David Thomsen
SEC-260

```
--8924f947-H--
Message: Access denied with code 403 (phase 2). Pattern match "(?i)(?:\\x5c|(?:%(?:2(?:5(?:2f|5c)|%46
%80%af|1u|5c)|\\/))(?:%(?:2(?:(?:52)?e|%45)|(?:e0%8|c)0%ae|u(?:002e|2024)|%32(?:%45|E))|\\.){2}(?:\\x
 at REQUEST_URI. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_42_tight_security.co
al Attack"] [data "Matched Data: /../ found within REQUEST_URI: /?../../boot"] [severity "CRITICAL"]
"OWASP_CRS/WEB_ATTACK/DIR_TRAVERSAL"]
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 192.168.7.122] ModSecurity: Access
\\\\x5c|(?:%(?:2(?:5(?:2f|5c)|%46|f)|c(?:0%(?:9v|af)|1%1c)|u(?:221[56]|002f)|%32(?:%46|F)|e0%80%af|1u
:002e|2024)|%32(?:%45|E))|\\\\\\\\\.){2}(?:\\\\\\\\\x5c|(?:%(?:2(?:5(?:2f|5c)|%46|f)|c(?:0%(?:9v|af)|1%
ctivated_rules/modsecurity_crs_42_tight_security.conf"] [line "20"] [id "950103"] [rev "2"] [msg "Pat
 REQUEST_URI: /?../../boot"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "
92.168.7.54"] [uri "/"] [unique_id "YjnW7D-oJQFlSKEQiKGhtAAAAAE"]
Action: Intercepted (phase 2)
Stopwatch: 1647957740528967 913 (- - -)
Stopwatch2: 1647957740528967 913; combined=527, p1=205, p2=288, p3=0, p4=0, p5=34, sr=60, sw=0, l=0,
Response-Body-Transformed: Dechunked
Producer: ModSecurity for Apache/2.9.2 (http://www.modsecurity.org/); OWASP_CRS/2.2.9.
Server: Apache/2.4.6 (CentOS)
Engine-Mode: "ENABLED"
```

```
Message: Access denied with code 403 (phase 2). Pattern match "(?i:([\\s'\"`\xc
99\xe2\x80\x98\\|\\|[*?|[?:]?:=|<=>|r?like|sounds\\s+like|regexp)([\\s'\"`\xc2\
 at ARGS_NAMES:?<script>XSS_Attack</script>. [file "/etc/httpd/modsecurity.d/ac
0901"] [rev "2"] [msg "SQL Injection Attack: SQL Tautology Detected."] [data "M
t>: ?<script>XSS_Attack</script>"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"
WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI
```

```
[root@apache-base httpd]# telnet localhost 80
Trying ::1...
Connected to localhost.
Escape character is '^]'.
GET / HTTP/1.1
Host: 192.168.7.54

HTTP/1.1 403 Forbidden
Date: Tue, 22 Mar 2022 14:11:31 GMT
Server: Apache/2.4.6 (CentOS)
Content-Length: 202
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /
on this server.</p>
</body></html>
Connection closed by foreign host.
[root@apache-base httpd]# _
```

```
--d0048a5c-H--
Message: Access denied with code 403 (phase 2). Operator EQ matched 0 at REQUEST_HEADERS. [file "/et
tocol_anomalies.conf"] [line "47"] [id "960015"] [rev "1"] [msg "Request Missing an Accept Header"]
accuracy "9"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/MISSING_HEADER_ACCEPT"] [tag "WASCTC/WASC-21"] [tag
Apache-Error: [file "apache2 util.c"] [line 271] [level 3] [client ::1] ModSecurity: Access denied w
```

The error code that I received is a 403 error due to violation of the MISSING_HEADER_ACCEPT protocol. I could change this rule so that it would be possible to telnet in or I could alter the telnet request and using a HEAD request.