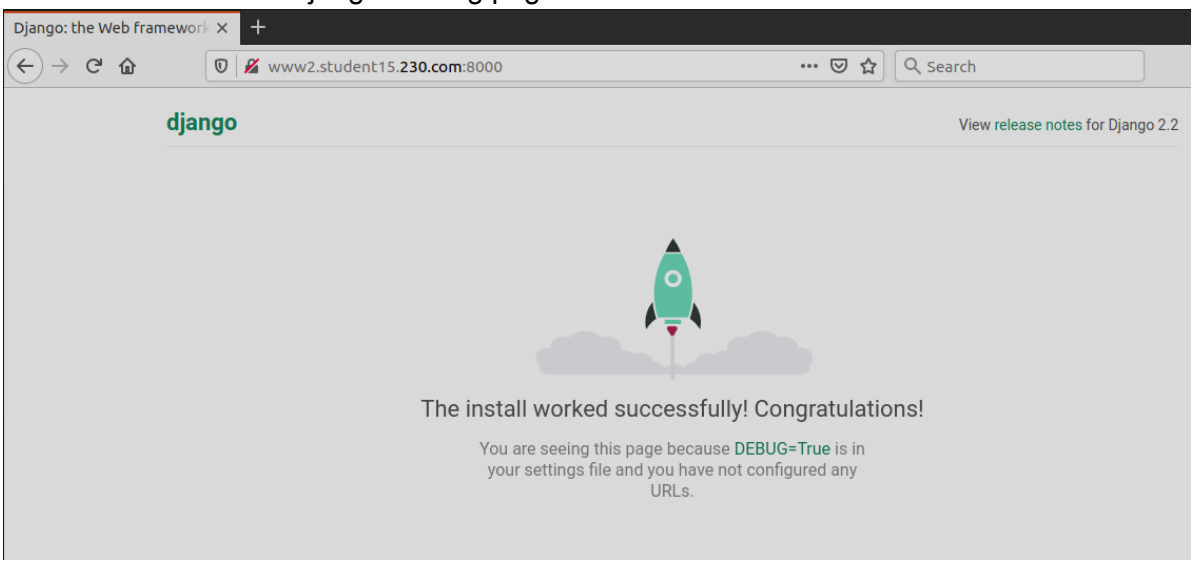
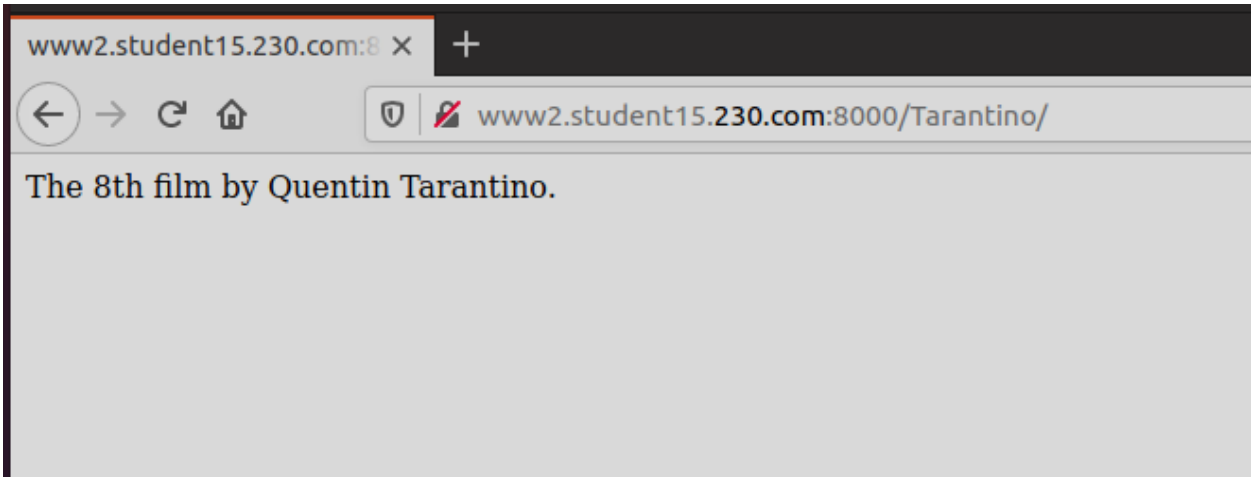
1. Screenshot of successful DNS query to www2.studentXX.230.com from new server

```
cpre230@www2:~$ dig www2.student15.230.com +noall +answer
www2.student15.230.com. 7167    IN      A       200.35.23.206
cpre230@www2:~$ _
```

2. Screenshot of default Django landing page

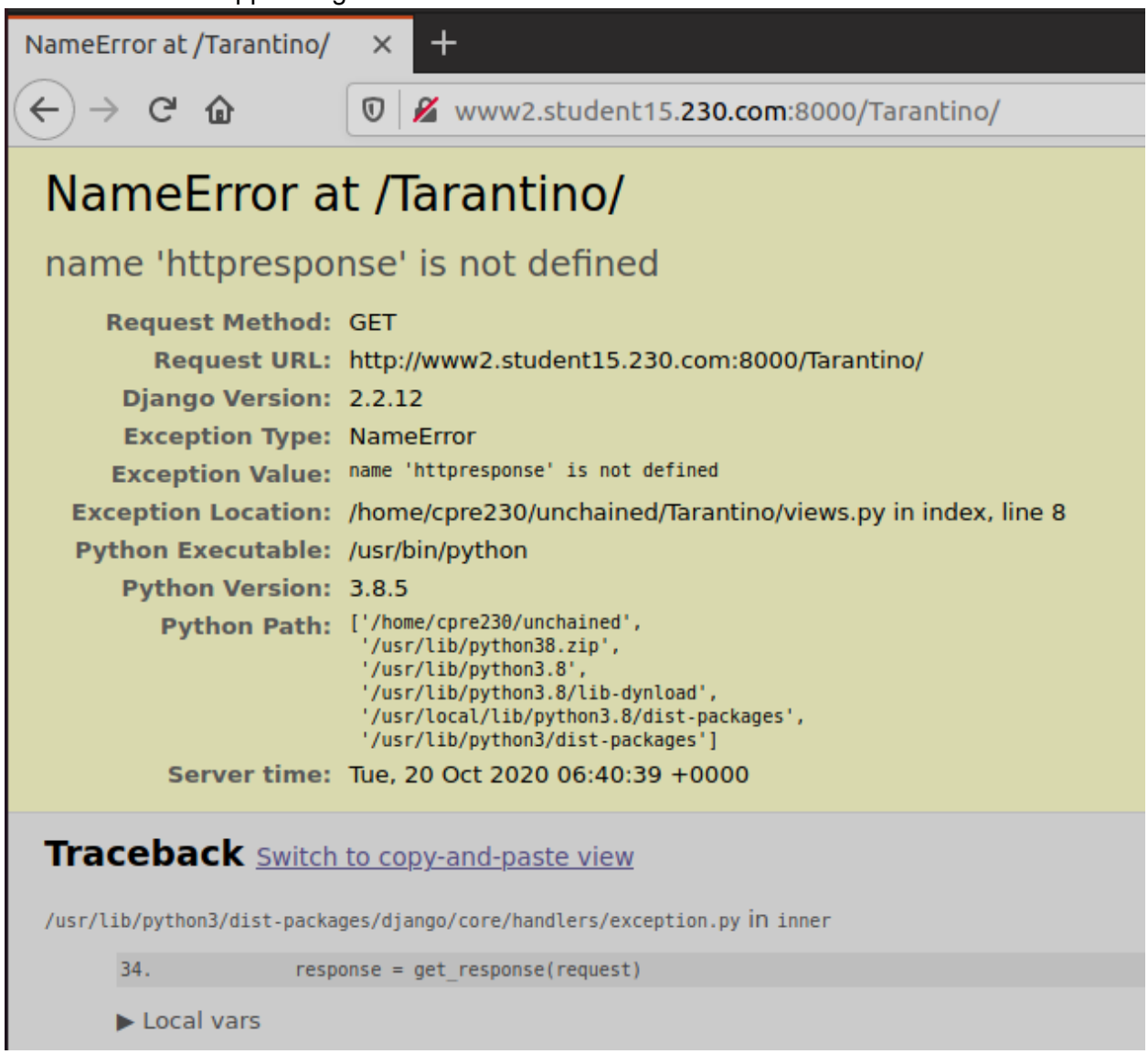



3. Screenshot of testapp “Hello World” page



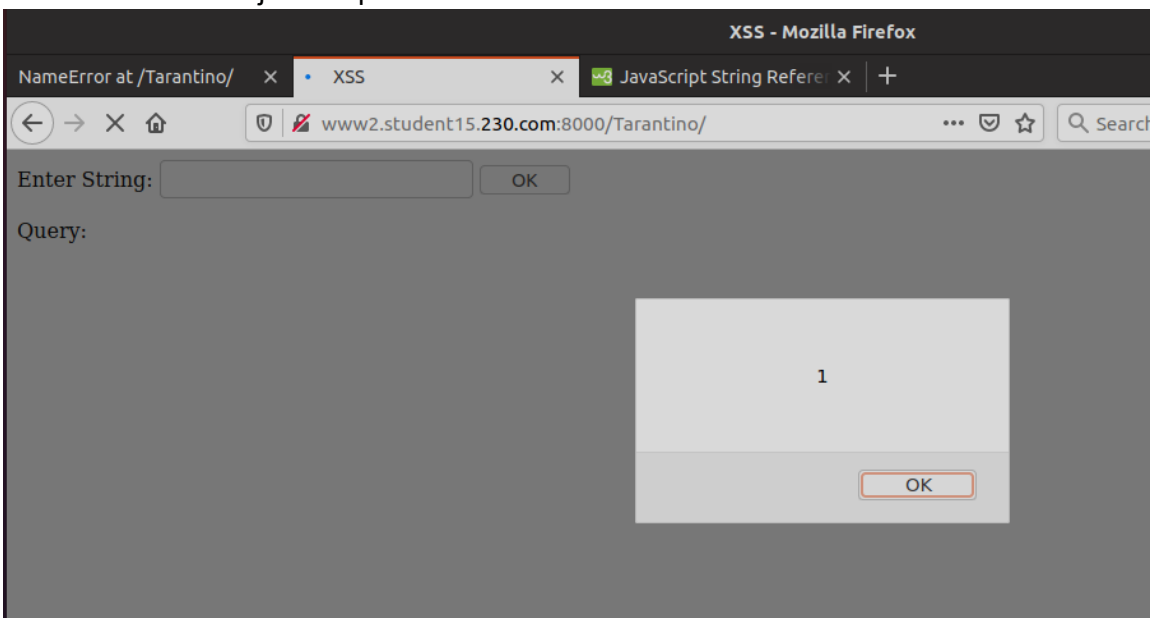

(Is that true? I’m not sure if Kill Bill counts as one or two movies.
Please comment if you know.)

4. Screenshot of testapp debug information



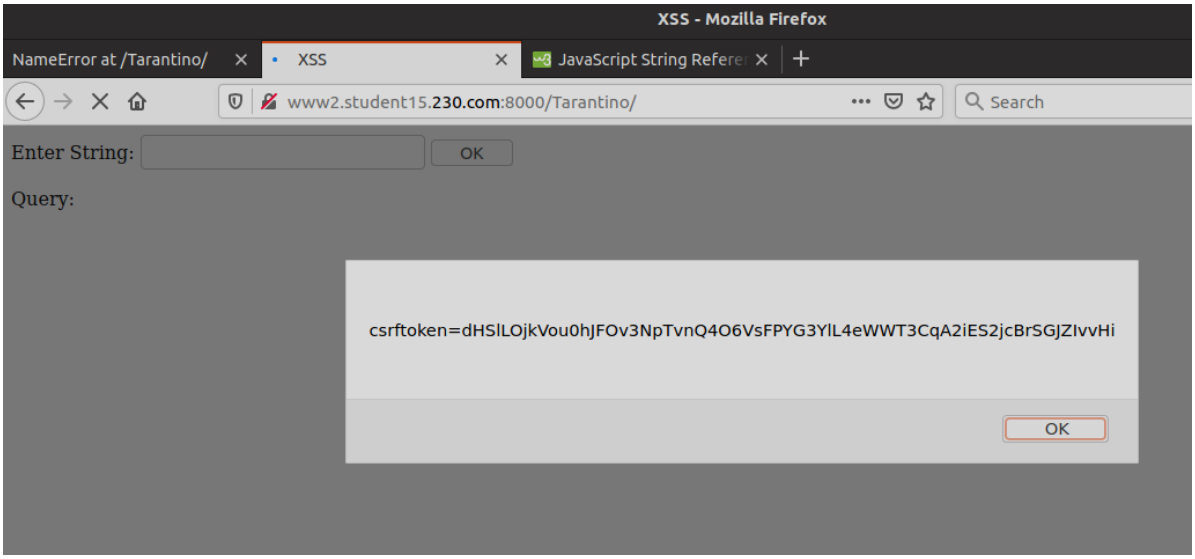

   a. Identify 5 potentially dangerous facts revealed by the debug page
      i. Exactly where the error is and what is causing the error. Show some of the code of the many different files.
      ii. All Environmental Variables set like the proxies and no proxies
      iii. System layout based upon where this server is running from on the machine
      iv. Logging information and files that the web server users
      v. It looks to give info on a secret key & password hashers these are hidden for use but could potential be shown from a setting
   b. How do you turn off the display of information?
      In settings.py, there is a config option of DEBUG that is set to true. Set it to false to hide the info.

5. Screenshot of XSS javascript alert



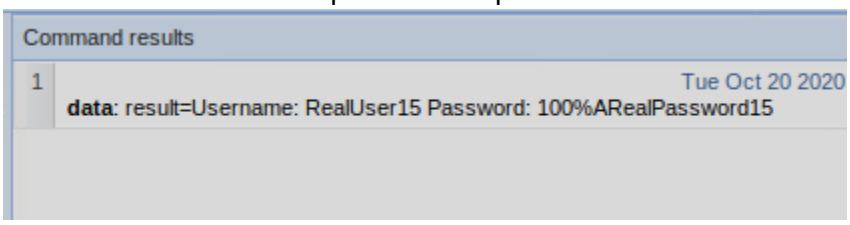

   a. Explain why the javascript isn't being displayed on the page
   The text is being handled by the html body, so it processes the <script> tag to mean that its interior is a script to be run. This causes the javascript code to be run instead of simply printing that text.

6. Screenshot of alert(document.cookie)

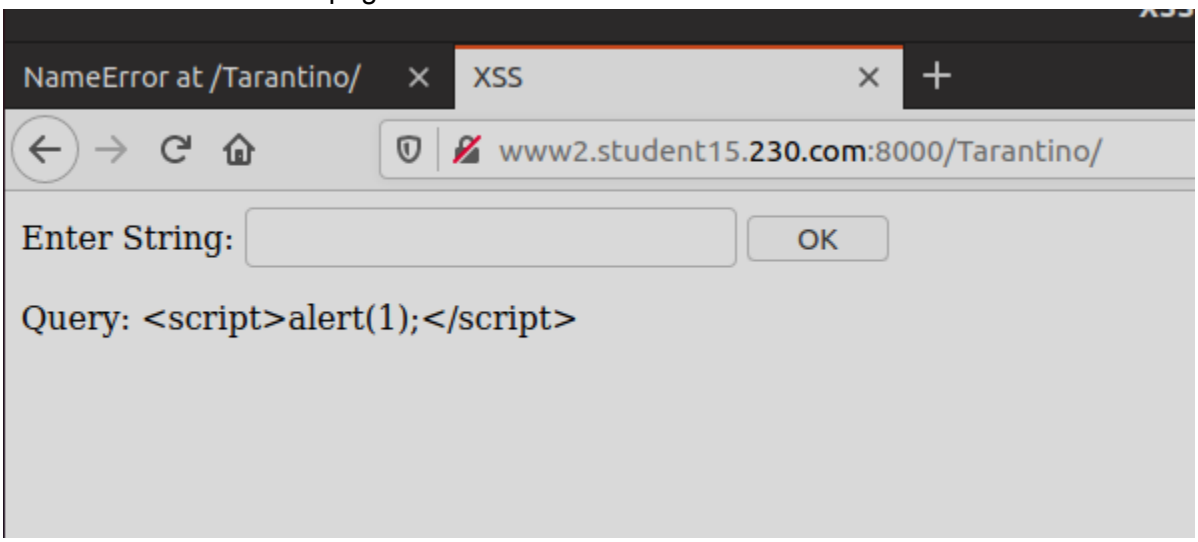



   a. How did we get this value?
   The javascript is run like before except instead of printing the value 1. It tells the system to retrieve the currently used cookie and print that out instead.
   b. Is it good or bad that we have that value?
   Bad as it means that an uncontrolled script by a malicious user can implant this in a webpage to retrieve and use people cookies.

7. Screenshot of username/password captured with BeEF




8. Screenshot of fixed XSS page




   a. Screenshot and explanation of the problem and how you fixed it.
      I forgot to take a screenshot of my changes. However, I didn't change html at all, and instead handled for the <, >, and / characters in the python code. I replaced those characters with the html literals for those characters. Those are &lt, &gt, and &#x2f.

9. Lookup the three types of XSS
   Stored, Reflected, DOM-based
   a. Which did we use in this lab?
      Reflected, since it isn't stored on the server and isn't purely handled by the browser. Requests go through python on the server and then get rendered.

10. Screenshot of running sshd process

```
cpre230@www2:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2020-10-20 08:00:16 UTC; 4min 4s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 7090 (sshd)
      Tasks: 1 (limit: 1041)
     Memory: 2.4M
     CGroup: /system.slice/ssh.service
             └─7090 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Oct 20 08:00:16 www2 systemd[1]: Starting OpenBSD Secure Shell server...
Oct 20 08:00:16 www2 sshd[7090]: Server listening on 0.0.0.0 port 22.
Oct 20 08:00:16 www2 sshd[7090]: Server listening on :: port 22.
Oct 20 08:00:16 www2 systemd[1]: Started OpenBSD Secure Shell server.
```

11. List of three other options for sshd that could be configured.
    PermitRootLogin, PubkeyAuthentication, PasswordAuthentication
    (Their names describe what they enable / disable)

12. Screenshot of successful SSH connection (from desktop)

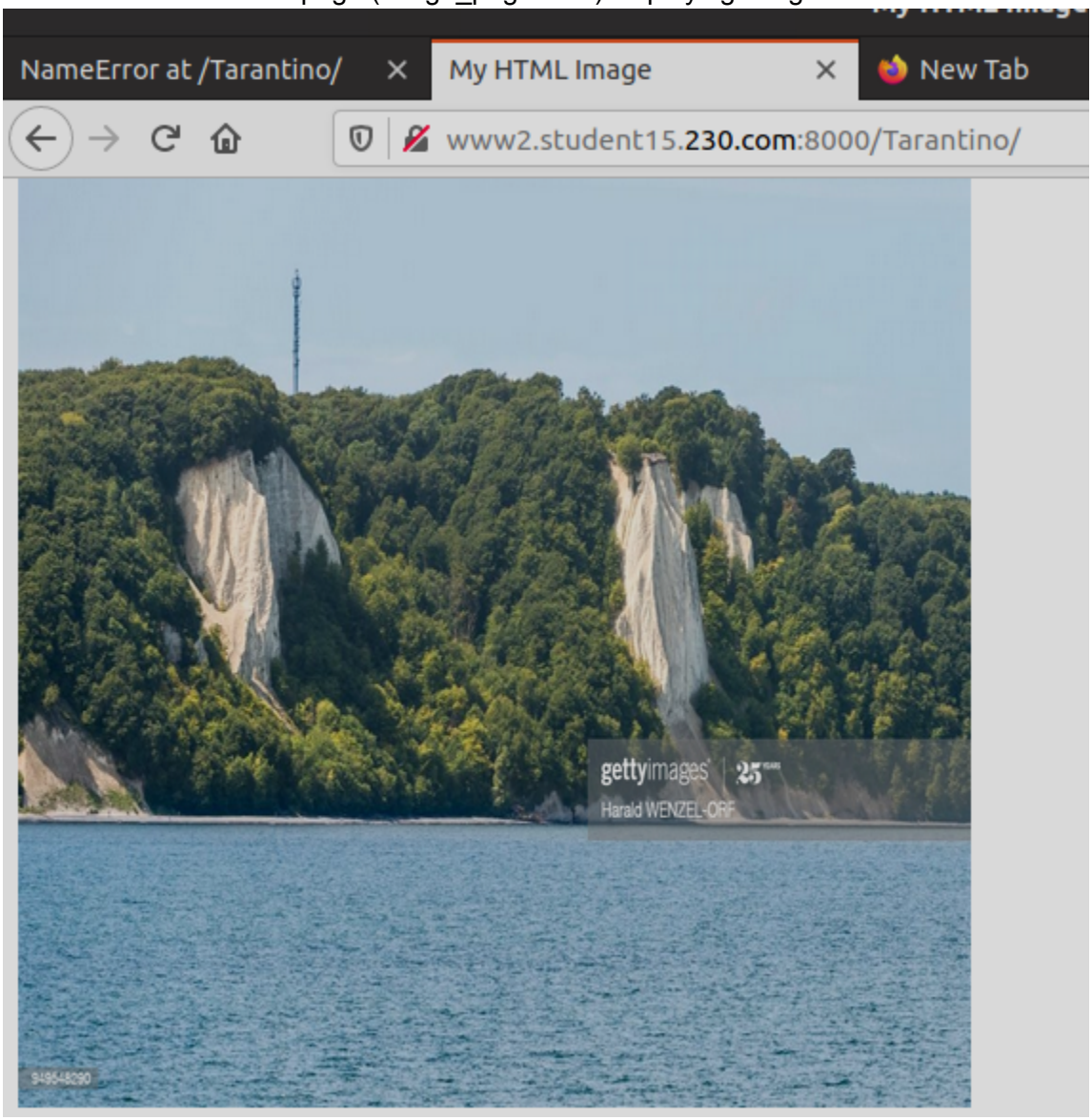
```
jboicken@desktop:~$ ssh cpre230@www2.student15.230.com
The authenticity of host 'www2.student15.230.com (200.35.23.206)' can't be established.
ECDSA key fingerprint is SHA256:U0HO/dh7EQNq41AaK/G5fNAbfF9DwG27U+SItO3TALo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'www2.student15.230.com,200.35.23.206' (ECDSA) to the list of known hosts.
cpre230@www2.student15.230.com's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue 20 Oct 2020 08:24:43 AM UTC

  System load:  0.0               Processes:             207
  Usage of /:   31.1% of 15.68GB  Users logged in:       1
  Memory usage: 35%               IPv4 address for ens32: 200.35.23.206
  Swap usage:   0%


0 updates can be installed immediately.
0 of these updates are security updates.


Last login: Tue Oct 20 05:56:58 2020
cpre230@www2:~$
```

13. Screenshot of public key.

```
jboicken@desktop:~/.ssh$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCzB8bqUoy68VEHrXWzJhv45ZrXh3TSGL3tNUREgWYhkKAIcsBonlNmN9WJGNENybIGGxL/cDNL1RM1LETVYSCVhUQ2l0bmNqdltlR
tdpdX9YKbRR4L0IfuEqIeNQoG9mZZhTm/NFBwyZZrkKWVgL4101FTAD3kBGYHG2TXtIfVTUHLLsCp4BmMFvQLPqIBD68Xw4JegEVkY8J+7XTO+EEWZiE6GK2gB6s5CL0+56uU/SdzMg
iDA5FXMP3CozM2AnU2HDTphYjo1syvurZk9CmuLs9z+NBYcPuQ8eChgi7QBbynlVb0awH2I03QsLPwh0t+MxjIn1UPzGmRPbk1mLJD63LpbC+ECfII+qFbBIHx4kp8f5gCW26vSziFf
Zu3nXp4iG7jG4VT/yTU3yUdriDA/APgpvFYHW3UQRbXxNMe2anrECdrugDffmX3e6aPcGBvwssAf/kTw6d3DyQvGYhpTY1X8V6V+d4+VlqyqpaTPsM2Fd16od5umz67kqrE= jboick
n@desktop
```

14.

Screenshot of new web page (image_page.html) displaying image




15. What is the difference between FTP, SFTP, and FTPS?
    FTP is file transfer with no encryption,
    SFTP is an extension to allow file transfer over SSH, and
    FTPS is the use of FTP with SSL/TLS encryption.