**HOWTO: Burp Scanner.**

Note you will need the JAVA JDK to be able to run Burp Scanner.

1. Get Burp Scanner: <https://portswigger.net/burp/scanner.html>
2. Login to get a license key:
   1. User:
   2. Password:
   3. Start Burp Scanner App
   4. Enter license key (available from logged in area)

Burp scanner will start with a dialog box prompting you to open or create a project. I always ignore this and just use the “Temporary project” option and in the next dialog box I “Use Burp defaults”.

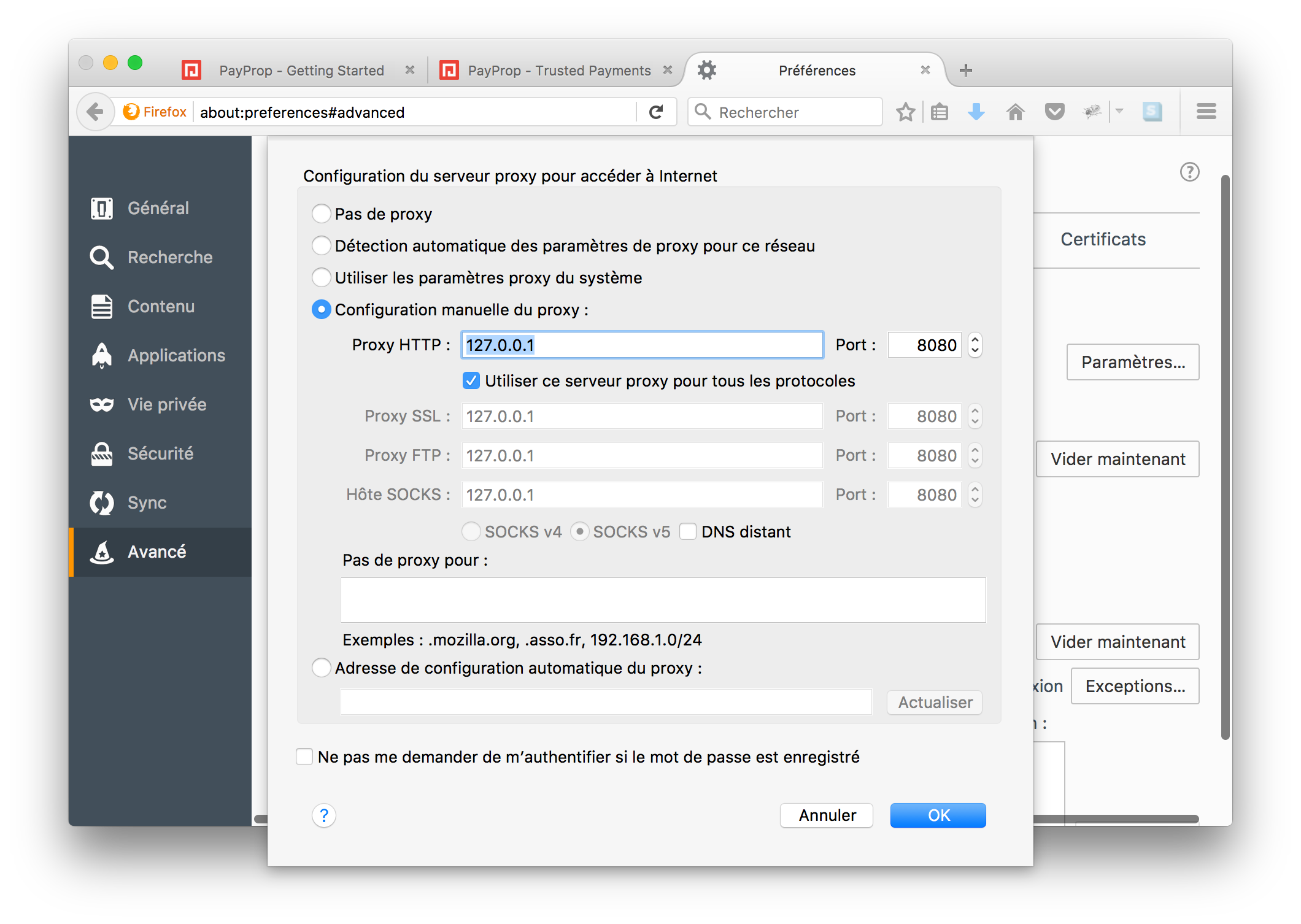
**Config Setup**

Make sure for the application that:

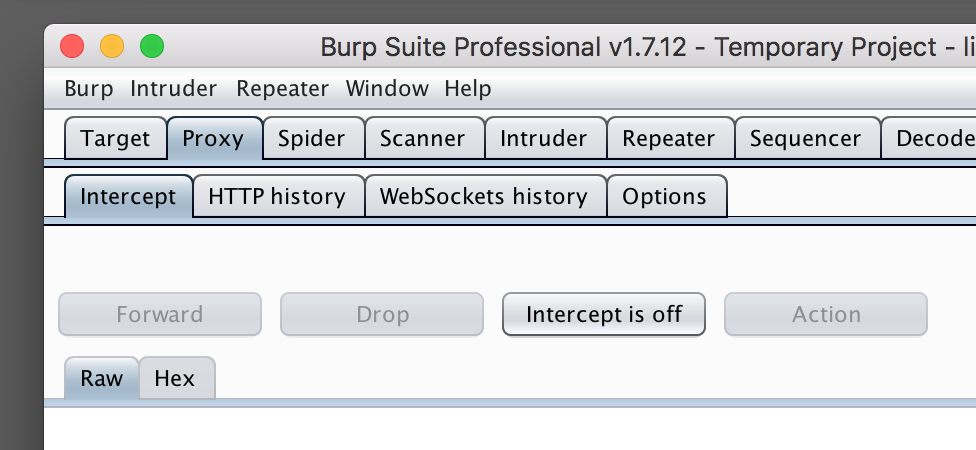
* Your database configuration is pointing at a local dev database
* E-mails are pointed at nullmailer or equivalent
* Third party integrations are pointing at emulators, etc
* Request throttling is disabled
* Account locking is disabled

**Initial Burp Scanner Setup**

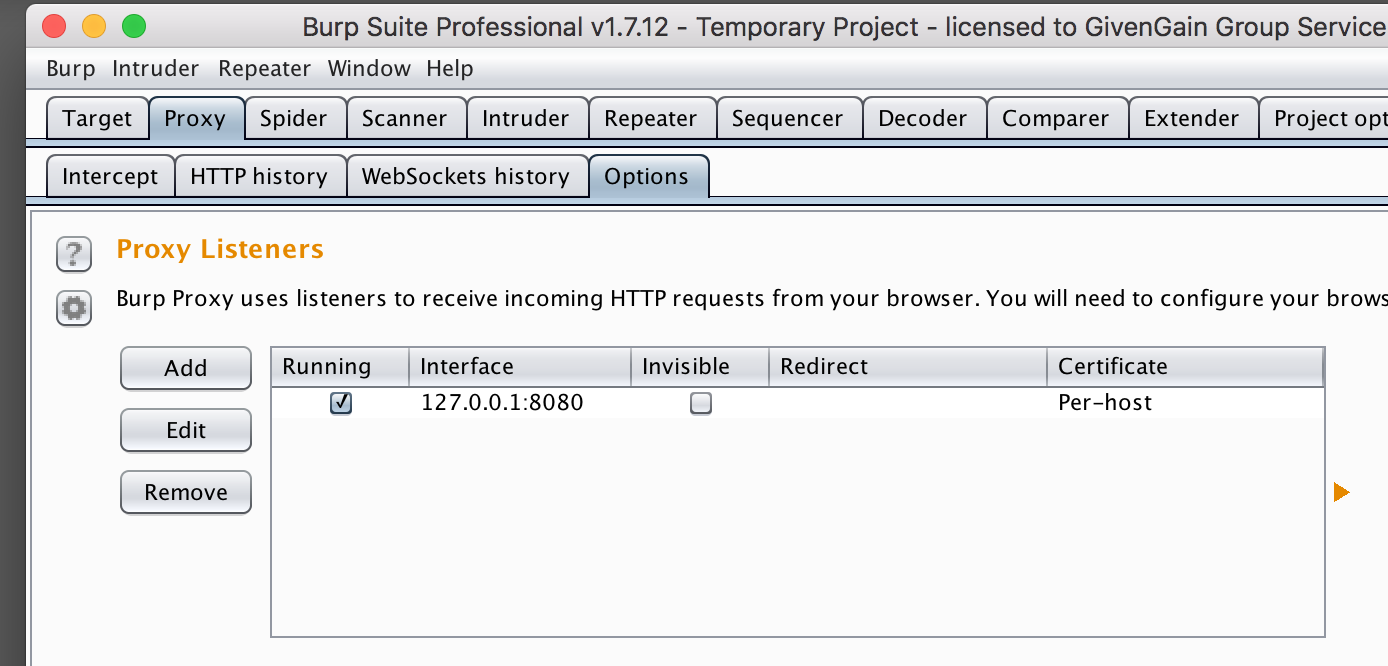
1. Make sure your browser is pointing at the Burp Scanner proxy:



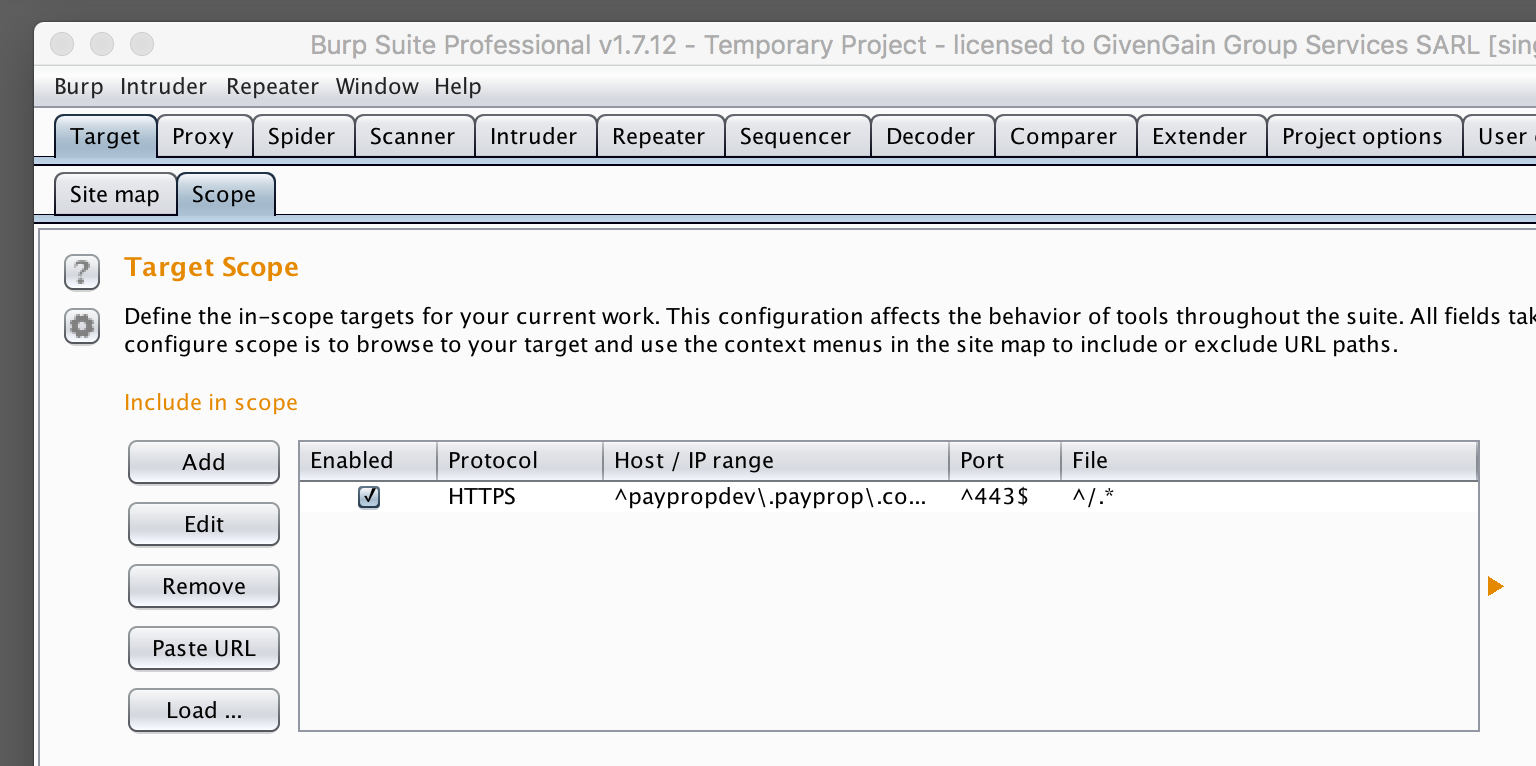
2. Make sure Burp Scanner -> Proxy -> Intercept is off otherwise when you visit any URL in your browser Burp will intercept requests. This is useful for debugging, but not if you want to have the scanner run without user input:



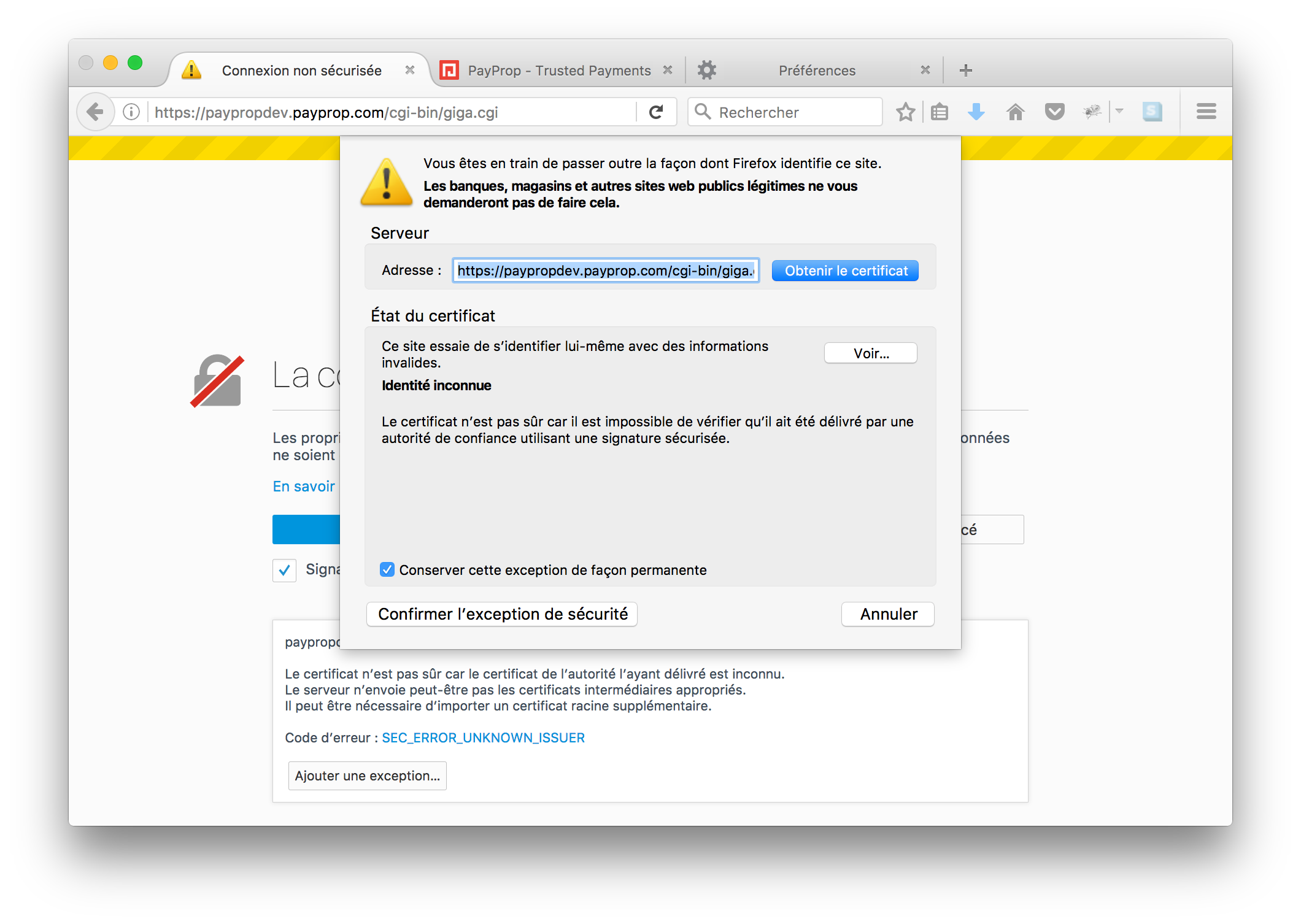
3. Confirm the Burp Scanner -> Proxy -> Options has the same settings as used in your browser proxy:



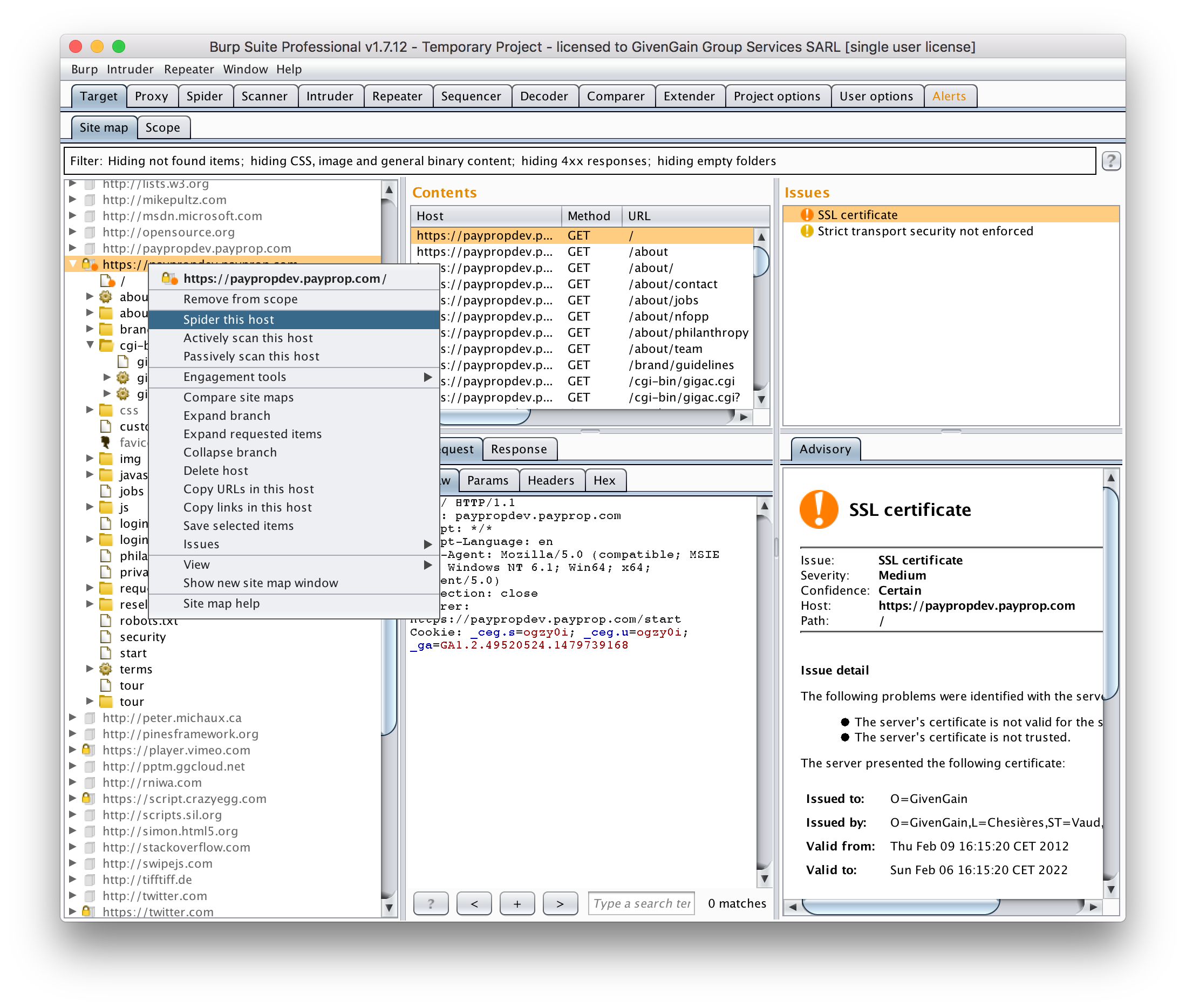
4. Set the Burp Scanner -> Target -> Scope to the host you will be scanning. This should be your dev box, and your dev box should probably be pointing at a small db:



5. Visit the URL you will be scanning in the browser that has the proxy set to Burp Scanner’s proxy and you will find Burp Scanner lists all possible targets in the Burp Scanner -> Target -> Site map tab. Note you will get a certificate security warning due to the proxy, so just ignore this.

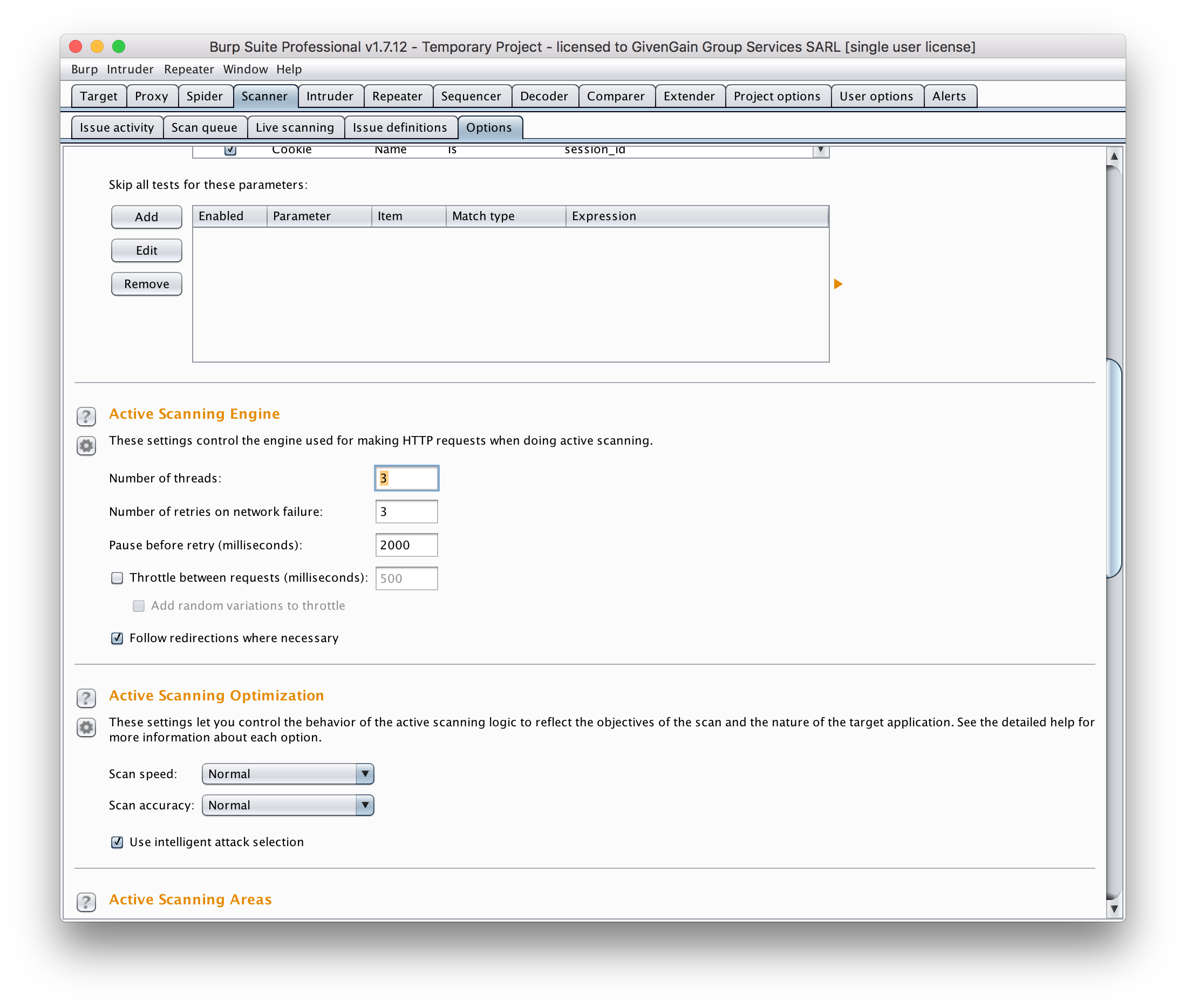


6. In the Burp Scanner -> Target -> Site map tab right click the relevant URL that you want to scan (i.e. the URL you just visited in your browser) and choose “Spider this host”:



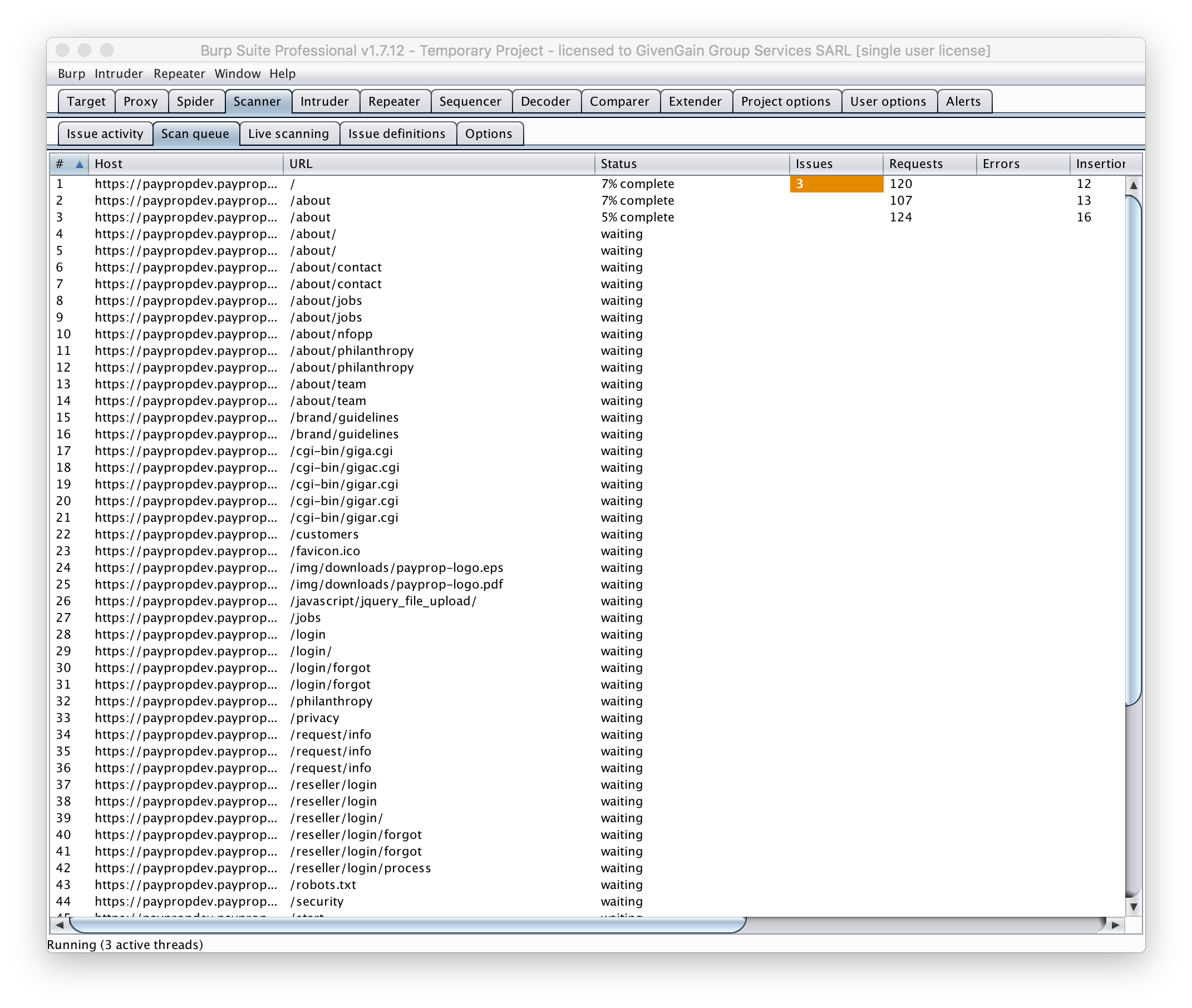
If you wish to do a full scan that includes logged in areas, then you will need to complete any form boxes that pop up with the relevant login information. Burp Scanner will take a few moments to spider the host, after which you can click on the various directories in the Burp Scanner -> Target -> Site map tab to see what will be included. Note also that any targets in grey will be ignored – you may find this with URLs in the logged in sections so double check those.

7. Note that before you scan the host you can play with the options in Burp Scanner -> Scanner -> Options, although the defaults are reasonably sensible. You may want to reduce the number of threads from 10 to 2 or 3:

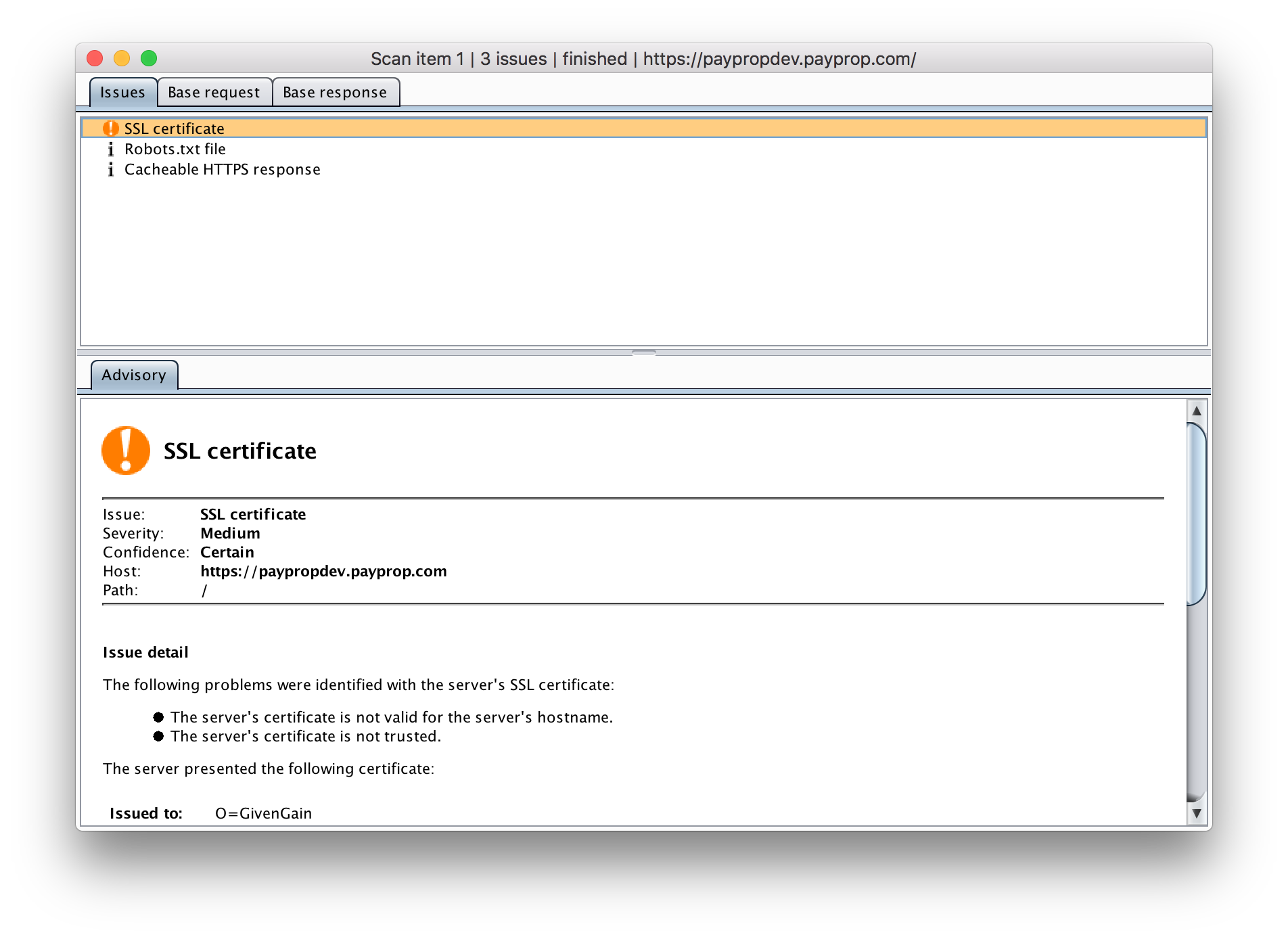


8. If you wish to scan the logged in areas then login to those areas using your browser so you have cookies to enable this to happen.

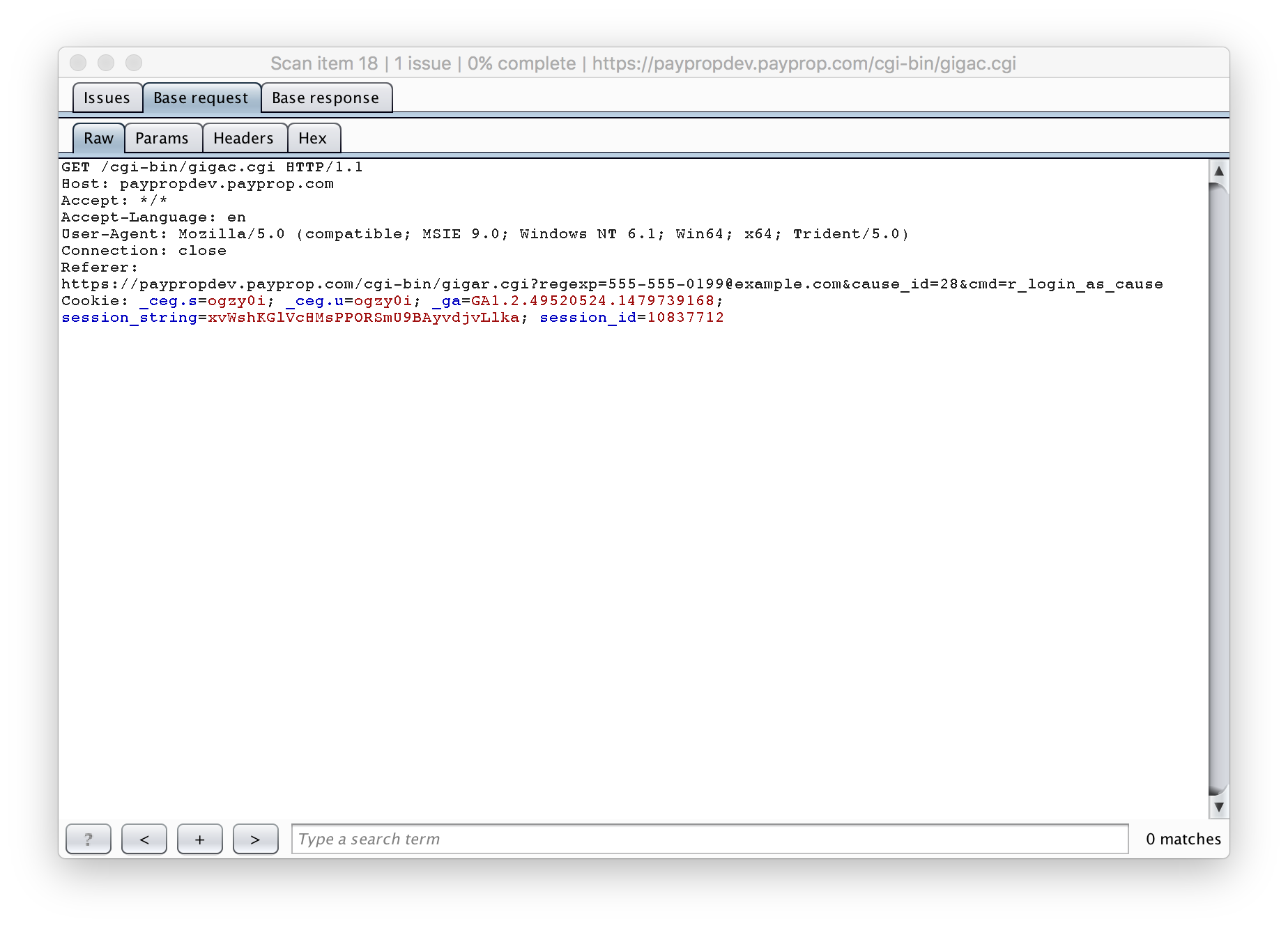
9. In the Burp Scanner -> Target -> Site map tab right click on the host and choose “Actively scan this host”. You will be prompted for some options in a dialog box, all of which should be self-explanatory. Change to the Burp Scanner -> Scanner -> Scan queue tab to see the progress:



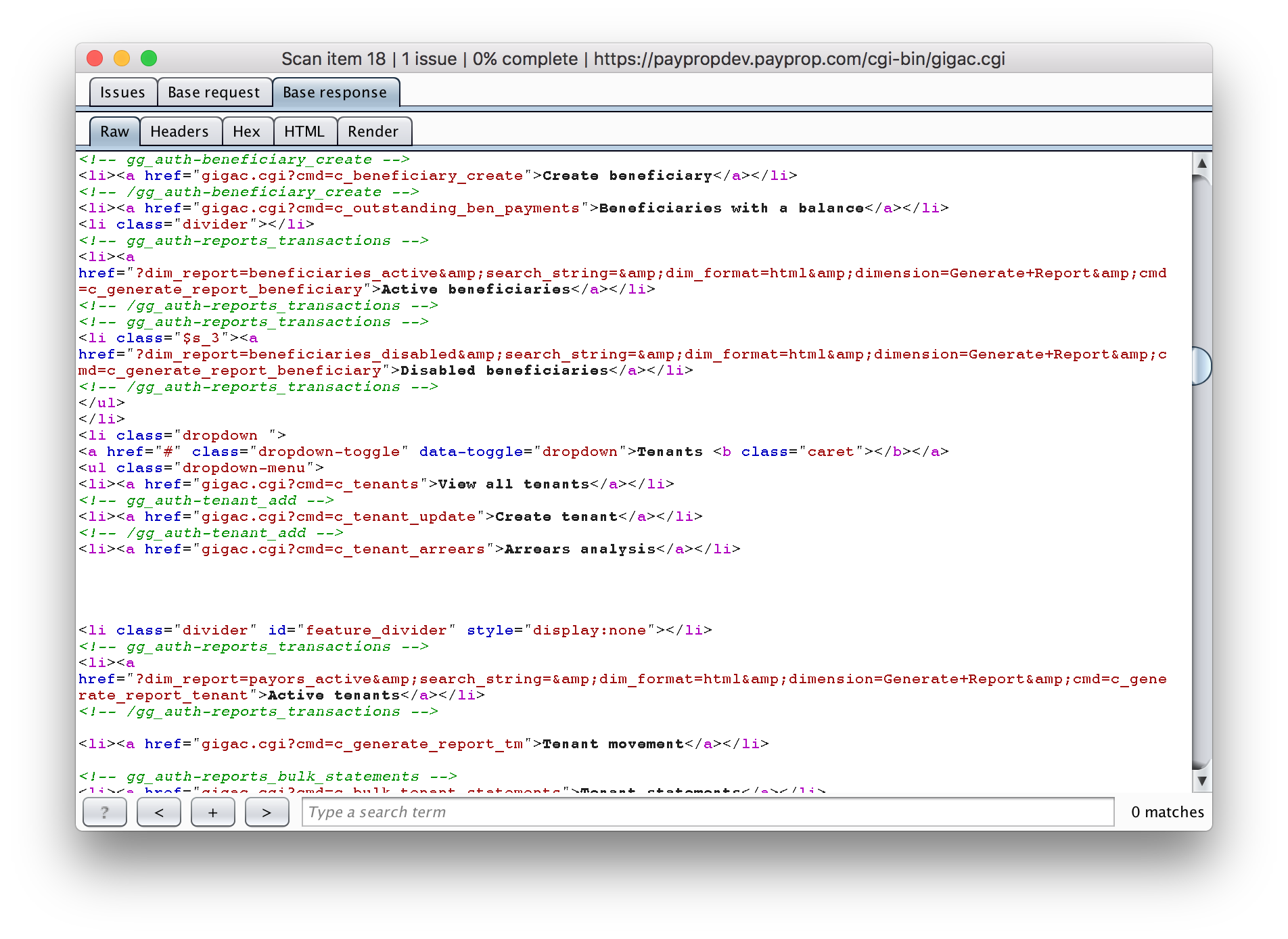
10. Leave the scanner to run and watch the log files on your vm. Issues will reveal themselves as the scan is in progress. You can double click on the entry to see more details and see the request/response:



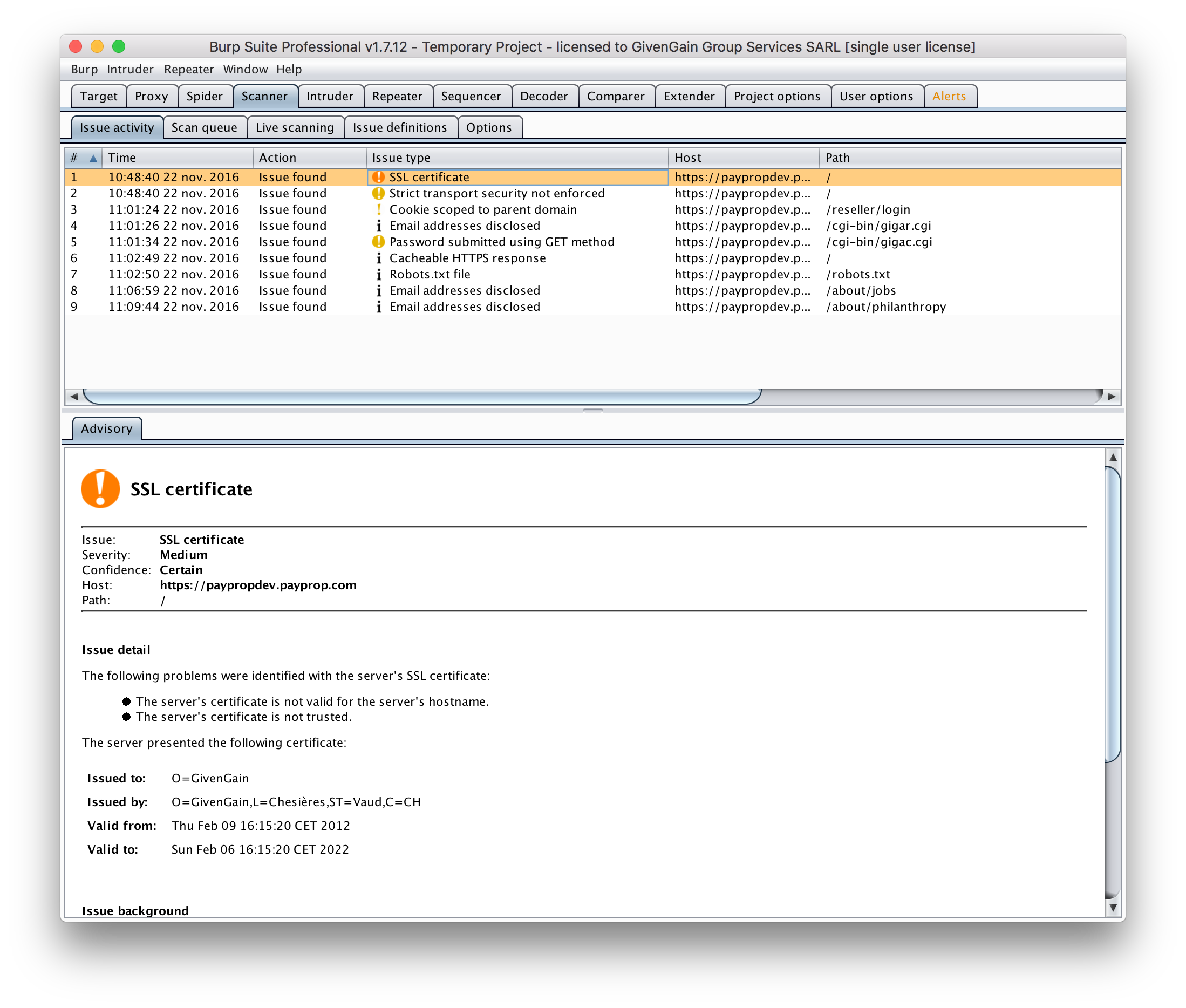
11. **NOTE** for logged in areas it is a good idea to click on the entry and check the Base request and Base response tabs to make sure the cookies have been effective and the response is not a logout redirect:



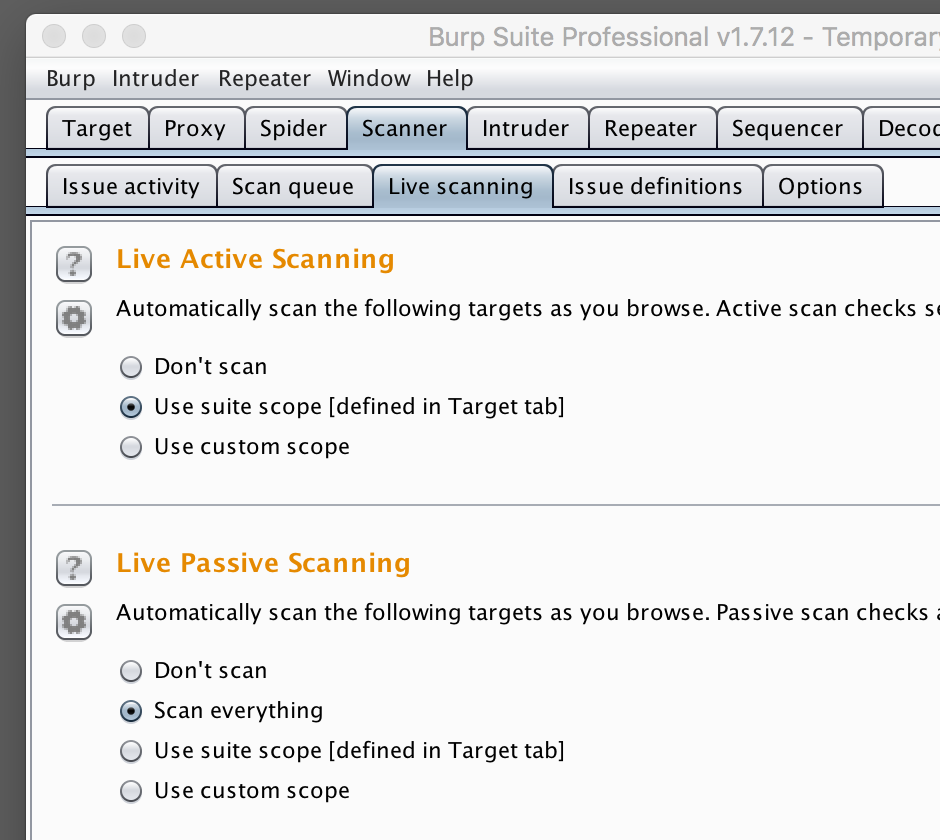
Note above how cookies were sent, and a full page was received (not a redirect to logout):



12. Once the scan is complete you can review the Burp Scanner -> Scanner -> Issue activity tab to see all issues and generate a report:



13. If you wish to scan more because you think Burp Scanner hasn’t gotten everything (possibly because sessions timed out, etc), then change the options in Burp Scanner -> Scanner -> Live scanning tab to actively scan as you browse then click around the site, log in, log in as a cause, etc:



14. Note if you are **still** having issues with sessions you can inject headers into the requests using the Burp Scanner -> Proxy -> Options tab (Match and Replace section):

