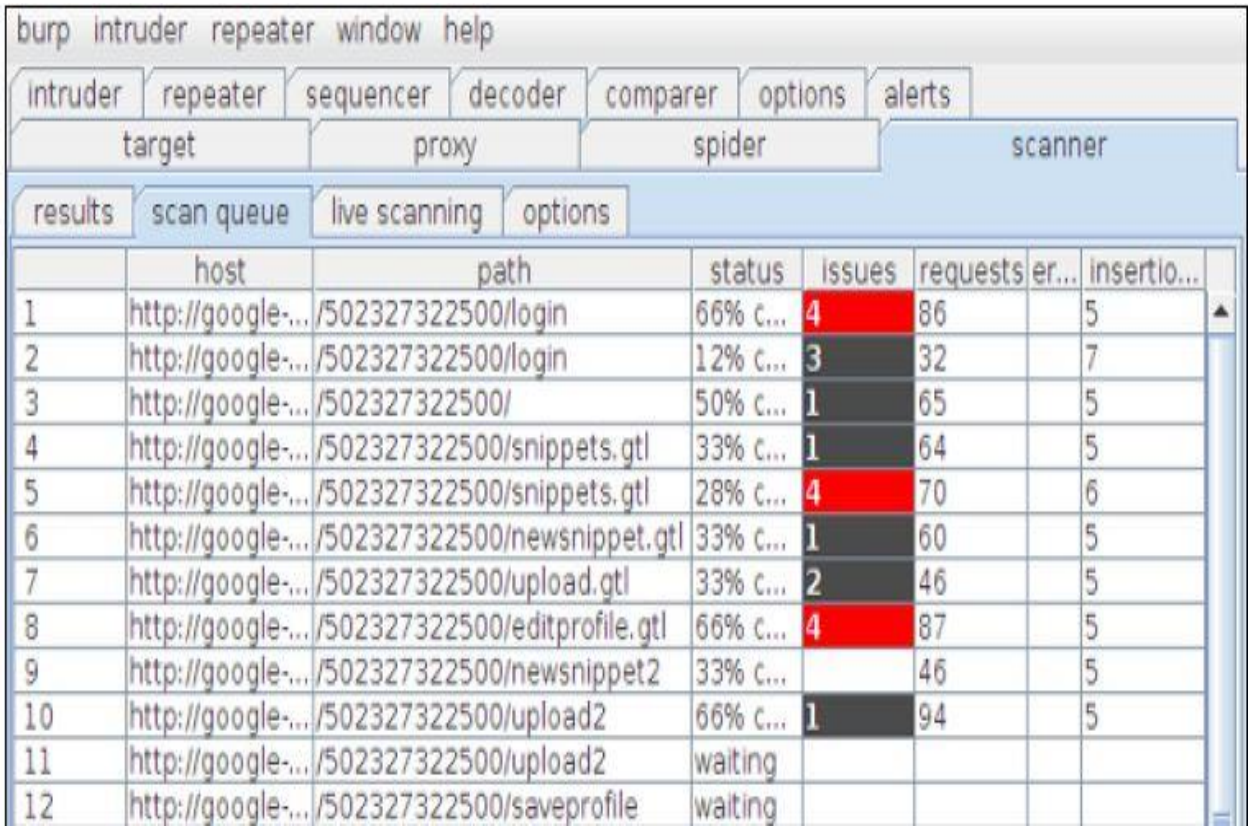
تب Options بروید و تنظیما مد نظر خود را در آنجا اعمال کنید. این تب شامل تعداد گزینه می شود که در زیر تشریح شده اند.

1. **URL parameter values :** این گزینه برای دستکاری کردن تمامی پارامتر هایGet ارسال شده از طریق پروتکلhttp مورد استفاده قرار می گیرد.
2. **Body parameter values :** این گزینه برای دستکاری کردن تمامی پارامتر هایPost ارسال شده از طریق پروتکل http مورد استفاده قرار می گیرد.
3. **Cookie parameter values :** این گزینه برای در نظر گرفتن تمامی Token ها به عنوان نقطه های ورودی استفاده می شود.
4. **Parameter name :** این گزینه برای در نظر گرفتن تمامی پارامتر های GET/POST به عنوان نقطه ورودی استفاده می شود.
5. **HTTP headers :** از این گزینه برای دستکاری کردن تمامی هدر های درخواست شده از جمله هدر های استاندارد و سفارشی استفاده می شود.
6. **AMF string parameters :** در حالت طراحی برنامه ها با استفاده از Adobe Flex برنامه Burp Scanner پروتکل باینری Action Message Format را تجزیه کرده و امکان دستکاری کردن تمامی پارامتر های رشته ای آن را فراهم می کند.
7. **REST-style URL parameters :** در حالت برنامه های کاربردی پیاده سازی شده با رابط REST برنامه Burp Scanner بخشی از URL که معمولا برای شناسایی عملیات ها و آرگومان ها استفاده می شود را دستکاری می کند.

همچنین اگر شما بدنبال دسته ای از ضعف های امنیتی خاصی هستید، می توانید هر کدام از آنها را که می خواهید در قسمت Active Scanning Area و Passive Scanning Areas با تیک زدن Checkbox هایشان فعال یا غیر فعال کنید. به عنوان مثال، اگر در حال بررسی کردن یک برنامه هستید که هیچ دسترسی به زیر سیستم های LDAP آن ندارید، می توانید پویش خودتان را با غیر فعال ساختن LDAP Injection بهینه سازی کنید.

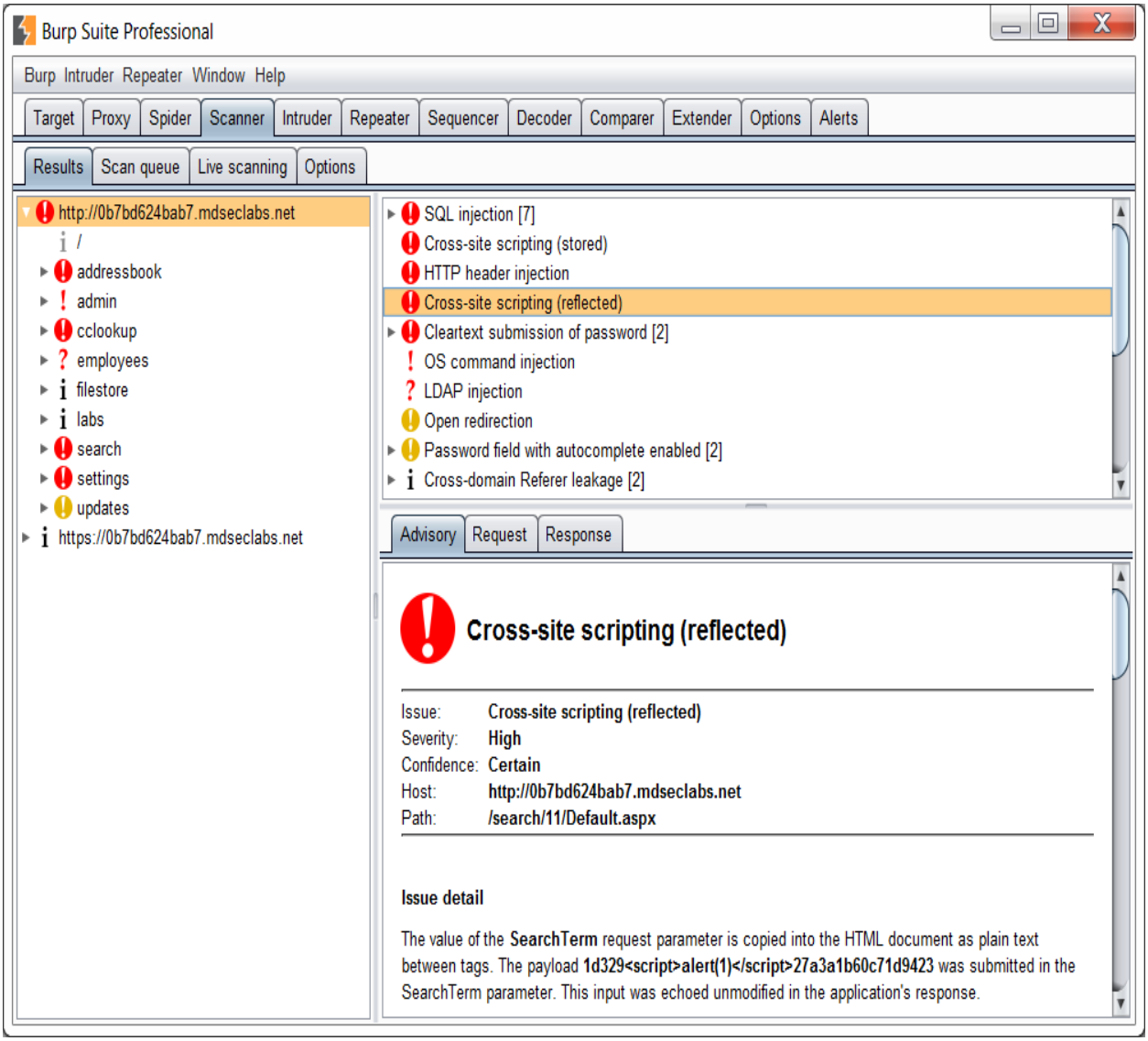
همچنین، تب Options موجود در Burp Scanner به شما اجازه می دهد، ترد های استفاده شده توسط ابزار یا افزایش زمان میان درخواست های متوالی را محدود کنید. همچنین شما می توانید مطابق با منابع سیستم موجود بر روی هدف تصمیم بگیرید فرآیند پویش خودتان را با دستکاری کردن گزینه های موجود در قسمت Active Scanning Engine سرعت ببخشید یا از سرعت آن کم کنید.

هنگامی که شما پویش خودتان را اجرا کنید، به راحتی می توانید فرآیند پویش را با استفاده از تب scan queue مانیتور کنید. این جدول اطلاعات پویش درخواست های کامل شده و در حال پیش رفت را ارائه می کند. همچنین این جدول با نمایش تعداد ضعف های کشف شده برای هر نقطه پایانی یک ارزیابی کلی از هدف ارائه می کند. همچنین در این جدول، شما می توانید آیتم های موجود را با کلیک راست کردن بر روی آنها و انتخاب گزینه Delete items از جدول حذف کنید. علاوه بر این، شما می توانید فرآیند پویش را با کلیک راست کردن بر روی محیط جدول و انتخاب گزینه های Pause Scanner یا Resume Scannner متوقف ساخته یا ادامه دهید.



	host	path	status	issues	requests	er...	insertio...
1	http://google-...	/502327322500/login	66% c...	4	86		5
2	http://google-...	/502327322500/login	12% c...	3	32		7
3	http://google-...	/502327322500/	50% c...	1	65		5
4	http://google-...	/502327322500/snippets.gtl	33% c...	1	64		5
5	http://google-...	/502327322500/snippets.gtl	28% c...	4	70		6
6	http://google-...	/502327322500/newsnippet.gtl	33% c...	1	60		5
7	http://google-...	/502327322500/upload.gtl	33% c...	2	46		5
8	http://google-...	/502327322500/editprofile.gtl	66% c...	4	87		5
9	http://google-...	/502327322500/newsnippet2	33% c...		46		5
10	http://google-...	/502327322500/upload2	66% c...	1	94		5
11	http://google-...	/502327322500/upload2	waiting				
12	http://google-...	/502327322500/saveprofile	waiting				

شایان ذکر است، پویش کردن تمامی منابع و صفحات برنامه تحت وب نیاز به مدت زمانی دارد، گاهی اوقات حتی پویشگری ساعت ها هم به طول می انجامد. به هر حال، نتایج پویشگری را در هر لحظه که می خواهید شما می توانید با کلیک کردن بر روی تب results موجود در Burp Scanner مورد بررسی قرار بدهید(این تب در تصویر بالا نمایش داده شده است). این تب همانند قسمت Site map برنامه Burp عمل کرده و تمامی ضعف های امنیتی پیدا شده در نقطه های پایانی برنامه تحت وب را به همراه نوع آن ضعف امنیتی مشخص می سازد. واقعا این نوع پویشگری خارق العاده است.



نتایج پویش Burp Scanner

اگر در این پنجره بر روی یک آیتم خاصی کلیک کنید، در قسمت advisory برای آیتم انتخاب شده جزئیات ضعف امنیتی آن نمایش داده می شود. در قسمت زیر پارامتر های موجود در قسمت Advisory مورد تشریح قرار گرفته است.

1. **Issue :** در قسمت Issue نوع صعف امنیتی مشخص می شود(به عنوان مثال Cross-Site Scripting).
2. **Severity :** در این قسمت ضریب خطر ضعف امنیتی تعریف می شود. کم ترین ضریب خطر را با Low و بیشترین ضریب خطر را با High مشخص می کند.
3. **Confidence :** در برخی ضعف های امنیتی برای تائید ضعف امنیتی ارزیابی دستی نیاز است، اما در برخی حالات دیگر، ابزار قادر به شناسایی کردن و تائید ضعف امنیتی بدون هیچ حاشیه و خطایی است. این گزینه ضریب دقت

شناسایی آن ضعف امنیتی توسط ابزار را مشخص می سازد که شامل سه مقدار (Certain، Firm و Tentative) می شود.

4. **Host :** در این قسمت آدرس میزبانی که در آن ضعف امنیتی وجود دارد مشخص می شود.

همچنین شایان ذکر است، شما می توانید از منوی متنی موجود در پنجره نتیجه های پویشگری Burp Scanner نتایج کشف شده را حذف کنید (Delete selected issues)، یک سطح شدت (Set severity) و یک سطح اعتماد به نفس در شناسایی (Set confidence) به آن آیتم انتخاب شده تخصیص دهید.

در پایان، هنگامی که تمامی منابع برنامه تحت وب تجزیه و تحلیل شد و پویش با موفقیت به اتمام رسید. شما می توانید از پویش خود یک خروجی بگیرید. خوشبختانه برنامه Burp Scanner به شما توانایی ایجاد کردن یک گزارش با قالب های XML یا HTML از ضعف های امنیتی کشف شده را ارائه می دهد که می توانید از آن برای تجزیه و تحلیل و ارزیابی امنیت کلی سیستم مد نظر خود استفاده کنید. علاوه بر این، ذکر این نکته خالی از توفیق نیست، شما علاوه بر اینکه می توانید آن گزارش را با دیگر افراد متخصص به اشتراک بگذارید، حتی می توانید آن گزارش تولید شده را در دیگر برنامه های امنیتی (به عنوان مثال متاسپلویت) وارد کنید و آنها را برای دیگر عملیات های نفوذگری مورد استفاده قرار بدهید. ه در زیر نحوه ایجاد کردن یک خروجی به شما نمایش داده شده است.

1. در تب Results برنامه Burp Scanner تمامی آیتم هایی را که می خواهید از آنها گزارش بگیرید را انتخاب کنید. البته شایان ذکر است، شما می توانید در منوی درختی با انتخاب شاخه root از تمامی منابع پویش شده توسط برنامه خروجی بگیرید.
2. سپس بر روی آن ها کلیک راست کرده و از منوی متنی گزینه Report selected issues را انتخاب کنید.
3. در این گام یک پنجره جدید با نام Burp Scanner reporting wizard باز می شود که شما را در انتخاب قالب خروجی گزارش راهنمایی می کند. با این حال اولین گام انتخاب نوع قالب خروجی گزارش است. این نوع ها شامل screen-friendly HTML، printer-friendly HTML، و XML می شود.
4. در گام بعدی، شما می توانید جزئیات گزارش را سفارشی سازی کنید. به عنوان مثال برای داشتن تمامی جزئیات پویش می توانید در این پنجره تیک تمامی checkbox ها را بزنید تا یک گزارش کامل ایجاد گردد.
5. گاهی اوقات snapshot گرفتن از درخواست ها و پاسخ های Http تاثیر گذار و ارائه آنها بسیار مفید است، بدین منظور کافیست تیک checkbox های مدنظرتان را بزنید.
6. در گام بعد، در قسمت Burp Scanner report wizard به شما اجازه داده می شود نوع ضعف های امنیتی که قصد دارید آن ها در گزارش قرار داده شوند را انتخاب کنید. پس از اینکه نوع ضعف های مد نظر خودتان را مشخص ساختید کافیست بر روی Next کلیک کنید.

7. در پایان، در مرحله آخرشما نیاز دارید نام فایل گزارش را مشخص سازید. بر روی Save file... کلیک کنید و فایل سیستم خودتان را مرور کنید و سپس محلی که می خواهید گزارش را در آنجا ذخیره سازید را انتخاب کنید. سپس نام فایل را به همراه قالب آن تایپ کنید . به عنوان مثال، اگر می خواهید نتیجه گزارش را با قالب Html ذخیره کنید بدین صورت تایگ کنید BurpResMilad.html و بر روی Save کلیک کنید.

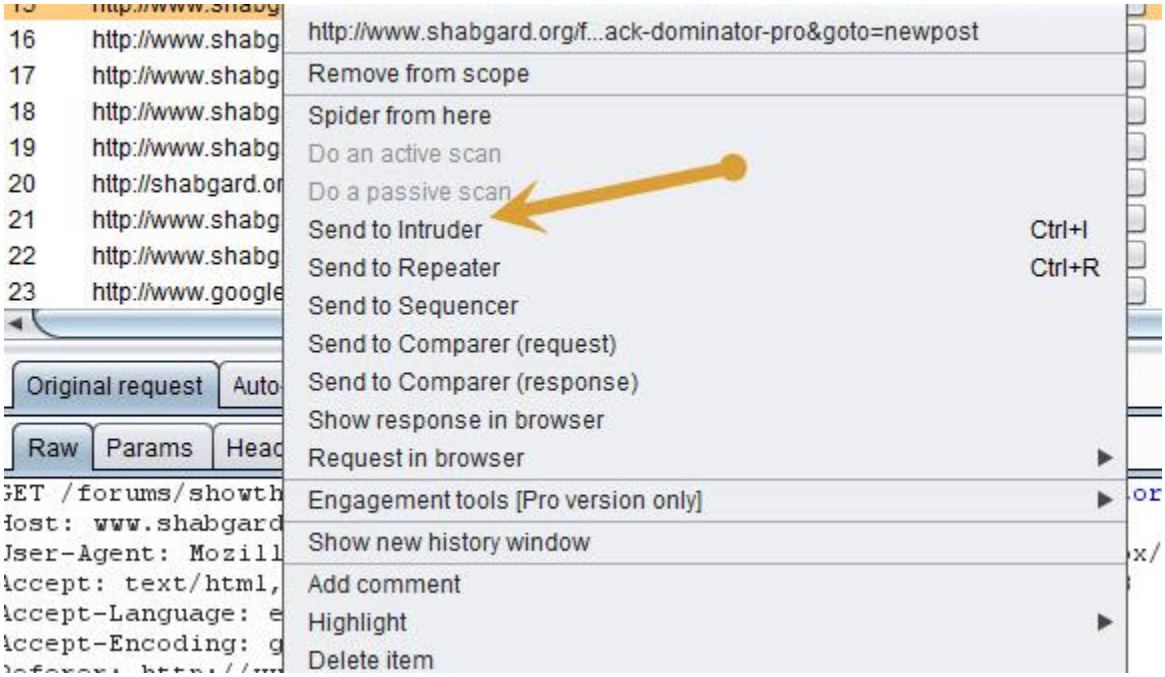
پس از انجام مراحل بالا و کلیک بر روی Ok باید یک فایل گزارش از نتیجه پویش ایجاد شده باشد. سپس می توانید با کلیک کردن بر روی فایل گزاری آن را در مرورگر باز کنید و گزارش را مورد مطالعه و بررسی قرار بدهید.

ویژگی چهارم؛ خودکار سازی حملات با Burp intruder

اگرچه ابزار Burp Scanner برای شناسایی خودکار ضعف های امنیتی بسیار مفید است، اما به شما اجازه نمی دهد الگوهای(Vector) حمله را برای هر درخواست، سفارشی سازی کنید. با این حال، در طی یادگیری فرآیند ارزیابی امنیت برنامه های تحت وب، درباره اساس امنیت آنها فهم دقیقی به دست خواهید آورد و انتظار خواهید داشت که بر روی هدفتان کنترل کامل داشته باشید. همچنین باید این نکته را هم در نظر بگیرید، پویشگر های امنیتی، ابزارهایی کامل و بی عیب در ارزیابی امنیت برنامه های تحت وب نیستند، لذا همیشه توصیعه می شود برای ارزیابی امنیت کامل برنامه های تحت وب به صورت دستی این کار انجام گیرد و در شرایط خاصی از ابزار های خودکار استفاده شود، یا حداقل بعد از انجام پویش با استفاده از ابزار های خودکار برای اطمینان بیشتر از امنیت سیستم، به صورت دستی هم برنامه مورد بررسی قرار گیرد.

ارزیابی امنیت یک برنامه تحت وب شامل بررسی کردن همه نقاط ورودی (پارامترهای GET/POST، کوکی ها، هدف ها و...) به همراه الگو های حمله می شود که در این فرآیند پاسخ سرور به آن درخواست ها برای شناسایی یک ضعف امنیتی خاص مورد بررسی قرار می گیرد. به عنوان مثال، اگر شما مشکوک هستید که یک نقطه پایانی از وب سایت مورد هدف شما دارای ضعف امنیتی SQL می باشد، باید برای شناسایی آن از درخواست های پیوسته به همراه الگوی های حمله متفاوتی (مثلا یک کوتیشن، یک کوتیشن به همراه یک پرانتز، اعداد منطقی و...) برای هر پارامتر استفاده کنید. این عملیات نیاز به زمان بسیاری برای انجام پذیری دارد، اما خوشبختانه در برنامه Burp Suite ابزاری با نام Burp Intruder وجود دارد که می تواند با سرعت بسیار بالایی این فرآیند را در مدت زمان محدودی برای شما انجام بدهد.

اولین گام استفاده از Burp Intruder شامل وارد کردن یک درخواست وب به درون این برنامه است. شما می توانید از تمامی قسمت های Burp Suite درخواست وب مدنظرتان را با استفاده از منوی متنی موجود در برنامه به این ابزار ارسال کنید. مثلا، اگر شما شروع به مرورکردن درخواست ها در تب history کنید، می توانید به سادگی با راست کلیک کردن بر روی یک آیتم خاص و انتخاب گزینه send to intruder آن را به ابزار intruder ارسال کنید. تب intruder برنامه Burp باید به سرعت به رنگ نارنجی در آید. به هر حال، چهار گام برای پیکربندی این ابزار قبل از اجرای حمله نیاز است که آنها را در زیر مورد بررسی قرار خواهیم داد.



وارد کردن یک درخواست به Burp Intruder

پیکربندی هدف

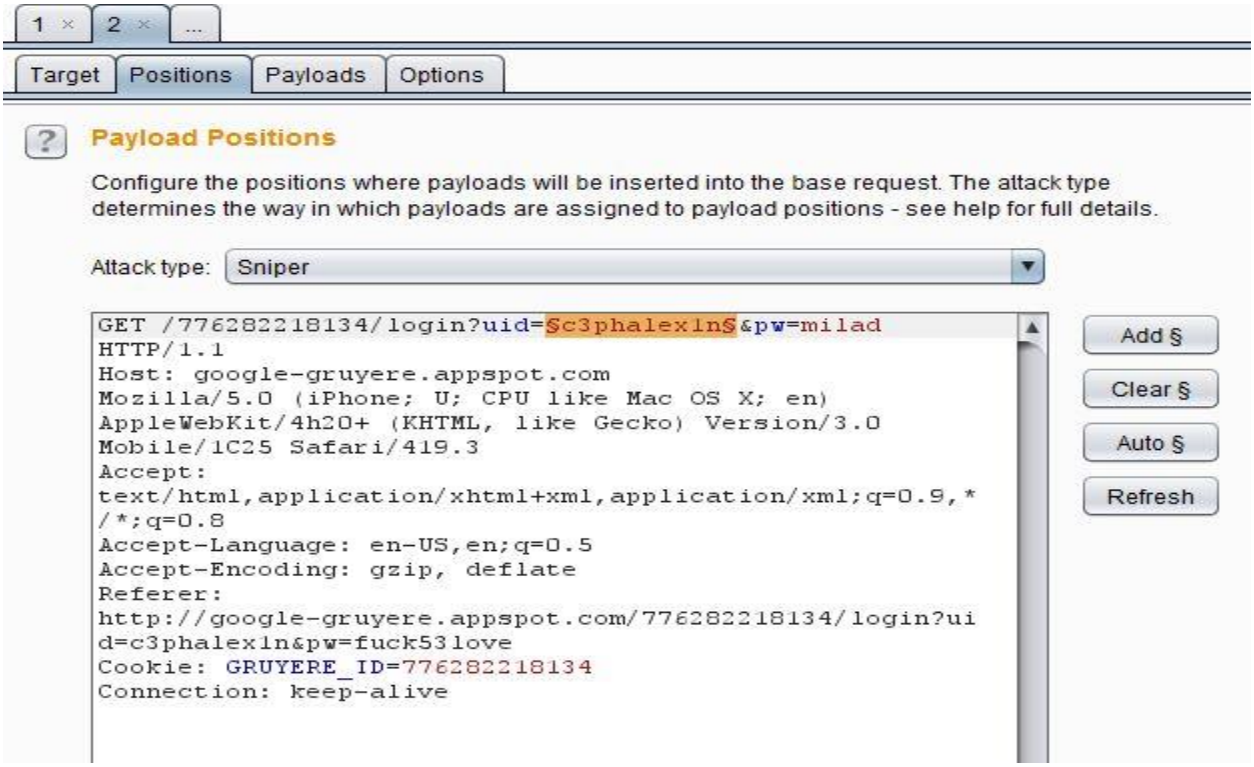
در ابزار Burp Intruder به تب Target بروید، در آنجا شما می توانید آدرس میزبان هدف و درگاه آن را مشخص سازید. در بیشتر حالات، در این تب نیاز به عوض کردن هیچ چیزی نیست، در نتیجه شما می توانید فقط دوباره محتویات آن را بررسی کنید و به تب بعد بروید.

نویسنده، میلاد کهساری الهادی : در این قسمت Position به موقعیت وPayload هم به پیلود ترجمه گشته است. با این حال اگر در قسمتی از این بخش دچار سوء فهم شدید می توانید به جای کلمه پارسی از اصل کلمه انگلیسی آن استفاده کنید.

پیکربندی نوع و موقعیت حمله

در تب positions شما نیاز به انتخاب کردن موقعیت پیلود به همراه تعریف یک الگو درخواست برای حمله دارید. در حالت پیش فرض، ابزار Burp Intruder به صورت خودکار مقدار تمامی پارامتر ها و کوکی ها را مشخص می کند. به هر حال، شما می توانید حمله را با اضافه کردن و حذف کردن موقعیت های گوناگون سفارشی سازی کنید. به عنوان مثال، بگذارید ببینیم چگونه می توانیم اولین پارامتر درخواست GET را انتخاب کنیم.

1. یک درخواست وب را از Burp Proxy به درون Burp Intruder وارد کنید که حداقل شامل یک پارامتر GET شود، به منظور انجام این کار کافیست بر روی یک آیتم کلیک راست کرده و از منوی متنی گزینه send to intruder را انتخاب کنید. مثلا هنگام استفاده از برنامه آسیب پذیر وب Google Gruyere شما می توانید از لینک درخواست Login به برنامه استفاده کنید. منظور از لینک همان نقطه پایانی (endpoint) است.
2. سپس در گام دوم در تب positions ابزار Burp Intruder بر روی دکمه clear کلیک کنید تا تمامی پارامتر های نشانه گذاری شده از حالت نشانه گذاری شده خارج شوند.
3. در گام سوم، موقعیت مکان نمای خود را قبل از اولین کاراکتر، مقدار پارامتر در Url قرار بدهید (به عنوان مثال، در آدرس رو به رو GET /<Your Gruyere Instance ID>/ login?uid=c3phalex1n&pw=milad مکانما باید میان کاراکتر = و c قرار بگیرد.
4. سپس بر روی add کلیک کنید.
5. در گام اخر مکانما را بعد از آخرین کاراکتر مقدار پارامتر قرار بدهید و دوباره بر روی add کلیک کنید، تا مقدار آن پارامتر انتخاب شود. همچنین، علاوه بر این روش شما می توانید با دو بار کلیک بر روی مقدار پارامتر و سپس کلیک کردن بر روی add آن را انتخاب کنید.



انتخاب موقعیت مقدار اولین پارامتر در Burp Scanner

در این قسمت ما توانستیم اولین نقطه ورودی خودمان را با موفقیت علامت گذاری کنیم. همچنین شما می توانید با کلیک کردن بر روی دکمه auto تمامی پارامتر های GET/POST و مقادیر کوکی های را انتخاب کنید.

در تب positions ابزار Burp Intruder شما همچنین لازم است یک نوع حمله مخصوص را با استفاده از منوی باز شو تعریف کنید. این تنظیمات روش اکتشافی مورد استفاده ابزار Burp Intruder را تعریف می کند که موقعیت انتخاب شده توسط شما را با پیلود های مخصوص حمله جایگزین می کند. شایان ذکرست برنامه Burp Intruder کمترین خطا را در شناسایی ضعف های امنیتی SQL دارد.

منوی باز شو دارای چهار نوع حمله می شود که هر کدام از آنها به یک شکل متفاوتی پیلود ها را برای شناسایی یک ضعف امنیتی مورد استفاده قرار می دهند. این چهار گزینه در زیر تشریح شده اند :

نویسنده، میلاد کهساری الهادی : در زیر بنده از کلمه موقعیت بسیار استفاده کرده ام که به نظرم لفظ ترجمه آن کمی گنگ و بعضا غیر مفید است. لذا به توضیح این نکته دقت داشته باشید، تا بتوانید متون زیر را بهتر درک کنید. به عنوان مثال، در قسمت زیر بنده می گویم (**تمامی موقعیت های انتخاب شده را با یک لیست از پیلودها از پیش تعریف شده جایگزین می کند**) در این متن، منظور بنده از موقعیت این است که در حملات تشخیص ضعف های امنیتی SQL، ما به جای اینکه مقدار یک پارامتر (مانند ?user=milad) را به سرور ارسال کنیم، به جای مقدار پارامتر یعنی کلمه milad از الگو های شناسایی خاصی (مانند تک کوتیشن ' یا اعداد منطقی مانند —1=1) استفاده می کنیم، در این قسمت این الگو ها در متن به پیلود ترجمه شده اند. لذا پس ترجمه اصلی روان متن تو پرانتز بدین شکل می شود (تمامی مقادیر پارامتر های انتخاب شده را با یک لیست از الگو های حمله از پیش تعریف شده جایگزین می کند) لذا به ذهن خود بسپارید که منظور نویسنده از موقعیت، مقدار پارامتر و از پیلود، الگو های شناسایی است.

1. **تیراندازی در خفا (Sniper) :** با استفاده از این نوع حمله شناسایی، برنامه Burp تمامی موقعیت های انتخاب شده را با لیستی از پیلودهای از پیش تعریف شده جایگزین می کند. در عمل، این گزینه تمامی پیلود ها را یکی پس از دیگری برای تمامی موقعیت ها بررسی می کند. همچنین این نوع حمله به شما اجازه می دهد تمامی ترکیبات پیلود ها و مقادیر اصلی درخواست ها را تغییر بدهید.

Request	Position	Payload
#1	1	Item_1_List_1
#2	1	Item_2_List_1
#3	2	Item_1_List_1
#4	2	Item_2_List_1

2. **دژکوب (battering ram) :** این نوع حمله مشابه نوع حمله شناسایی sniper است. این نوع حمله اکتشافی از یک لیست پیلود استفاده می کند. در این حالت، تمامی موقعیت های بطور مشابه با پیلود های مشابه ای جایگزین می شوند.

Request	Position	Payload
#1	1, 2	Item_1_List_1
#2	1, 2	Item_2_List_1

3. **نیزه دو شاخه (pitchfork) :** در این نوع حمله شناسایی، ابزار Burp Intruder از دو یا بیشتر از دو لیست پیلود مطابق با تعداد موقعیت های مشخص شده استفاده می کند.در این روش در طی اولین تکرار، Burp موقعیت های مشخص شده را با اولین پیلود لیست جایگزین می کند. به عبارتی دیگر، این نوع حمله از اولین پیلود موجود در لیست برای اولین موقعیت استفاده می کند.

Request	Position	Payload
#1	1, 2	Item_1_List_1, Item_1_List_2
#2	1, 2	Item_2_List_1, Item_2_List_2

4. **بمب خوشه ای (cluster bomb) :** این گزینه مشابه نوع pitchfork است. در این روش چندین لیست از پیلود ها برای اکتشاف ضعف امنیتی مورد استفاده قرار می گیرند. به هر حال، در این حالت، Burp Intruder تمامی ترکیبات ممکن را تکرار می کند.

Request	Position	Payload
#1	1, 2	Item_1_List_1, Item_1_List_2
#2	1, 2	Item_2_List_1, Item_1_List_2
#3	1, 2	Item_1_List_1, Item_2_List_2
#4	1, 2	Item_2_List_1, Item_2_List_2

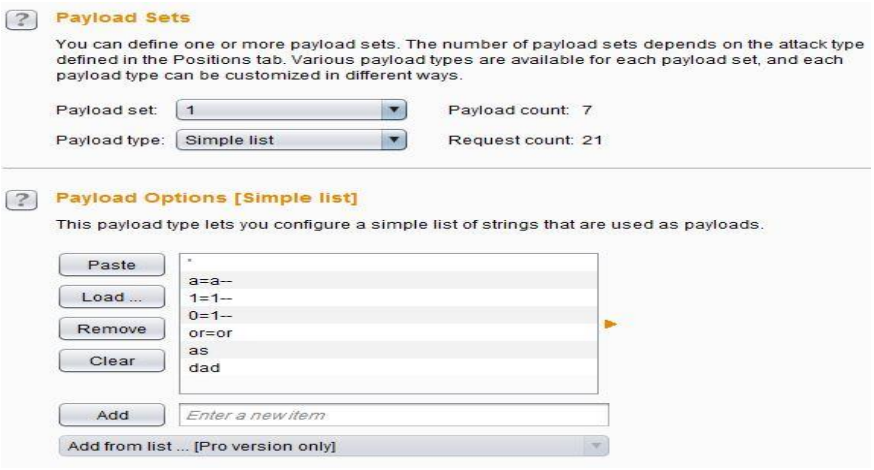
پیکربندی پیلود ها

بعد از انتخاب تمامی موقعیت ها و نوع حمله، تعریف نوع دقیق پیلودها نیاز است که تعریف شود. در تب پیلود(Payload) موجود در ابزار Burp Intruder تعریف یک لیست سفارشی از پیلود ها برای شما ممکن است. همچنین شایان ذکر است

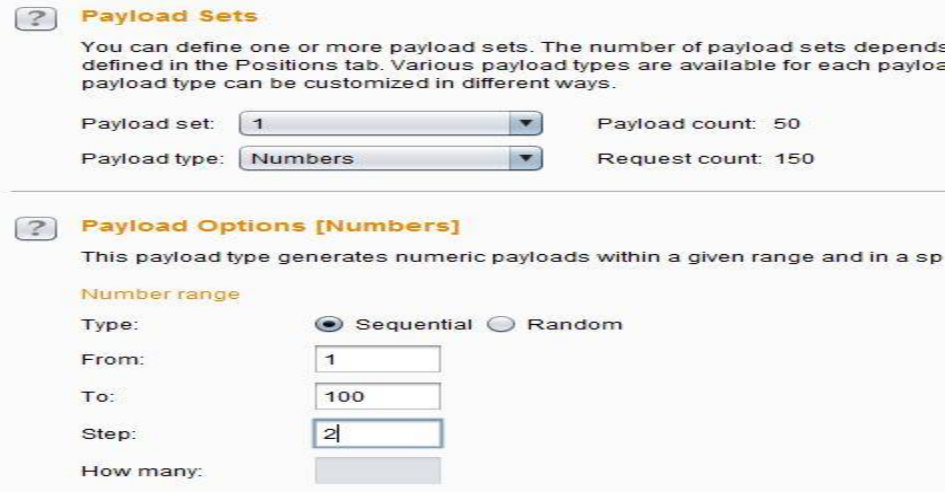
اینجا این نکته را دوباره گوش زد کنم که نویسنده کتاب در اینجا از پیلود های حمله اشاره به الگوی های حمله یا به عبارتی رشته هایی دارد که اگر در یک پارامتر آسیب پذیر تزریق شوند موجب شناسایی آن ضعف امنیتی می گردند.

همانطور که ذکر شد، برخی از حملات نیاز به بیش از یک لیست پیلود دارند. که بدین منظور شما می توانید از اولین منوی باز شوی موجود در قسمت Payload Set برای پیکربندی تعداد پیلود مورد استفاده در حمله شناسایی استفاده کنید. همچنین در منوی باز شو دومی شما می توانید نوع پیلود را مشخص سازید که برخی از آنها در زیر تشریح شده اند.

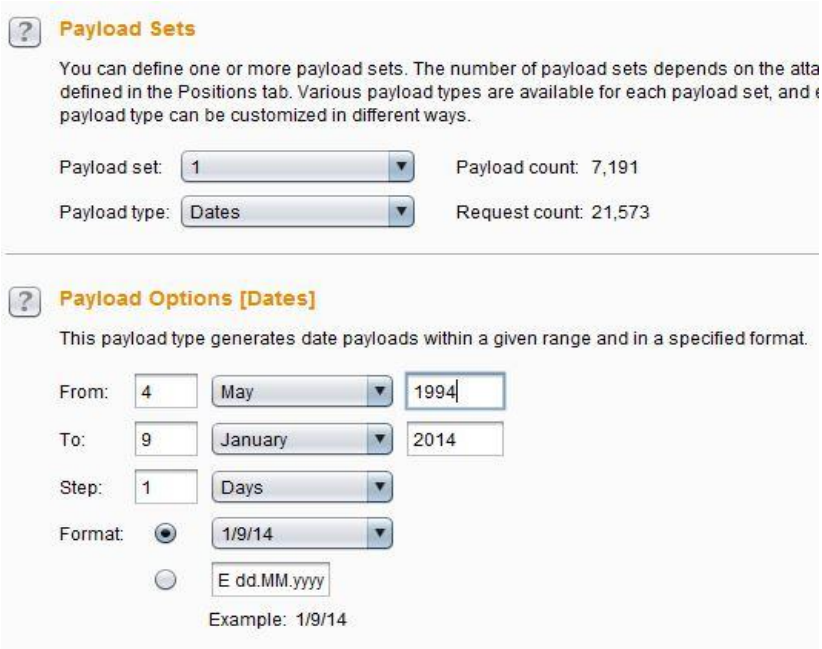
1. **Simple list :** با استفاده از این گزینه، کاربر می تواند یک لیست از الگو های شناسایی را از یک فایل متنی خارجی(.txt) به ابزار Burp Intruder وارد کند. همچنین شما می توانید بجای اینکه یک لیست وارد کنید با وارد کردن الگوهای حمله مد نظرتان در فیلد رو به روی دکمه Add آنها را به صورت مجزا به ابزار معرفی کنید.



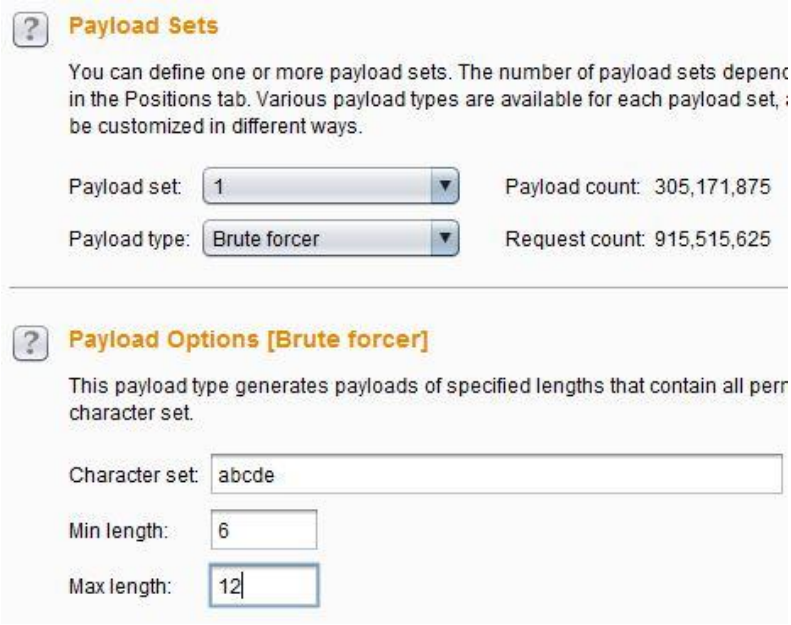
2. **Numbers :** با استفاده از یک لیست از اعداد، ابزار Burp Intruder به صورت خودکار اعداد را مبتنی بر یک پیکربندی خاص تولید می کند. همچنین در استفاده از این گزینه کاربر نیاز دارد عدد آغازین و پایانی و همچنین تعداد گام های این گزینه را تعریف کند.



3. **Dates :** با استفاده از این گزینه، ابزار Burp Intruder اجازه می دهد یک پیلود با قالب تاریخ به صورت خودکار با مقداری پیش فرض تا یک زمان مشخصی تولید کند.

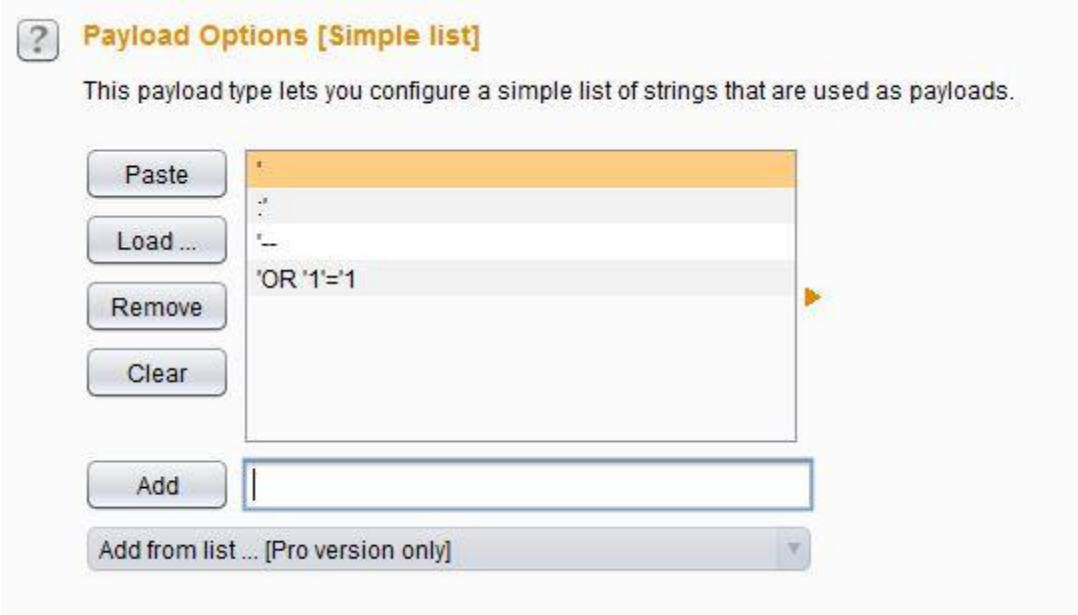


4. **Bruteforcer :** با انتخاب این گزینه، ابزار Burp Intruder می تواند از کاراکتر هایی که شما به قسمت تنظیمات آن وارد می کنید با طولی مشخص به صورت جایگشت پیلود تولید می کند.

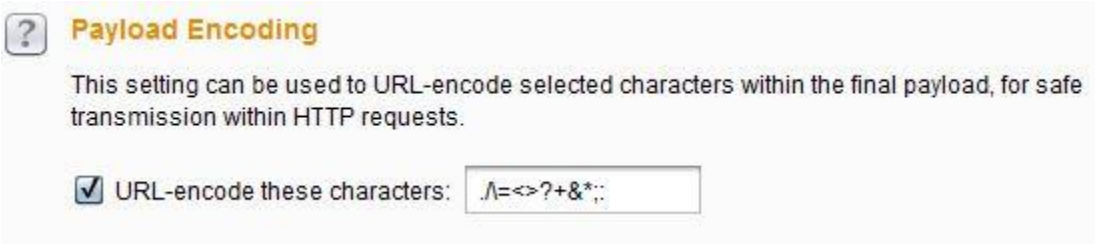


خب حال بگذارید برای درک بهتر این قمت یک لیست از الگو های شناسایی برای ضعف های امنیتی SQL ایجاد کنیم. بدین منظور گام های آورده شده در زیر را دنبال کنید.

1. در تب payloads ابزار burp intruder از اولین منوی باز شو که در آن تعداد پیلود های مورد استفاده در موقعیت های انتخاب شده توسط شما مشخص می شود عدد یک را وارد کرده و از منوی باز شو دومی نوع پیلود را Simple list انتخاب کنید.
2. در قسمت پایین، یعنی قسمت Payload Options الگوهای(پیلود ها) شناسایی مورد نظر خود را وارد کرده و بر روی Add کلیک کنید. به عنوان مثال، شما می توانید برای شروع یک تک کوتیشن به Intruder اضافه کنید. تک کوتیشن رایجترین رشته مورد استفاده برای شناسایی ضعف های امنیتی SQL می باشد که موجب به وجود آمدن وقفه در دیتابیس می شود.
3. به هر حال اضافه کردن رشته ها را تا جایی که می خواهید ادامه دهید. همچنین اگر به اشتباه رشته ای را به ابزار وارد کردید که بعد خواستید آنرا حدف کنید، به سادگی می توانید با انتخاب کردن آن از جدول و کلیک کردن بر روی دکمه Delete آن را از لیست حذف کنید.



همچنین در پایین تب payloads به قسمت Payload Encoding توجه کنید. در حالت پیش فرض، ابزار Burp Intruder به صورت خودکار تمامی کارکتر های مشخص شده در فیلد متنی این قسمت را در Url رمزنگاری می کند. به عنوان مثال، کاراکتر تک کوتیشن در URL با مقدار 27٪ جایگزین خواهد شد. با این حال، اگر شما می خواهید که این رمزنگاری صورت نگیرد کافیست که الگو مد نظر خودتان را از فیلد متنی این قسمت حذف کنید.

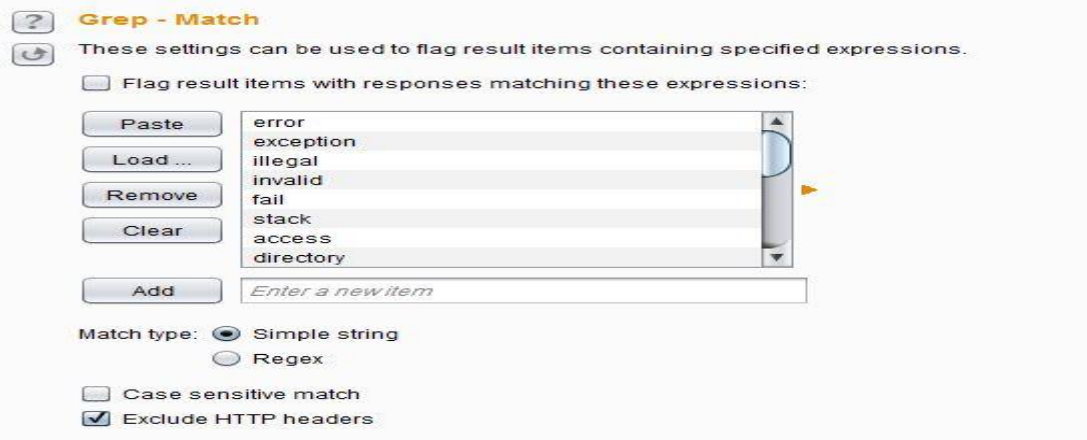


گزینه های اضافی Burp Intruder

ابزار Burp Intruder یک ابزار همه کاره است، در نتیجه باید گزینه های بسیاری برای پیکربندی داشته باشید. به هر حال شما باید خودتان بسیار تمرین کنید تا تمامی ویژگی هایی که این گزینه ها به شما ارائه می دهند را درک کنید. به عنوان مثال، در تب Options ابزار Burp Intruder شما می توانید تعداد ترد های مورد استفاده توسط ابزار را مشخص سازید.

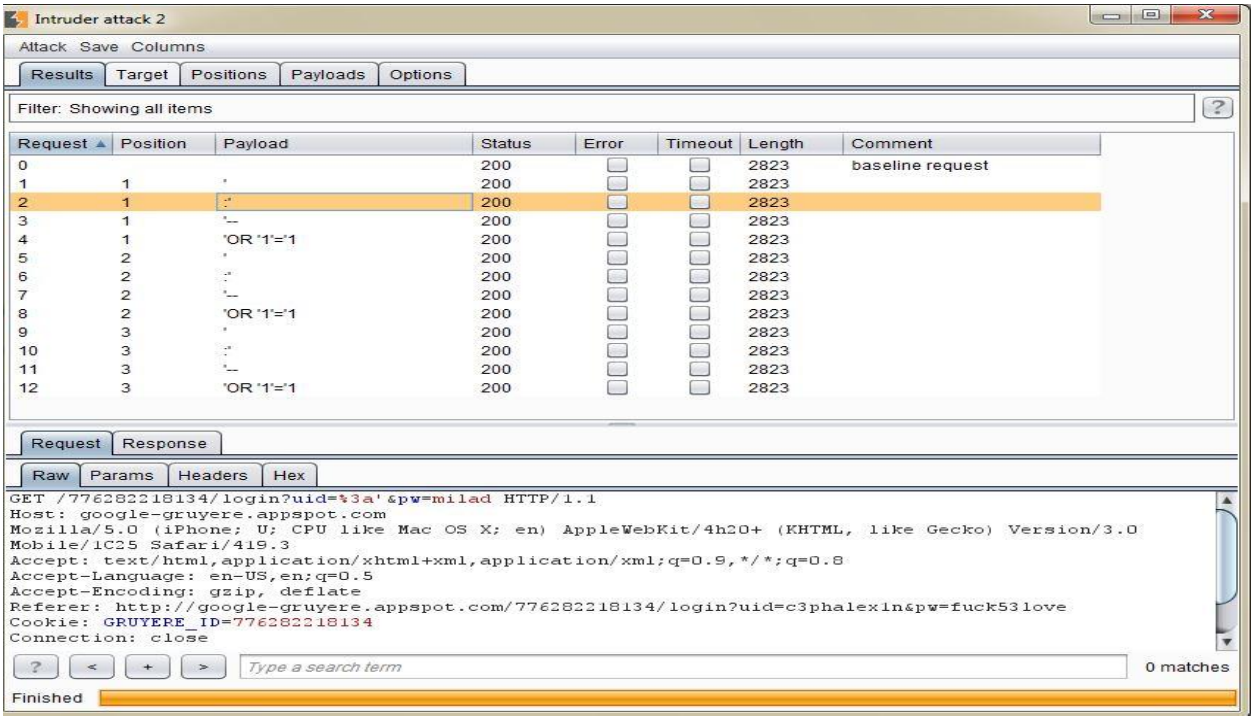
یکی دیگر از تنظیمات جالب موجود در Burp Intruder قسمت Grep است. با استفاده از این گزینه موجود، شما می توانید رشته یا عبارت های منظمی را مشخص سازید که ابزار آنها را در پاسخ های سرور به درخواست های ارسالی شما

مورد جستجو قرار بدهید. این گزینه در شناسایی وقفه ها و رشته های خطای عمومی که می توانند مشخص ساز ضعف های امنیتی باشند بسیار مفید است.



انجام یک حمله

حالا که همه چیز به درستی پیکربندی شده است، ما می توانیم یک حمله انجام بدهیم. بدین منظور از منوی بالایی موجود در Burp ابتدا به منو Intruder بروید و بر روی start attack کلیک کنید. پس از کلیک بر روی این گزینه، برنامه Burp ابتدا پیکربندی ها را بررسی کرده و یک هشدار نمایش می دهد. سپس یک پنجره باز کرده و شروع به انجام حمله می کند.



نویسنده، میلاد کهساری الهادی : به این نکته توجه داشته باشید، نسخه رایگان این برنامه، تمامی پیکربندی های پیشرفته موجود در برنامه را شامل نمی شود. و از همه مهم تر در نسخه رایگان این برنامه دارای یک سرعت محدود است.

با این حال شایان ذکر است، در طی انجام حمله، شما می توانید نتایج حمله را در پنجره results table مشاهده کنید. مطابق با پیکربندی برنامه، Burp جداول متفاوتی از جمله request ID، پیلود استفاده شده، وضعیت Http پاسخ وب، زمان پاسخگویی و ... را نشان خواهد داد. همچنین شما می توانید محتویات تمامی این جداول را ضبط و ذخیره کنید.

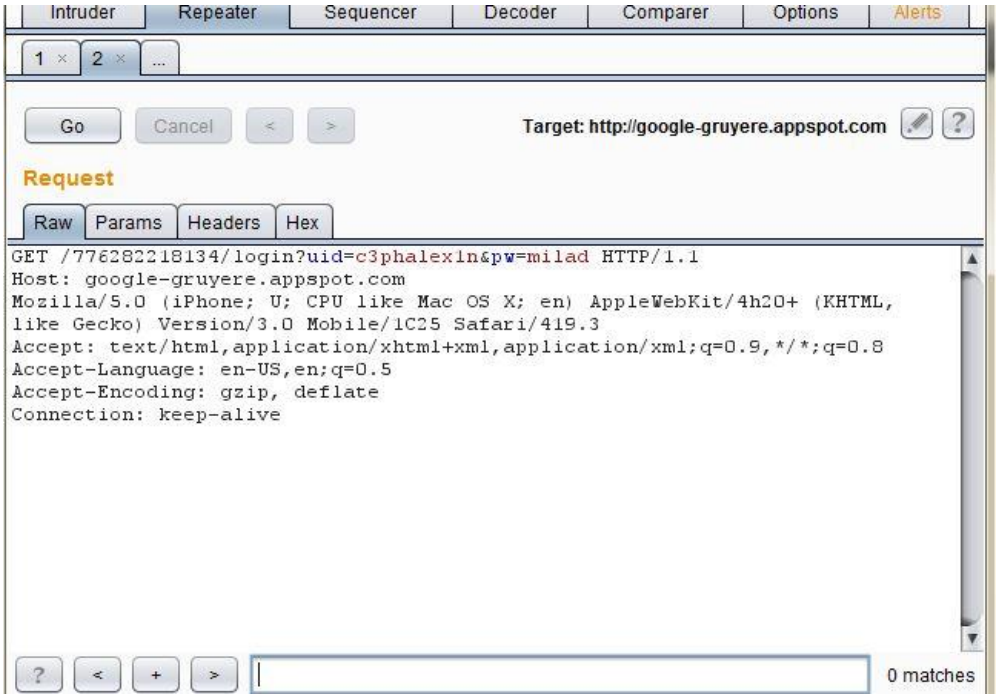
نویسنده، میلاد کهساری الهادی : کشف ضعف های امنیتی جدید کاملا به صبر و تلاش شما بستگی دارد. به محض اینکه شروع به ارزیابی امنیت برنامه های تحت وب کنید، خواهید فهمید که چگونه حداقل تغییرات در پاسخ به یک درخواست می تواند به شناسایی یک ضعف امنیتی کمک کند. با استناد به این موضوع، همیشه به اندازه و تفاوت وضعیت پاسخ های Http به تمامی درخواست های وب دقت کنید. همچنین استفاده از ویژگی grep به شما در شناسایی کردن باگ ها که در نتیجه درخواست ها پیام خطا صادر می کنند بسیار می تواند مفید واقع شود.

ویژگی پنجم؛ تغییر ایجاد کردن و تکرار کردن درخواست های وب با Burp Repeater

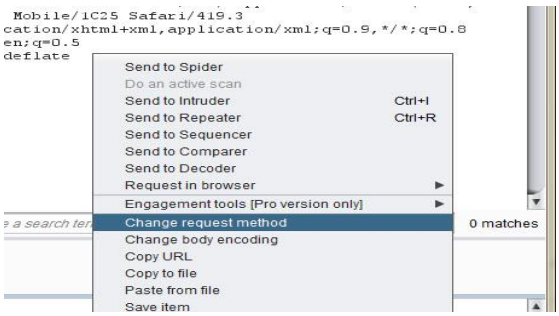
در قسمت قبل، ما مشاهده کردیم چگونه به صورت خودکار چندین درخواست با پیلود های متفاوت تولید کنیم. به هر حال در شرایطکی که شما به تازگی یک ضعف امنیتی کشف کرده اید یا می خواهید اطمینان حاصل کنید که یک نقطه پایانی ایمن است، باید یک درخواست وب را با الگو های حمله متفاوتی چندین بار تکرار کنید. این روش trial-and-error نامیده می شود که به صبر و تجربه نیازمند است.

خوشبختانه؛ ابزار Burp Repeater به شما اجازه می دهد تمامی جنبه های یک درخواست Http را تغییر داده و چندین بار آن را ارسال کنید. بدین منظور کافیست ابتدا یک درخواست وب را انتخاب کرده و با استفاده از منوی متنی آن را به این ابزار وارد کنید. به هر حال گام های زیر را دنبال کنید.

1. در گام اول؛ یک درخواست وب را انتخاب کنید و بر روی آن کلیک راست کرده، سپس از منوی متنی گزینه send to repeater را انتخاب کنید تا درخواست مورد نظرتان به ابزار Burp Repeater ارسال شود.
2. در گام دوم؛ به ابزار Burp Repeater بروید. شما باید در این پنجره محتویات کامل درخواست انتخاب شده خود را مشاهده کنید.

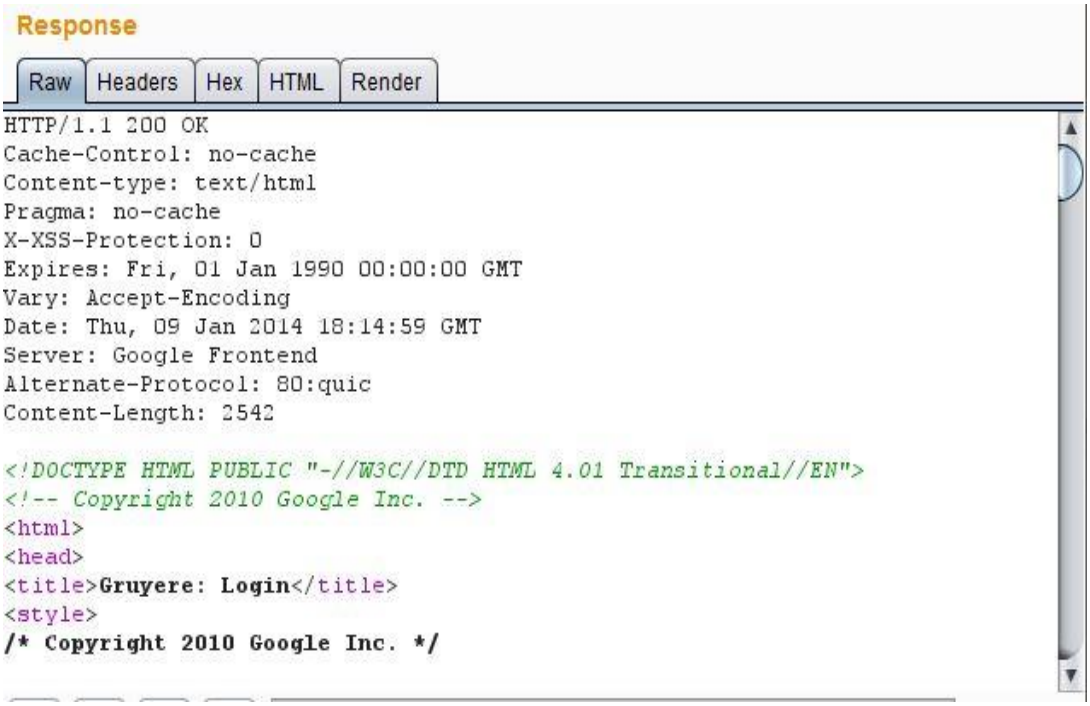


3. در گام سوم؛ شما می توانید هر کدام از جنبه های درخواست را که می خواهید تغییر بدهید. به عنوان مثال بگذارید در این قسمت یک درخواست GET را به POST تغییر بدهیم. بدین منظور کافیست در پنجره request کلیک راست کرده و سپس گزینه change request method را انتخاب کنید.



4. همچنین اجازه بدهید یک پارامتر تقلبی با رشته &debug=true در پایان رشته Url بیفزایم.

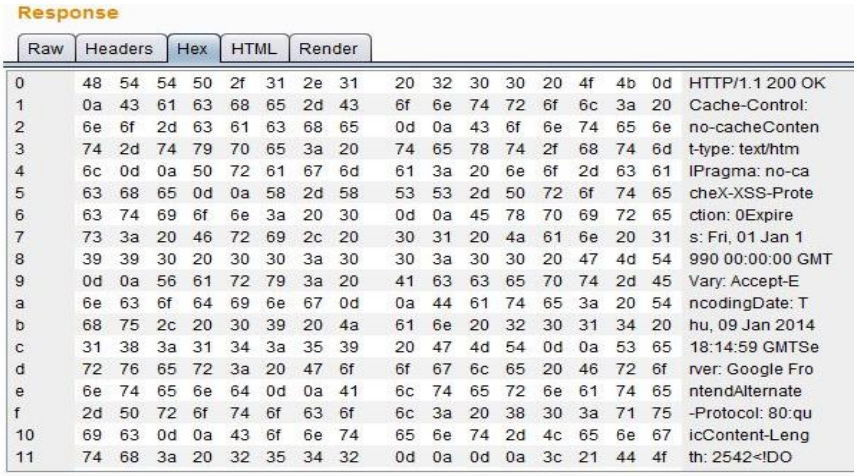
5. در پایان، بر روی go کلیک کنید تا درخواست ارسال شود. پس از چند ثانیه باید ابزار Burp Repeater قادر به نمایش دادن پاسخ به درخواست ارسالی شما باشد. در حالت معمول، شما می توانید محتویات خام پاسخ را در قسمت Response در تب Raw مشاهده کنید، همچنین در تب های دیگر می توانید پارامتر ها و هدرها، کد HTML صفحه وب هدف را مشاهده کنید و حتی می توانید از قسمت render صفحه وب سایت هدفتان را مشاهده کنید.



محتویات خام پاسخ ارائه شده به درخواست ارسالی

محتویات صفحه HTML هدف

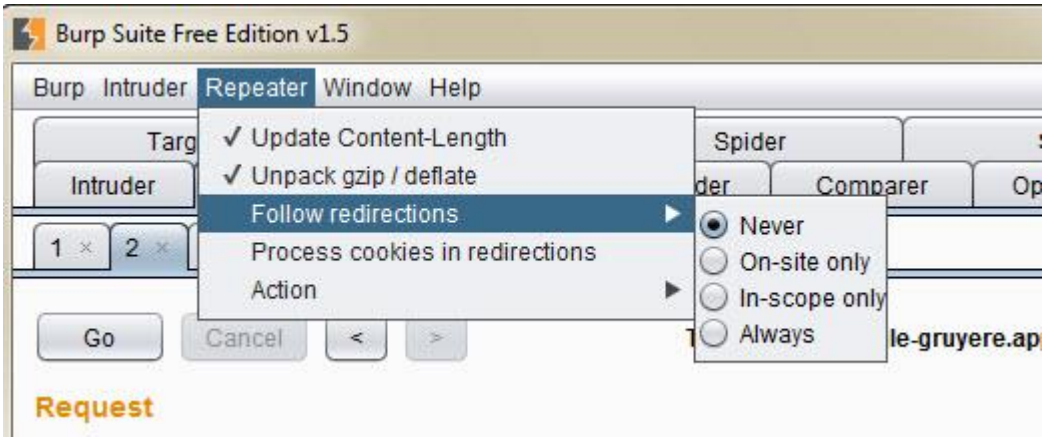
سرآیند های پاسخ ارائه شده به درخواست ارسالی



محتویات پاسخ ارائه شده به درخواست در قالب هکسادسیمال

گرچه به نظر می رسد ابزار Burp Intruder یک ابزار فوق العاده ساده باشد، اما او واقعا یک ابزار مفید و بسیار کاربردی است.

اگر شما بر روی منوی repeater کلیک کنید، می توانید لیست ویژگی های موجود در آن را مشاهده کنید.



در گزینه های نمایش داده شده در تصویر بالا، با زدن checkbox گزینه update Content-Length اجازه داده می شود فیلد هدر درخواست Http به صورت پویا به روز رسانی شود. در این روش، ابزار Burp Intruder به صورت خودکار اندازه درخواست های تغییر داده شده را قبل از ارسال محاسبه می کند.

انتخاب کردن گزینه follow redirects اجازه می دهد ابزار Burp repeater پاسخ های وب واقعی را نمایش دهد یا بجای آنها همه تغییر مسیر ها (302 Redirect status code) را دنبال کند و صفحه اصلی را نمایش دهد. با انتخاب checkbox گزینه process cookies in redirects، اضافه کردن عملیات به توکن های جلسه درخواست در طی تغیر مسیر برنامه امکان پذیر می شود.

در پایان، ابزار Burp Repeater اجازه می دهد به صورت دستی تب هایی را ایجاد، حذف و تغییر نام دهید. به عنوان مثال، اگر شما یک ضعف امنیتی کشف کردید و خواستید که یک اکسپلویت برای آن ایجاد کنید، می توانید با ایجاد کردن یک تب جدید و دادن یک نام با معنا به آن تب آن را از مابقی تب های موجود جدا کنید.

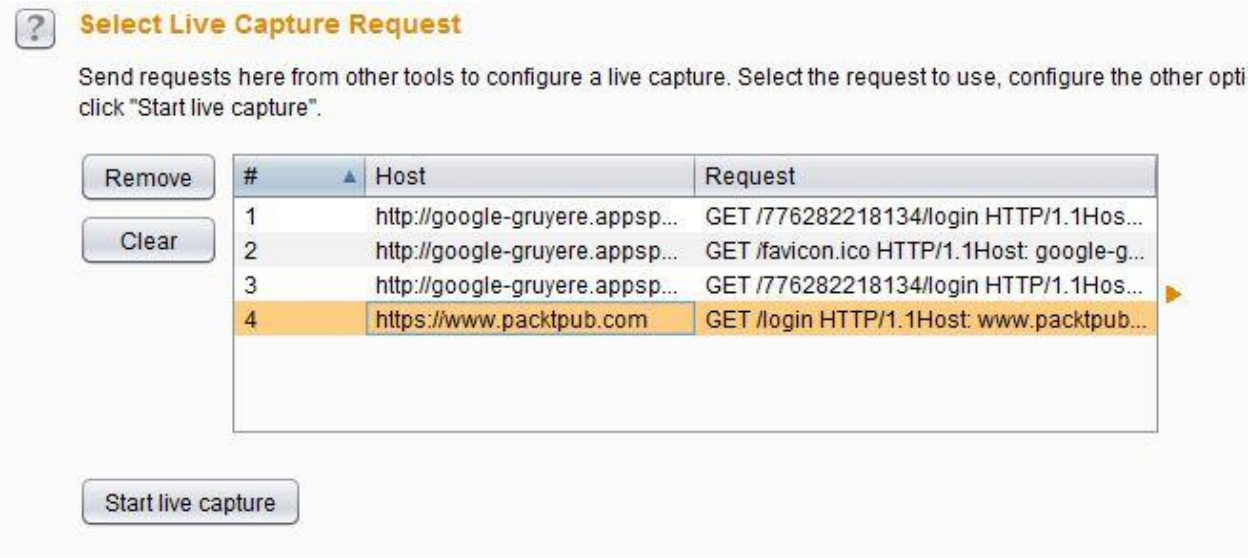
همچنین اگر شما در حال تجزیه و تحلیل کردن ضعف های امنیتی Cross-Site Request Forgery (CSRF) هستید یا حملات XSS را توسعه می دهید، می توانید با راست کلیک کردن بر روی درخواست هدف مدنظرتان و انتخاب کردن گزینه generates CSRF PoC از قسمت engagement tools می توانید برای آن ضعف امنیتی یک POC تولید کنید. این ویژگی به شما اجازه می دهد یک صفحه HTML ایجاد کنید که دارای آسیب پذیری هدف شما باشد. البته شایان ذکر است این ویژگی در نسخه Pro این برنامه وجود دارد.

ویژگی ششم؛ تجزیه و تحلیل کردن تصادفی داده های برنامه با Burp Sequencer

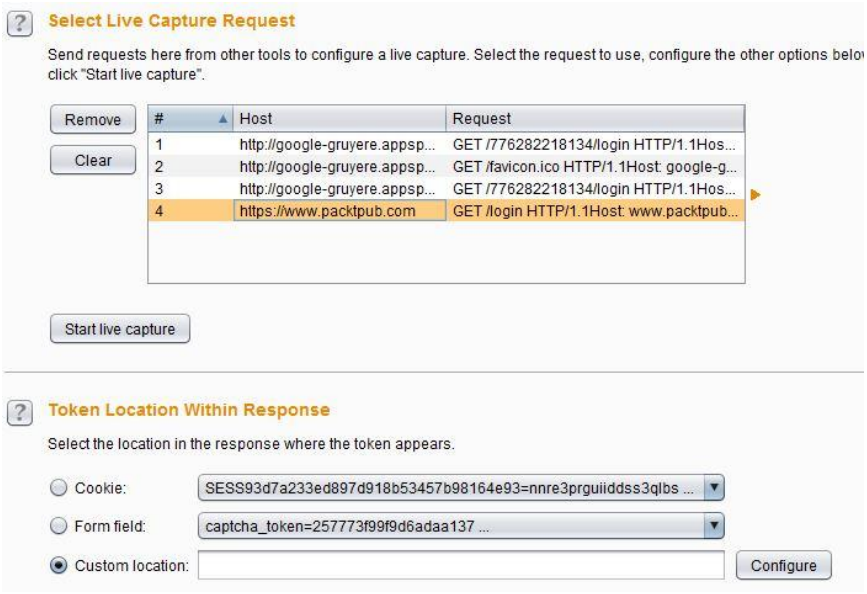
ابزار Burp Sequencer به شما اجازه می دهد تا داده های پیش بینی شده برنامه از جمله کوکی های نشست و توکن های anti-CSRF را تجزیه و تحلیل کنید. این ابزار به شما اجازه می دهد به سادگی داده ها را جمع آوری کرده و تحلیل کنید. به هر حال بگذارید کاربرد این ابزار را در یک محیط واقعی نشان دهیم.

1. پس از پیکربندی Burp Proxy، به صفحه https://www.packtpub.com/login بروید.
2. در تب history ابزار Burp Proxy آیتم درخواست login را انتخاب کرده و بر روی آن کلیک راست کنید، سپس از منوی متنی گزینه send to intruder را انتخاب کنید.
3. خب ما در مرحله قبل توانستیم با موفقیت یک درخواست را به Burp Sequencer وارد کنیم، حال که یک درخواست را به آن وارد کردیم می توانیم این ابزار را راه اندازی کنیم. پس از اینکه درخواست های وبی را به این ابزار وارد کردید باید آن درخواست ها را در قسمت Select Live Capture Request مشاهده کنید. شایان ذکر است، در این

قسمت ما یک درخواست به این ابزار وارد کردیم، که در حالت پیش فرض توسط ابزار انتخاب می شود، با این حال اگر انتخاب نشده است بر روی آن کلیک کنید تا به حالت انتخاب در آید.

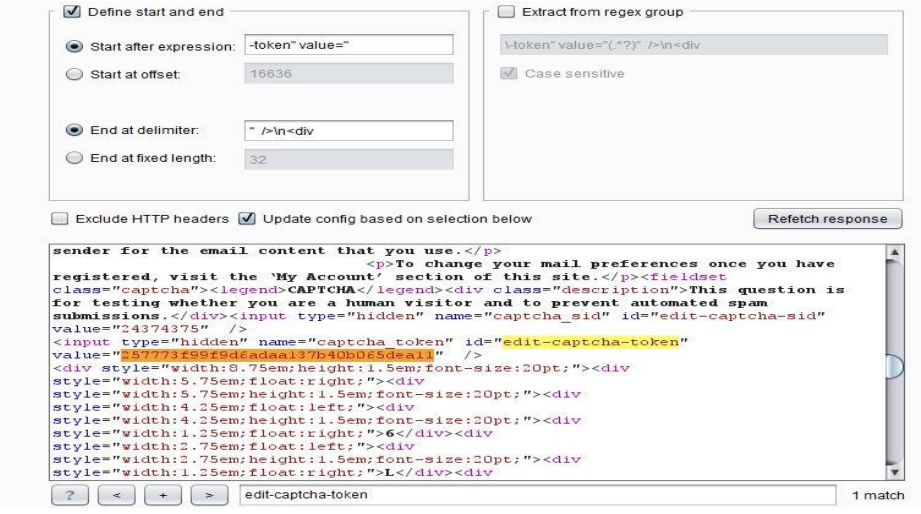


4. سپس در قسمت Token Location Within Response در تب Live Capture نیاز است که چگونگی شناسایی توکن ها و دیگر داده ها که ما می خواهیم آنها را درون صفحه پاسخ ارائه شده مورد تحلیل قرار بدهیم را پیکربندی کنیم. با این حال، به منظور سرعت بخشیدن به این فرآیند، در منوی باز شو form field و cookie، ابزار Burp Sequencer تمامی کوکی ها یا پارامتر های حاضر در صفحه پاسخ را نمایش خواهد داد.

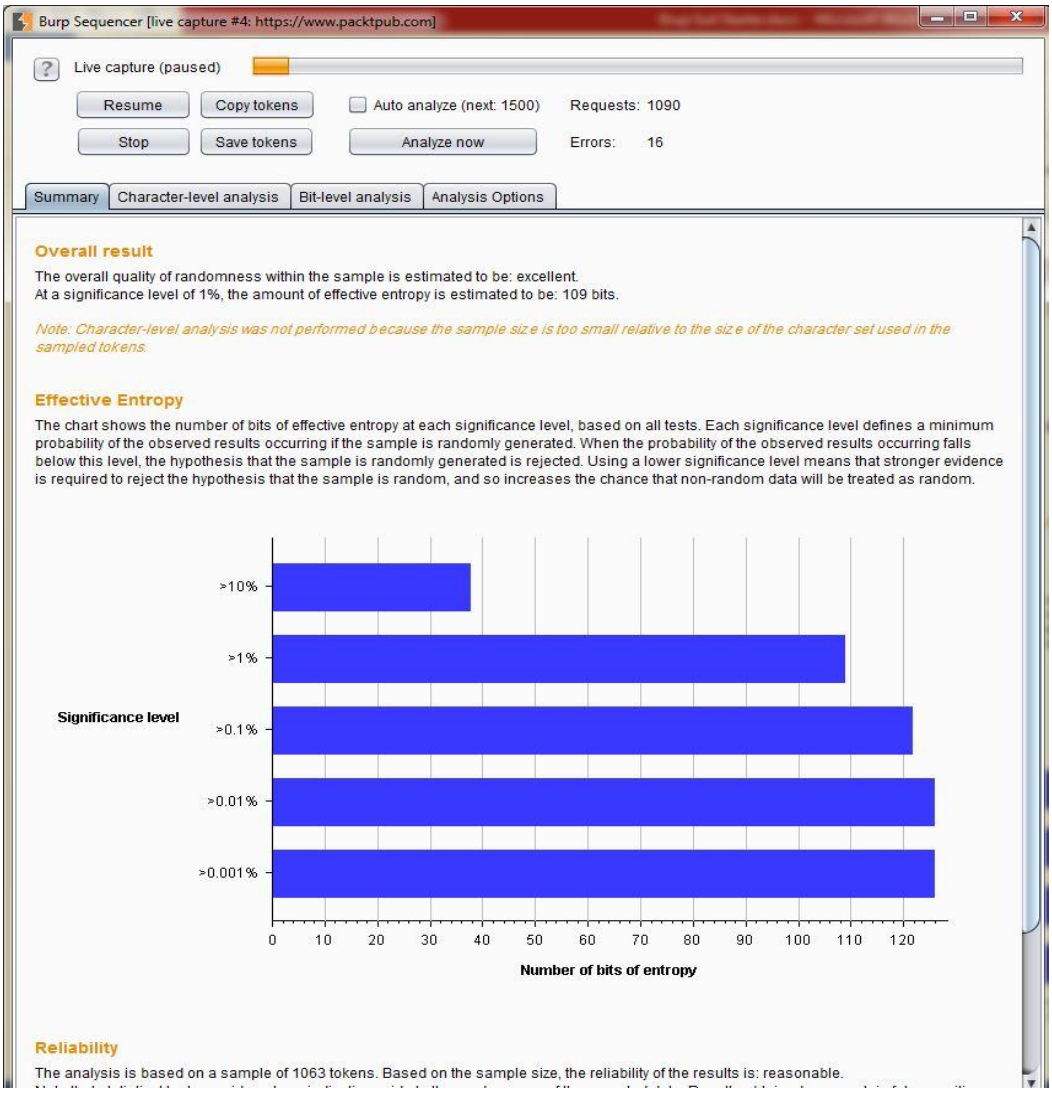


5. در گام بعد Custom Location را انتخاب کرده و بر روی Configure کلیک کنید. سپس در پنجره جدیدی که باز می شود به دنبال edit-captcha-token بگردید. این توکن خاص برنامه وب تحت تجزیه و تحلیل است. به منظور پیدا کردن این توکن می توانید از فیلد جستجو موجود در ابزار استفاده کنید.

6. همانطور که مشاهده می کنید، مقدار عنصر edit-captcha-token شامل یک توکن شبه تصادفی شده است. حال بگذارید به بررسی آنتروپی (واحد اندازه‌گیری در ترمودینامیک است که برای مقیاس های کوچیک استفاده می شود) این رشته بپردازیم. به هر حال، ابتدا تمام رشته را انتخاب کنید. پس از انتخاب کردن آن رشته Burp Sequencer به صورت خودکار فیلد های متنی start after expression و End at delimiter رو پر می کند. در عمل، این ابزار کمک به شناسایی کردن محدوده ای می کند که می تواند برای استخراج توکن از صفحه پاسخ مورد استفاده قرار گیرد.



7. هنگامی که گام های بالا را انجام دادید بر روی Start live capture کلیک کنید تا برنامه شروع به جمع آوری نمونه ها کند. ابزار Burp Sequencer درخواست های مشابه را چندین بار تکرار می کند و به صورت خودکار گزینه های تعریف شده را از صفحه استخراج می کند. همچنین این ابزار یک پنجره جدید برای مانیتور کردن عملیات برای شما باز خواهد کرد.
8. بعد از جمع آوری داده ها به اندازه کافی، حداقل 100 نمونه، توقف فرآیند بازیابی نمونه ها با کلیک کردن بر روی دکمه Puase ممکن است. همچنین توجه کنید که دکمه analyze now فعال باشد. بر روی آن کلیک کنید تا شروع به تحلیل داده ها دریافت شده کند. تصویر زیر یک ترافیک متوقف و تحلیل شده را نمایش می دهد.



پس از چند ثانیه، ابزار Burp Sequencer باید قادر به نمایش دادن نتایج باشد. اگر شما می خواهید داده های جمع آوری شده را بررسی کنید بر روی دکمه copy tokens کلیک کرده و محتویات آن را در یک ویرایشگر متن paste کنید. همچنین اگر متعوجه شدید که به اندازه کافی اطلاعات و داده جمع آوری نکرده اید به راحتی می توانید با کلیک کردن بر روی دکمه resume فرآیند جمع آوری را ادامه دهید.

شایان ذکر است ابزار Burp Sequncer نتایج بدست آورده خود را در قسمت نمایش می دهد.

1. **تب summary**
2. **تب character-level analysis**
3. **تب bit-level analysis**

تب summary یک مرورکلی از نتایج تحلیل ارائه می دهد. معمولا این پنجره برای فهمیدن اینکه آیا توکن شبیه تصادفی بوده است یا خیر کافیست. در مثال ما، ابزار Burp Sequncer پیام زیر را گزارش داده است.

The overall quality of randomness within the sample is estimated to be: excellent

همچنین این تب یک ارزیابی از قابل اعتماد بودن تحلیل مبتنی بر تعداد نمونه های جمع آوری شده ارائه می دهد. به عنوان مثال، نتیجه ارزیابی تصادفی یک توکن غیر شبه تصادفی، در پیام خطای زیر ارائه شده است.

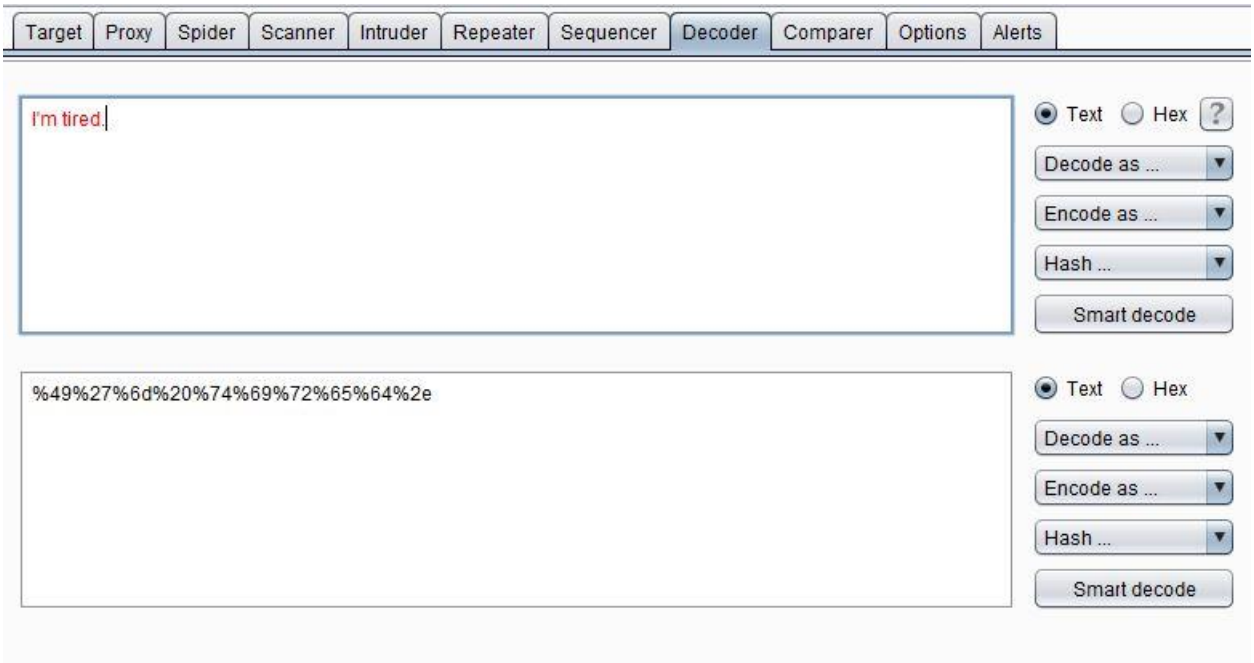
The overall quality of randomness within the sample is estimated to be: extremely poor

در حالت معمول، ابزار Burp Sequncer یک براورد کلی اتفاقی ارائه می دهد. گرچه نتایج اغلب صحیح هستند، اما با این تفاصیر این ابزار همیشه قابل اعتماد نیست. همچنین شایان ذکر است، کاربران پیشرفته می توانند از ویژگی بررسی کردن character-level و bit-level برای فهمیدن داده های پیش بینی شده استفاده کنند. شایان ذکر است، تب character-level analysis شامل چندین دیاگرام و جدول مقایسی برای تفهیم صحت میان کاراکتر ها، موقعیت ها و انتقال کاراکتر ها درون توکن ها می شود و تب bit-level analysis عملا برای شناسایی آنومالی مفید است.

ویژگی هفتم؛ رمزگشایی و رمزنگاری داده ها با Burp Decoder

ابزار Burp Decoder یک ابزار ساده است اما برای رمزنگاری و رمزگشایی رشته ها با چندین قالب بسیار مفید است. در طی ارزیابی امنیت یک برنامه تحت وب، نیاز به ارزیابی کردن قدرت مکانیزم های امنیتی اعتبار سنجی ورودی ها است. رمزنگاری رشته ها در چندین قالب یک روش خیلی رایج برای دور زدن کنترل های امنیتی و فیلتر ها است. به هر حال، هر از جای این ابزاز شما می توانید درخواست یا پاسخی را با استفاده از منوی متنی استاندارد به این ابزار وارد کنید. گام های زیر را دنبال کنید .

1. یک رشته را با مکانما انتخاب کنید و بر روی آن کلیک راست کرده و از منوی متنی گزینه send to decoder را انتخاب کنید.
2. هنگامی که رشته به این ابزار وارد شد رمزگشایی و رمزنگاری رشته با انتخاب قالب مدنظرتان از منو های decode as و encode as ممکن خواهد بود. علاوه بر این، ابزار Burp Decoder اجازه می دهد از قسمت ...Hash رشته ها را با توابع هش کننده رایج مانند MD2, MD5، SHA، SHA256 و SHA512 رمزنگاری و رمزگشایی کنید.



همچنین شما می توانید با استفاده از دکمه smart decode، محتویات یک رشته را با یک قالب مناسب رمزنگاری کنید. گرچه روش هوشمند همیشه نتایج درستی را تولید نمی کند اما با این حال این گزینه می توانید در طی شناسایی محتویات مبهم سازی شده بسیار مفید واقع شود.

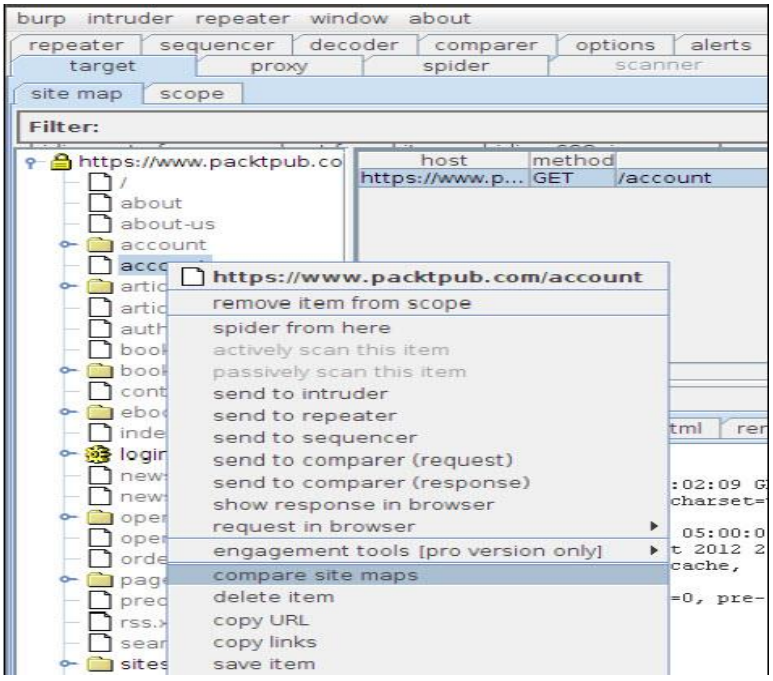
ویژگی هشتم؛ مقایسه کردن نقشه وب سایت ها

پوشاندن ضعف های امنیتی کنترل دسترسی کاربران در برنامه های بزرگ یک کار بسیار سخت و دشوار است. به همین دلیل ویژگی در برنامه Burp تعریف شده است که از آن می توانید برای شناسایی این ضعف های امنیتی استفاده کنید.این ویژگی در برنامه Burp با نام compare site maps یا مقایسه نقشه وب سایت ها شناخته می شود. این ویژگی در برنامه Burp Suite اجازه می دهد نقشه دو وب سایت را با هم مقایسه کرده و تفاوت های آن ها را با هم دیگر بررسی کنید، البته شایان ذکر است برنامه به صورت خودکار تفاوت ها را مشخص می سازد. با این حال، به طور خلاصه این ویژگی یک راه ساده برای مرور نقشه منابع تحت وب هدف با استفاده از حساب های کاربری با سطوح دسترسی مختلف را ارائه می دهد.

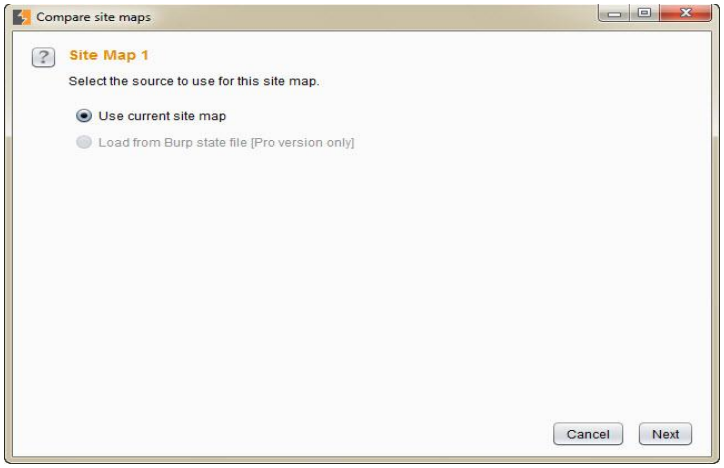
به عنوان مثال، شما می توانید برنامه تحت وب را با یک حساب کاربری استاندارد مرور کرده و سپس تمامی درخواست ها را با استفاده از یک کاربر با سطح دسترسی مدیریت تکرار کنید. این روش به مشخص ساختن باگ های سطح دسترسی کمک کند، به طور معمول به این روش بالا بردن سطح دسترسی به صورت عمودی گویند. همچنین شما می توانید برنامه تحت وب هدفتان را با حساب های کاربری مشابه مرور کرده و کنترل های دسترسی به منابع را بررسی کنید.

این ویژگی هم در نسخه Free هم نسخه Pro برنامه Burp Suite وجود دارد. به هر حال بگذارید از این ویژگی استفاده کنیم و آن را مورد بررسی قرار بدهیم. در طی این تمرین، ما می خواهیم بررسی کنیم که یک نقطه پایانی برنامه تحت وب فقط برای کاربر اهراز هویت شده موجود است یا خیر:

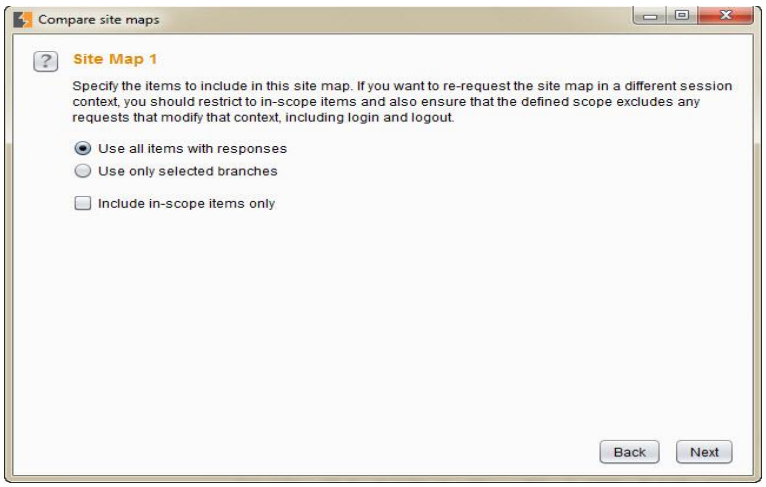
1. پس از پیکربندی Burp Proxy، به لینک https://www.packtpub.com/login بروید. سپس با حساب کاربری خود به آن وارد شود. به این نکته هم توجه کنید، منابع یا محتویات صفحه کاربری شما فقط برای حساب کاربری که با آن به برنامه اهراز هویت شده اید موجود است. و اگر از حساب کاربری خود خارج شوید دیگر نمی توانید به آن منابع دست پیدا کنید.
2. در گام بعد، در تب site map ابزار Burp Proxy به دنبال نقطه پایانی account باشید.
3. همانطور که در تصویر آورده شده در زیر نمایش داده شده است، بر روی آن کلیک راست کرده و گزینه compare site maps را انتخاب کنید. همچنین اطمینان حاصل کنید که فقط آیتم account را انتخاب کرده اید.



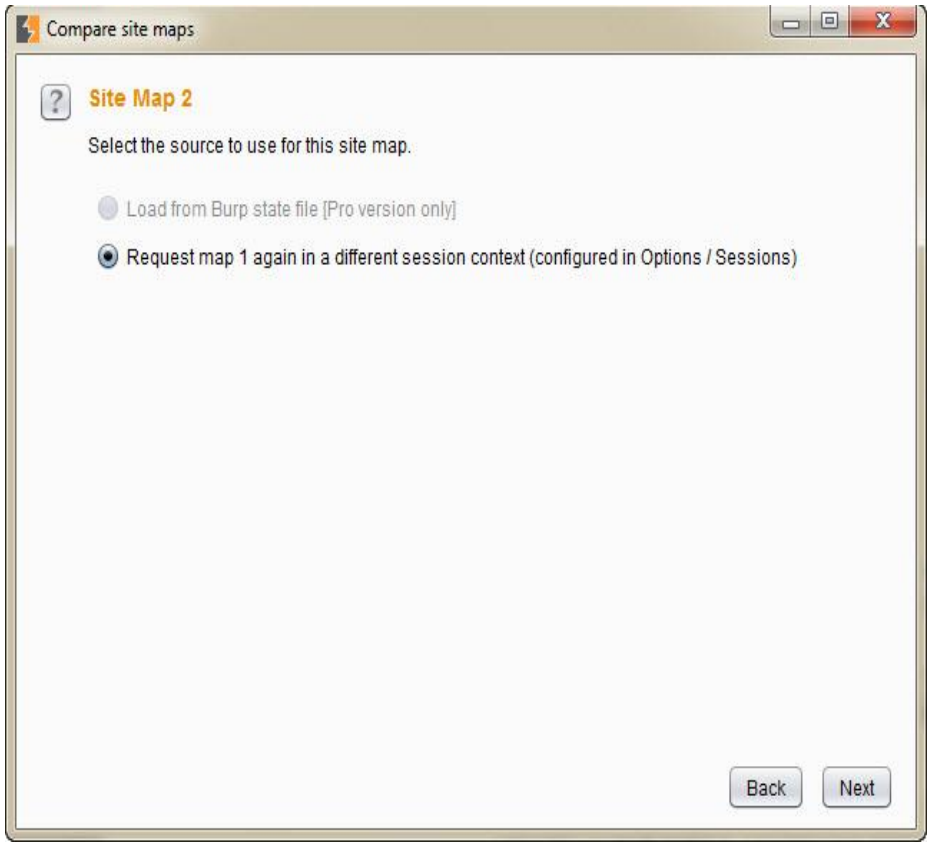
4. پس از انتخاب گزینه compare site maps، برنامه Burp یک پنجره ویزارد باز خواهد کرد. در این قسمت، اولین گام شامل تعریف کردن نقشه سایت اولی می شود. از این نقشه سایت به عنوان یک منبع پایه برای مقایسه ما استفاده می شود. اگر شما از نسخه Free برنامه Burp Suite استفاده می کنید فقط گزینه use current site map برای شما وجود خواهد داشت. آن را انتخاب کنید و بر روی next کلیک کنید.



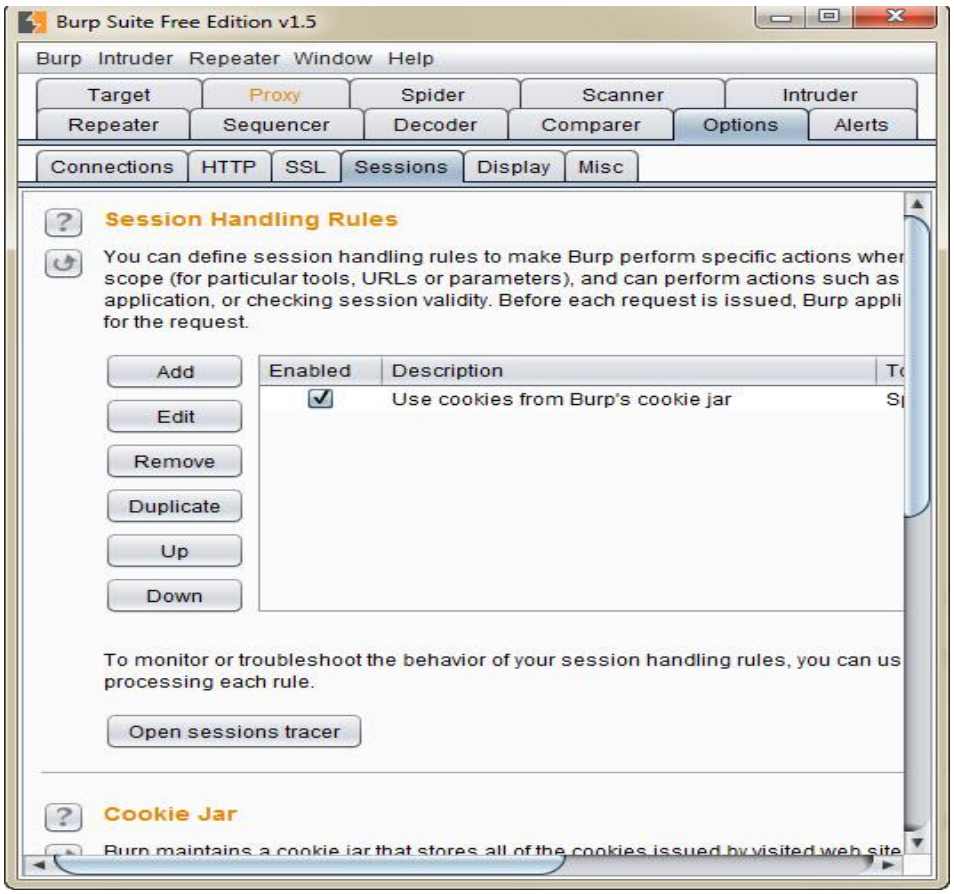
5. در گام دوم، شما باید آیتم های مشخصی را برای مقایسه انتخاب کنید. به عنوان مثال با انتخاب گزینه use only selected branches شما ویژگی مقایسه نقشه وب سایت ها را برای یک نقطه پایانی محدود می کنید. همچنین ممکن است در هنگام بررسی کردن برنامه هدفتان، بخواهید تمامی نقاط پایانی را مقایسه کنید بدین منظور کافیست گزینه use all items with responses را برای ارزیابی انتخاب کنید. همچنین، شما ممکن است بخواهید سایت های موجود در in-scope ابزار Burp را برای مقایسه انتخاب کنید، بدین منظور می توانید گزینه include in-scope items only را انتخاب کنید و بر روی next کلیک کنید.



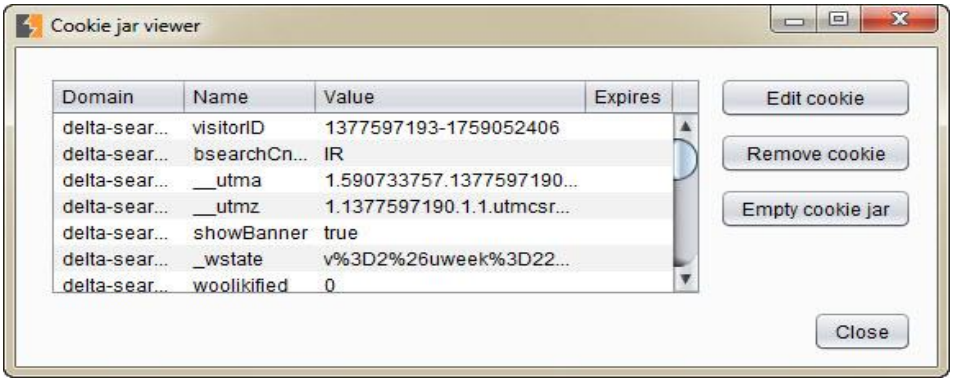
6. در گام سوم، شما باید نقشه سایت دوم را مشخص سازید. همچنین شایان ذکر است؛ اگر شما از نسخه Free این برنامه استفاده می کنید گزینه request map 1 again in a different session context فقط برای شما موجود خواهد بود. آن را انتخاب کنید و بر روی Next کلیک کنید.



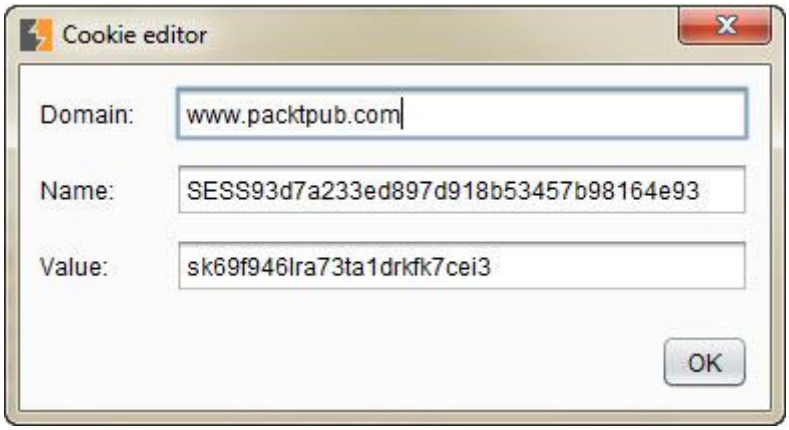
7. برنامه Burp از اولین نشست برای دسترسی گرفتن به تمامی منابع تعریف شده در قسمت site map 1 استفاده خواهد کرد. در طی این تمرین، ما می خواهیم بررسی کنیم که آیا نقطه پایانی مد نظر ما فقط برای حساب های کاربری اهراز هویت شده موجود است یا خیر.
8. در گام های قبلی، ما نقطه پایانی حساب کاربری را با یک کاربر اهراز هویت شده ضبط کردیم. در این نقطه، ما نیاز داریم کوکی های خودمان را باطل کنیم و از یک نشست جدید برای site map 2 استفاده کنیم. به هر حال ویزارد compare site maps را minimize کنید و به تب Options و سپس به تب Sessions بروید.



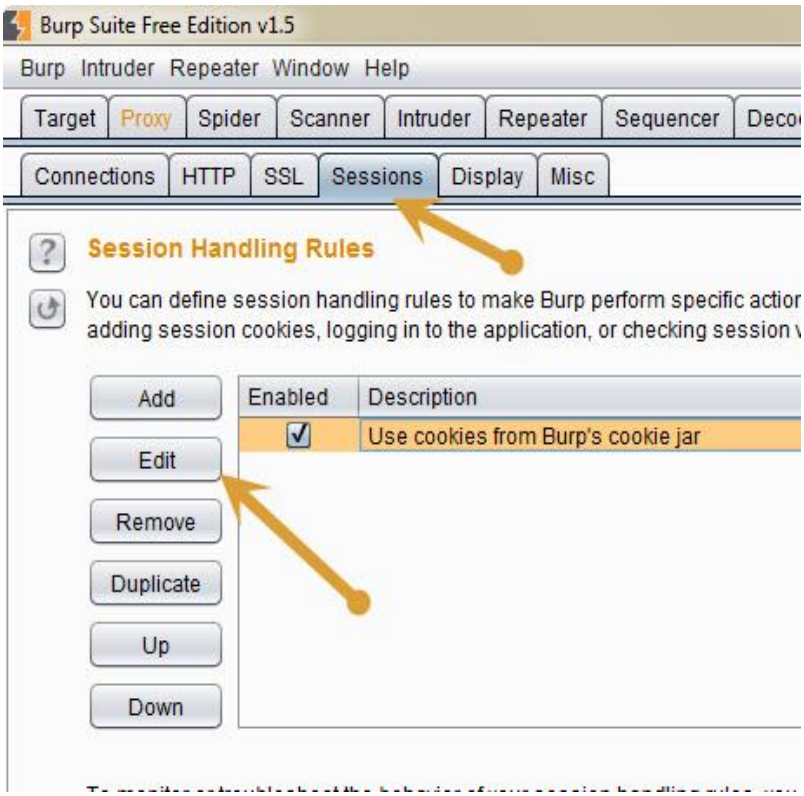
9. سپس بر روی Open cookie jar کلیک کنید. پنجره جدیدی که باز می شود مخزن تمامی توکن های نشست های استفاده شده توسط Burp را نمایش می دهد.



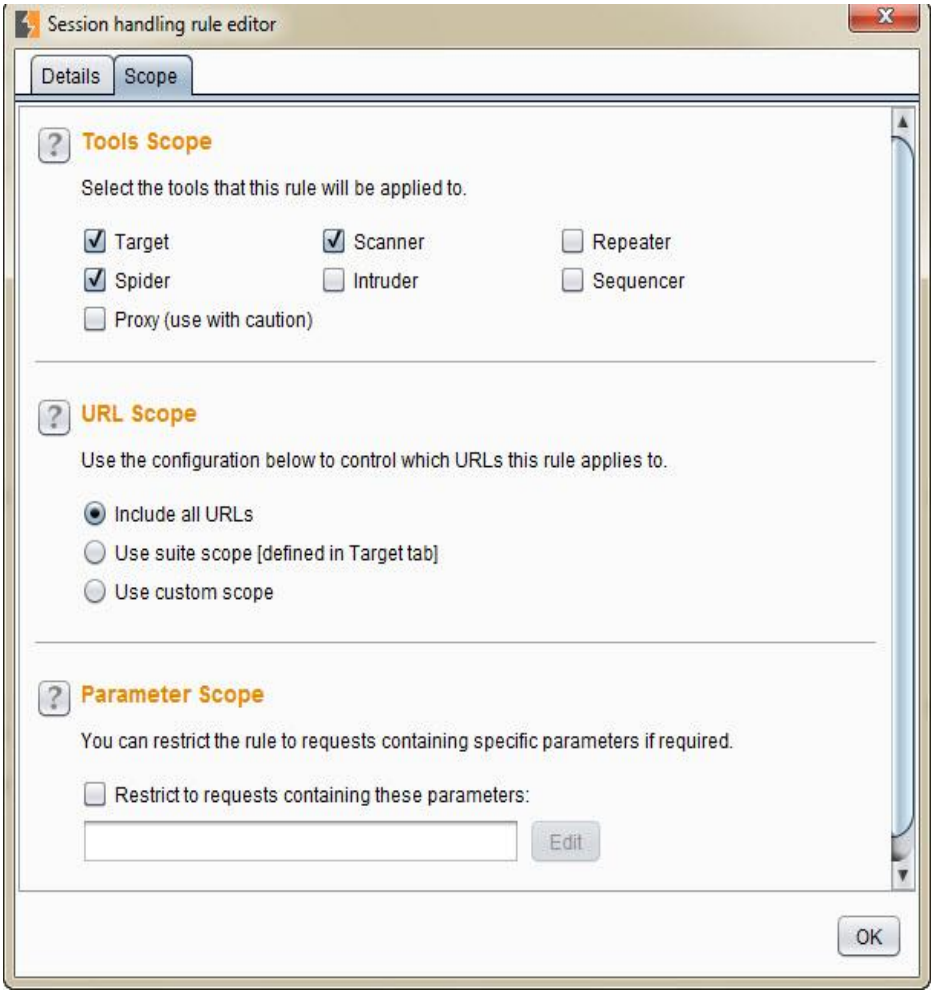
10. چونکه ما می خواهیم یک کاربر اهزار هویت نشده را شبیه سازی کنیم، می توانیم به سادگی تمامی کوکی های مرتبط با دامنه www.packtpub.com را دستکاری کنیم. بدین منظور کافیست، یکی یکی آنها را انتخاب کرده و بر روی edit cookie کلیک کنید.



11. همچنین ما نیاز داریم site map ابزار Burp را وادار کنیم عملیات مقایسه را با کوکی هایی که تغییر در آنها ایجاد کرده ایم انجام دهد. بدین منظور، در برنامه Burp Suite به تب Options و سپس Sessions بروید و از سمت چپ بر روی دکمه edit در جدول session handling rules کلیک کنید.

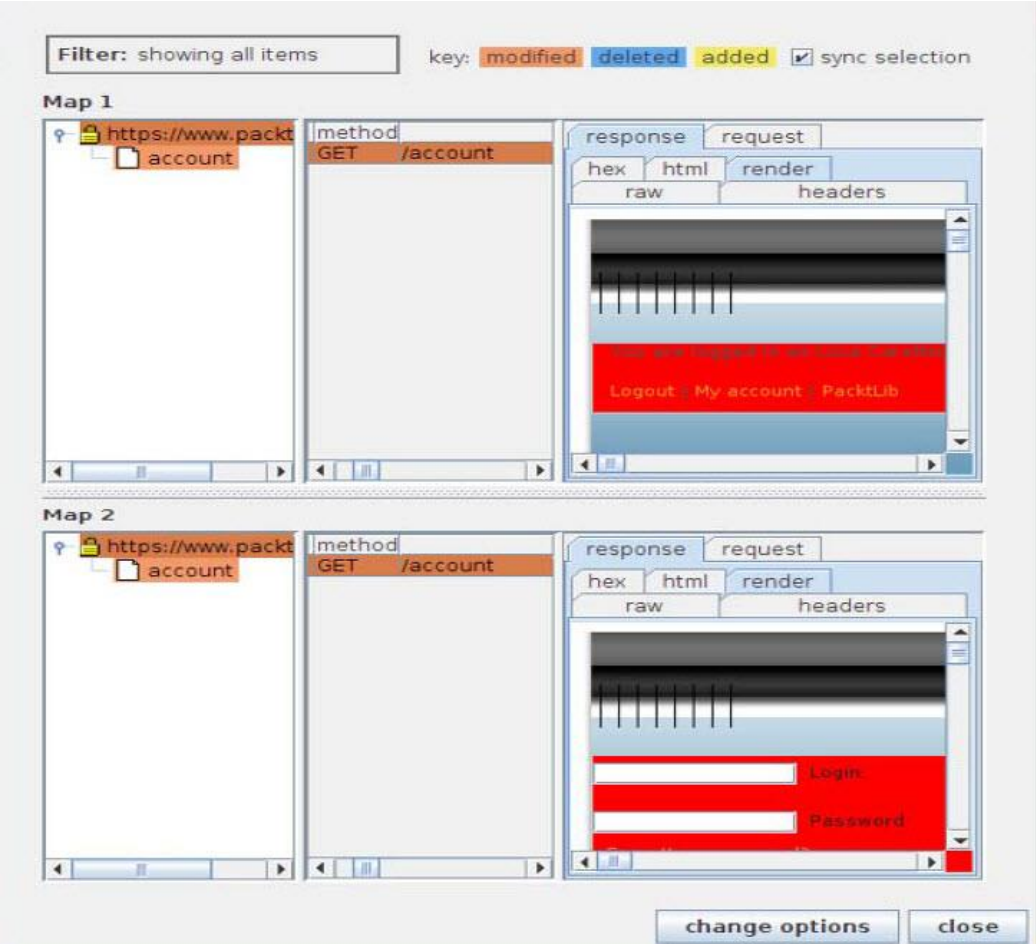


12. پس از کلیک کردن بر روی دکمه edit برنامه Burp یک پنجره جدید با نام Session handling rule editor باز خواهد کرد. این گام بسیار مهم است، اطمینان حاصل کنید که همانند تصویر آورده شده در زیر تنظیمات اعمال شده باشند. در پایان، بر روی Ok کلیک کنید و به پنجره ویزارد compare site maps برگردید.



13. در گام چهارم ویزار compare site maps ابزار burp به شما اجازه می دهد تعداد ترد های مورد استفاده در تجزیه و تحلیل را سفارشی سازی کنید، علاوه بر این اجازه سفارشی سازی دیگر گزینه های زمانی را هم به شما ارائه می دهد. ما تمامی تنظیمات این بخش را به صورت پیش فرض رها کرده و بر روی Next کلیک می کنیم.
14. در گام پنجم، یعنی قسمت request matching پیشنهاد می شود از تنظیمات پیش فرض برنامه استفاده شود، چون در بیشتر شرایط به خوبی کار می کند. به همین دلیل در این قسمت هم بر روی next کلیک می کنیم و به مرحله بعد می رویم.
15. دوباره در گام ششم یعنی قسمت Responses comparisons پیشنهاد می شود از تنظیمات پیش فرض اعمال شده در برنامه استفاده کنید. به همین دلیل دوباره بر روی next کلیک می کنیم و به مرحله بعد می رویم.

16. در این نقطه برنامه burp شروع به درخواست دادن به منابع site map 1 به منظور ایجاد کردن site map 2 با جلسه های تغییر داده شده می کند. پس از کامل شدن این فرآیند، برنامه burp به صورت خودکار تمامی تفاوت ها را محاسبه کرده و نمایش می دهد.



پنجره نتایج به شما اجازه می دهد به سادگی منابع site map 1 و site map 2 را با هم مقایسه کنید. با این حال، در طی ارزیابی امنیت یک برنامه تحت وب، شما می توانید از این ویژگی برای تمامی نقاط پایانی برنامه مد نظرتان استفاده کنید. به عنوان مثال، شما می توانید به راحتی تفاوت ها را میان یک نشست اهراز هویت شده و یک نشست اهراز هویت نشده بررسی کنید. سپس می توانید site map 1 و site map 2 را با استفاده از دو نام کاربری متفاوت ایجاد کرده و مکانیزم های کنترل دسترسی را بررسی کنید.