Hackerscheuche: Fail2ban

„einfach“ & schön

Dr. Dirk Wetter, 20.6.2024

Motivation

- Klassiker
- Vorinstalliert, Default „suboptimal“
- Schattendasein, kann viel mehr
- Quick-wins, aber: Shoot in foot

- Tipps, wie man das meiste einbremsen kann

about:me

- Open Source
  - testssl.sh
  - OWASP: Stammtisch Hamburg, Konferenzen, Projekte
  - 2006 Koautor Linux-Buch
- Brotwerb: Selbständiger Sicherheitsberater >14 Jahren
  - Technik: Pentests (Webapps, Netze, Systeme)
  - Beratung
  - Informationsecuritymanagement

Agenda

- Funktionsprinzip
- Konfiguration 101: wo finde ich was?
  - Beispiele zur Verdeutlichung
- Webserver-Verteidigung:
  - Scanner, Bots
  - Login, Formulare, Admin-Logins
  - Krude GET-Requests
  - Und was ist mit POST??

Funktionsprinzip

- Python-Service
  - Analysiert Logdateien —> Posthum
  - Pattern Matching
  - Basierend darauf: Aktionen
    - Standard: iptables (nftables, firewall-cmd, pf, ip route)
    - Benachrichtigung: E-Mail, Slack, Matrix , irc/xmpp, $whatsoever

Und meine Container??

- Microservices (TBC 🧐)
  - Plain Docker / `docker-compose`
    - Urgs: `/var/lib/docker/containers/<id>/<datei>`
    - Besser: volume mount in host
  - `podman --log-opt path=/var/log/container/file.json`
  - K8s 🤷‍♂️
    - RAW tables?
    - Networking API (fail2ban/#3644)

`docker ps`

Und meine Container??

- Microservices (TBC 🧐)
  - Plain Docker / `docker-compose`
    - Urgs: `/var/lib/docker/containers/<id>/<datei>`
    - Besser: volume mount in host
  - `podman --log-opt path=/var/log/container/file.json`
  - K8s 🤷‍♂️
    - RAW tables?
    - Networking API (fail2ban/#3644)

`docker ps`

Konfiguration 101

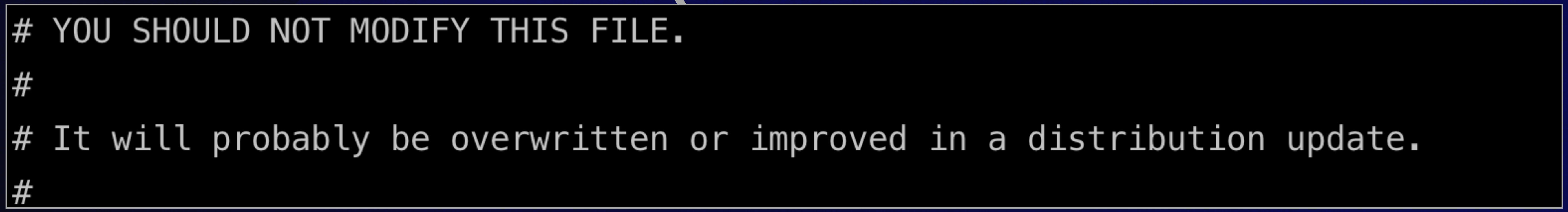
`– /etc/fail2ban/`	Hauptverzeichnis
`|__ fail2ban.conf`	Haupt-Konfigurationsdatei (Distributor)
`|__ fail2ban.local`	hier lokal, wenn nötig

Konfiguration 101 - Jails

```
– /etc/fail2ban/

        |__ jail.conf        Jail-Konfigurationsdatei  (Distributor)

        |__ jail.local       hier lokal, meistens nötig
```

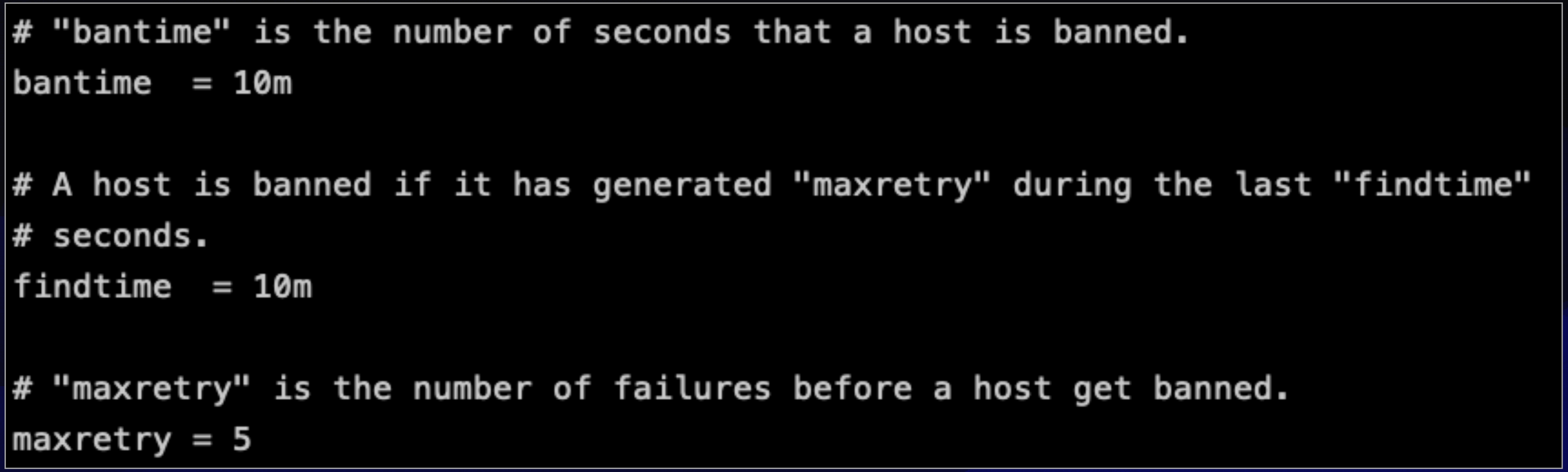
Konfiguration 101 - Jails

```
– /etc/fail2ban/

          |__ jail.conf          Jail-Konfigurationsdatei  (Distributor)

          |__ jail.local         hier lokal, meistens nötig
```



```
# YOU SHOULD NOT MODIFY THIS FILE.
#
# It will probably be overwritten or improved in a distribution update.
#
```

/etc/fail2ban/jail.conf



```
# "bantime" is the number of seconds that a host is banned.
bantime  = 10m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime  = 10m

# "maxretry" is the number of failures before a host get banned.
maxretry = 5
```

/etc/fail2ban/jail.local (1)

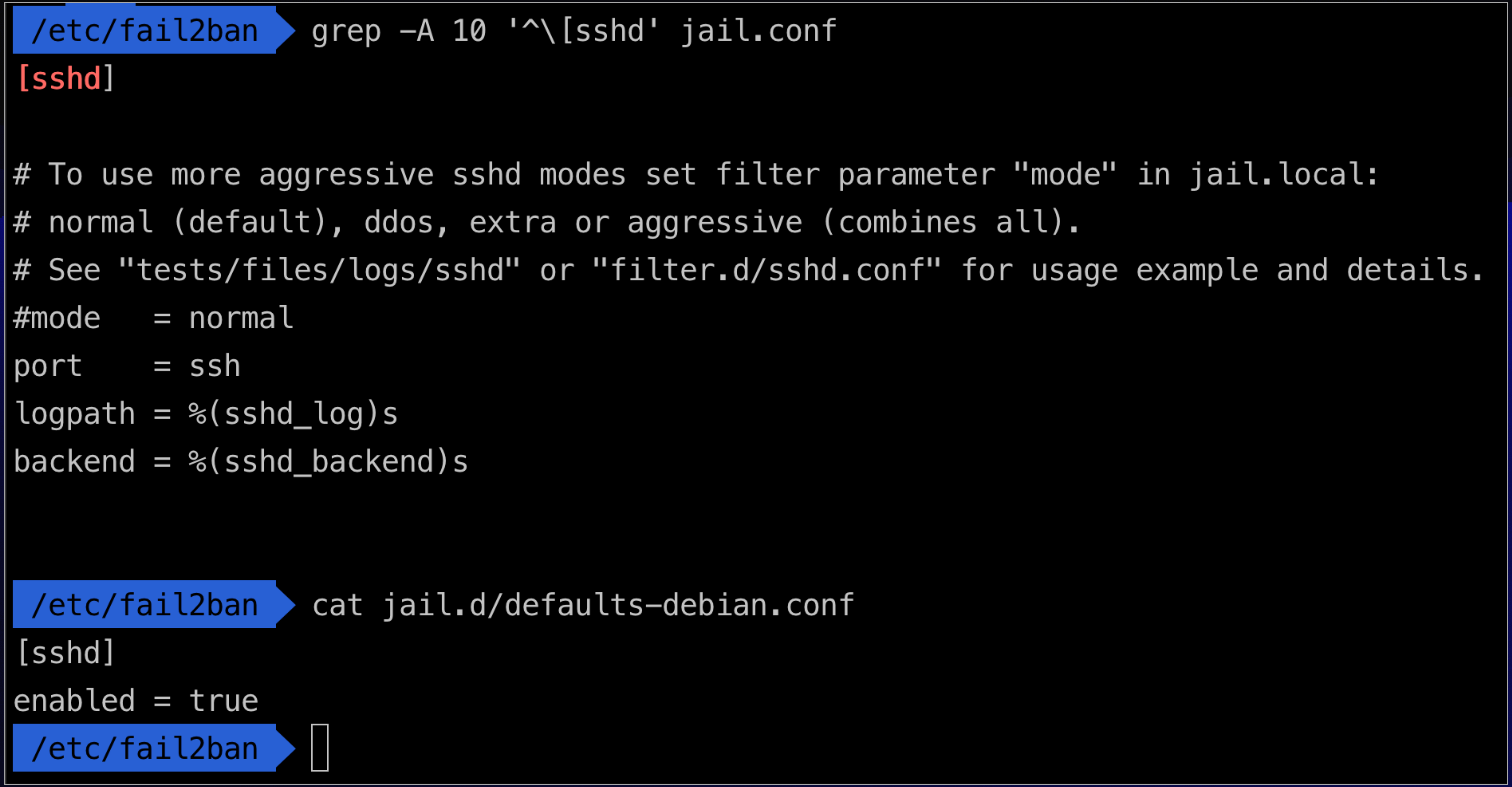
```
[redacted]:/etc/fail2ban 0# cat jail.local

[DEFAULT]
ignoreip = 127.0.0.1/8 81.169.[redacted]/32 81.169.[redacted]/32 198.245[redacted]/32 2a01:238:4308:[redacted]/128

bantime.increment = true
bantime.rndtime = 360
bantime.factor = 1
bantime.formula = ban.Time * math.exp(float(ban.Count+1)*banFactor)/math.exp(1*banFactor)
[redacted]:/etc/fail2ban 0#
```

Konfiguration 101

`– /etc/fail2ban/`	
`|__ action.d/`	Was soll passieren?
`|__ filter.d/`	Regex pattern für Logdatei
`|__ jail.d/`	Hier deine Konfigurationen rein

Los gehts

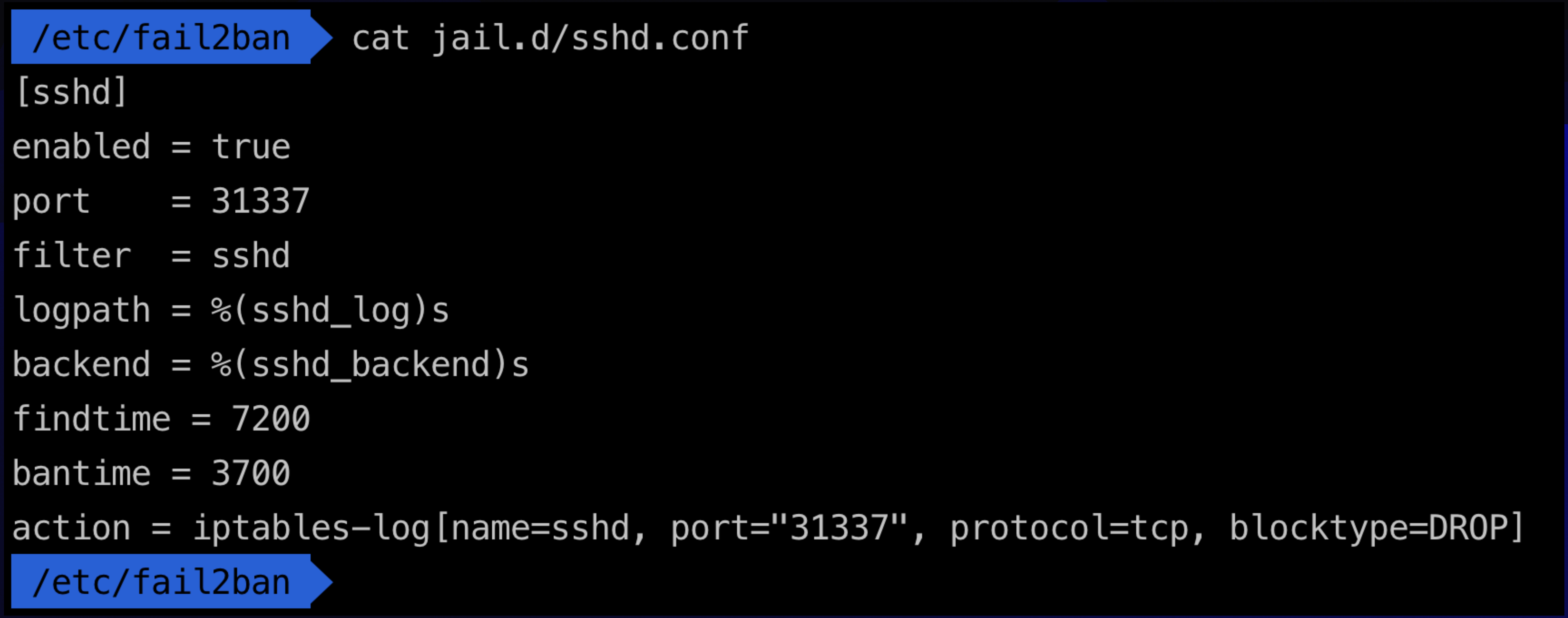
- Klassiker SSH — vorkonfiguriert



```
/etc/fail2ban  grep -A 10 '^\[sshd' jail.conf
[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode   = normal
port    = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s


/etc/fail2ban  cat jail.d/defaults-debian.conf
[sshd]
enabled = true
/etc/fail2ban  
```

Los gehts

- SSH mit speziellen Ansprüchen



```
/etc/fail2ban  cat jail.d/sshd.conf
[sshd]
enabled = true
port    = 31337
filter  = sshd
logpath = %(sshd_log)s
backend = %(sshd_backend)s
findtime = 7200
bantime = 3700
action = iptables-log[name=sshd, port="31337", protocol=tcp, blocktype=DROP]
/etc/fail2ban 
```

```
/etc/fail2ban  grep -v '^#' filter.d/sshd.conf | sed '/^$/d'
[INCLUDES]
before = common.conf
[DEFAULT]
_daemon = sshd
__pref = (?:(?:error|fatal): (?:PAM: )?)?
__suff = (?: (?:port \d+|on \S+|\[preauth\])){0,3}\s*
__on_port_opt = (?: (?:port \d+|on \S+)){0,2}
__authng_user = (?: (?:invalid|authenticating) user <F-USER>\S+|.*?</F-USER>)?
__alg_match = (?:(?:\w+ (?!found\b)){0,2}\w+)
__pam_auth = pam_[a-z]+
[Definition]
prefregex = ^<F-MLFID>%(__prefix_line)s</F-MLFID>%(__pref)s<F-CONTENT>.+</F-CONTENT>$
cmnfailre = ^[aA]uthentication (?:failure|error|failed) for <F-USER>.*</F-USER> from <HOST>( via \S+)?%(__suff)s$
            ^User not known to the underlying authentication module for <F-USER>.*</F-USER> from <HOST>%(__suff)s$
            <cmnfailre-failed-pub-<publickey>>
            ^Failed <cmnfailed> for (?P<cond_inv>invalid user )?<F-USER>(?P<cond_user>\S+)|(?(cond_inv)(?:(?! from ).)*?|[^:]+)</F-USER> from <HOST>%(__on_port_opt)s(?: ssh\d*)?(?(cond_user): |(?:(?:(?! from ).)*)$)
            ^<F-USER>ROOT</F-USER> LOGIN REFUSED FROM <HOST>
            ^[iI](?:llegal|nvalid) user <F-USER>.*?</F-USER> from <HOST>%(__suff)s$
            ^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because not listed in AllowUsers%(__suff)s$
            ^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because listed in DenyUsers%(__suff)s$
            ^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because not in any group%(__suff)s$
            ^refused connect from \S+ \(<HOST>\)
            ^Received <F-MLFFORGET>disconnect</F-MLFFORGET> from <HOST>%(__on_port_opt)s:\s*3: .*: Auth fail%(__suff)s$
            ^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because a group is listed in DenyGroups%(__suff)s$
            ^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because none of user's groups are listed in AllowGroups%(__suff)s$
            ^<F-NOFAIL>%(__pam_auth)s\(sshd:auth\):\s+authentication failure;</F-NOFAIL>(?:\s+(?:(?:logname|e?uid|tty)=\S*)){0,4}\s+ruser=<F-ALT_USER>\S*</F-ALT_USER>\s+rhost=<HOST>(?:\s+user=<F-USER>\S*</F-USER>)?%(__suff)s$
            ^maximum authentication attempts exceeded for <F-USER>.*</F-USER> from <HOST>%(__on_port_opt)s(?: ssh\d*)?%(__suff)s$
            ^User <F-USER>\S+|.*?</F-USER> not allowed because account is locked%(__suff)s
            ^<F-MLFFORGET>Disconnecting</F-MLFFORGET>(?: from)?(?: (?:invalid|authenticating)) user <F-USER>\S+</F-USER> <HOST>%(__on_port_opt)s:\s*Change of username or service not allowed:\s*.*\[preauth\]\s*$
            ^Disconnecting: Too many authentication failures(?: for <F-USER>\S+|.*?</F-USER>)?%(__suff)s$
            ^<F-NOFAIL>Received <F-MLFFORGET>disconnect</F-MLFFORGET></F-NOFAIL> from <HOST>%(__on_port_opt)s:\s*11:
            <mdre-<mode>-other>
            ^<F-MLFFORGET><F-MLFGAINED>Accepted \w+</F-MLFGAINED></F-MLFFORGET> for <F-USER>\S+</F-USER> from <HOST>(?:\s|$)
cmnfailed-any = \S+
cmnfailed-ignore = \b(?!publickey)\S+
cmnfailed-invalid = <cmnfailed-ignore>
cmnfailed-nofail = (?:<F-NOFAIL>publickey</F-NOFAIL>|\S+)
cmnfailed = <cmnfailed-<publickey>>
mdre-normal =
mdre-normal-other = ^<F-NOFAIL><F-MLFFORGET>(Connection (?:closed|reset)|Disconnected)</F-MLFFORGET></F-NOFAIL> (?:by|from)%(__authng_user)s <HOST>(?:%(__suff)s|\s*)$
mdre-ddos = ^Did not receive identification string from <HOST>
            ^kex_exchange_identification: (?:read: )?(?:[Cc]lient sent invalid protocol identifier|[Cc]onnection (?:closed by remote host|reset by peer))
            ^Bad protocol version identification '.*' from <HOST>
            ^<F-NOFAIL>SSH: Server;Ltype:</F-NOFAIL> (?:Authname|Version|Kex);Remote: <HOST>-\d+;[A-Z]\w+:
            ^Read from socket failed: Connection <F-MLFFORGET>reset</F-MLFFORGET> by peer
            ^banner exchange: Connection from <HOST><__on_port_opt>: invalid format
mdre-ddos-other = ^<F-MLFFORGET>(Connection (?:closed|reset)|Disconnected)</F-MLFFORGET> (?:by|from)%(__authng_user)s <HOST>%(__on_port_opt)s\s+\[preauth\]\s*$
                  ^<F-NOFAIL><F-MLFFORGET>(Connection (?:closed|reset)|Disconnected)</F-MLFFORGET></F-NOFAIL> (?:by|from)%(__authng_user)s <HOST>(?:%(__on_port_opt)s|\s*)$
mdre-extra = ^Received <F-MLFFORGET>disconnect</F-MLFFORGET> from <HOST>%(__on_port_opt)s:\s*14: No(?: supported)? authentication methods available
            ^Unable to negotiate with <HOST>%(__on_port_opt)s: no matching <__alg_match> found.
            ^Unable to negotiate a <__alg_match>
            ^no matching <__alg_match> found:
mdre-extra-other = ^<F-MLFFORGET>Disconnected</F-MLFFORGET>(?: from)?(?: (?:invalid|authenticating)) user <F-USER>\S+|.*?</F-USER> <HOST>%(__on_port_opt)s \[preauth\]\s*$
mdre-aggressive = %(mdre-ddos)s
                  %(mdre-extra)s
mdre-aggressive-other = %(mdre-ddos-other)s
publickey = nofail
cmnfailre-failed-pub-invalid = ^Failed publickey for invalid user <F-USER>(?P<cond_user>\S+)|(?:(?! from ).)*?</F-USER> from <HOST>%(__on_port_opt)s(?: ssh\d*)?(?(cond_user): |(?:(?:(?! from ).)*)$)
cmnfailre-failed-pub-any =
cmnfailre-failed-pub-nofail = <cmnfailre-failed-pub-invalid>
cmnfailre-failed-pub-ignore =
cfooterre = ^<F-NOFAIL>Connection from</F-NOFAIL> <HOST>
failregex = %(cmnfailre)s
            <mdre-<mode>>
            %(cfooterre)s
mode = normal
ignoreregex =
maxlines = 1
journalmatch = _SYSTEMD_UNIT=sshd.service + _COMM=sshd
/etc/fail2ban 
```

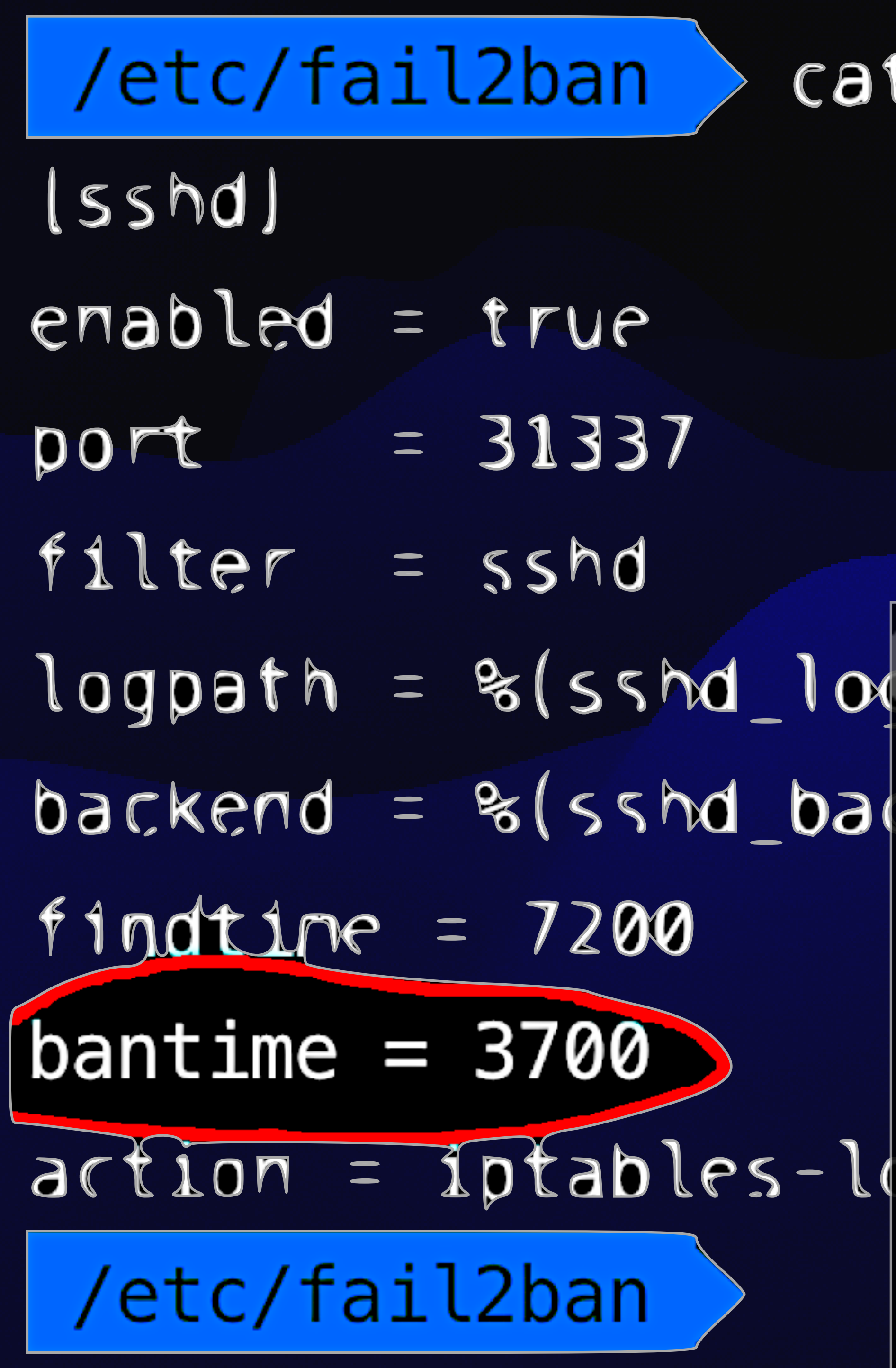
```
/etc/fail2ban  grep -v '^#' filter.d/sshd.conf | sed '/^$/d' | wc -l
69
/etc/fail2ban 
```

- SSH – Regexe sind vorkonfiguriert (puh)

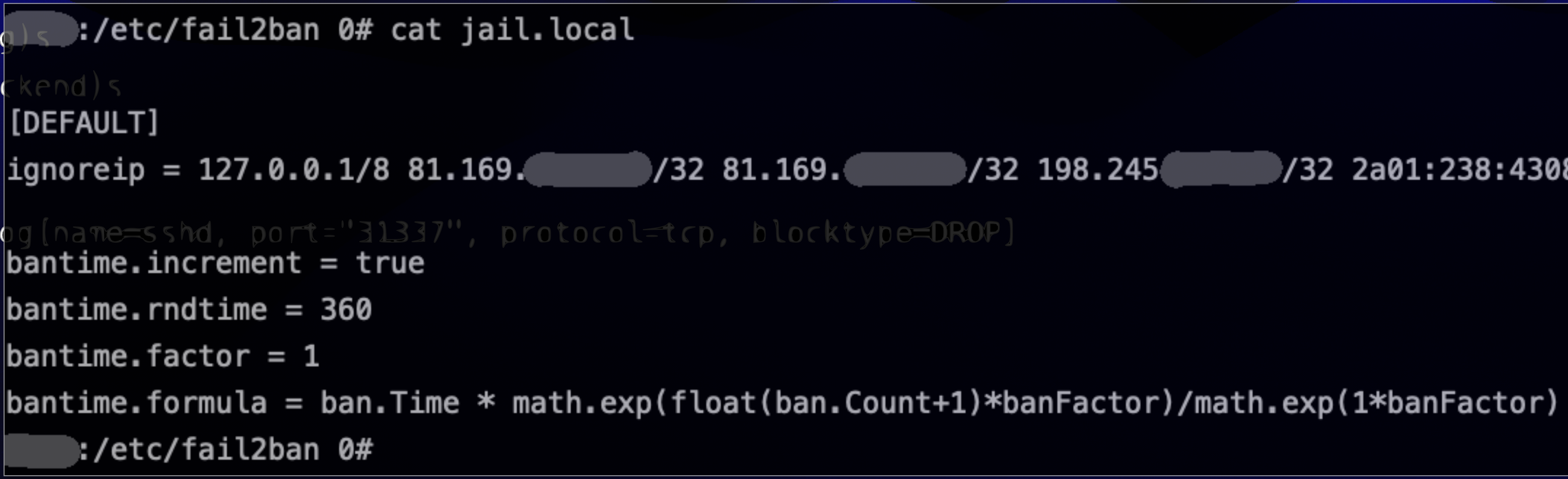
```
cmnfailre =
```

```
^[aA]uthentication (?:failure|error|failed) for <F-USER>.*</F-USER> from <HOST>( via \S+)?%(__suff)s$
^User not known to the underlying authentication module for <F-USER>.*</F-USER> from <HOST>%(__suff)s$
<cmnfailre-failed-pub-<publickey>>
^Failed <cmnfailed> for (?P<cond_inv>invalid user )?<F-USER>(?P<cond_user>\S+)|(?(cond_inv)(?:(?! from ).)*?|[^:]+)</F-USER> from <HOST>%(__on_port_opt)s(?: ssh\d*)?(?(cond_us
^<F-USER>ROOT</F-USER> LOGIN REFUSED FROM <HOST>
^[iI](?:llegal|nvalid) user <F-USER>.*?</F-USER> from <HOST>%(__suff)s$
^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because not listed in AllowUsers%(__suff)s$
^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because listed in DenyUsers%(__suff)s$
^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because not in any group%(__suff)s$
^refused connect from \S+ \(<HOST>\)
^Received <F-MLFFORGET>disconnect</F-MLFFORGET> from <HOST>%(__on_port_opt)s:\s*3: .*: Auth fail%(__suff)s$
^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because a group is listed in DenyGroups%(__suff)s$
^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because none of user's groups are listed in AllowGroups%(__suff)s$
^<F-NOFAIL>%(__pam_auth)s\(sshd:auth\):\s+authentication failure;</F-NOFAIL>(?:\s+(?:(?:logname|e?uid|tty)=\S*)){0,4}\s+ruser=<F-ALT_USER>\S*</F-ALT_USER>\s+rhost=<HOST>(?:\s+
^maximum authentication attempts exceeded for <F-USER>.*</F-USER> from <HOST>%(__on_port_opt)s(?: ssh\d*)?%(__suff)s$
```

/etc/fail2ban/jail.local (2)



```
/etc/fail2ban  cat jail.d/sshd.conf
[sshd]
enabled = true
port     = 31337
filter   = sshd
logpath  = %(sshd_log)s
backend  = %(sshd_backend)s
findtime = 7200
bantime = 3700
action = iptables-log[name=sshd, port="31337", protocol=tcp, blocktype=DROP]
/etc/fail2ban
```



```
[redacted]:/etc/fail2ban 0# cat jail.local

[DEFAULT]
ignoreip = 127.0.0.1/8 81.169.[redacted]/32 81.169.[redacted]/32 198.245[redacted]/32 2a01:238:4308
bantime.increment = true
bantime.rndtime = 360
bantime.factor = 1
bantime.formula = ban.Time * math.exp(float(ban.Count+1)*banFactor)/math.exp(1*banFactor)
[redacted]:/etc/fail2ban 0#
```

/etc/fail2ban/jail.local (2)

```
[redacted]:/var/log 0# zgrep -h  '193.32.162.80'  fail2ban.log-2024*.gz  fail2ban.log | grep  'postfix_unknown] Increase'
2024-02-15 02:31:27,215 fail2ban.observer [1387]: NOTICE  [postfix_unknown] Increase Ban 193.32.162.80 (2 # 2:48:44 -> 2024-02-15 05:20:11)
2024-02-23 17:17:44,542 fail2ban.observer [1387]: NOTICE  [postfix_unknown] Increase Ban 193.32.162.80 (2 # 2:45:25 -> 2024-02-23 20:03:09)
2024-02-23 20:44:40,787 fail2ban.observer [1387]: NOTICE  [postfix_unknown] Increase Ban 193.32.162.80 (3 # 7:24:59 -> 2024-02-24 04:09:39)
2024-02-24 04:30:45,250 fail2ban.observer [1387]: NOTICE  [postfix_unknown] Increase Ban 193.32.162.80 (4 # 20:10:11 -> 2024-02-25 00:40:55)
2024-02-25 00:41:21,155 fail2ban.observer [1387]: NOTICE  [postfix_unknown] Increase Ban 193.32.162.80 (5 # 2 days, 6:36:05 -> 2024-02-27 07:17:25)
2024-02-27 11:36:54,159 fail2ban.observer [1387]: NOTICE  [postfix_unknown] Increase Ban 193.32.162.80 (6 # 6 days, 4:26:14 -> 2024-03-04 16:03:07)
2024-03-04 17:22:17,338 fail2ban.observer [1387]: NOTICE  [postfix_unknown] Increase Ban 193.32.162.80 (7 # 16 days, 19:28:10 -> 2024-03-21 12:50:26)
2024-04-01 12:09:37,347 fail2ban.observer [24933]: NOTICE  [postfix_unknown] Increase Ban 193.32.162.80 (8 # 45 days, 16:38:58 -> 2024-05-17 04:48:34)
2024-05-25 19:26:45,896 fail2ban.observer [1423]: NOTICE  [postfix_unknown] Increase Ban 193.32.162.80 (9 # 124 days, 5:00:32 -> 2024-09-27 00:27:17)
[redacted]:/var/log 0#
```

/etc/fail2ban/jail.local (2)

https://www.abuseipdb.com/check/193.32.162.80

AbuseIPDB » *193.32.162.80*

Check an IP Address, Domain Name, or Subnet
e.g. [redacted], **microsoft.com**, or **5.188.10.0/24**

193.32.162.80 was found in our database!

This IP was reported **4,302** times. Confidence of Abuse is **100%**:

100%

IP Abuse Reports for **193.32.162.80**:

This IP address has been reported a total of **4,302** times from 224 distinct sources. 193.32.162.80 was first reported on February 7th 2024, and the most recent report was **1 day ago**.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

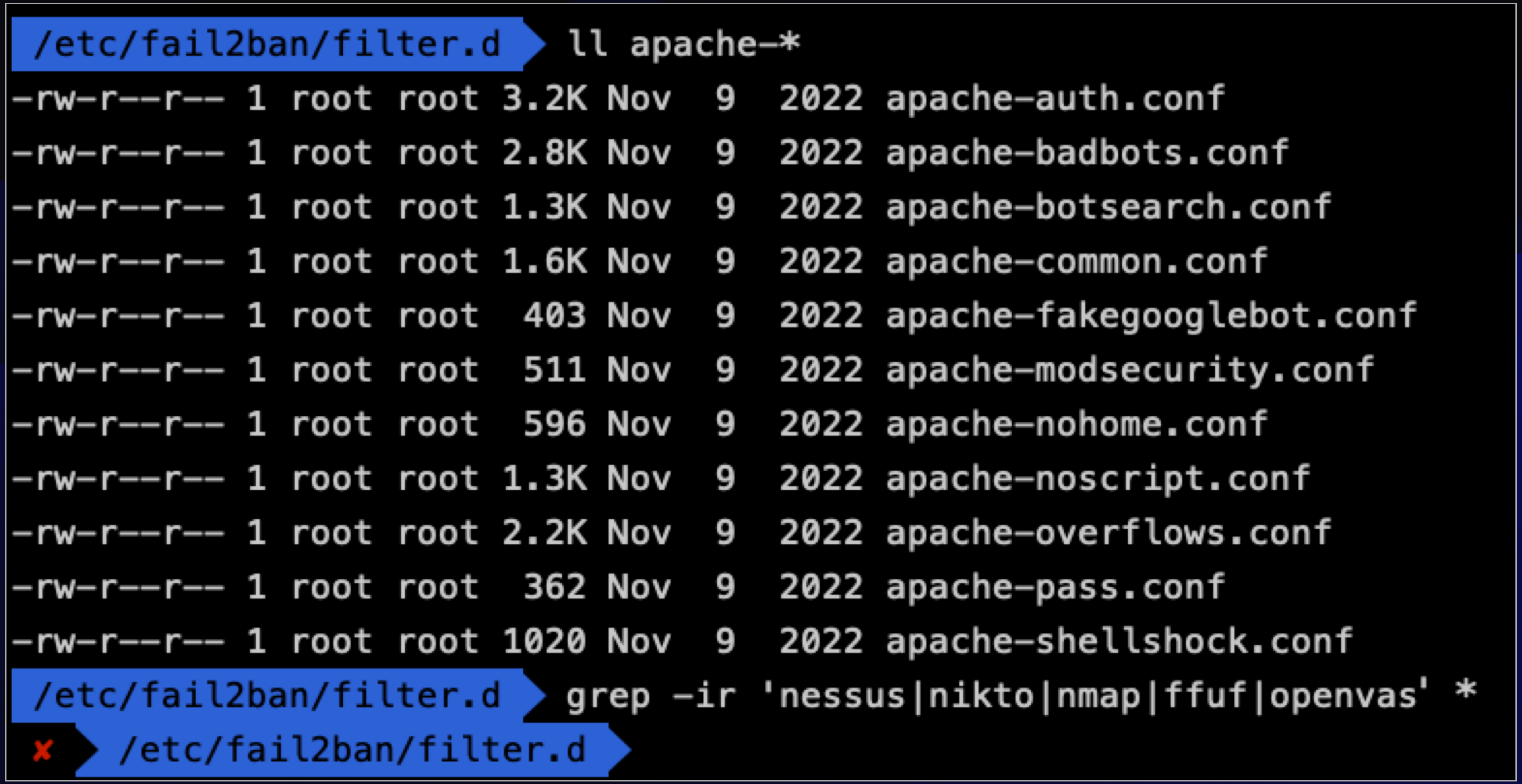
Reporter	IoA Timestamp in UTC	Comment	Categories
✓ CRSSkynet	2024-06-07 11:24:05 (1 day ago)	Jun 7 11:55:16 hosting vpopmail[36225]: vchkpw-smtp: vpopmail user not found info@getonair.uk:193.3 ... show more	Brute-Force
✓ dwmp	2024-06-07 00:56:22 (1 day ago)	Jun 7 02:56:20 plesk postfix/smtpd[166294]: warning: unknown[193.32.162.80]: SASL LOGIN authenticat ... show more	Brute-Force SSH
✓ swehosting.se	2024-06-07 00:32:08 (1 day ago)	(smtpauth) Failed SMTP AUTH login from 193.32.162.80 (NL/The Netherlands/-): 5 in the last 3600 secs ... show more	Port Scan

Web

- Vieles vorkonfiguriert
  - Einiges suboptimal. Einiges verwendbar.
  - Alles: Nicht scharf geschaltet
- Achtung: erstes Beispiel —> reines Lehrbeispiel

Web

Auch vieles vorkonfiguriert. Leider einiges „suboptimal"



```
/etc/fail2ban/filter.d  ll apache-*
-rw-r--r-- 1 root root 3.2K Nov  9  2022 apache-auth.conf
-rw-r--r-- 1 root root 2.8K Nov  9  2022 apache-badbots.conf
-rw-r--r-- 1 root root 1.3K Nov  9  2022 apache-botsearch.conf
-rw-r--r-- 1 root root 1.6K Nov  9  2022 apache-common.conf
-rw-r--r-- 1 root root  403 Nov  9  2022 apache-fakegooglebot.conf
-rw-r--r-- 1 root root  511 Nov  9  2022 apache-modsecurity.conf
-rw-r--r-- 1 root root  596 Nov  9  2022 apache-nohome.conf
-rw-r--r-- 1 root root 1.3K Nov  9  2022 apache-noscript.conf
-rw-r--r-- 1 root root 2.2K Nov  9  2022 apache-overflows.conf
-rw-r--r-- 1 root root  362 Nov  9  2022 apache-pass.conf
-rw-r--r-- 1 root root 1020 Nov  9  2022 apache-shellshock.conf
/etc/fail2ban/filter.d  grep -ir 'nessus|nikto|nmap|ffuf|openvas' *
✘  /etc/fail2ban/filter.d
```

Lehrbeispiel, weil

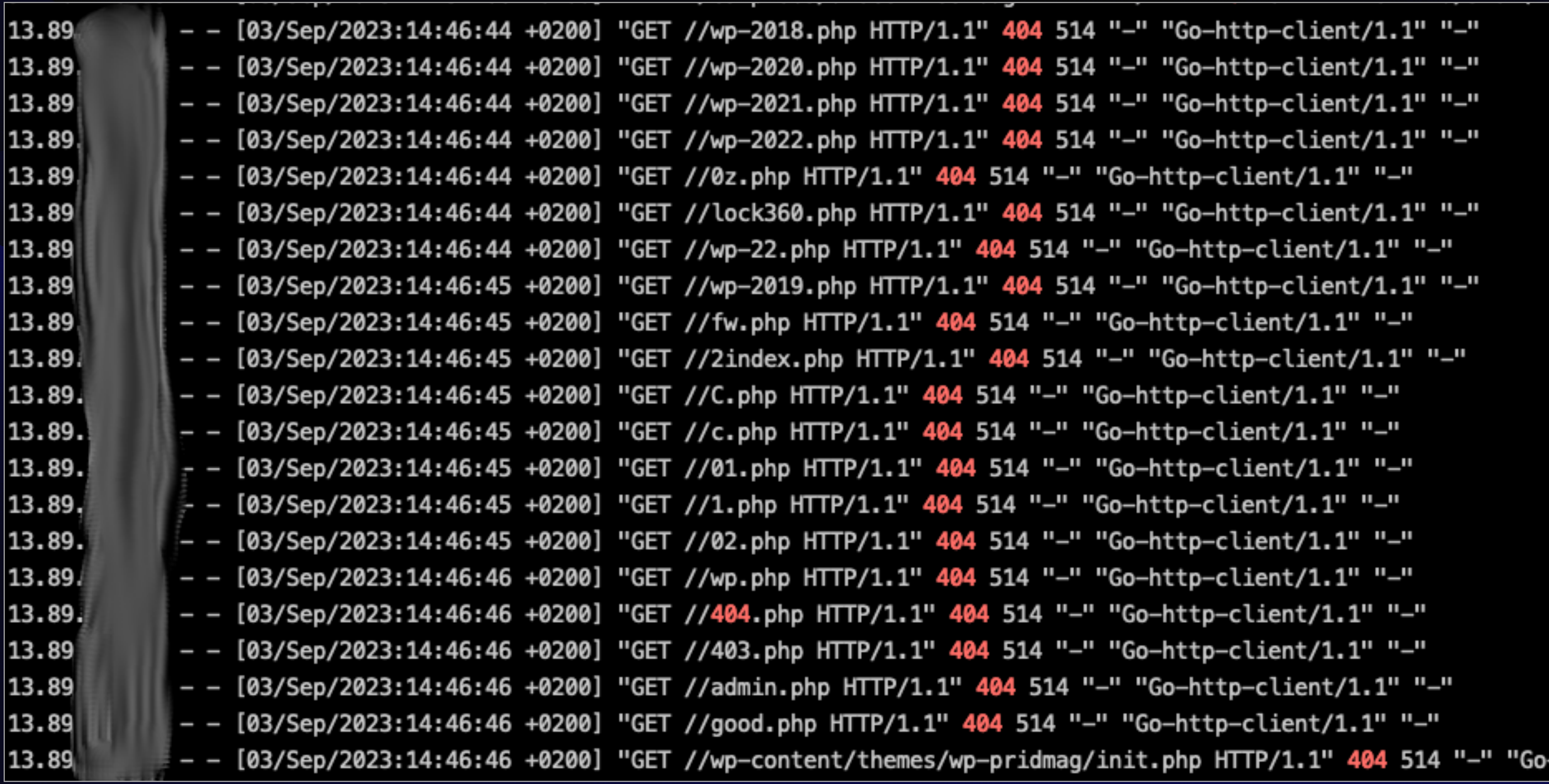
Lehrbeispiel, weil

- ein Zugriff muss ich gestatten — Operation ist Log-basiert
- Gerade User-Agents gehen besser am Webserver
  - (Zumindest solche, die nicht „hämmern“)
- Wer wirklich solche 5kr1p7k1d5 blocken will
  - Andere Methoden weit aus effektiver

„404-Methode“

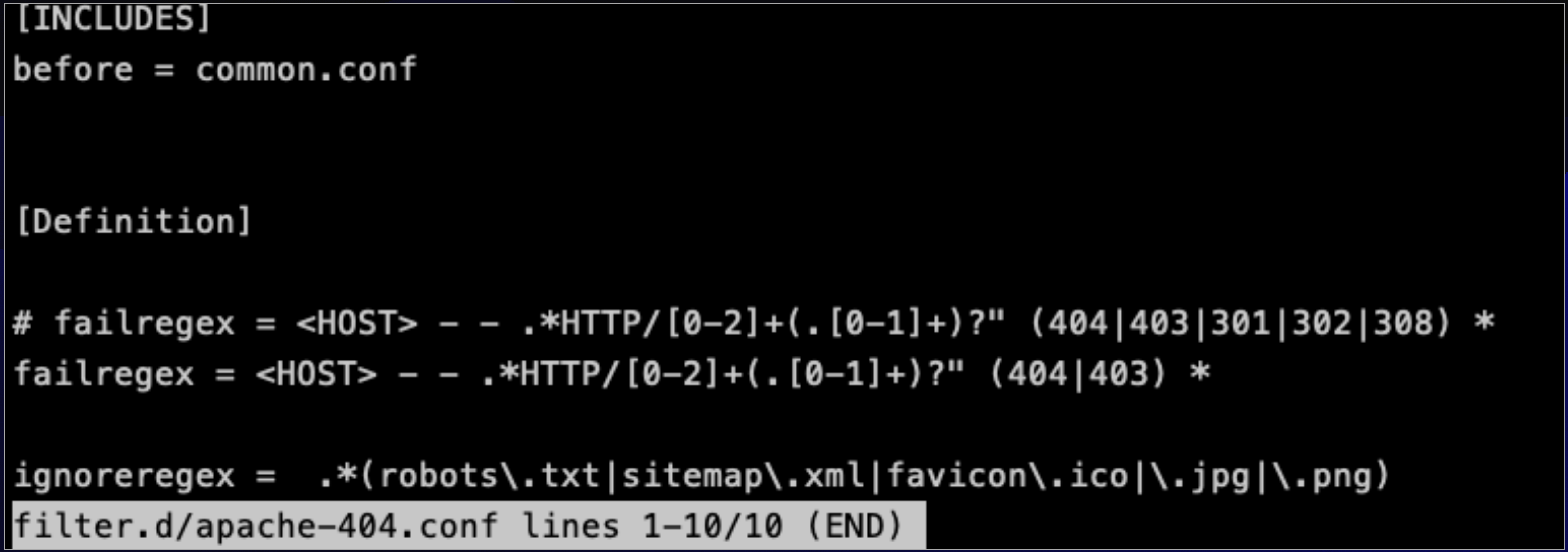
- Idee:

  1. Zähle 404s
  2. Reißleine nach Gusto



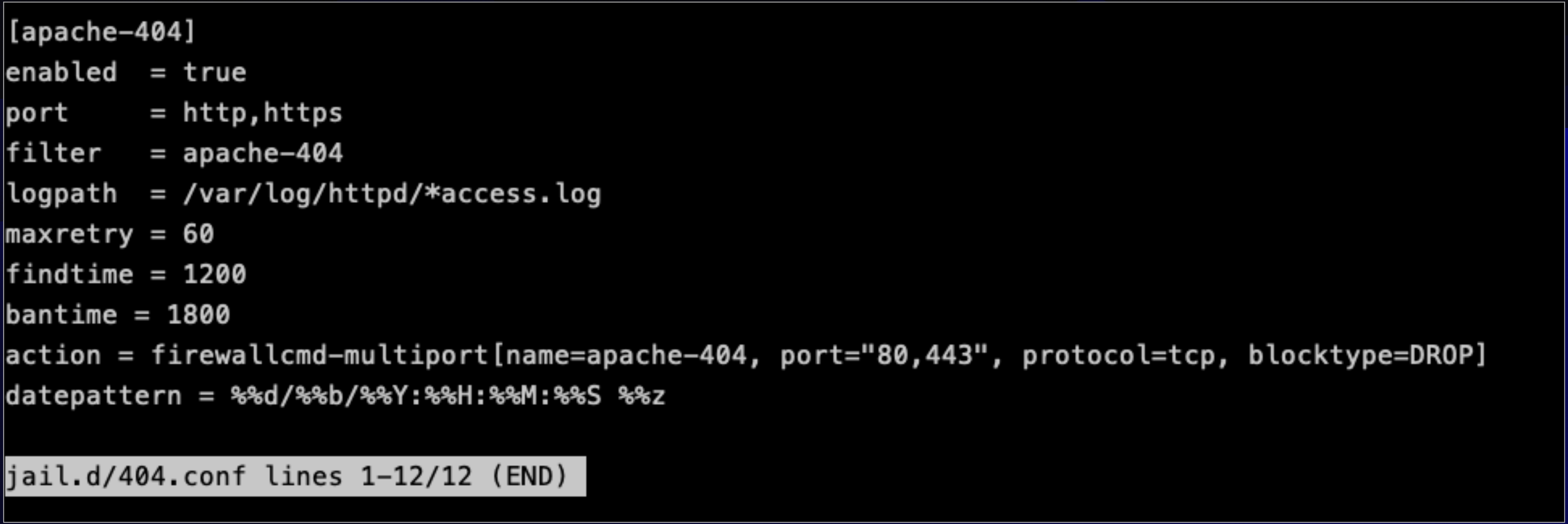
```
13.89[redacted] - - [03/Sep/2023:14:46:44 +0200] "GET //wp-2018.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:44 +0200] "GET //wp-2020.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:44 +0200] "GET //wp-2021.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:44 +0200] "GET //wp-2022.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:44 +0200] "GET //0z.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:44 +0200] "GET //lock360.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:44 +0200] "GET //wp-22.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:45 +0200] "GET //wp-2019.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:45 +0200] "GET //fw.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:45 +0200] "GET //2index.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:45 +0200] "GET //C.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:45 +0200] "GET //c.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:45 +0200] "GET //01.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:45 +0200] "GET //1.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:45 +0200] "GET //02.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:46 +0200] "GET //wp.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:46 +0200] "GET //404.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:46 +0200] "GET //403.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:46 +0200] "GET //admin.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:46 +0200] "GET //good.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89[redacted] - - [03/Sep/2023:14:46:46 +0200] "GET //wp-content/themes/wp-pridmag/init.php HTTP/1.1" 404 514 "-" "Go
```

404-Trick, bitte nicht 1:1 übernehmen



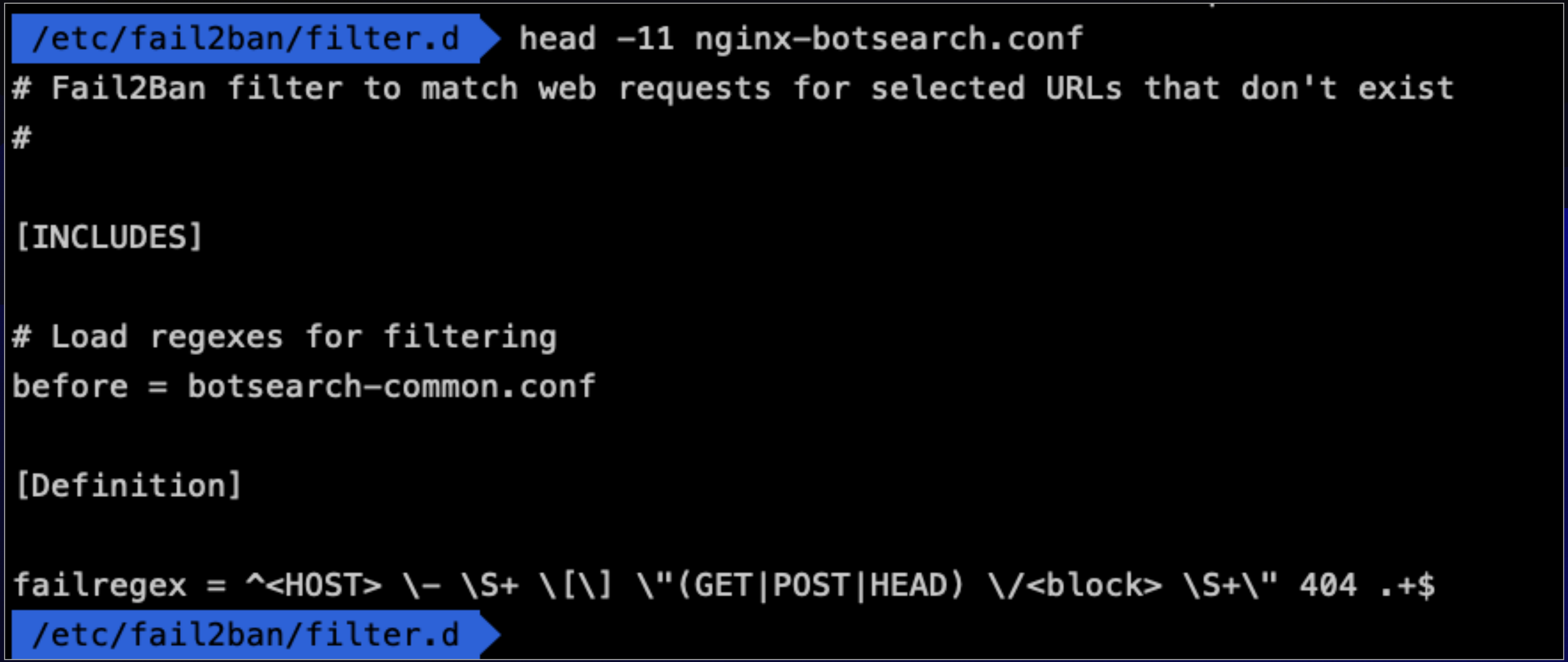
```
[INCLUDES]
before = common.conf


[Definition]

# failregex = <HOST> - - .*HTTP/[0-2]+(.[0-1]+)?" (404|403|301|302|308) *
failregex = <HOST> - - .*HTTP/[0-2]+(.[0-1]+)?" (404|403) *

ignoreregex =  .*(robots\.txt|sitemap\.xml|favicon\.ico|\.jpg|\.png)
filter.d/apache-404.conf lines 1-10/10 (END)
```

404-Trick weiter: anzupassen



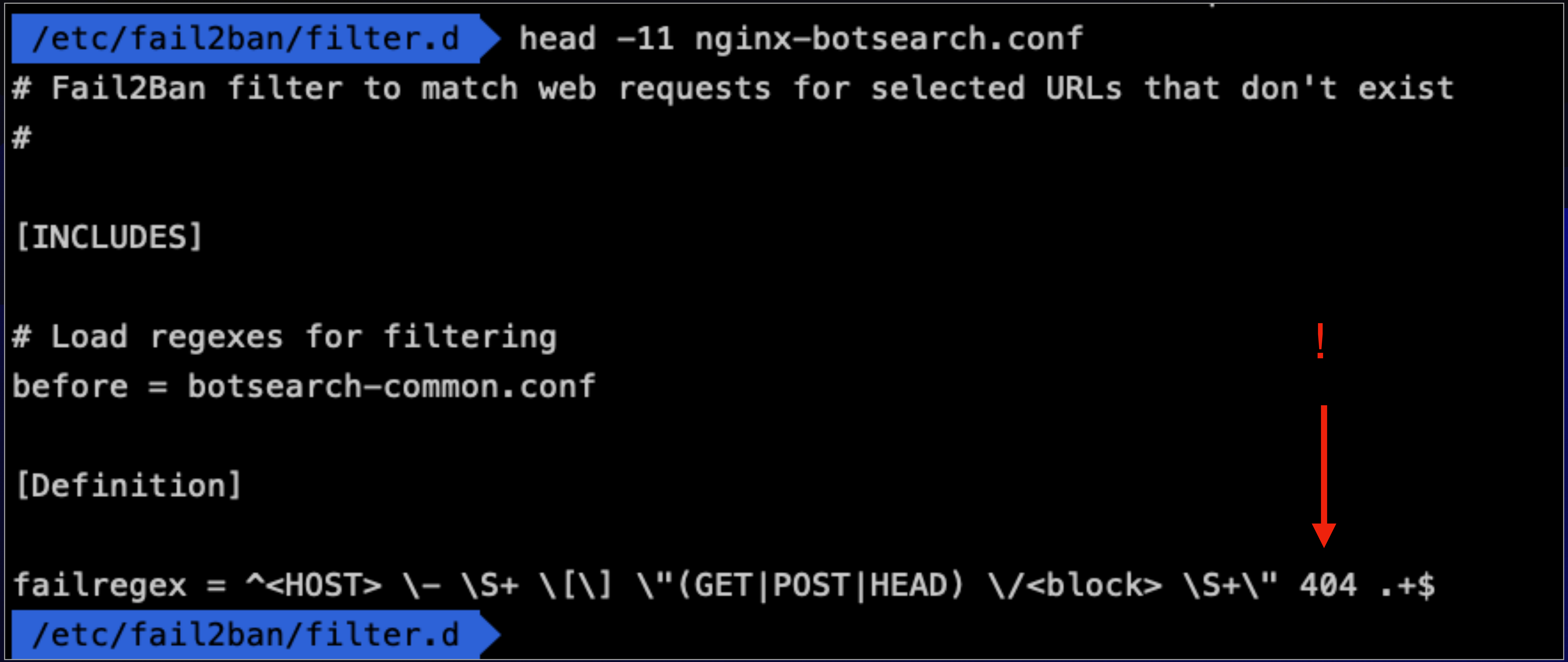
```
[apache-404]
enabled  = true
port     = http,https
filter   = apache-404
logpath  = /var/log/httpd/*access.log
maxretry = 60
findtime = 1200
bantime = 1800
action = firewallcmd-multiport[name=apache-404, port="80,443", protocol=tcp, blocktype=DROP]
datepattern = %%d/%%b/%%Y:%%H:%%M:%%S %%z

jail.d/404.conf lines 1-12/12 (END)
```

In etwa



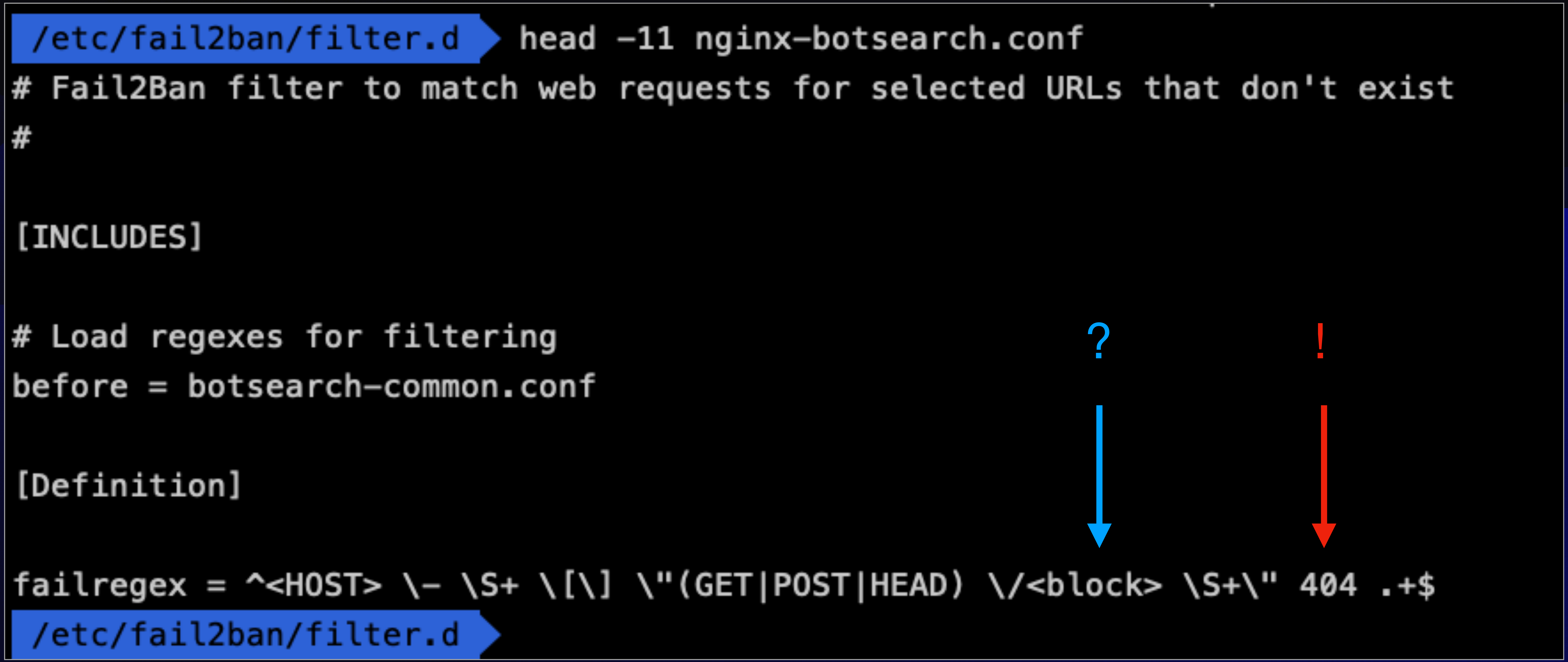
```
/etc/fail2ban/filter.d  head -11 nginx-botsearch.conf
# Fail2Ban filter to match web requests for selected URLs that don't exist
#

[INCLUDES]

# Load regexes for filtering
before = botsearch-common.conf

[Definition]

failregex = ^<HOST> \- \S+ \[\] \"(GET|POST|HEAD) \/<block> \S+\" 404 .+$
/etc/fail2ban/filter.d
```

In etwa



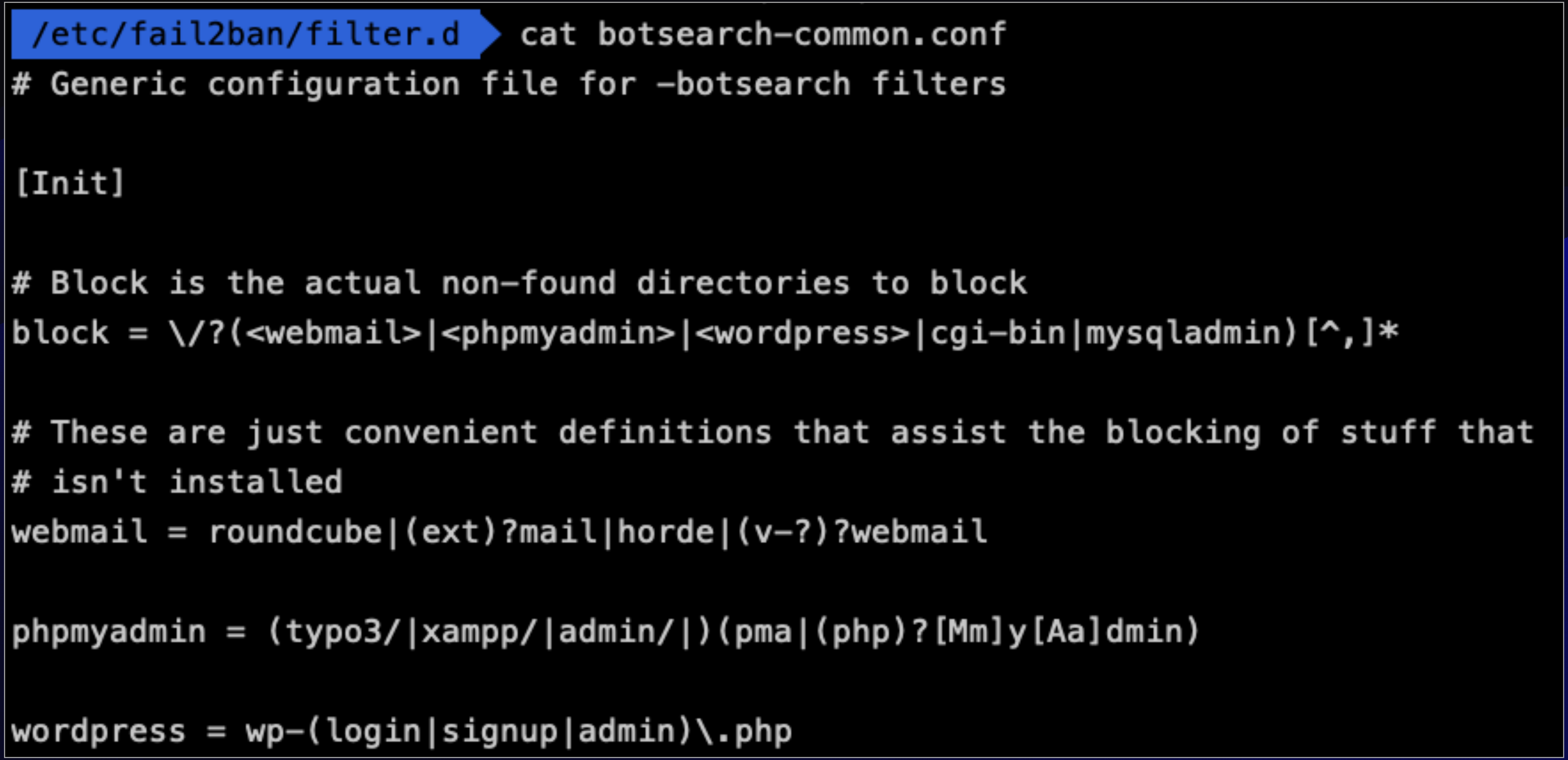
```
/etc/fail2ban/filter.d  head -11 nginx-botsearch.conf
# Fail2Ban filter to match web requests for selected URLs that don't exist
#

[INCLUDES]

# Load regexes for filtering
before = botsearch-common.conf

[Definition]

failregex = ^<HOST> \- \S+ \[\] \"(GET|POST|HEAD) \/<block> \S+\" 404 .+$
/etc/fail2ban/filter.d
```

In etwa



```
/etc/fail2ban/filter.d  head -11 nginx-botsearch.conf
# Fail2Ban filter to match web requests for selected URLs that don't exist
#

[INCLUDES]

# Load regexes for filtering
before = botsearch-common.conf

[Definition]

failregex = ^<HOST> \- \S+ \[\] \"(GET|POST|HEAD) \/<block> \S+\" 404 .+$
/etc/fail2ban/filter.d
```

Referenzen

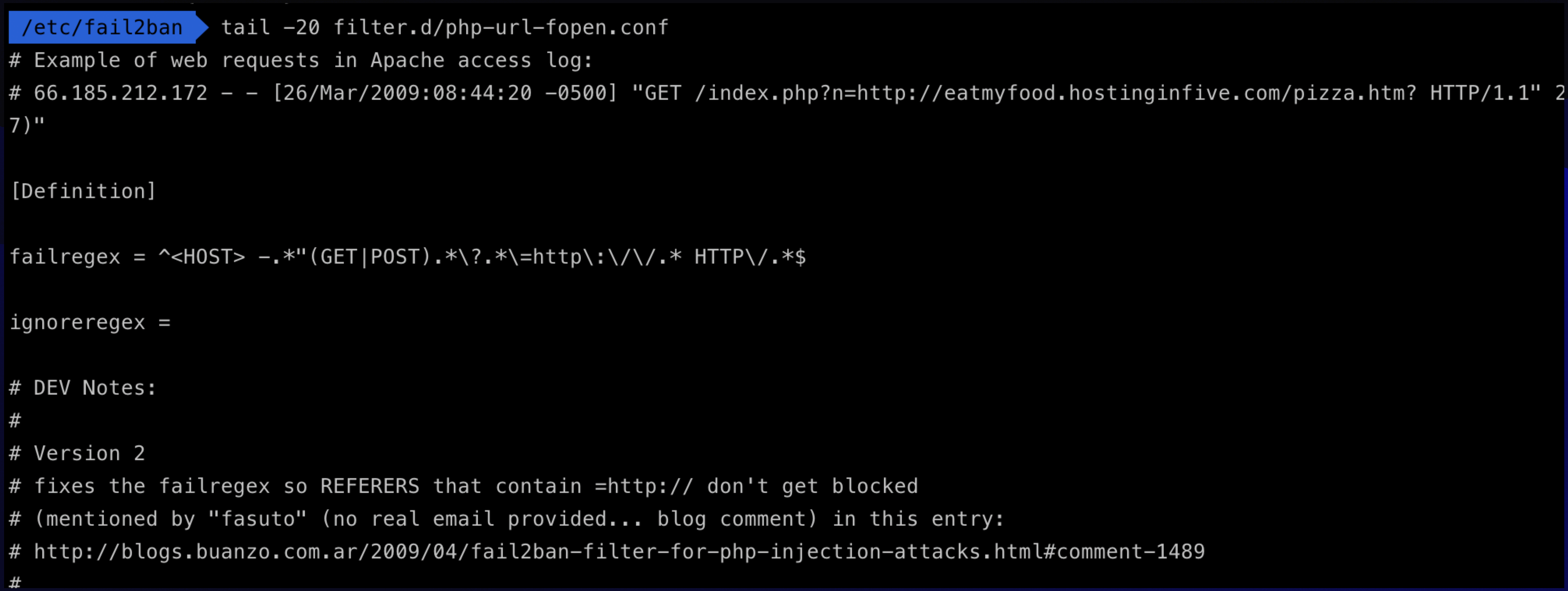


```
 /etc/fail2ban/filter.d  cat botsearch-common.conf
# Generic configuration file for -botsearch filters

[Init]

# Block is the actual non-found directories to block
block = \/?(<webmail>|<phpmyadmin>|<wordpress>|cgi-bin|mysqladmin)[^,]*

# These are just convenient definitions that assist the blocking of stuff that
# isn't installed
webmail = roundcube|(ext)?mail|horde|(v-?)?webmail

phpmyadmin = (typo3/|xampp/|admin/|)(pma|(php)?[Mm]y[Aa]dmin)

wordpress = wp-(login|signup|admin)\.php
```

GET-Request, Web-Hacks

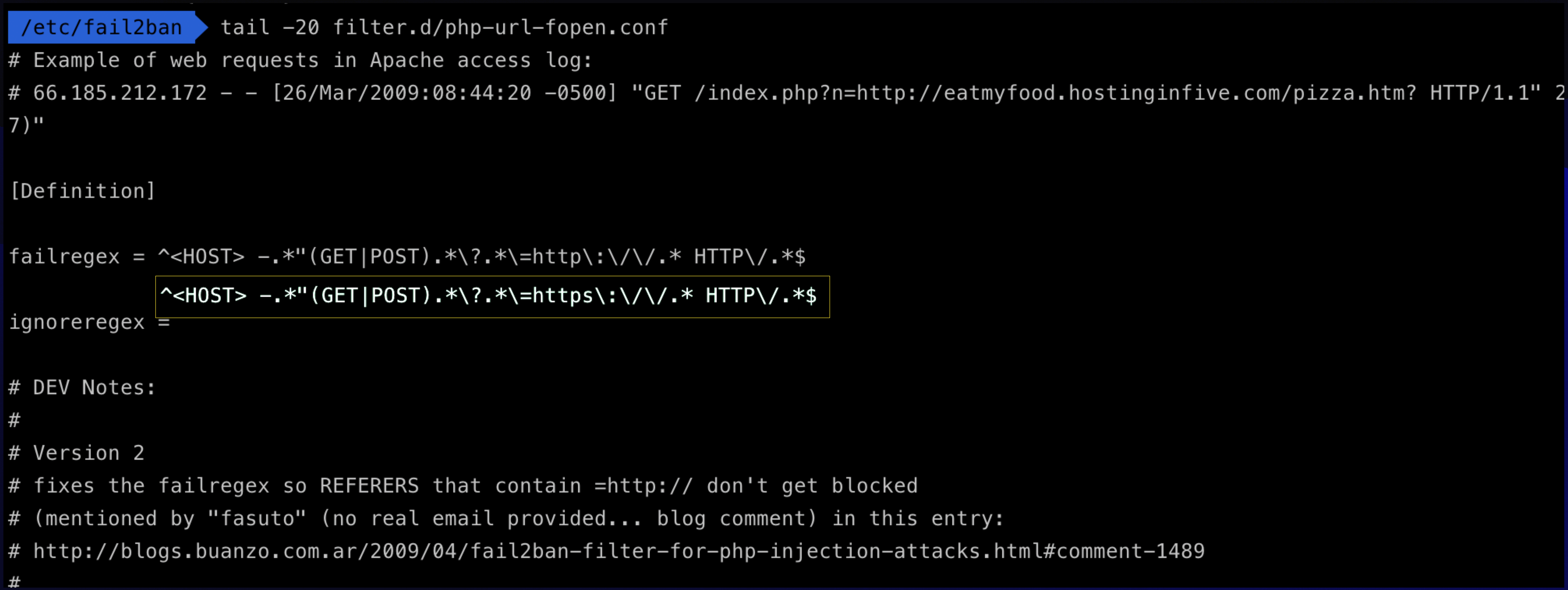
```
[INCLUDES]



[Definition]
failregex = ^<HOST> .* "(GET|POST|HEAD|PROPFIND) .*(?i)(union|select|concat|information_schema\.tables|unhex|benchmark|md5|sleep|order|%%20and%%20|%%20or%%20).* (404|403)
            ^<HOST> .* "(GET|POST|HEAD|PROPFIND) .*(?i)(fromCharCode|ONLOAD|alert|base64|innerHTML|onmouseover|x22|88,83,83|onerror|prompt).* (404|403)
            ^<HOST> .* "(GET|POST|HEAD|PROPFIND) .*(?i)(\.\.|%%2e|etc\/passwd|etc\/shadow).* (404|403)
            ^<HOST> .* "(GET|POST|HEAD|PROPFIND) .*(?i)(urldecode|explode|\$_REQUEST|\$_GET).* (404|403)
```

Open Redirect



```
/etc/fail2ban  tail -20 filter.d/php-url-fopen.conf
# Example of web requests in Apache access log:
# 66.185.212.172 - - [26/Mar/2009:08:44:20 -0500] "GET /index.php?n=http://eatmyfood.hostinginfive.com/pizza.htm? HTTP/1.1" 2
7)"

[Definition]

failregex = ^<HOST> -.*"(GET|POST).*\?.*\=http\:\/\/.* HTTP\/.*$

ignoreregex =

# DEV Notes:
#
# Version 2
# fixes the failregex so REFERERS that contain =http:// don't get blocked
# (mentioned by "fasuto" (no real email provided... blog comment) in this entry:
# http://blogs.buanzo.com.ar/2009/04/fail2ban-filter-for-php-injection-attacks.html#comment-1489
#
```

Open Redirect



```
/etc/fail2ban  tail -20 filter.d/php-url-fopen.conf
# Example of web requests in Apache access log:
# 66.185.212.172 - - [26/Mar/2009:08:44:20 -0500] "GET /index.php?n=http://eatmyfood.hostinginfive.com/pizza.htm? HTTP/1.1" 2
7)"

[Definition]

failregex = ^<HOST> -.*"(GET|POST).*\?.*\=http\:\/\/.* HTTP\/.*$
            ^<HOST> -.*"(GET|POST).*\?.*\=https\:\/\/.* HTTP\/.*$
ignoreregex =

# DEV Notes:
#
# Version 2
# fixes the failregex so REFERERS that contain =http:// don't get blocked
# (mentioned by "fasuto" (no real email provided... blog comment) in this entry:
# http://blogs.buanzo.com.ar/2009/04/fail2ban-filter-for-php-injection-attacks.html#comment-1489
#
```

POST-Request

POST-Request

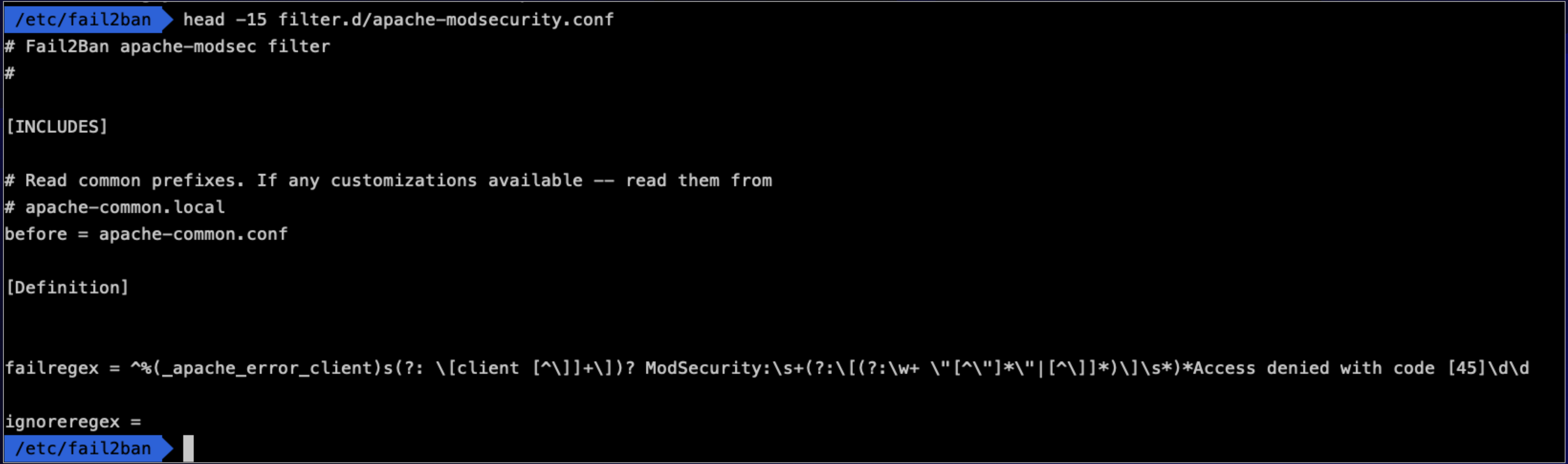
- Nginx kann POST-Parameter loggen

```
~log_format postlogs '$remote_addr - $remote_user [$time_local] '
'"$request" $status $bytes_sent '  '"$http_referer"
"$http_user_agent" "$request_body"';
```

- Apache: mod_dumpio
  - `LogLevel dumpio:trace7`
  - `DumpIOInput On`
  - `DumpIOOutput On`

POST-Request

- Apache: mod_security



```
/etc/fail2ban  head -15 filter.d/apache-modsecurity.conf
# Fail2Ban apache-modsec filter
#

[INCLUDES]

# Read common prefixes. If any customizations available -- read them from
# apache-common.local
before = apache-common.conf

[Definition]


failregex = ^%(_apache_error_client)s(?: \[client [^\]]+\])? ModSecurity:\s+(?:\[(?:\w+ \"[^\"]*\"|[^\]]*)\]\s*)*Access denied with code [45]\d\d

ignoreregex =
/etc/fail2ban 
```

POST-Request: ACHTUNG

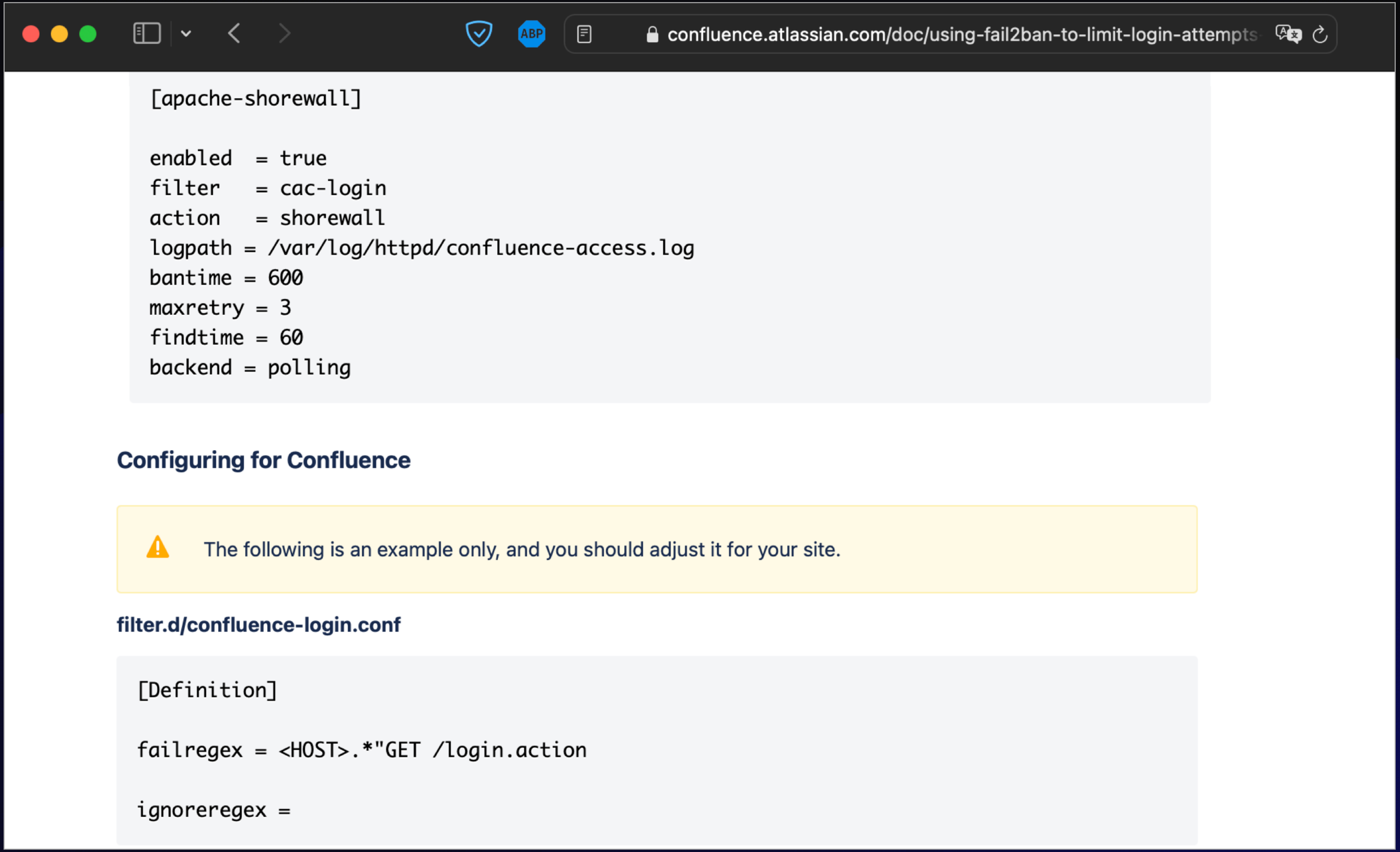
- Passwörter u.a. !

```
[12/Jun/2024:13:55:16 +0200] "POST /login HTTP/2.0" 200 12 "-" "curl/8.4.0" "user=max,passwd=1234"
[12/Jun/2024:13:55:30 +0200] "POST /login HTTP/2.0" 200 12 "-" "curl/8.4.0" "user=micheala,passwd=meinpwistvielbesseralsMax"
[12/Jun/2024:13:56:41 +0200] "POST /login HTTP/2.0" 200 12 "-" "curl/8.4.0" "user=deinciso,passwd=Postlogs: Ganz schlechte Idee"
```

- Besser: mod_security + SecRule sanitiseArg

Logins schützen

Logins schützen



confluence.atlassian.com/doc/using-fail2ban-to-limit-login-attempts

```
[apache-shorewall]

enabled  = true
filter   = cac-login
action   = shorewall
logpath = /var/log/httpd/confluence-access.log
bantime = 600
maxretry = 3
findtime = 60
backend = polling
```

Configuring for Confluence

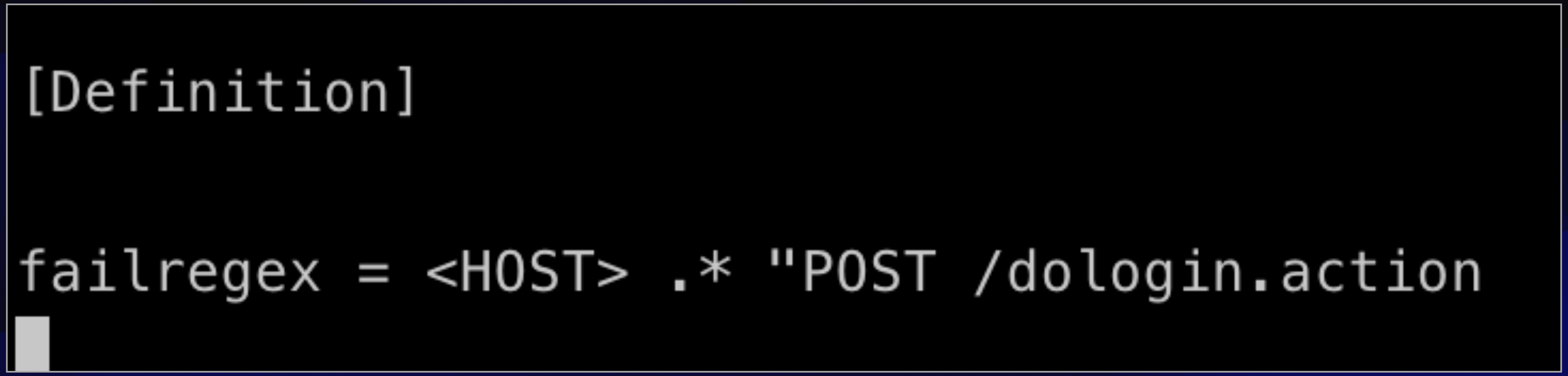
⚠ The following is an example only, and you should adjust it for your site.

filter.d/confluence-login.conf

```
[Definition]

failregex = <HOST>.*"GET /login.action

ignoreregex =
```

Logins schützen

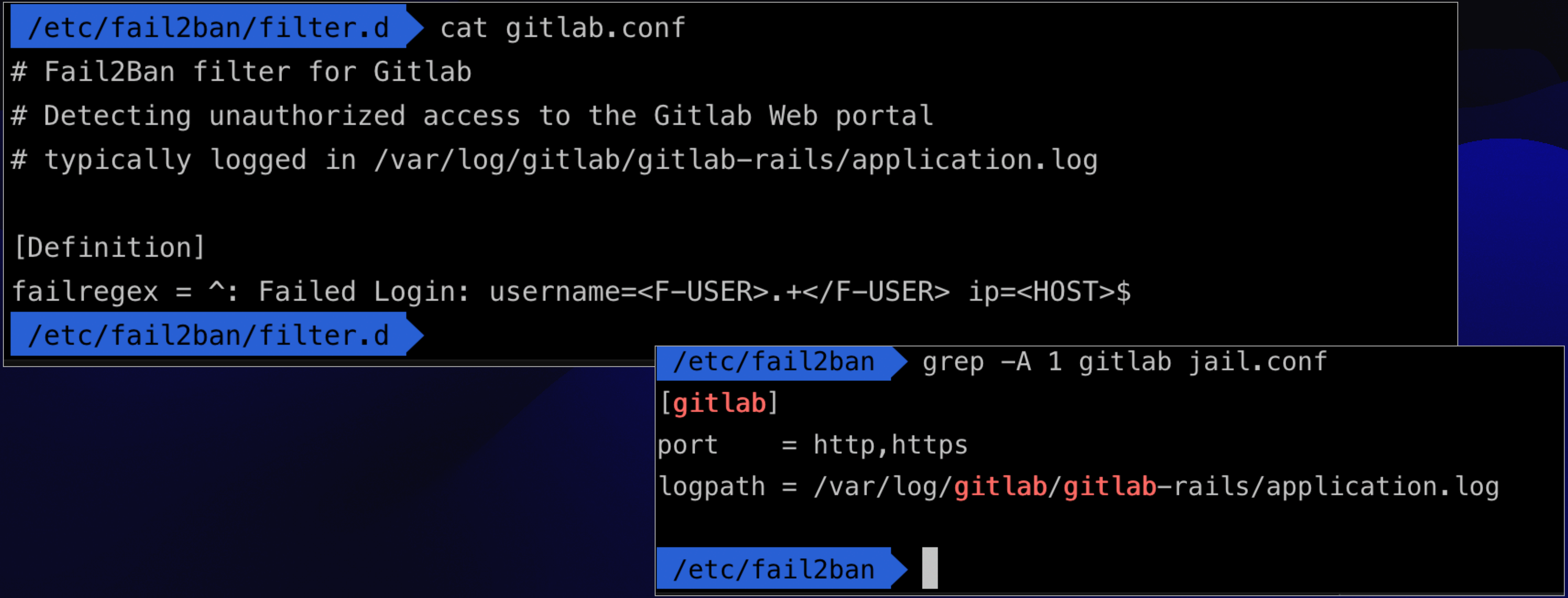
Confluence POST



```
[Definition]

failregex = <HOST> .* "POST /dologin.action
```

Logins

Mitgeliefert: gitlab, grafana



```
/etc/fail2ban/filter.d  cat gitlab.conf
# Fail2Ban filter for Gitlab
# Detecting unauthorized access to the Gitlab Web portal
# typically logged in /var/log/gitlab/gitlab-rails/application.log

[Definition]
failregex = ^: Failed Login: username=<F-USER>.+</F-USER> ip=<HOST>$
/etc/fail2ban/filter.d
```

```
/etc/fail2ban  grep -A 1 gitlab jail.conf
[gitlab]
port     = http,https
logpath = /var/log/gitlab/gitlab-rails/application.log

/etc/fail2ban
```

Logins

Mitgeliefert: gitlab, grafana

```
/etc/fail2ban/filter.d  cat grafana.conf
# Fail2Ban filter for Grafana
# Detecting unauthorized access
# Typically logged in /var/log/grafana/grafana.log

[Init]
datepattern = ^t=%%Y-%%m-%%dT%%H:%%M:%%S%%z

[Definition]
failregex = ^(?: lvl=err?or)? msg="Invalid username or password"(?: uname=(?:"<F-ALT_USER>[^"]+</F-ALT_USER>"|<F-USER>\S+</F-USER>)|
error="<F-ERROR>[^"]+</F-ERROR>"| \S+=(?:\S*|"[^"]+"))* remote_addr=<ADDR>$
/etc/fail2ban/filter.d
```

```
/etc/fail2ban  grep -A 1 grafana jail.conf
[grafana]
port    = http,https
logpath = /var/log/grafana/grafana.log

/etc/fail2ban
```

CC-BY-SA 3.0 Royce SPAM http://xrl.us/rspam, CC0 https://www.pexels.com/de-de/foto/kondom-neben-orangenfrucht-5187879/

Spamkondom

CC-BY-SA 3.0 Royce SPAM http://xrl.us/rspam, CC0 https://www.pexels.com/de-de/foto/kondom-neben-orangenfrucht-5187879/

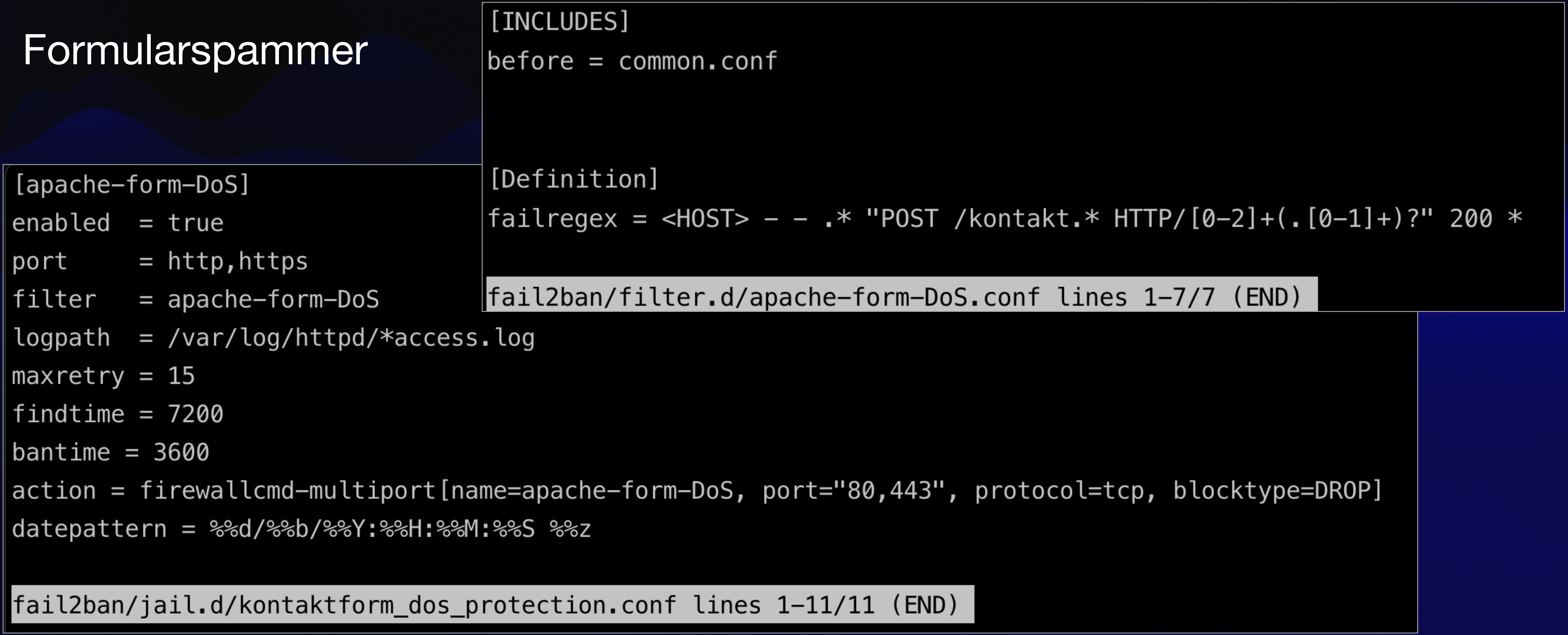
Spamkondom

- Formularspammer

CC-BY-SA 3.0 Royce SPAM http://xrl.us/rspam, CC0 https://www.pexels.com/de-de/foto/kondom-neben-orangenfrucht-5187879/

Spamkondom

- Formularspammer



```
[INCLUDES]
before = common.conf



[Definition]
failregex = <HOST> - - .* "POST /kontakt.* HTTP/[0-2]+(.[0-1]+)?" 200 *

fail2ban/filter.d/apache-form-DoS.conf lines 1-7/7 (END)
```

```
[apache-form-DoS]
enabled  = true
port     = http,https
filter   = apache-form-DoS
logpath  = /var/log/httpd/*access.log
maxretry = 15
findtime = 7200
bantime = 3600
action = firewallcmd-multiport[name=apache-form-DoS, port="80,443", protocol=tcp, blocktype=DROP]
datepattern = %%d/%%b/%%Y:%%H:%%M:%%S %%z

fail2ban/jail.d/kontaktform_dos_protection.conf lines 1-11/11 (END)
```

CC-BY-SA 3.0 Royce SPAM http://xrl.us/rspam. CC0 https://www.pexels.com/de-de/foto/kondom-neben-orangenfrucht-5187879/

Bonus feature

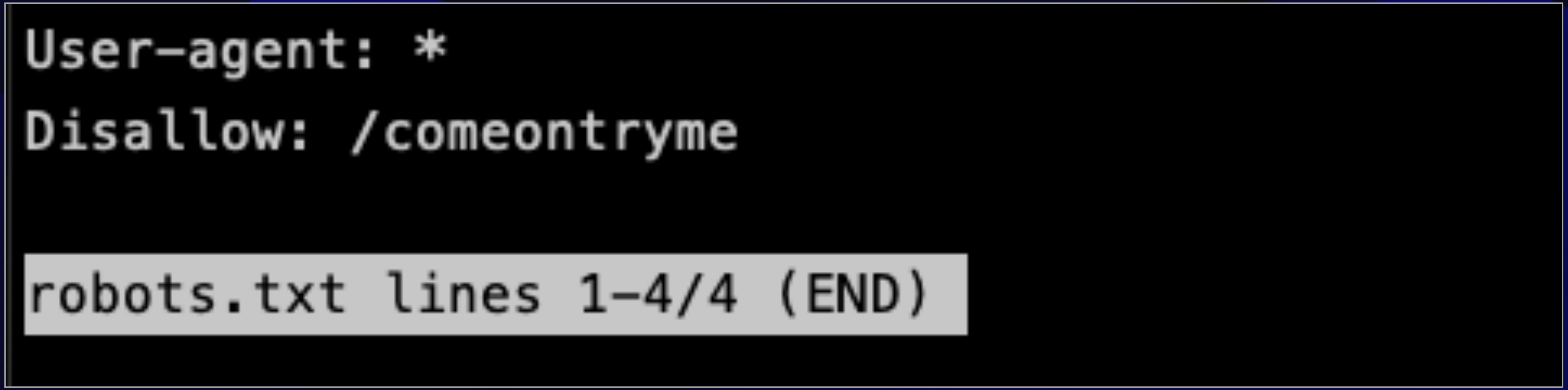
CC-BY 3.0 MaksKochanowicz123 https://www.deviantart.com/makskochanowicz123/art/Misty-Island-Rescue-Bonus-Features-TPATD-RAS-927084576

Bonus feature

- Booby trap

BONUS FEATURES
"The Search for Thomas" Game
"Misty Island Rescue" Karaoke Music Video
"Sir Topham Hatt" Karaoke Music Video
"Thomas and Percy and the Dragon" Read-Along Story
Trailers
MAIN MENU

CC-BY 3.0 MaksKochanowicz123 https://www.deviantart.com/makskochanowicz123/art/Misty-Island-Rescue-Bonus-Features-TPATD-RAS-927084576



```
User-agent: *
Disallow: /comeontryme

robots.txt lines 1-4/4 (END)
```

Take aways (1)

- fail2ban ist 😎
  - Aber: greift erst nach 1+ failed request(s)
- Nicht vergessen:
  - Fail2ban ist eine *reaktive* Maßnahme
  - **Macht Apps / Server besser *proaktiv* sicher!**

Take aways (2)

- Regex testen!
  - regex101.com
  - fail2ban-regex
- Webseite/Service auf Funktion testen
  - Klassiker: (AAA|BBB|CCC|DDD|)
  - Schwellwerte ok?

Danke

Eigenes Bild. Wegweiser in Pyrenäen. CC-BY-SA 4.0

- Kontakt: https://drwetter.eu/ oder linked.in
- Folien sind CC-BY-SA 4.0 und auf der Webseite.