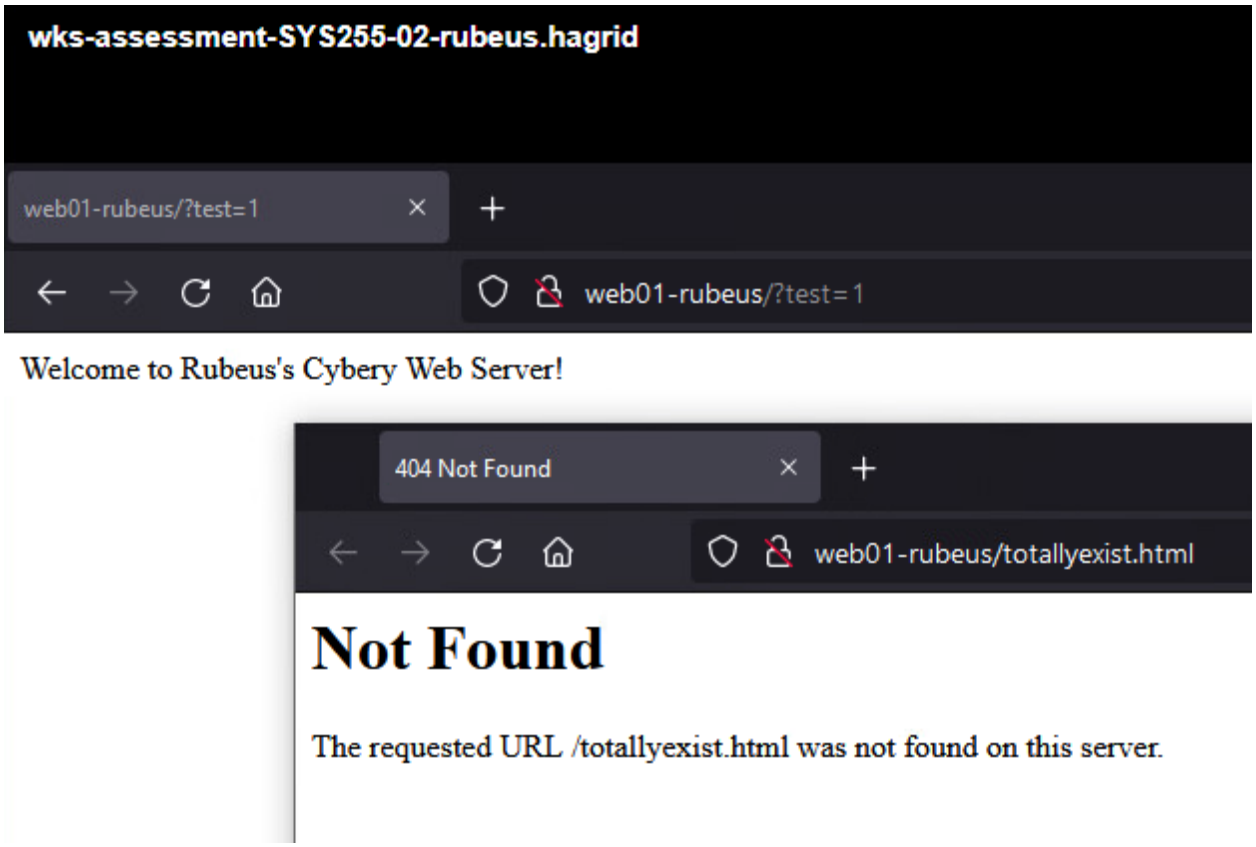
Apache Logging

💡 Nearly every linux/unix service stores logs in the /var/log directory. HTTPD is no exception. HTTPD logs are stored in /var/log/httpd. These logs are critical for both systems administration and security.

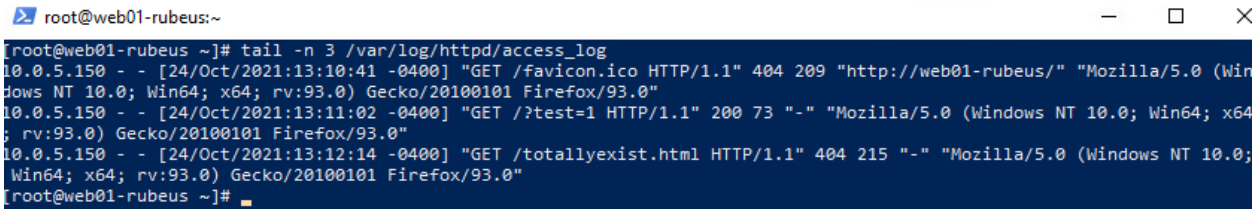
Conduct and experiment similar to the one below where the first search *http://web01-yourname/?test=1* (this will be successful and easy to find in the logs) is followed by an http request to a non-existent resource *http://web01-yourname/totallyexist.html*.



root@web01-rubeus:~

```
PS C:\Users\rubeus-adm> ssh rubeus@web01-rubeus
rubeus@web01-rubeus's password:
Last login: Sun Oct 24 11:34:19 2021 from ad02-rubeus.rubeus.local
Last login: Sun Oct 24 11:34:19 2021 from ad02-rubeus.rubeus.local
[rubeus@web01-rubeus ~]$ sudo -i
[sudo] password for rubeus:
[root@web01-rubeus ~]# ls /var/log/httpd
access_log  error_log
[root@web01-rubeus ~]#
```

Deliverable 1. Provide a similar screenshot to the one below:



Deliverable 2. Research the Apache Logging Format. For each of YOUR log entries that reflect the first successful (?test) and then an unsuccessful URL (totallyexist.html) attempts, fill out a table similar to the one below.

You must figure out which fields (space delimited are in your log). There are 11 fields, and a couple has been completed for you & Apache has solid documentation:

*Note: The field above that begins with GET has multiple fields within it.

Field Name	?test=1 event (successful), so ID the log fields and their values	doesnotexist.html event (unsuccessful), so ID the log fields and their values (some will be same; others not)
1. Remote Host	10.0.5.150	10.0.5.150
2. Browser Type	Mozilla 5.0	Mozilla 5.0
3. GET Method		
4. HTTP Status Code		
5.		
6.		
7.		
8.		
9.		
10.		
11.		