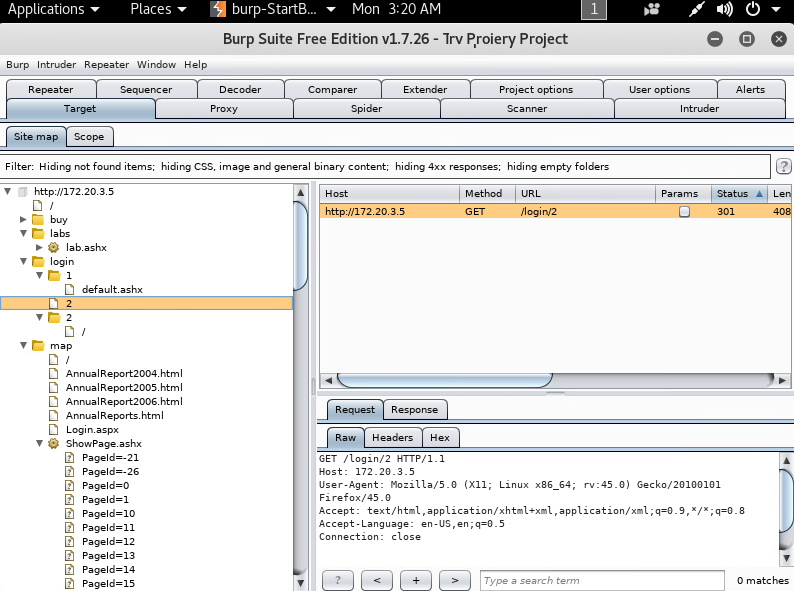
Lab 03 – Spidering

10 Points

In this lab we’ll begin practicing our information discovery techniques and use spidering. For this lab, complete the following tasks in **Lab 1. Mapping the application** on Pablo.

1. No screenshot required - this step is required to complete the lab.
2. **[1 point]** Provide a screenshot of your Target->Site Map page after performing manual spidering.



**I went through a bit of guesswork for the numbered page Id’s on /map/ShowPage.ashx?PageId=\*\*\* so the site map became longer than my vm’s screen: here’s a gif scrolling through it:**

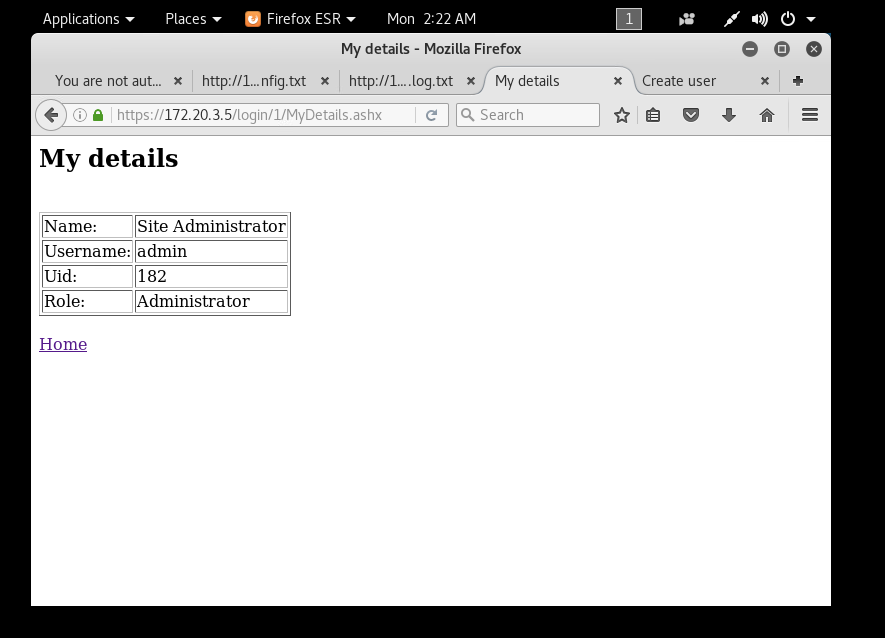
<https://i.gyazo.com/c0b903a5e64db2b9f933fff5073a3247.mp4>

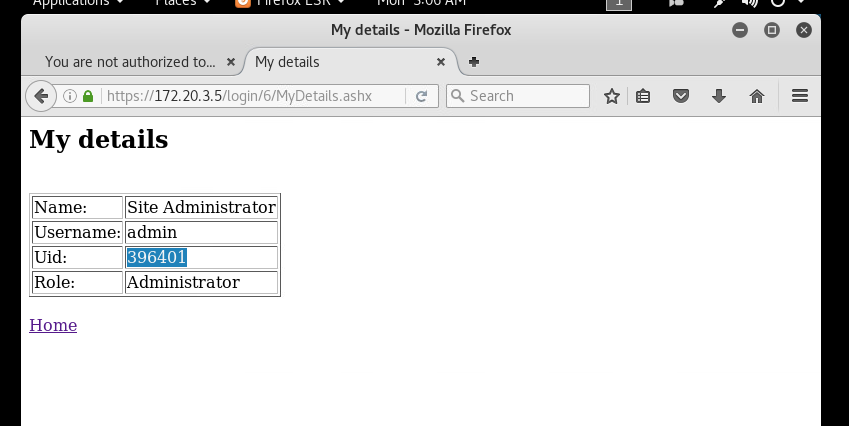
1. **[2 points]** Provide an answer for each:
   1. What links did you find?
   2. Did you find any other sensitive information? Hint, there is something…
2. **[2 points]** Provide an answer or screenshots showing additional content you discovered.

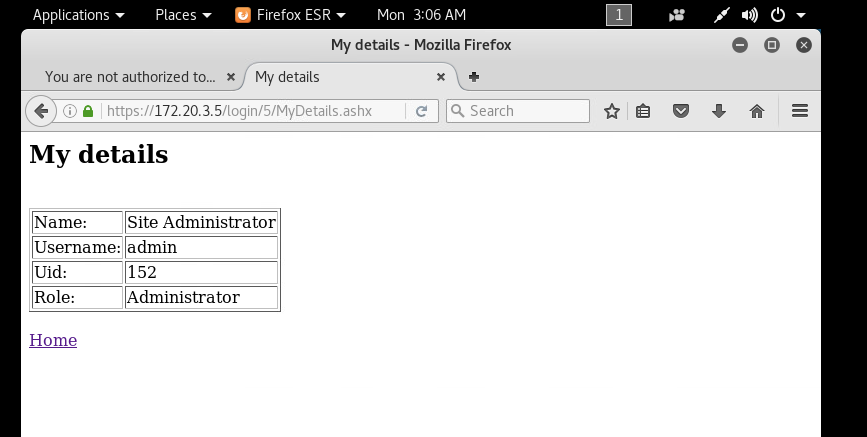
**Jeff’s username & Password**

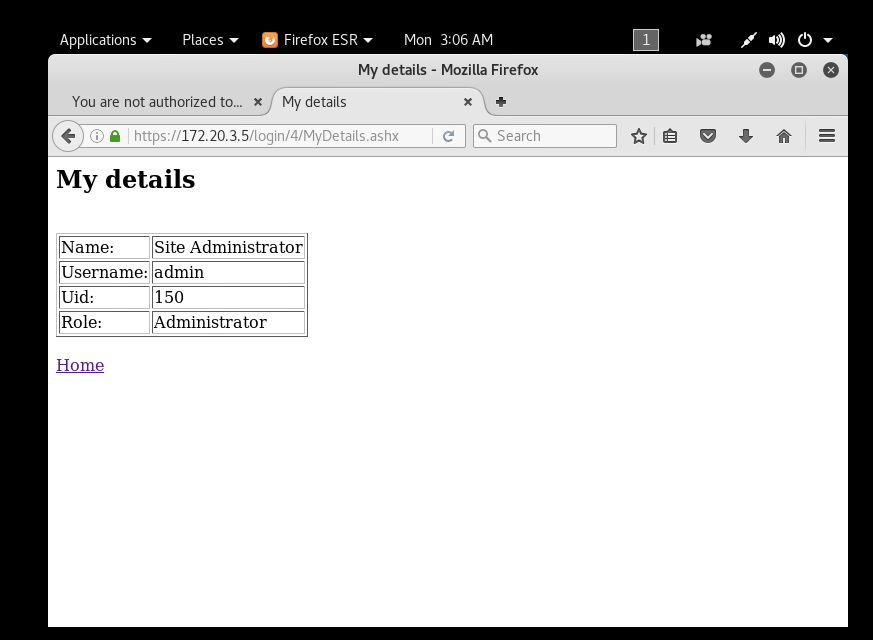
https://i.gyazo.com/65f3d2cae0fac77dda987bf0af5dbf54.png

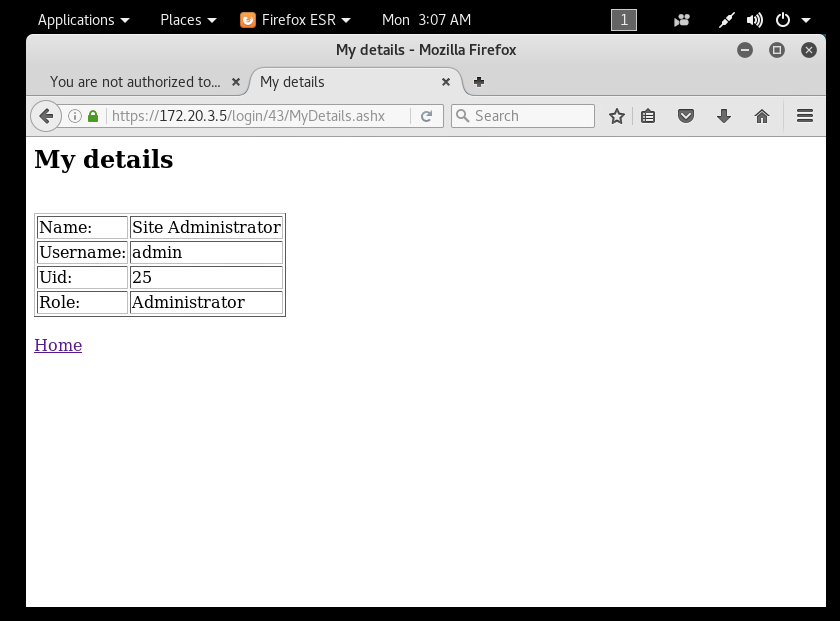
**I noticed the number in the URL of the admin login page…. Tried incrementing it. Brought up the same page each time BUT… it made me relog each time…. Using the same username/pass I checked the details page. Each time would bring up a new Uid (presumably a ‘user ID’) I don’t know what it is used for but it appeared randomized, perhaps it could be useful later? idk:**

Login/1/MyDetails.ashx 

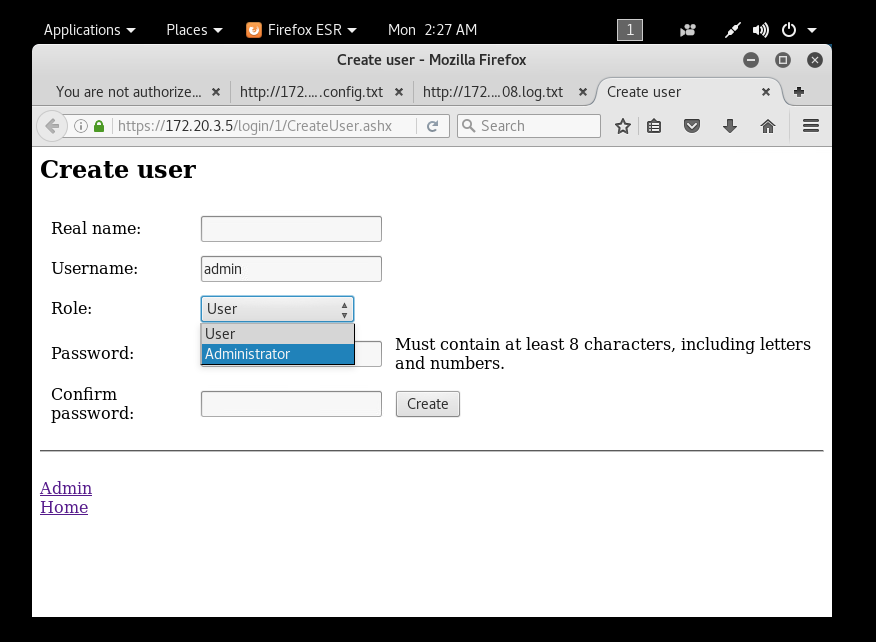
Login/6/MyDetails.ashx 

Login/5/MyDetails.ashx 

Login/4/MyDetails.ashx 

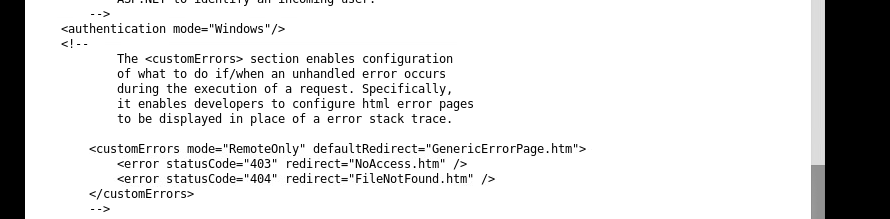
Login/43/MyDetails.ashx 

**We can create new Admin level user for ourself from the admin’s page, awesome!**



**Also The same page gives us information on password requirements,** https://i.gyazo.com/ee1ccdd9efab30c58a0a686ef81b16c4.png

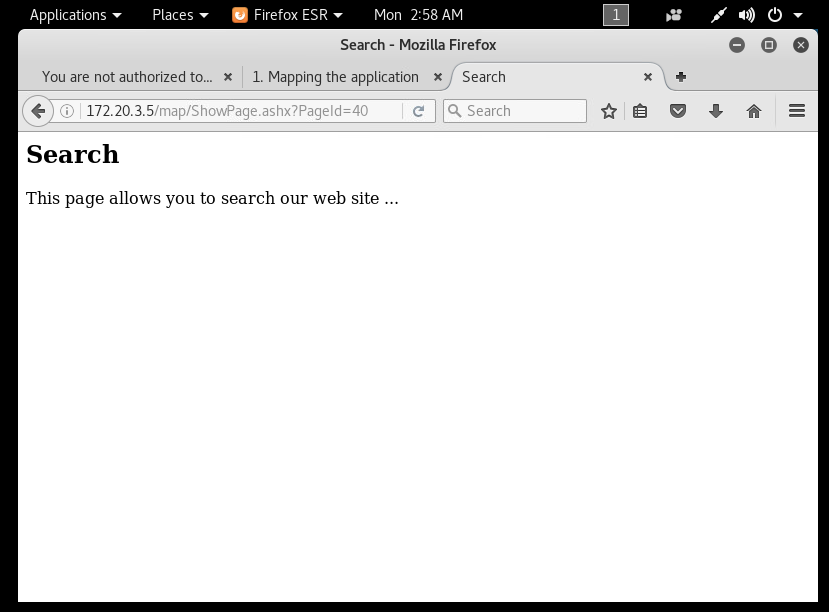
On the config page there was a comment about error pages, if we could write to that file and specify to display stack traces on errors and we could try to pull them to get some more information on the system...

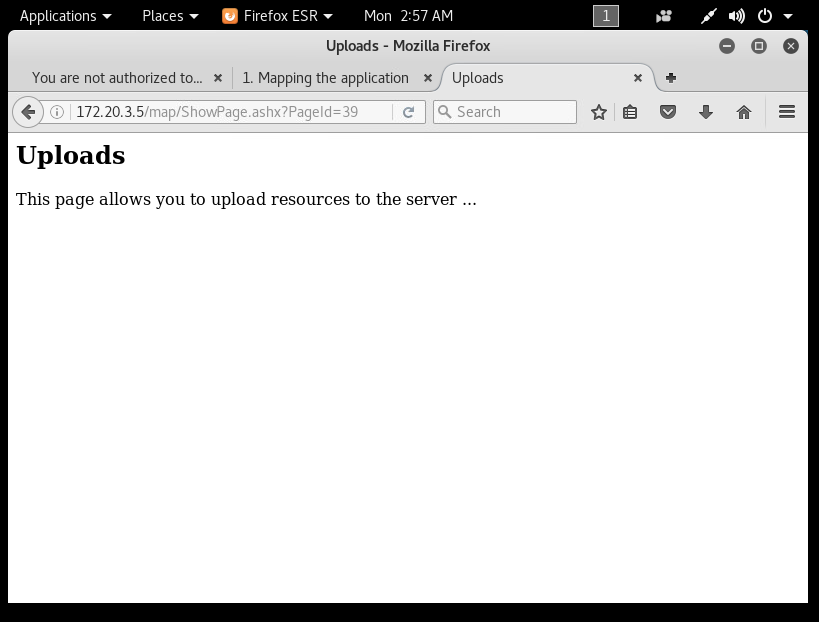


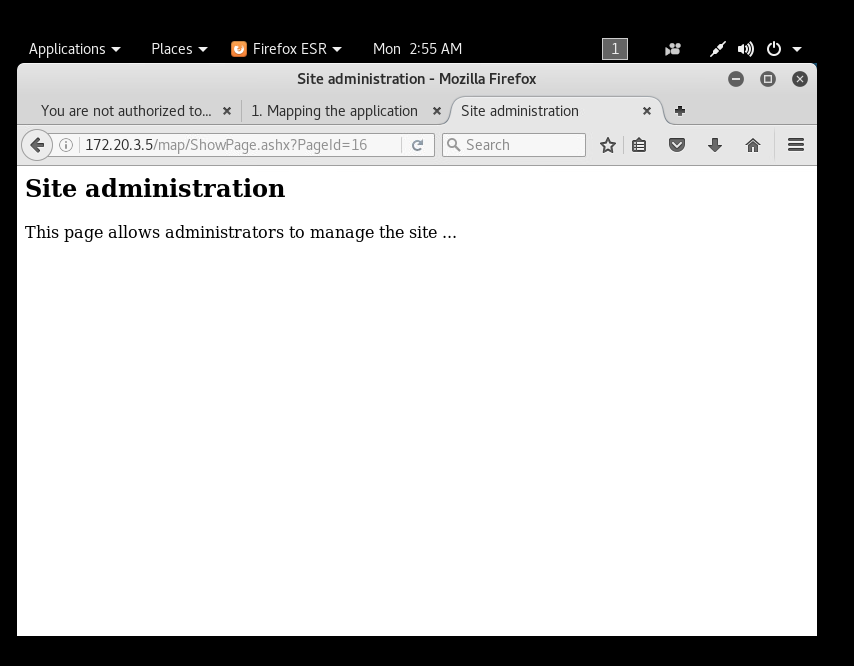
**This webapp is vulnerable to header injections!!!, I don’t know hot to capitalize on it yet, but it’s clearly been designed to enable that exploit.**

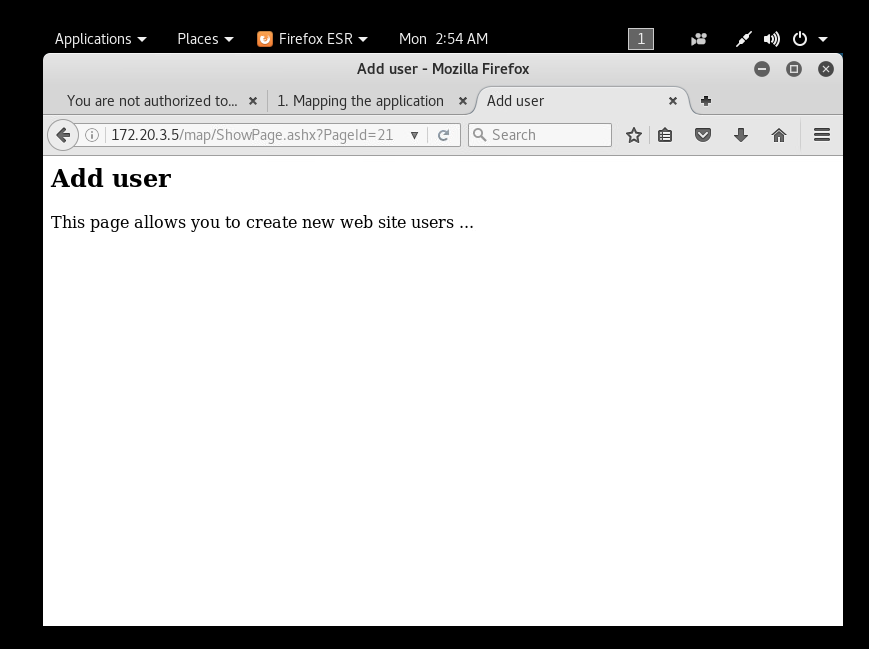


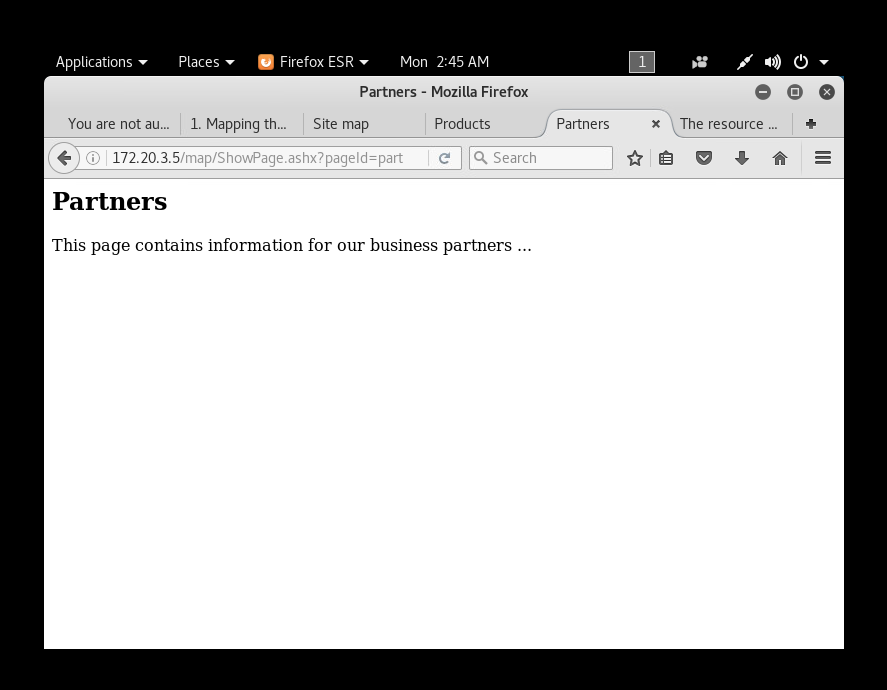
**Here were the pages I found through enumerating the pageIDs that weren’t listed:**











**[5 points] Additional Questions:**

This is an intentionally vulnerable application in a safe environment, would you change your approach for mapping an application if this was a ‘real’ application? Provide at least a paragraph in discussing your answer.

**I would personally prefer a hybrid approach, probably because I’m just lazy. I would give it a once-over with a spider and then manually check what it finds for potentially useful pages that it found on its own. I would manually go through all pages like robots.txt and the listed directories… with something this small, the patterns I found were more to do with the urls and less to do with opening up the page source – I wasted a lot of time checking each page source.**

**If I was doing this professionally and stealth was a concern, then I would suck it up and stick to manual, but I’m all for saving myself time and effort when it’s an option.**

**Deliverable:**

Turn in a Word Document or PDF that contains screenshots for each task as well as an explanation of what you are doing. If there are any additional questions, provide answers for those as well.