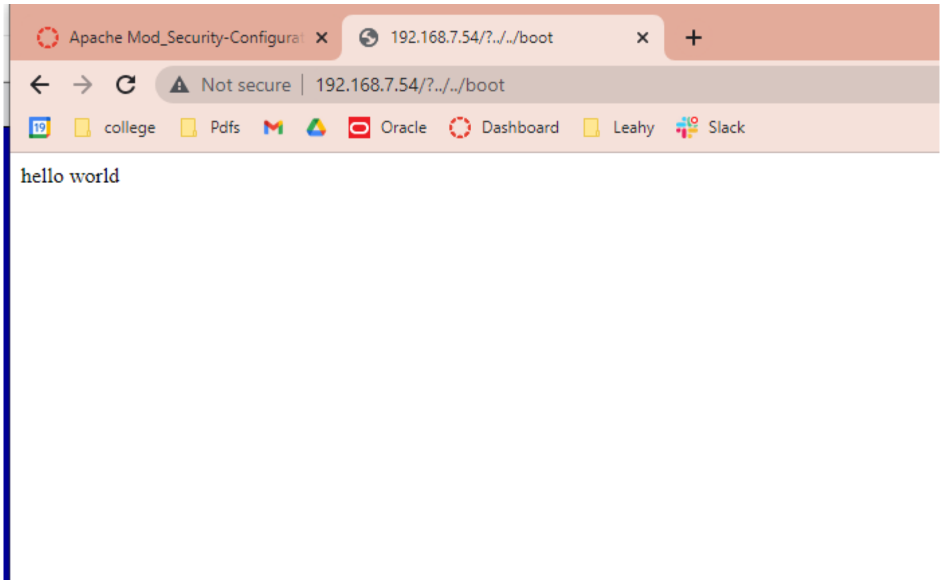
David Thomsen
SEC-260

3. To compare with later results, try the following simulated URLs attacks (read: not real) to your server from a browser and **record what happens:**

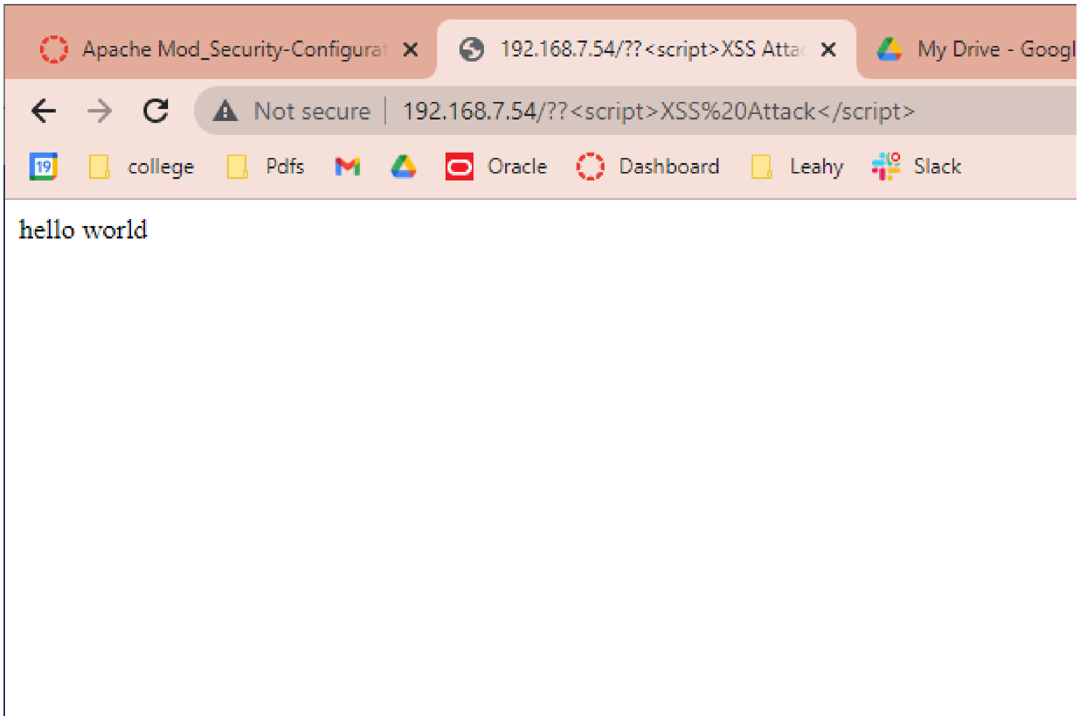
   -
     ```
     http://server-IP/?../../boot
     ```

   -
     ```
     http://server_ip??<script>XSS Attack</script>
     ```



192.168.7.54/?../../boot

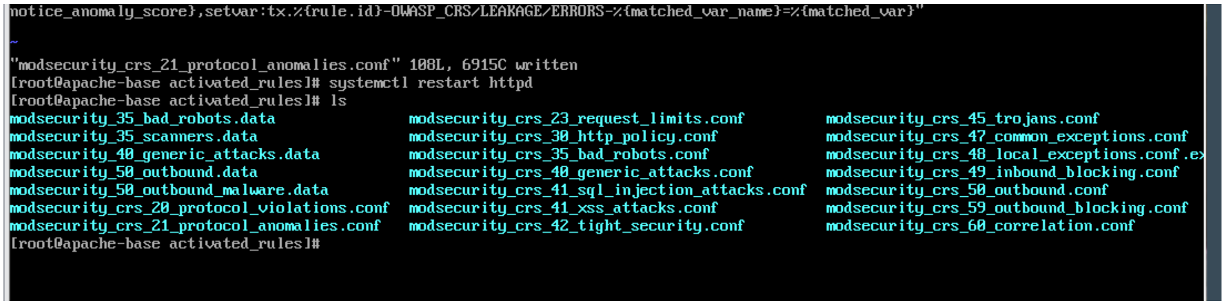
hello world


Apache Mod_Security-Configurat
192.168.7.54/??<script>XSS Attac
My Drive - Googl
Not secure
college
Pdfs
Oracle
Dashboard
Leahy
Slack

192.168.7.54/??<script>XSS%20Attack</script>

hello world

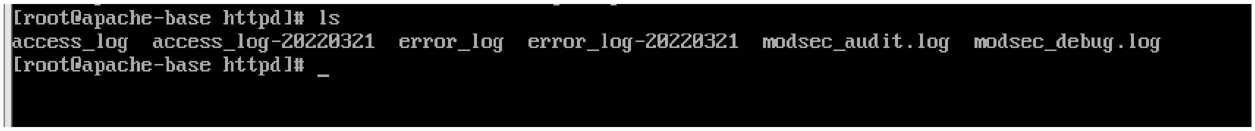
Screenshot of a 'ls' of /etc/httpd/modscurity.d/activated_rules showing that the rules were installed.



```
notice_anomaly_score},setvar:tx.%{rule.id}-OWASP_CRS/LEAKAGE/ERRORS-%{matched_var_name}=%{matched_var}"

~
"modsecurity_crs_21_protocol_anomalies.conf" 108L, 6915C written
[root@apache-base activated_rules]# systemctl restart httpd
[root@apache-base activated_rules]# ls
modsecurity_35_bad_robots.data               modsecurity_crs_23_request_limits.conf         modsecurity_crs_45_trojans.conf
modsecurity_35_scanners.data                 modsecurity_crs_30_http_policy.conf            modsecurity_crs_47_common_exceptions.conf
modsecurity_40_generic_attacks.data          modsecurity_crs_35_bad_robots.conf             modsecurity_crs_48_local_exceptions.conf.ex
modsecurity_50_outbound.data                 modsecurity_crs_40_generic_attacks.conf        modsecurity_crs_49_inbound_blocking.conf
modsecurity_50_outbound_malware.data         modsecurity_crs_41_sql_injection_attacks.conf  modsecurity_crs_50_outbound.conf
modsecurity_crs_20_protocol_violations.conf  modsecurity_crs_41_xss_attacks.conf            modsecurity_crs_59_outbound_blocking.conf
modsecurity_crs_21_protocol_anomalies.conf   modsecurity_crs_42_tight_security.conf         modsecurity_crs_60_correlation.conf
[root@apache-base activated_rules]#
```

Screenshot showing that the /var/log/httpd/modsec_audit.log was created



```
[root@apache-base httpd]# ls
access_log  access_log-20220321  error_log  error_log-20220321  modsec_audit.log  modsec_debug.log
[root@apache-base httpd]# _
```