Breaking the Perfect HTTP Feedback Loop with Chaos Fortress

Christian Folini

netnea

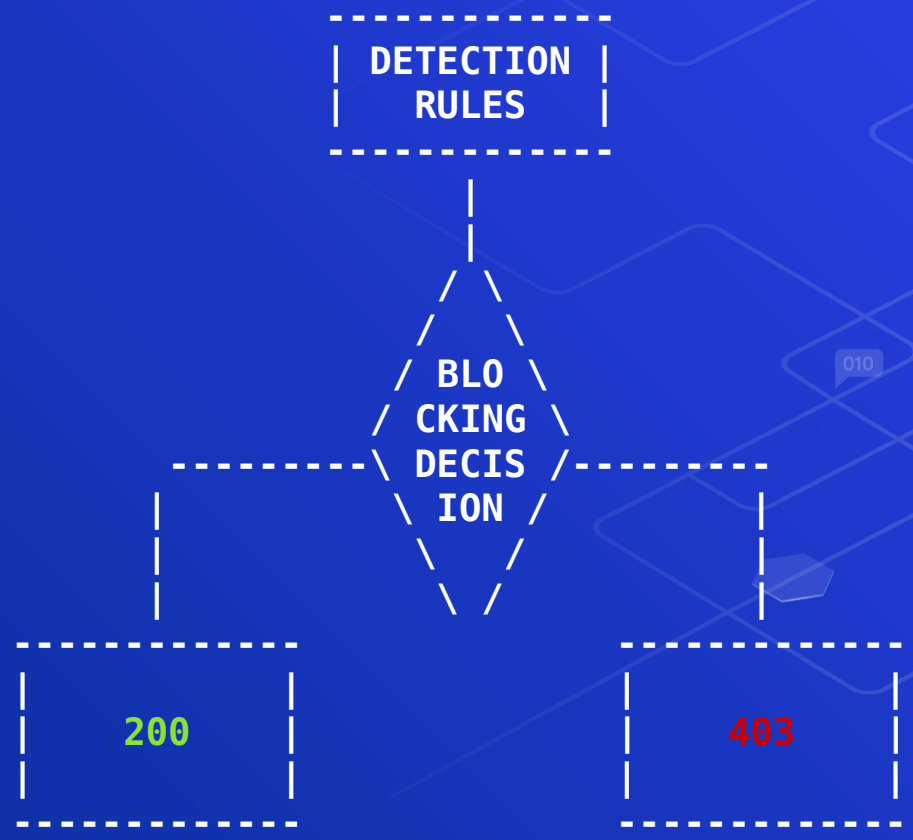
Chaos Fortress Plugin

Chaos Fortress is a CRS extension that delays attackers and thwarts their feedback loop.

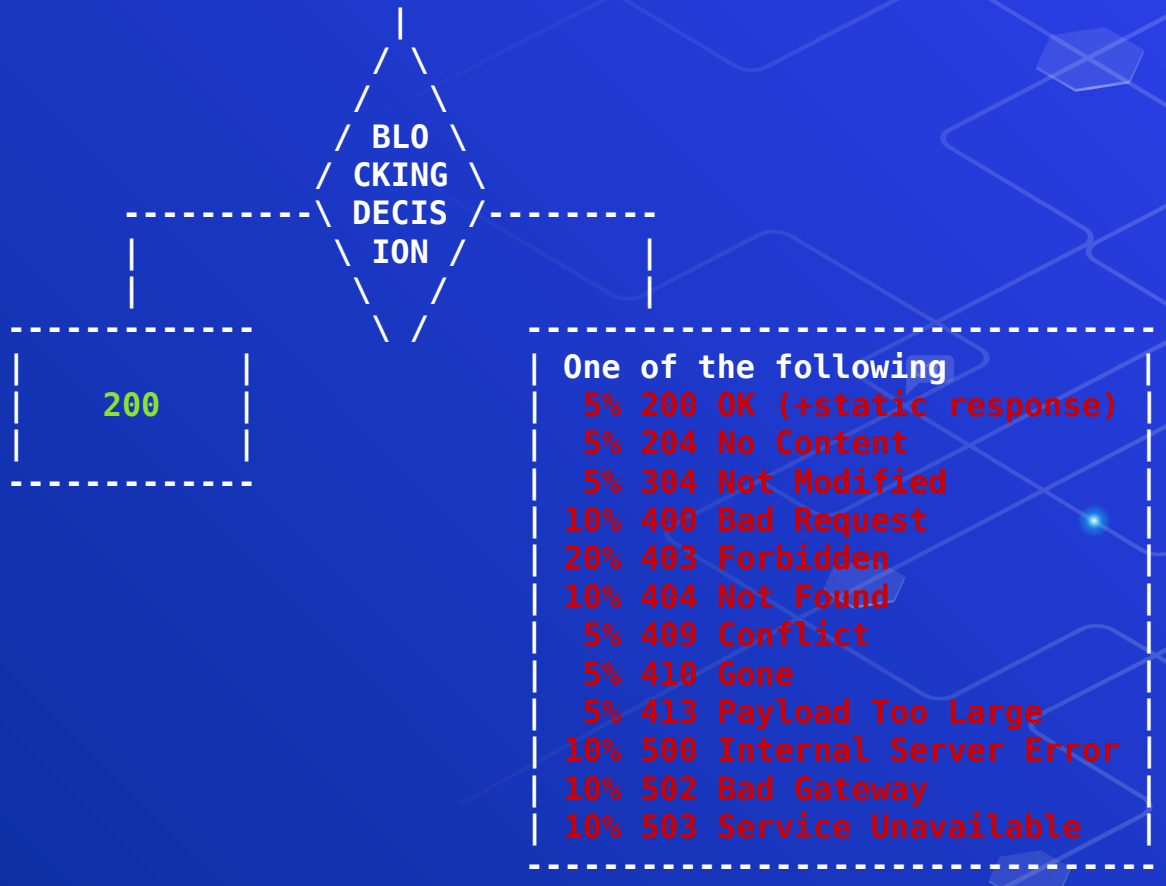
Don´t use around False Positives!

Parents are responsible for their kids.

Standard CRS Blocking



Chaos Fortress Blocking



But how to do random status code?

Problem 1: There is nothing like a random function in the ModSec rule language.

Problem 2: You can´t set the response status code dynamically.

Getting Entropy


```
SecRule UNIQUE_ID "@rx ^[a-f]*([0-9])[a-f]*([0-9])"
    "id:9500510,\
    phase:2,\
    pass,\
    capture,\
    t:sha1,t:hexEncode,\
    nolog,\
    setvar:'TX.cf_block_num=%{TX.1}%{TX.2}'"
```

```
Example UNIQUE_ID: ZzTenElNpV4Xq8o128k6OAAAABQ
```

Responding with a random status code

```
SecRule TX:BLOCKING_INBOUND_ANOMALY_SCORE "@lt %{tx.inbound_anomaly_score_threshold}" \
    "id:9500610,\
    phase:2,\
    pass,\
    t:none,\
    nolog,\
    skipAfter:'Chaos-Fortress-Blockade'"

SecRule TX:cf_block_num "@lt   5"  "id:9500620,phase:2,deny,status:200,...
SecRule TX:cf_block_num "@lt  10"  "id:9500621,phase:2,deny,status:204,...
SecRule TX:cf_block_num "@lt  15"  "id:9500622,phase:2,deny,status:304,...
SecRule TX:cf_block_num "@lt  25"  "id:9500623,phase:2,deny,status:400,...
SecRule TX:cf_block_num "@lt  45"  "id:9500624,phase:2,deny,status:403,...
SecRule TX:cf_block_num "@lt  55"  "id:9500625,phase:2,deny,status:404,...
SecRule TX:cf_block_num "@lt  65"  "id:9500626,phase:2,deny,status:409,...
SecRule TX:cf_block_num "@lt  70"  "id:9500627,phase:2,deny,status:410,...
SecRule TX:cf_block_num "@lt  75"  "id:9500628,phase:2,deny,status:413,...
SecRule TX:cf_block_num "@lt  80"  "id:9500629,phase:2,deny,status:500,...
SecRule TX:cf_block_num "@lt  90"  "id:9500630,phase:2,deny,status:502,...
SecRule TX:cf_block_num "@lt 100"  "id:9500631,phase:2,deny,status:503,...

SecMarker Chaos-Fortress-Blockade
```

Adding Random Delay!

```
SecRule REQUEST_FILENAME \
   "@inspectFile chaos-fortress-delay.lua" \
   "id:9500611,phase:2,pass,nolog"


chaos-fortress-delay.log:

function main()

    math.randomseed(os.time())

    pause=tostring(math.random(1, 100) / 10)

    m.log(2, string.format("Chaos Fortress plugin pausing %s seconds", pause))

    os.execute("sleep " .. pause)

    return 1

end
```

Consistent Random Status Codes


```
SecAction "id:9500501,phase:2,pass,nolog, \
        setvar:'TX.cf_hash_base=%{REMOTE_ADDR}%{REQUEST_METHOD}%{REQUEST_FILENAME} \
        %{ARGS_GET_NAMES}%{ARGS_GET}%{ARGS_POST_NAMES}%{ARGS_POST}'"

SecRule TX:cf_hash_base "@rx ^[a-f]*([0-9])[a-f]*([0-9])" \
    "id:9500510,\
    phase:2,\
    pass,\
    capture,\
    t:sha1,t:hexEncode,\
    nolog,\
    setvar:'TX.cf_block_num=%{TX.1}%{TX.2}'"
```

Let’s look at code

Demo Time

Security Scanner Output


```
+ OSVDB-3092: /webcgi/webutils.pl: This might be interesting...
+ OSVDB-3092: /cpa.nsf: This database can be read without authentication, ...
+ /webcgi/perl?-v: Perl is installed in the CGI directory. This essentially ...
+ OSVDB-3093: /webcgi/csPassword/csPassword.cgi: This might be interesting...
+ /webcgi/admin/admin.cgi: May be ImageFolio Pro administration CGI.
+ OSVDB-3233: /servlet/SearchServlet: Novell Netware default servlet found...
+ OSVDB-3093: /ows-bin//_vti_pvt/doctodep.btr: This might be interesting...
+ OSVDB-3092: /publicar/: This might be interesting...
+ /webcgi/mkilog.exe: This CGI can give an attacker a lot of information.
+ OSVDB-3092: /shopper/: This might be interesting...
+ OSVDB-3092: /webcgi/stats/: This might be interesting...
+ OSVDB-3093: /scripts/cli.dll?tpl=nonexistfile?template=..\winnt\system32\cmd.exe?/c+dir
+ OSVDB-3092: /activex/: This might be interesting...
+ OSVDB-3092: /samples/search/queryhit.htm: This might be interesting...
+ /webcgi/photo/manage.cgi: My Photo Gallery management interface. May allow full access ...
...
272 Findings in total
```

5.
Q&A

Christian Folini

https://christian-folini.ch
https://www.linkedin.com/in/christian-folini-588ba278/
mailto:christian.folini@netnea.com
X: @ChrFolini

https://github.com/dune73/chaos-fortress-plugin