Reverse Proxy

實作登入與防護機制

110年台大區網-網路技術推廣研討會 (2021/12/14)

台大計中

童鵬哲

Outlines

- ELK Security
- Nginx
- Reverse proxy with login func.
- ModSecurity
- Web server and WAF

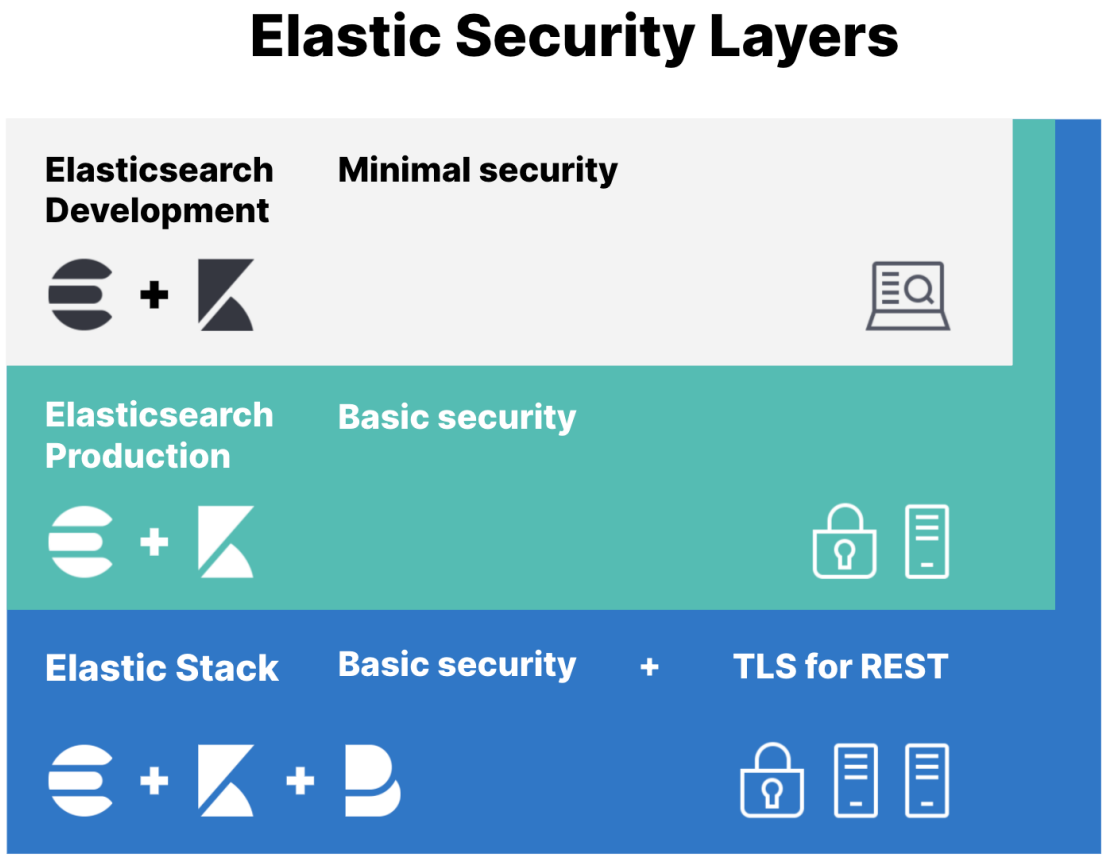
ELK security

Elastic stack

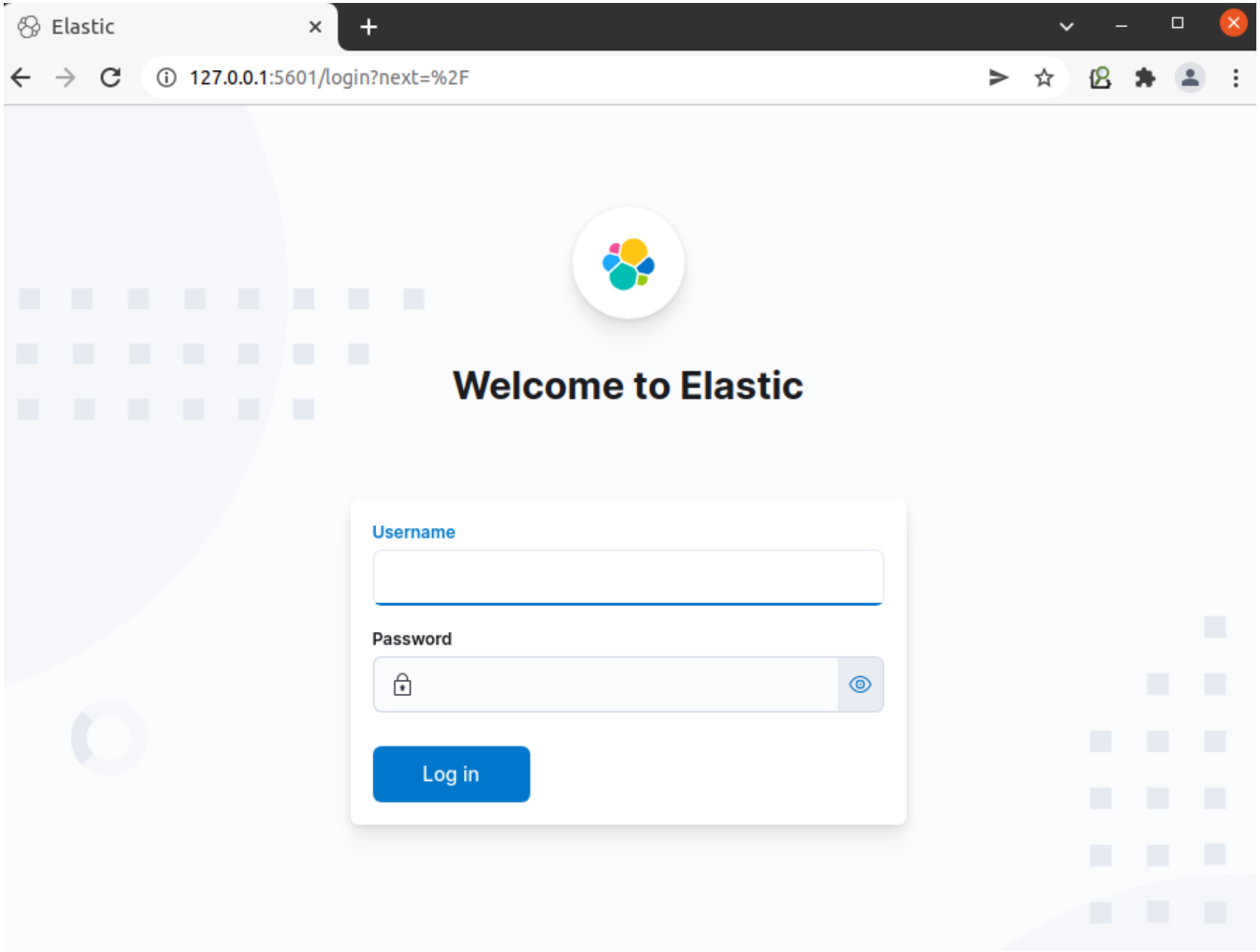
- **Elasticsearch**
  - 資料儲存、搜尋使用
  - RESTful API
- **Logstash (or Beat 家族)**
  - inputs → filters → outputs
  - Parse
- **Kibana**
  - 視覺化
  - 圖表

Stack

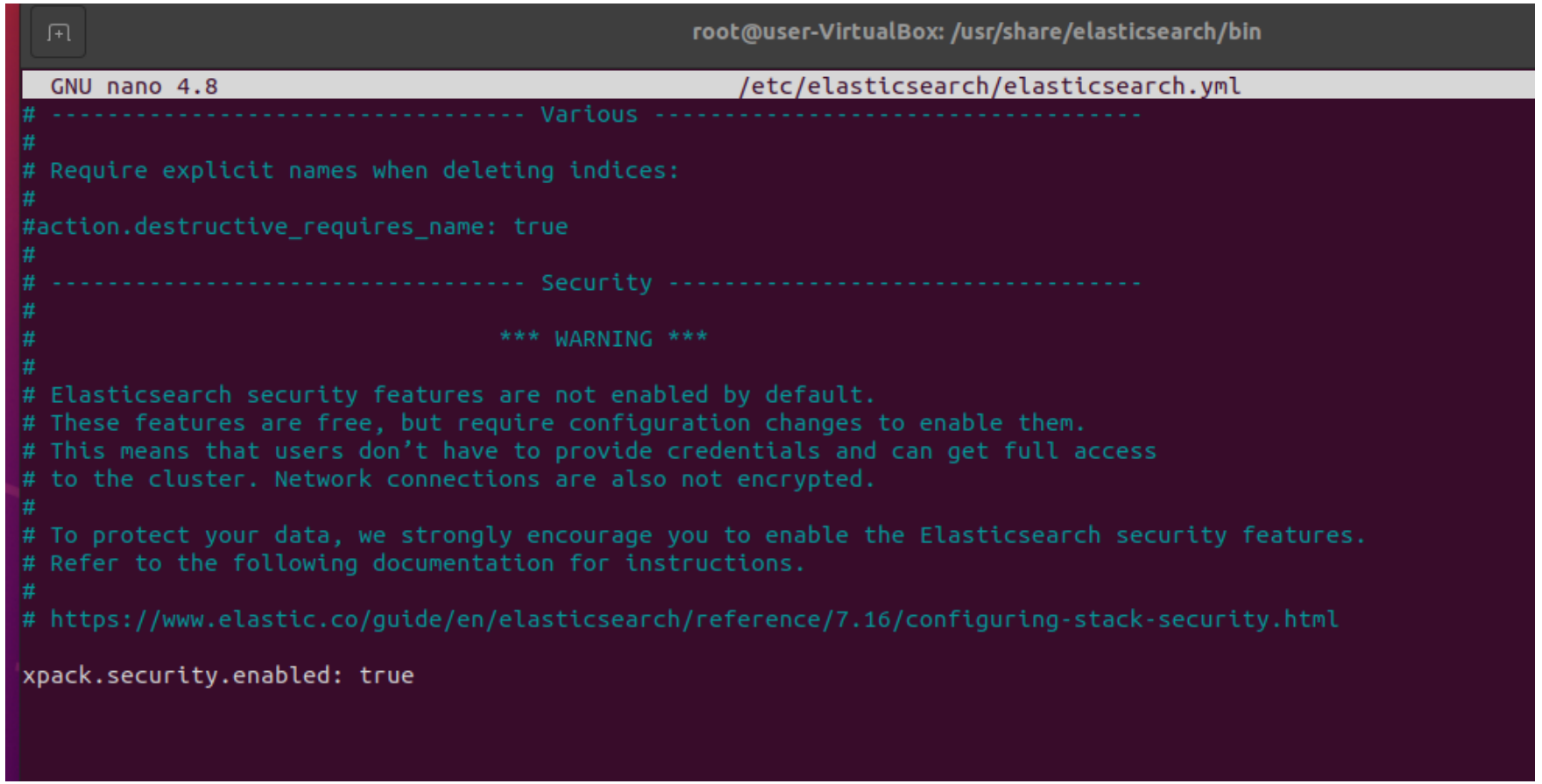
Elastic Security



https://www.elastic.co/guide/en/elasticsearch/reference/current/configuring-stack-security.html


Elastic
127.0.0.1:5601/login?next=%2F
Welcome to Elastic
Username
Password
Log in

啟動 security xpack



啟動密碼

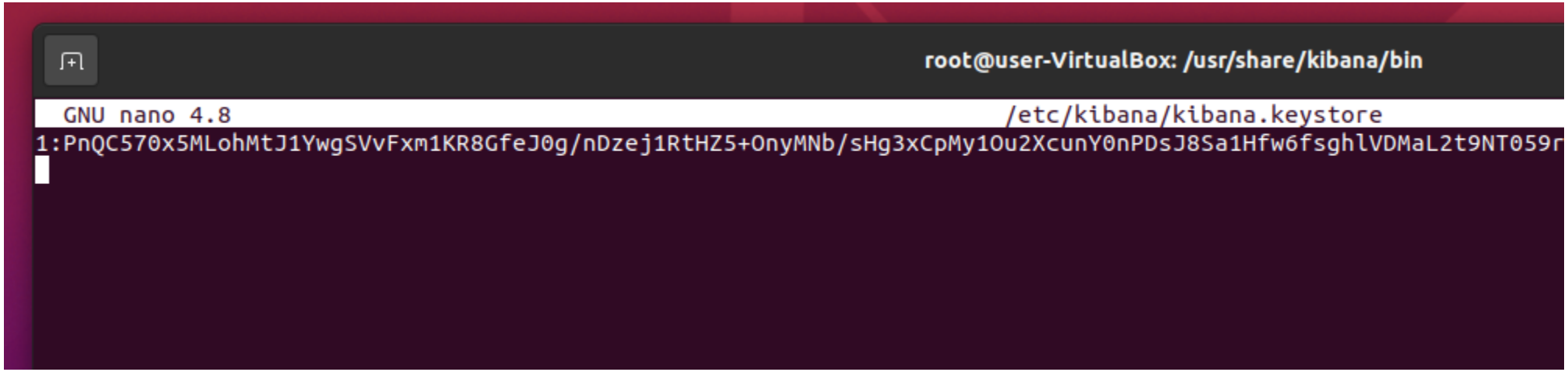
```
ERROR: User cancelled operation
root@user-VirtualBox:/usr/share/elasticsearch/bin# ./elasticsearch-setup-passwords auto
Initiating the setup of passwords for reserved users elastic,apm_system,kibana,kibana_system,logstash_system,beats_system,remote_monito
ring_user.
The passwords will be randomly generated and printed to the console.
Please confirm that you would like to continue [y/N]y


Changed password for user apm_system
PASSWORD apm_system = BtZRaIA4G9feTfDtnYnN

Changed password for user kibana_system
PASSWORD kibana_system = NTgD0zkvsqNAFcrDCLMi

Changed password for user kibana
PASSWORD kibana = NTgD0zkvsqNAFcrDCLMi

Changed password for user logstash_system
PASSWORD logstash_system = kUgUHfwTrcFFaHiekvXa

Changed password for user beats_system
PASSWORD beats_system = TyRFufOq9qKPyEPjytBr

Changed password for user remote_monitoring_user
PASSWORD remote_monitoring_user = P5D0J3kyUbxw6O9ci71n

Changed password for user elastic
PASSWORD elastic = UZhTH1B5a7pboQ5WTGwU
```

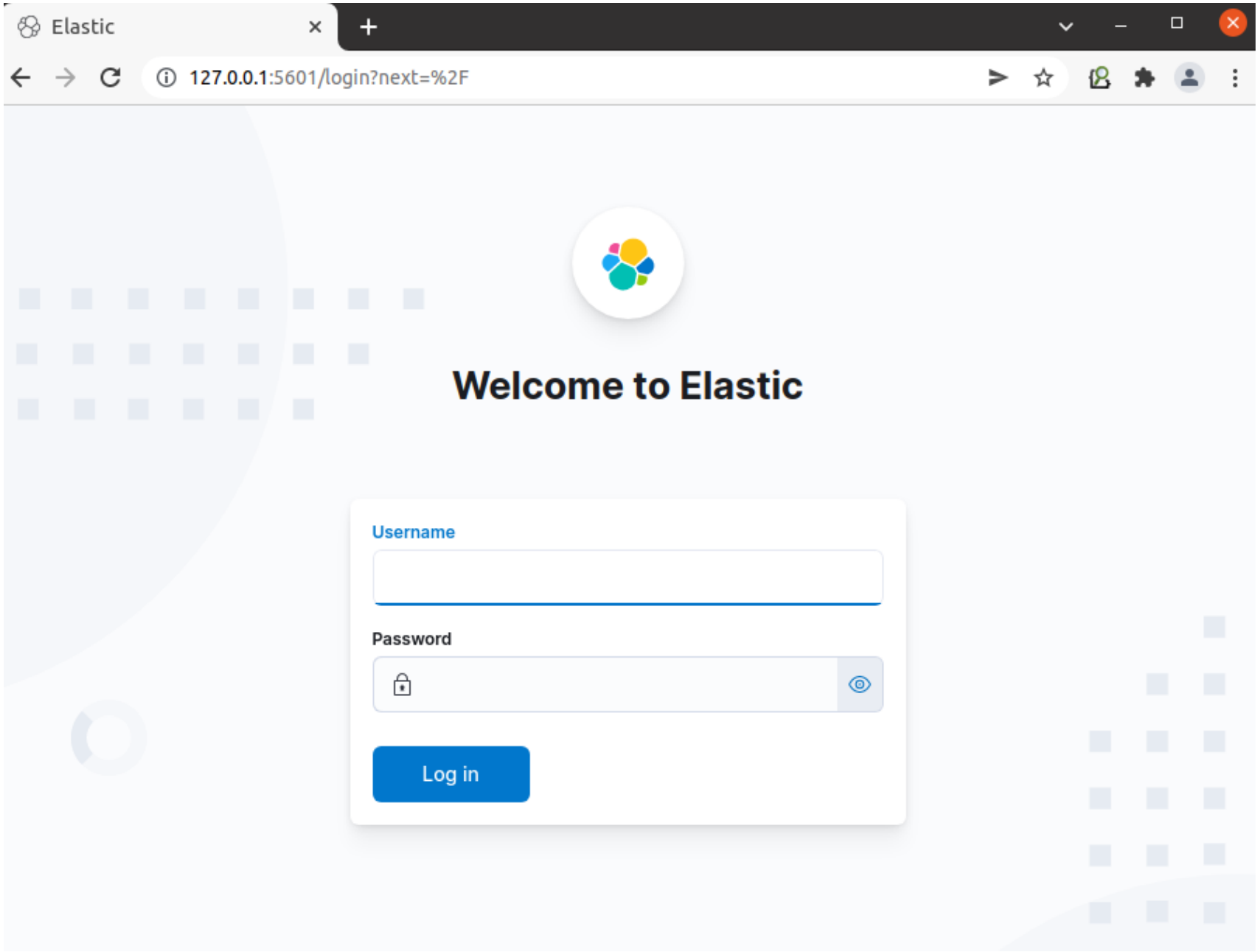
Kibana設定 帳號密碼

```
  GNU nano 4.8                                                  /etc/kibana/kibana.yml
#elasticsearch.hosts: ["http://localhost:9200"]

# Kibana uses an index in Elasticsearch to store saved searches, visualizations and
# dashboards. Kibana creates a new index if the index doesn't already exist.
#kibana.index: ".kibana"

# The default application to load.
#kibana.defaultAppId: "home"

# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the Kibana
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
elasticsearch.username: "kibana_system"
#elasticsearch.password: "NTgD0zkvsqNAFcrDCLMi"

# Kibana can also authenticate to Elasticsearch via "service account tokens".
# If may use this token instead of a username/password.
# elasticsearch.serviceAccountToken: "my_token"

# Enables SSL and paths to the PEM-format SSL certificate and SSL key files, respectively.
# These settings enable SSL for outgoing requests from the Kibana server to the browser.
#server.ssl.enabled: false
#server.ssl.certificate: /path/to/your/server.crt
#server.ssl.key: /path/to/your/server.key

# Optional settings that provide the paths to the PEM-format SSL certificate and key files.
# These files are used to verify the identity of Kibana to Elasticsearch and are required when
```

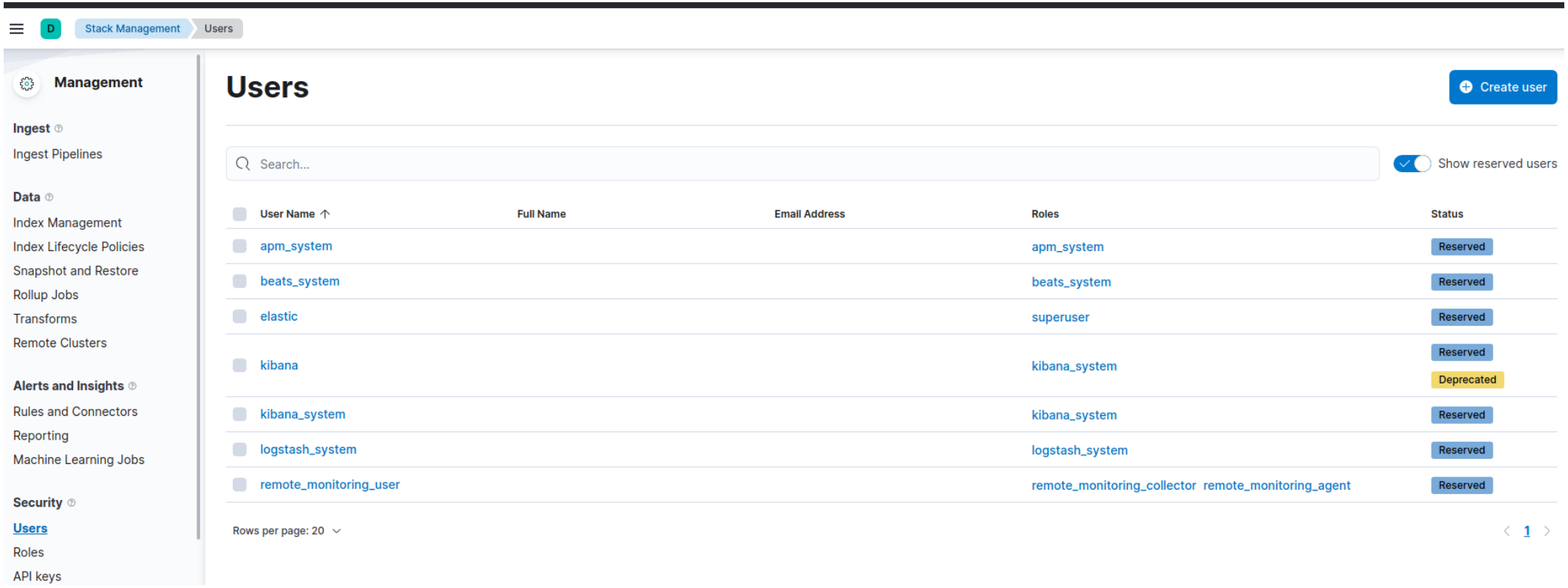
利用keystore儲存密碼

使用keystore儲存密碼，避免於kibana.yml 的 config 檔存入明碼。

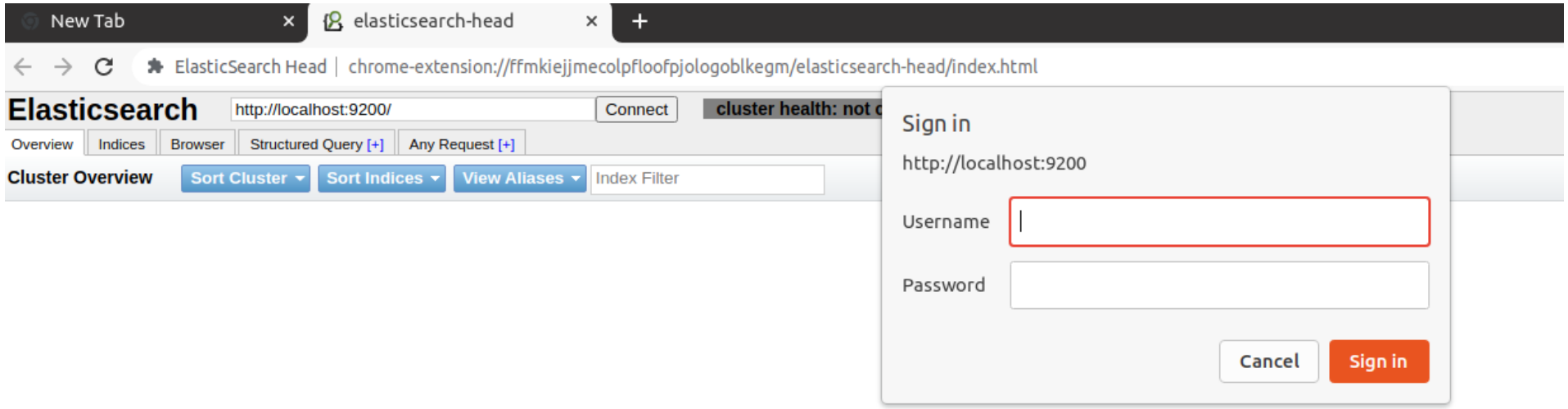


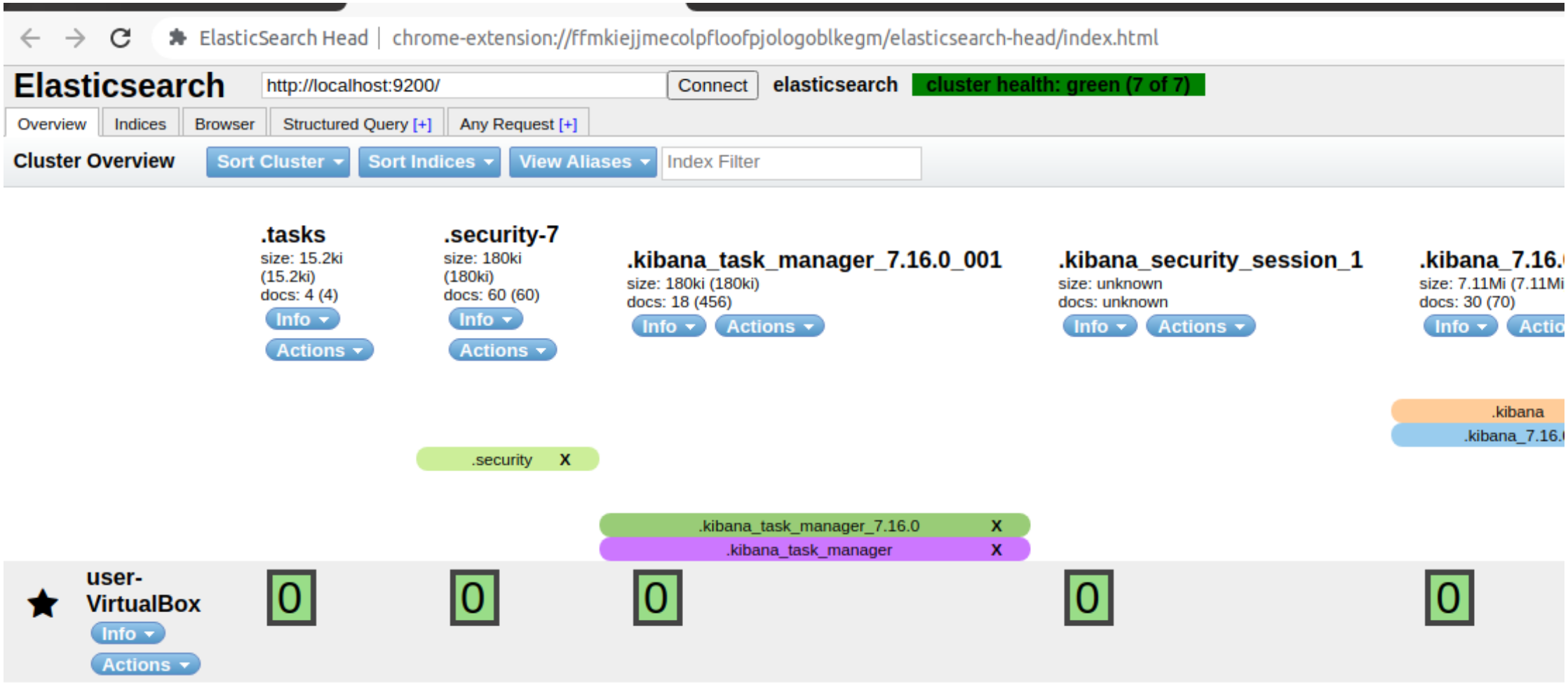

Elastic
127.0.0.1:5601/login?next=%2F
Welcome to Elastic
Username
Password
Log in

帳號管理


D
Stack Management
Users
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Rules and Connectors
Reporting
Machine Learning Jobs
Security
Users
Roles
API keys
Users
Create user
Search...
Show reserved users
User Name
Full Name
Email Address
Roles
Status
apm_system
apm_system
Reserved
beats_system
beats_system
Reserved
elastic
superuser
Reserved
kibana
kibana_system
Reserved
Deprecated
kibana_system
kibana_system
Reserved
logstash_system
logstash_system
Reserved
remote_monitoring_user
remote_monitoring_collector remote_monitoring_agent
Reserved
Rows per page: 20
1

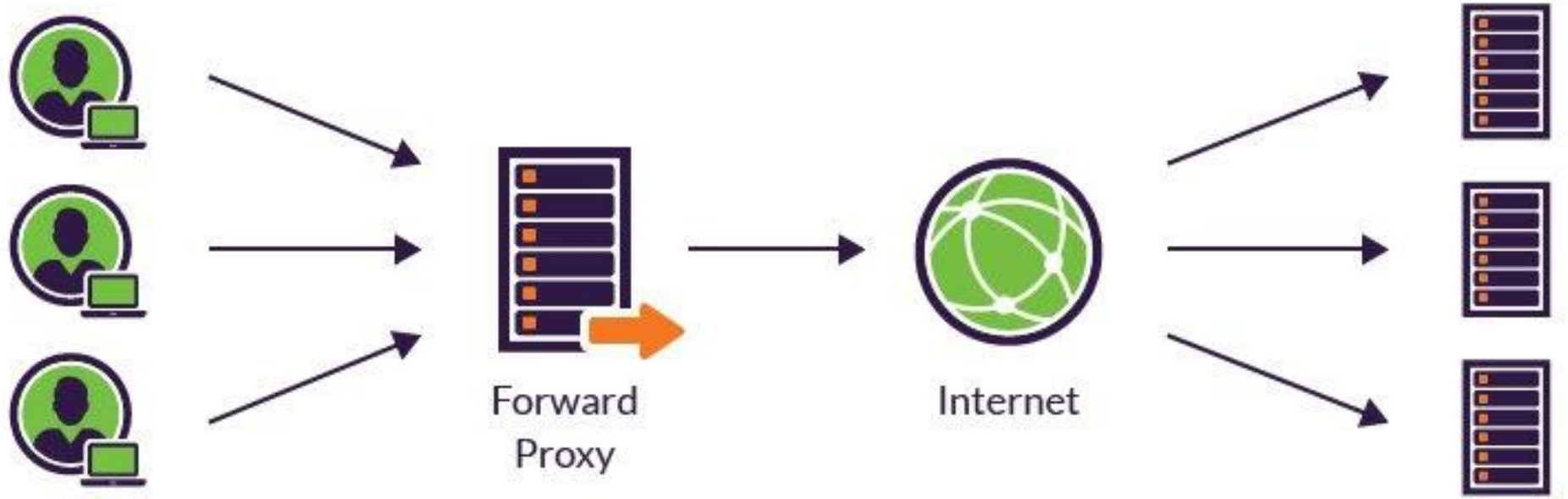
http auth


New Tab
elasticsearch-head
ElasticSearch Head | chrome-extension://ffmkiejjmecolpfloofpjologoblkegm/elasticsearch-head/index.html
Elasticsearch
http://localhost:9200/
Connect
cluster health: not c
Overview
Indices
Browser
Structured Query [+]
Any Request [+]
Cluster Overview
Sort Cluster
Sort Indices
View Aliases
Index Filter
Sign in
http://localhost:9200
Username
Password
Cancel
Sign in


ElasticSearch Head | chrome-extension://ffmkiejjmecolpfloofpjologoblkegm/elasticsearch-head/index.html
Elasticsearch
http://localhost:9200/
Connect
elasticsearch
cluster health: green (7 of 7)
Overview
Indices
Browser
Structured Query [+]
Any Request [+]
Cluster Overview
Sort Cluster
Sort Indices
View Aliases
Index Filter
.tasks
size: 15.2ki (15.2ki)
docs: 4 (4)
Info
Actions
.security-7
size: 180ki (180ki)
docs: 60 (60)
Info
Actions
.kibana_task_manager_7.16.0_001
size: 180ki (180ki)
docs: 18 (456)
Info
Actions
.kibana_security_session_1
size: unknown
docs: unknown
Info
Actions
.kibana_7.16.
size: 7.11Mi (7.11Mi
docs: 30 (70)
Info
Actio
.kibana
.kibana_7.16.
.security X
.kibana_task_manager_7.16.0 X
.kibana_task_manager X
user-VirtualBox
Info
Actions
0
0
0
0
0

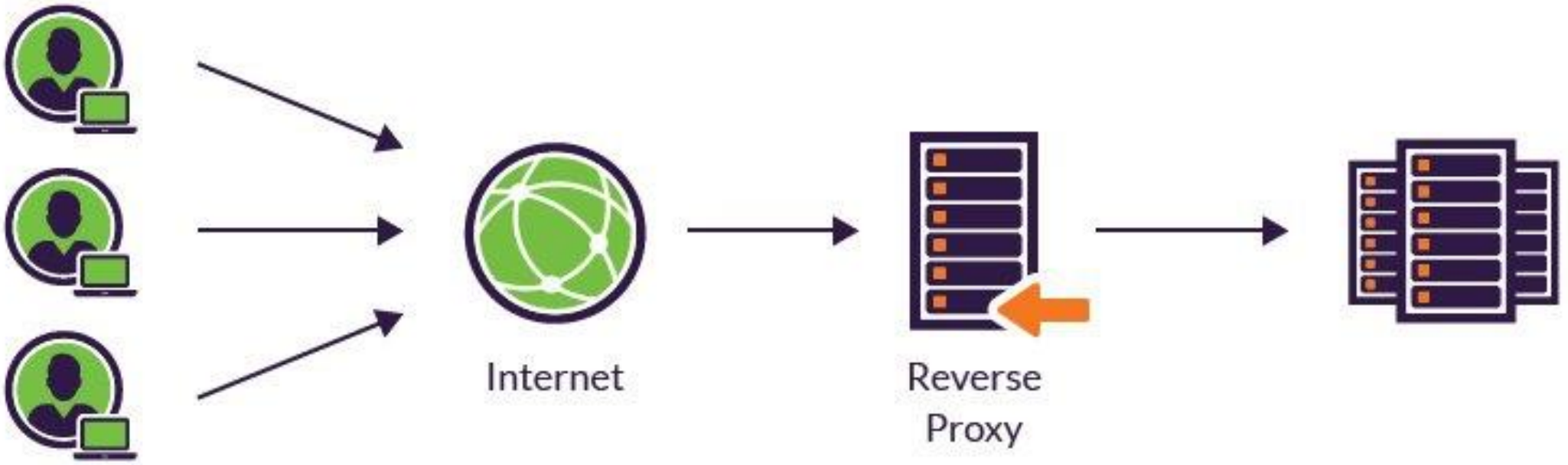
Nginx

Proxy



https://www.imperva.com/learn/performance/reverse-proxy/

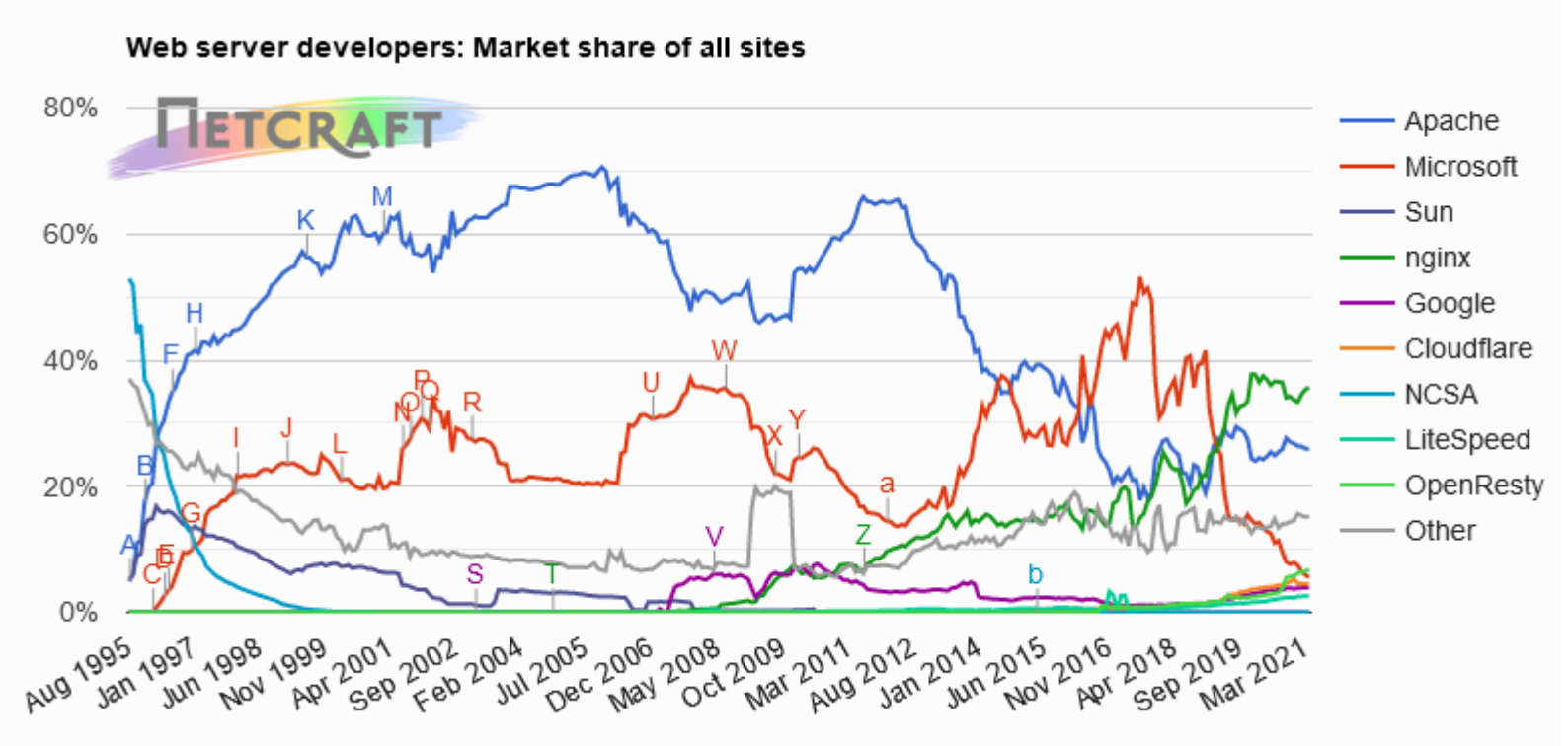
Reverse proxy



https://www.imperva.com/learn/performance/reverse-proxy/

About

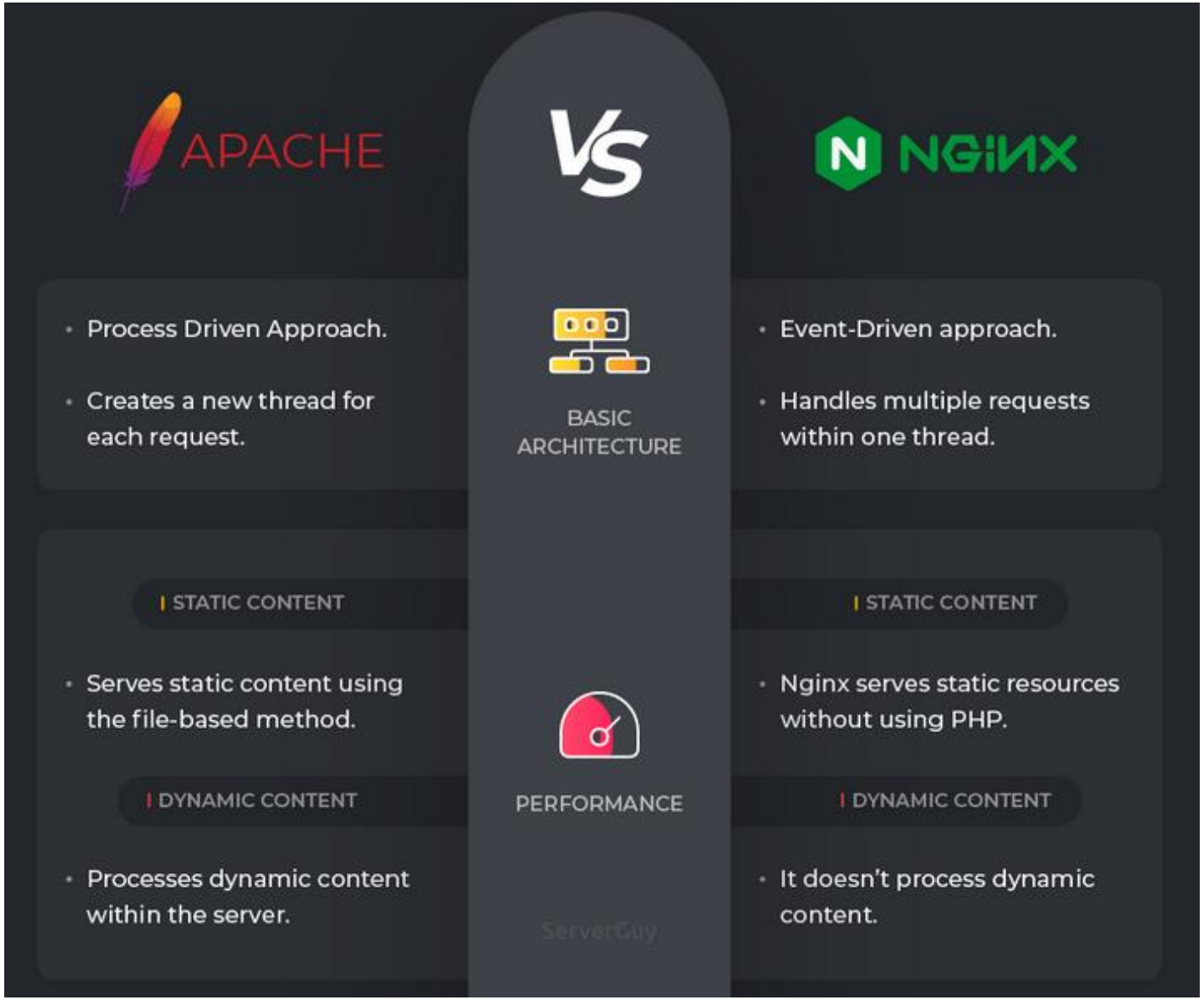
- Nginx pronounced as “ Engine X ”.
- 原先是設計用來服務 static files，但經過改進目前功能已相當完整，可並駕Apache。
- 常用於 reverse proxy, load balancer, mail proxy and for HTTP caching.



市佔率

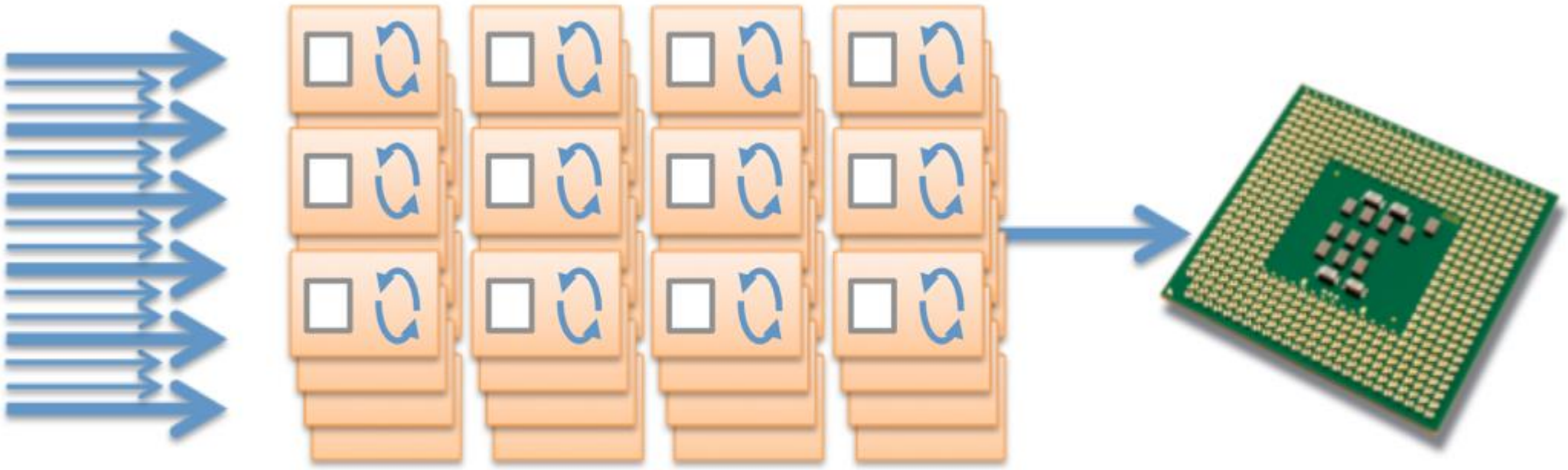
Developer	March 2021	Percent	April 2021	Percent	Change
nginx	419,637,923	35.34%	432,167,302	35.65%	0.32
Apache	308,509,042	25.98%	313,948,741	25.90%	-0.08
OpenResty	77,819,490	6.55%	81,935,391	6.76%	0.21
Microsoft	70,826,342	5.96%	67,182,740	5.54%	-0.42

https://news.netcraft.com/archives/category/web-server-survey/



https://serverguy.com/comparison/apache-vs-nginx/

Apache Thread-based



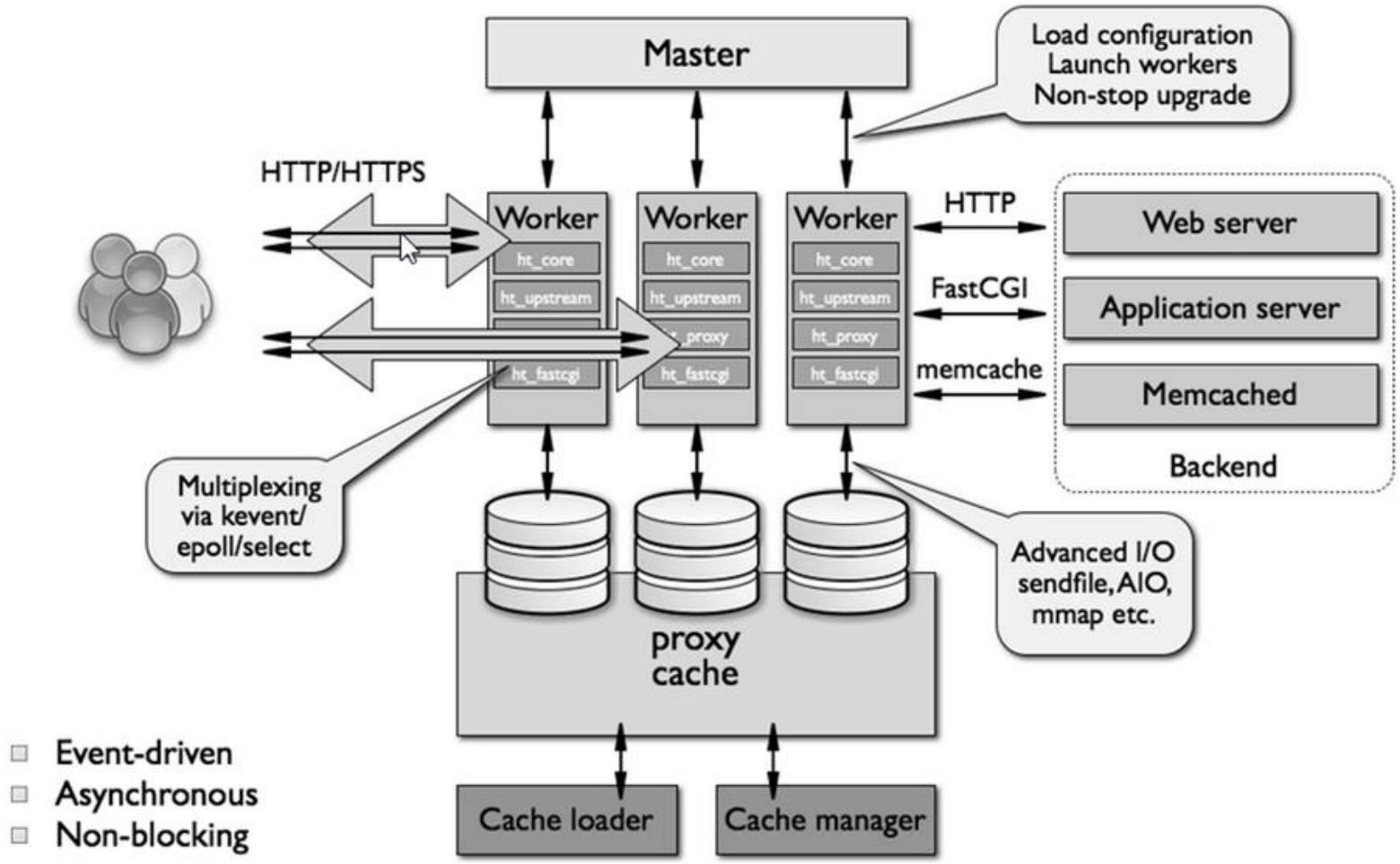
Hundreds of concurrent connections...

require hundreds of heavyweight threads or processes...

competing for limited CPU and memory

https://serverguy.com/comparison/apache-vs-nginx/

Nginx Event-based



https://serverguy.com/comparison/apache-vs-nginx/

Performance (Static content)

- 架構 差異：
  Apache : select (block)
  Nginx : epoll (non-block)
- Apache : Serves static content using the file-based method.
- Nginx : At serving static content, Nginx is the king!

  By default, NGINX handles file transmission itself and copies the file into the buffer before sending it.

Performance (Dynamic content)

- 動態資源：需求轉發到 Application Server，由 Application Server 處理完後，在 response 回去，由 Web Server 進行 Response，最後回到 User 端。
- Application Server：以程式語言建立出之 Server，並且可以靜態跟動態解析。
- Apache：能夠自己處理動態內容(如PHP…等)，也可以 pass 到後端 application server。
- Nginx：無法自己處理動態內容 (輕量導向)，皆須 pass 到後端 application server。

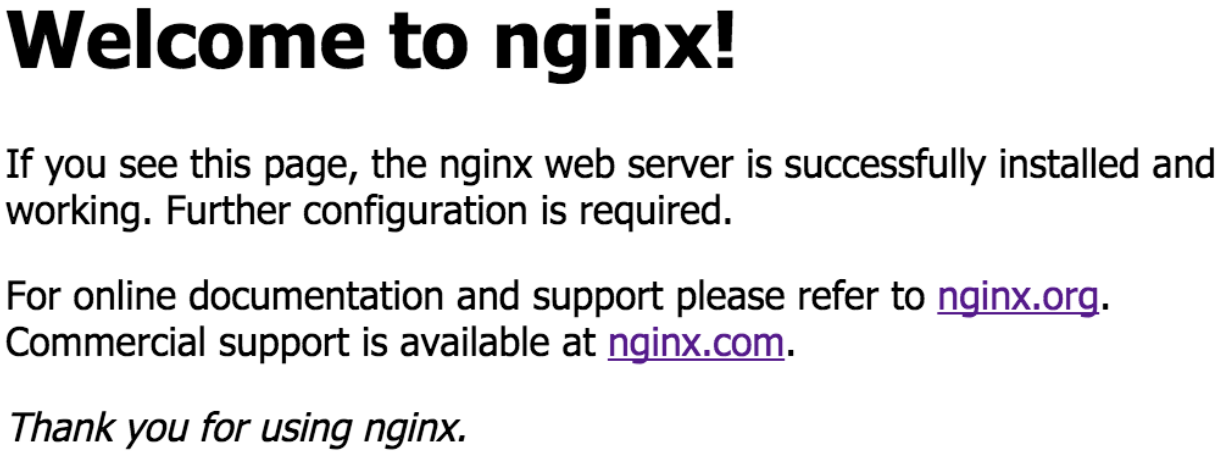
Nginx

reverse proxy with login func.

使用前 記得先安裝

- Centos
- sudo yum install epel-release
- sudo yum install nginx

- Ubuntu
- sudo apt install nginx



設定

- Centos & ubuntu
- /etc/nginx/nginx.conf
- /etc/nginx/conf.d/xxx.conf
- 使用 reverse proxy 功能，log format 記得加入欄位：$http_x_forwarded_for，記錄正確之 client IP。

```
# For more information on configuration, see:
#   * Official English Documentation: http://nginx.org/en/docs/
#   * Official Russian Documentation: http://nginx.org/ru/docs/

user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;

# Load dynamic modules. See /usr/share/doc/nginx/README.dynamic.
include /usr/share/nginx/modules/*.conf;

events {
    worker_connections 1024;
}

http {
    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    sendfile            on;
    tcp_nopush          on;
    tcp_nodelay         on;
    keepalive_timeout   65;
    types_hash_max_size 2048;

    include             /etc/nginx/mime.types;
    default_type        application/octet-stream;

    # Load modular configuration files from the /etc/nginx/conf.d directory.
    # See http://nginx.org/en/docs/ngx_core_module.html#include
    # for more information.
"/etc/nginx/nginx.conf" 90L, 2475C
```

Nginx & application server

- Kibana (ELK) web application server

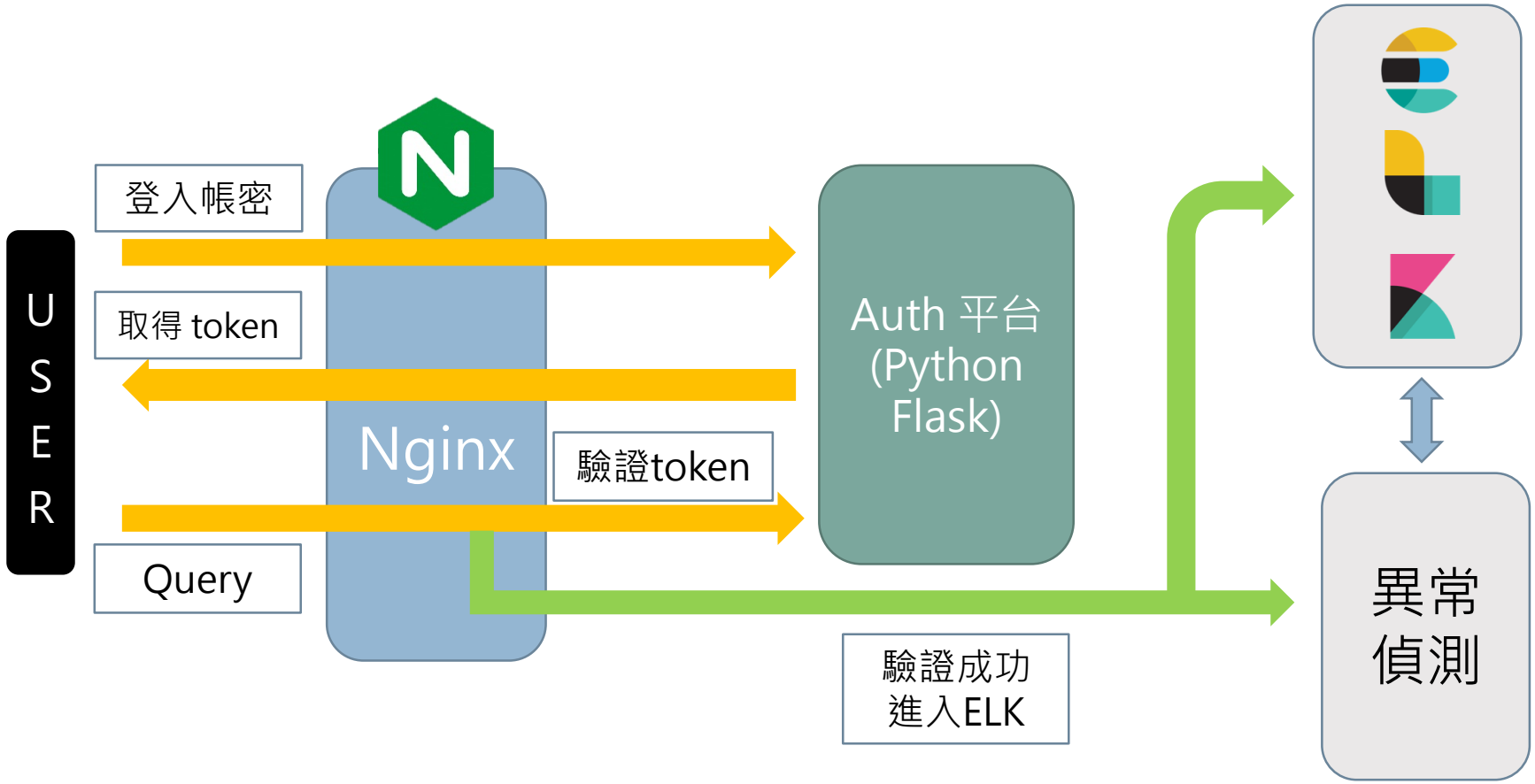
  Listen on 127.0.0.1:5601

- Nginx server

  Listen on 0.0.0.0:443 and 0.0.0.0:80

```
[root@elk-arcsight-node50 ~]# netstat -nlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      7304/nginx: master
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      7012/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      7288/master
tcp        0      0 127.0.0.1:5050          0.0.0.0:*               LISTEN      12459/python3
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      7304/nginx: master
tcp        0      0 127.0.0.1:5601          0.0.0.0:*               LISTEN      19497/node
tcp6       0      0 :::5000                 :::*                    LISTEN      22125/java
tcp6       0      0 192.168.21.50:9200      :::*                    LISTEN      18417/java
tcp6       0      0 127.0.0.1:9200          :::*                    LISTEN      18417/java
tcp6       0      0 ::1:9200                :::*                    LISTEN      18417/java
```

ELK_單一登入驗證機制



Nginx 設定

```
server {
    listen 80 default_server;
    server_name _ ;
    return 301 https://$host$request_uri;
}


server {

   listen 443 ssl;
   client_max_body_size 4G;

   # set the correct host(s) for your site
   server_name                ;

   keepalive_timeout 5;

   ssl_certificate /home/cert/server.crt;
   ssl_certificate_key /home/cert/server.key;


   location / {

     try_files $uri @proxy_to_app;

     #auth_basic "I'm watching you...";
     #auth_basic_user_file /etc/nginx/.servpwd;
   }
```

Use reverse proxy module

```
location @proxy_to_app {
  proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
  proxy_set_header X-Forwarded-Proto $scheme;
  proxy_set_header Host $http_host;
  # we don't want nginx trying to do something clever with
  # redirects, we set the Host: header above already.
  proxy_redirect off;
  proxy_pass http://127.0.0.1:5601;

}
```

Nginx 設定 (conti.)

- 使用 auth_request module ，使用者須先認證(登入)，才可進入允許的連結(kibana)

```
location / {

  auth_request /auth;
  error_page 401 = @error401;

  try_files $uri @proxy_to_app;

  #auth_basic "I'm watching you...";
  #auth_basic_user_file /etc/nginx/.servpwd;
}

location = /auth {
  internal;
  proxy_pass http://127.0.0.1:5050/auth;

  proxy_pass_request_body off;
  proxy_set_header Content-Length "";
  proxy_set_header X-Original-URI $request_uri;
  proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
  proxy_set_header X-Forwarded-Proto $scheme;
  proxy_set_header Host $http_host;
  proxy_redirect off;

}
```

```
location @error401 {
  proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
  proxy_set_header X-Forwarded-Proto $scheme;
  proxy_set_header Host $http_host;
  proxy_redirect off;

  return 302 https://$host/appv2/login?next=https://$http_host$request_uri;
}
```

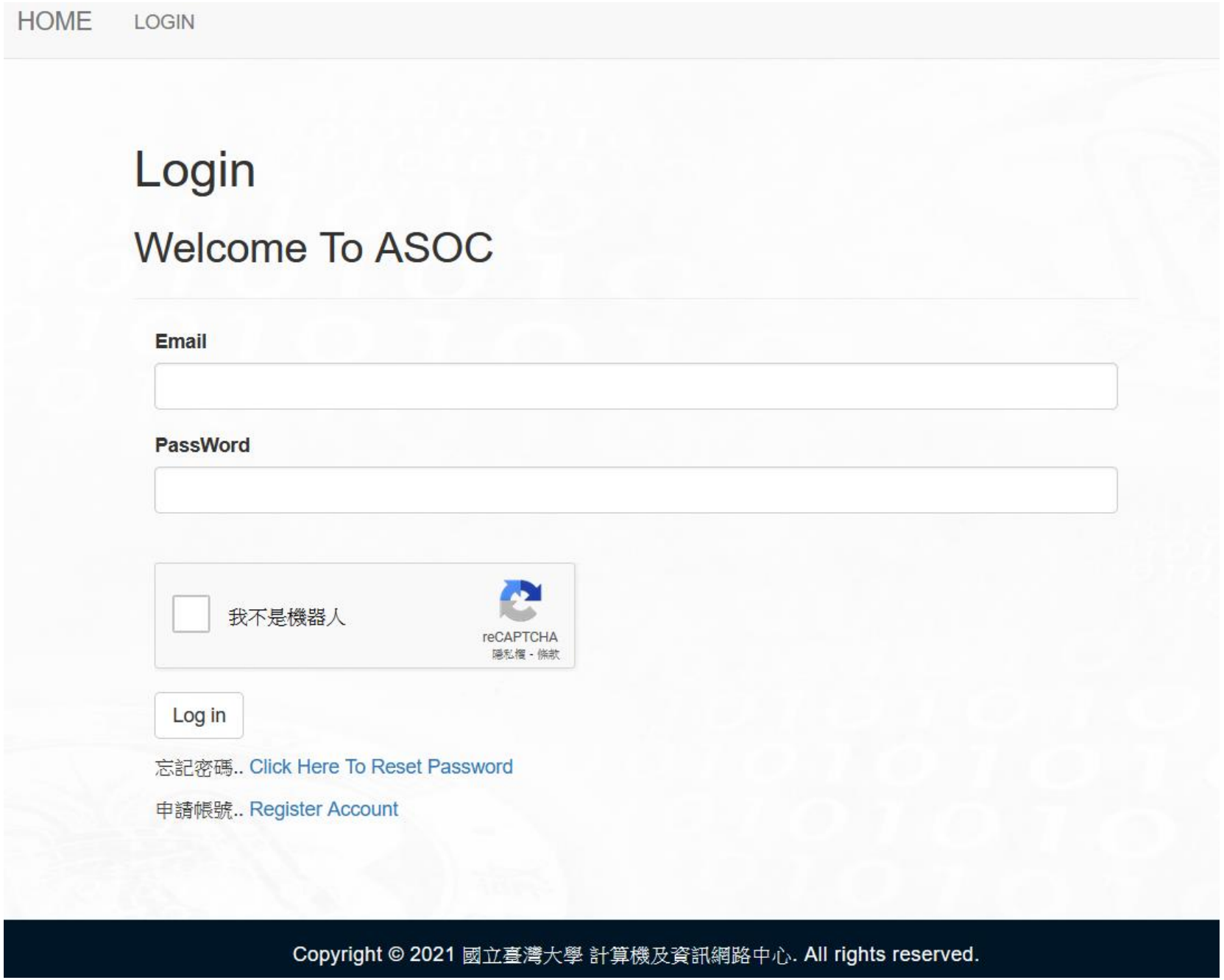
```
@app.route('/auth')
def auth():

    if (current_user.is_authenticated and current_user.confirm):
        return "You are logged in!"

    else:
        return 'Sorry, you\'re not logged in.', 401
```

Nginx 設定 (conti.)

- **auth_request module**
- If the subrequest returns a 2xx response code, the access is allowed.
- If it returns 401 or 403, the access is denied with the corresponding error code.

```
@app.route('/auth')
def auth():

    if (current_user.is_authenticated and current_user.confirm):
        return "You are logged in!"

    else:
        return 'Sorry, you\'re not logged in.', 401
```

Default response code = 200


HOME
LOGIN
Login
Welcome To ASOC
Email
PassWord
我不是機器人
reCAPTCHA
隱私權 - 條款
Log in
忘記密碼.. Click Here To Reset Password
申請帳號.. Register Account
Copyright © 2021 國立臺灣大學 計算機及資訊網路中心. All rights reserved.

HOME ELK CHANGEPASSWORD LOGOUT

國立臺灣大學計算機及資訊網路中心
Computer and Information Networking Center, National Taiwan University

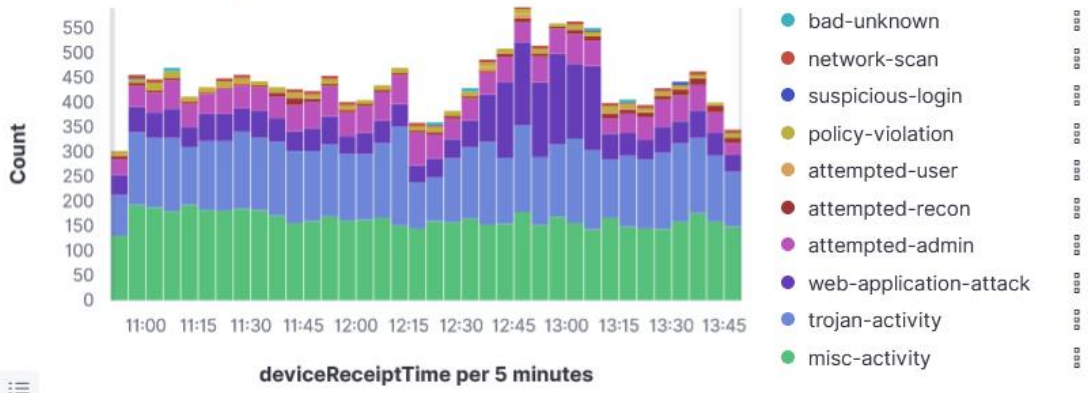
北區學術資訊安全維運中心

Academic Security Operation Center

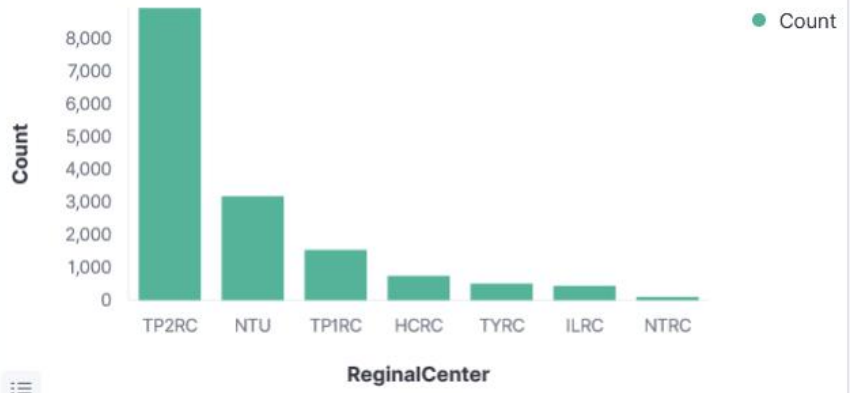
Cyber Security Threat Dashboard

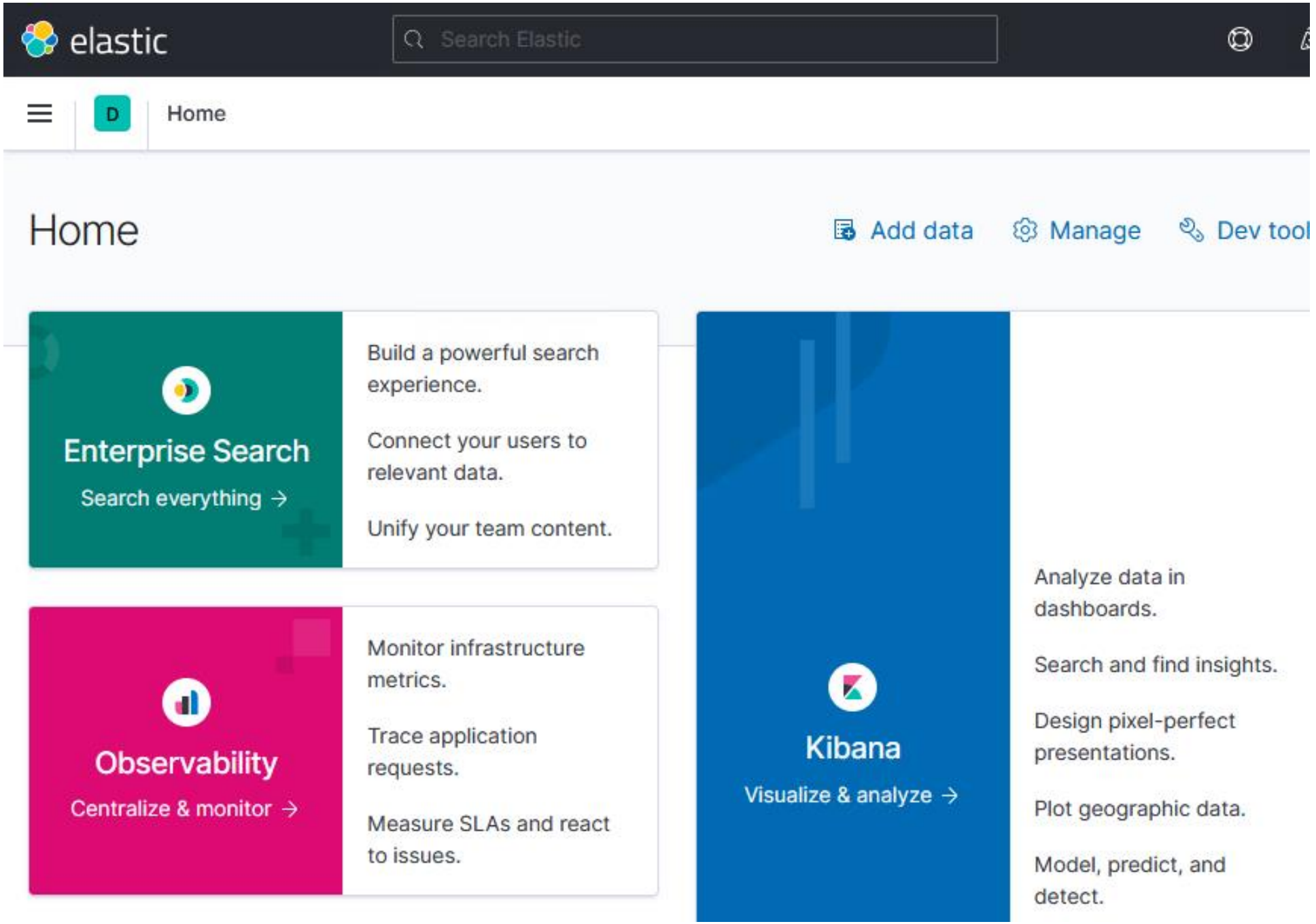
+ Add filter

ASOC - Event Category (Bar)



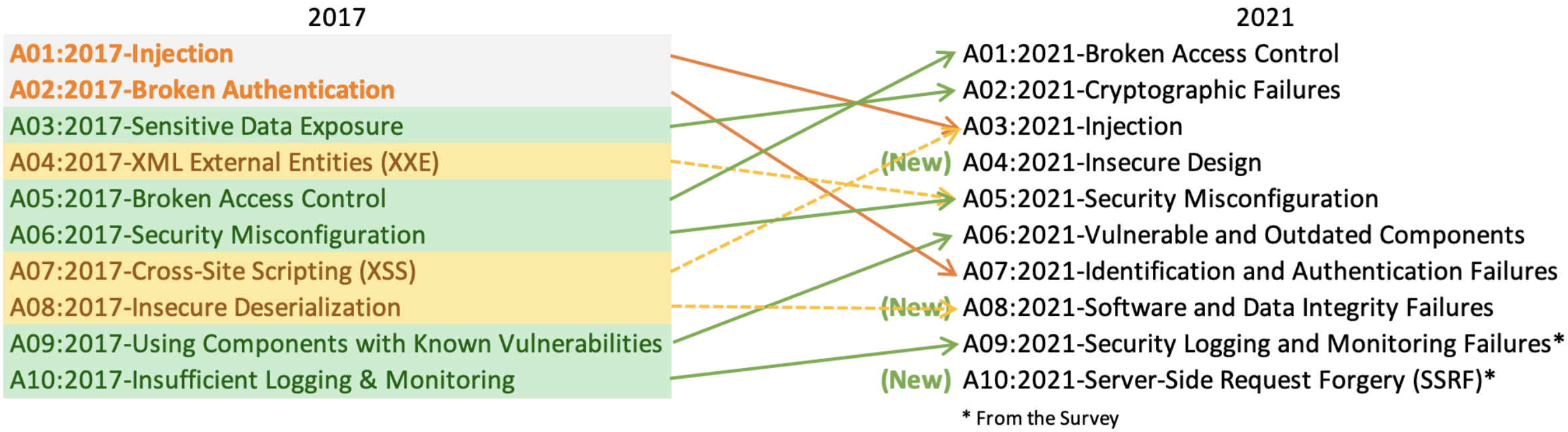
ASOC - RegionalCenter number




elastic
Search Elastic
D
Home
Home
Add data
Manage
Dev tool
Enterprise Search
Search everything →
Build a powerful search experience.
Connect your users to relevant data.
Unify your team content.
Observability
Centralize & monitor →
Monitor infrastructure metrics.
Trace application requests.
Measure SLAs and react to issues.
Kibana
Visualize & analyze →
Analyze data in dashboards.
Search and find insights.
Design pixel-perfect presentations.
Plot geographic data.
Model, predict, and detect.

ModSecurity
(OWASP CRS)

OWASP Top 10



https://owasp.org/Top10/

A04:2021-Insecure Design

- **A04:2021-不安全設計** 這是 2021 年版本的新類別，並特別針注在與設計相關的缺失。如果我們真的希望讓整個產業"向左移動" * 註一 * ，那我們必須進一步的往威脅建模，安全設計模塊的觀念，和安全參考架構前進。
- * 註一: Move Left 於英文原文中代表在軟體開發及交付過程中，在早期找出及處理相關問題，同 Shift Left Testing。 *
- A04:2021-Insecure Design is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, we need more threat modeling, secure design patterns and principles, and reference architectures. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks.

A08:2021-Software and Data Integrity Failures

- **A08:2021-軟體及資料完整性失效** 這是 2021 年版本全新的類別，並在軟體更新，機敏及重要資料，和 CI/CD 管道中並沒有做完整性的確認為前提做假設並進行評估。在評估中影響權重最高分的 CVE/CVSS 資料都與這類別中的 10 個 CWE 對應到。2017 年版本中不安全的反序列化現在被合併至此類別。
- A08:2021-Software and Data Integrity Failures is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. **A8:2017-Insecure Deserialization** is now a part of this larger category.

A10:2021-Server-Side Request Forgery

- **A10:2021-伺服端請求偽造** 這個類別是在業界問卷排名第一名，並在此版本內納入。由資料顯示此問題有較低被驗測次數和範圍，但有高於平均的威脅及影響權重比率。這個類別的出現也是因為業界專家重複申明這類別的問題相當重要，即使在本次資料中並沒有足夠的資料去顯示這個問題。
- A10:2021-Server-Side Request Forgery is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

Top vulnerabilities x OWASP Top 10

Top Vulnerabilities With Known Exploits or Proofs of Concept	CVE	Severity	Related Top 10 2021
Apache Struts2 remote code execution (RCE) vulnerability	CVE-2017-5638	Critical	A03, A06
Apache Struts 2 REST plugin XStream RCE vulnerability	CVE-2017-9805	High	A03, A06
Drupal Core RCE vulnerability	CVE-2018-7600	Critical	A03
Oracle WebLogic server RCE vulnerabilities	CVE-2020-14750	Critical	A03
WordPress file manager plugin RCE vulnerability	CVE-2020-25213	Critical	A03, A06
vBulletin 'subwidgetConfig' unauthenticated RCE vulnerability	CVE-2020-17496	Critical	A03
SaltStack salt authorization weakness vulnerability	CVE-2020-11651	Critical	A01, A02
Apache Struts OGNL expression RCE vulnerability	CVE-2017-12611	Critical	A03, A08
Eclipse Jetty chunk length parsing integer overflow vulnerability	CVE-2017-7657	Critical	A03, A08
Alibaba Nacos AuthFilter authentication bypass vulnerability	CVE-2021-29441	Critical	A07
Atlassian Jira information disclosure vulnerability	CVE-2020-14179	Medium	A05
Nginx crafted URI string handling access restriction bypass vulnerability	CVE-2013-4547	N/A	A01
Apache Struts 2 RCE vulnerability	CVE-2019-0230	Critical	A03, A06
Apache Struts OGNL expression RCE vulnerability	CVE-2018-11776	High	A03, A08
Liferay portal untrusted deserialization vulnerability	CVE-2020-7961	Critical	A08

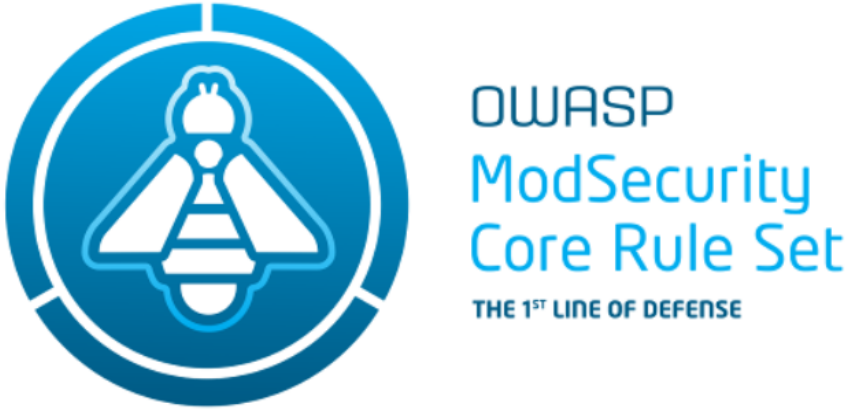
https://www.trendmicro.com/en_us/devops/21/k/overview-owasp-top-10-2021.html

OWASP ModSecurity Core Rule Set

OWASP ModSecurity Core Rule Set

The 1st Line of Defense Against Web Application Attacks

The OWASP ModSecurity Core Rule Set (CRS) is a set of generic attack detection rules for use with ModSecurity or compatible web application firewalls. The CRS aims to protect web applications from a wide range of attacks, including the OWASP Top Ten, with a minimum of false alerts. The CRS provides protection against many common attack categories, including SQL Injection, Cross Site Scripting, Local File Inclusion, etc.



The official website of the project can be found at https://coreruleset.org.

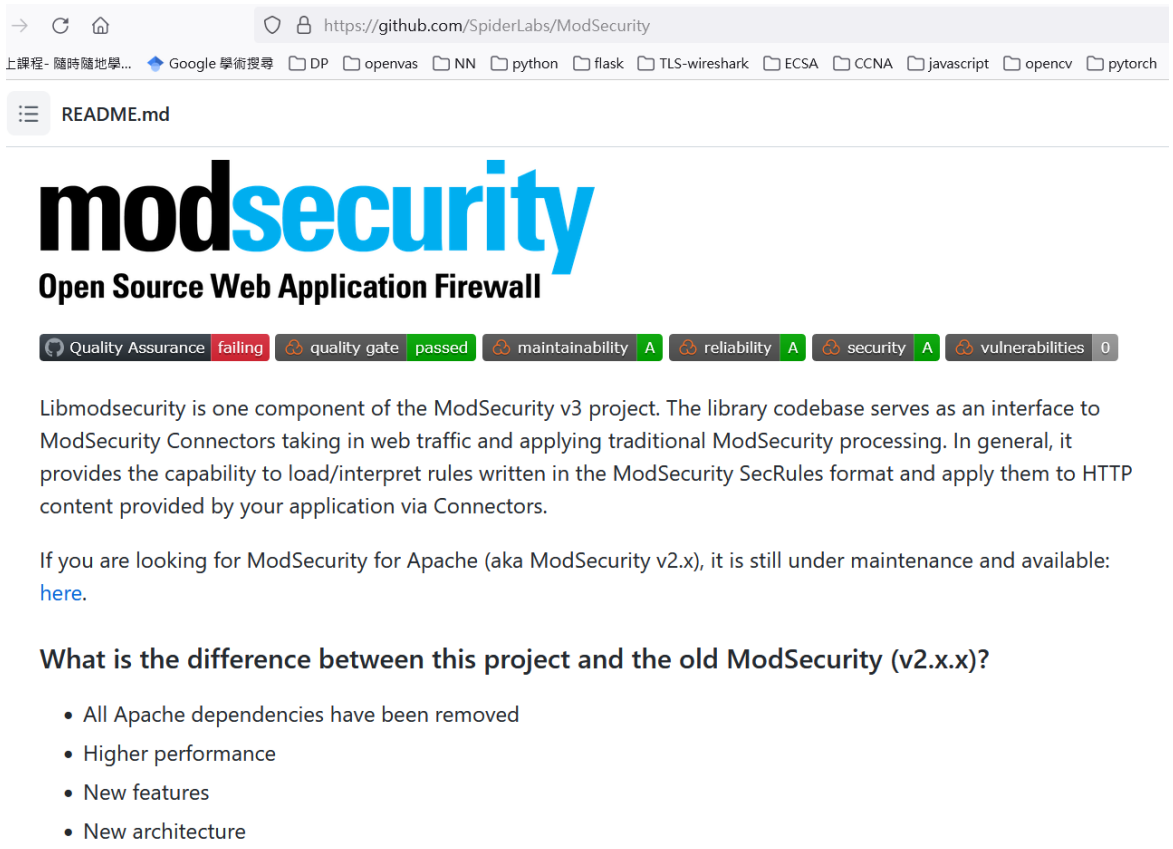
https://owasp.org/www-project-modsecurity-core-rule-set/

OWASP ModSecurity Core Rule Set

- 一套已經成形的網站，修補程式漏洞勢必牽動複雜的設計變更，比較經濟的作法即是 Virtual Patching，不直接針對程式本體修補，而是導入WAF (Web Application Firewall)，為符合是類需求，ModSecurity 開發平台提供規則設定語言 SecRules。
- 使用者可自行定義切合實需的規則，即時監控、記錄所有出入http通訊封包。
- 基於 ModSecurity 之普遍性，OWASP(Open Web Application Security Project) 專案維護核心規則集(Core Rule Set)，縮寫CRS，能抗衡一般類別的漏洞攻擊手法，CRS 在 ModSecurity 官網免費釋出，當然也有需付費的規則集。

https://www.twcert.org.tw/newepaper/cp-67-2548-0b788-3.html

ModSecurity



https://github.com/SpiderLabs/ModSecurity

ModSecurity 簡介

- ModSecurity 係普遍應用之公開網頁程式防火牆(WAF)，可搭配OWASP(Open Web Application Security Project)維護的免費核心規則集(Core Rule Set：CRS)，初始設計為Apache HTTP Server之模組，後續發展成http封包過濾軟體，亦支援Microsoft IIS、NGINX等伺服器平台。
- ModSecurity是防火牆引擎，單靠引擎無法偵測惡意特徵，需要搭配時常更新的檢測規則。
- 其商用CRS維護者Trustwave SpiderLabs研究室，新加坡電信下轄資安公司。

https://www.twcert.org.tw/newepaper/cp-67-2548-0b788-3.html

Core Rule Set (CRS)

The **OWASP® ModSecurity Core Rule Set (CRS)** is a set of generic attack detection rules for use with **ModSecurity** or compatible web application firewalls. The CRS aims to protect web applications from a wide range of attacks, including the OWASP Top Ten, with a minimum of false alerts. The CRS provides protection against many common attack categories, including:

- SQL Injection (SQLi)
- Cross Site Scripting (XSS)
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- PHP Code Injection
- Java Code Injection
- HTTPoxy
- Shellshock
- Unix/Windows Shell Injection
- Session Fixation
- Scripting/Scanner/Bot Detection
- Metadata/Error Leakages

https://coreruleset.org/

Core Rule Set (CRS)

- CRS 將WAF規則分四等，每項規則均配賦ID、等級、重要性、偵測條件，經由crs-setup.conf組態值設定所需安全等級Paranoia Level 1～4，預設值Paranoia Level 1(PL1)為通用性防護規則，誤判率最低，隨等級提高其累加安全限制更為嚴苛，至PL4可謂最偏執，甚或阻擋相當數量的合法請求。

CRS Paranoia Levels

- PL 1: Baseline Security with a minimal need to tune away false positives. This is CRS for everybody running an HTTP server on the internet. If you encounter a false positive on a PL 1 system, please report it via GitHub.
- PL 2: Rules that are adequate when real customer data is involved. Perhaps an off-the-shelf online shop. Expect false positives and learn how to tune them away.
- PL 3: Online banking level security with lots of false positives. From a project perspective, false positives are accepted here, so you need to be able to help yourself by writing rule exclusions.
- PL 4: Rules that are so strong (or paranoid) they are adequate to protect the crown jewels. Use at your own risk and be prepared to get a large number of false positives.

- https://coreruleset.org/20211028/working-with-paranoia-levels/

CRS 中文說明

- https://docs.microsoft.com/zh-tw/azure/web-application-firewall/ag/application-gateway-crs-rulegroups-rules?tabs=owasp32

OWASP CRS 3.2 (公開預覽)

CRS 3.2 包含13個規則群組，如下表所示。 每個群組包含多個可以停用的規則。

> ⓘ 注意
>
> 只有 WAF_v2 SKU 可使用 CRS 3.2。

規則群組	描述
一般	一般群組
REQUEST-911-METHOD-ENFORCEMENT	(PUT、PATCH) 的鎖定方法
REQUEST-913-SCANNER-DETECTION	防止埠和環境掃描器
REQUEST-920-PROTOCOL-ENFORCEMENT	防範通訊協定和編碼問題
REQUEST-921-PROTOCOL-ATTACK	防止標頭插入、要求走私和回應

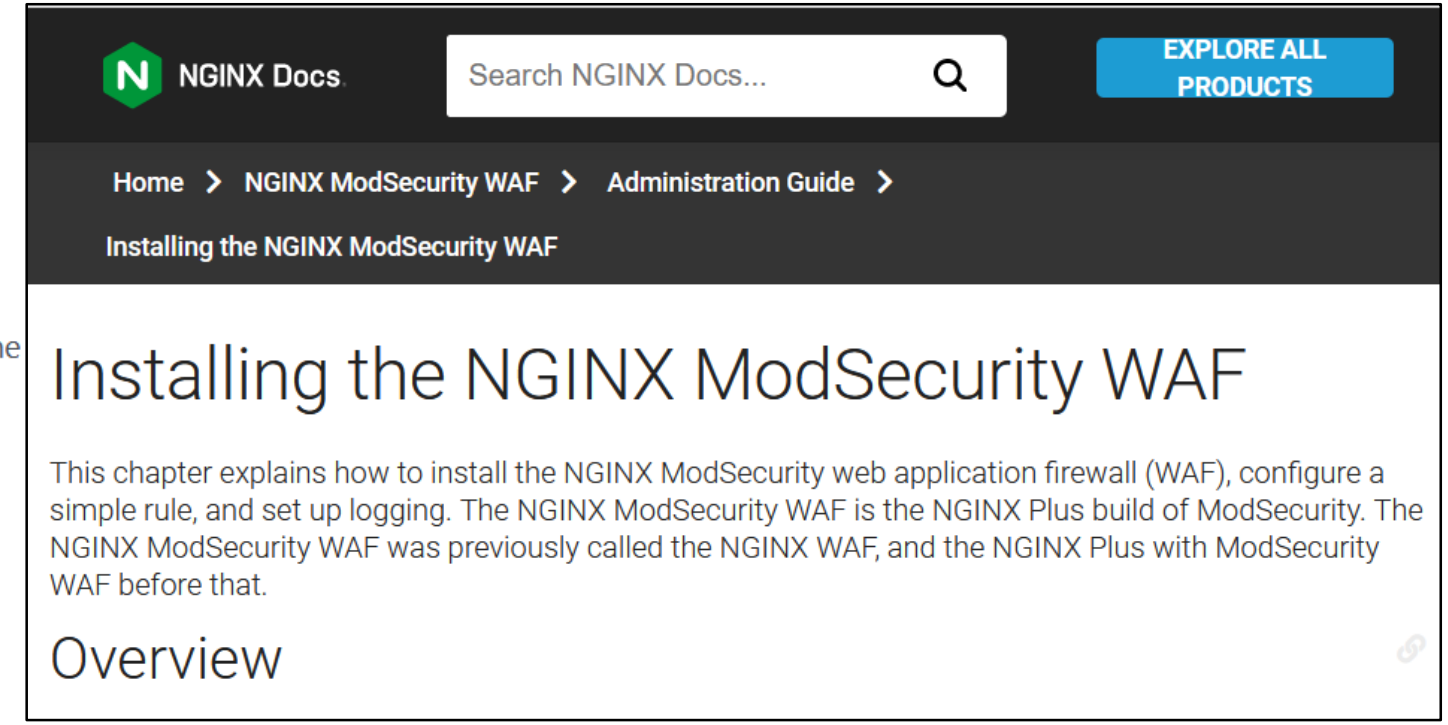
Nginx 安裝 modsecurity

Installation

Requirements

CRS 3 requires a web server with ModSecurity. We recommend the

- **Apache** web server with **ModSecurity** 2.9.x
- **IIS/Nginx** web server with **ModSecurity** 3.0.3 or higher

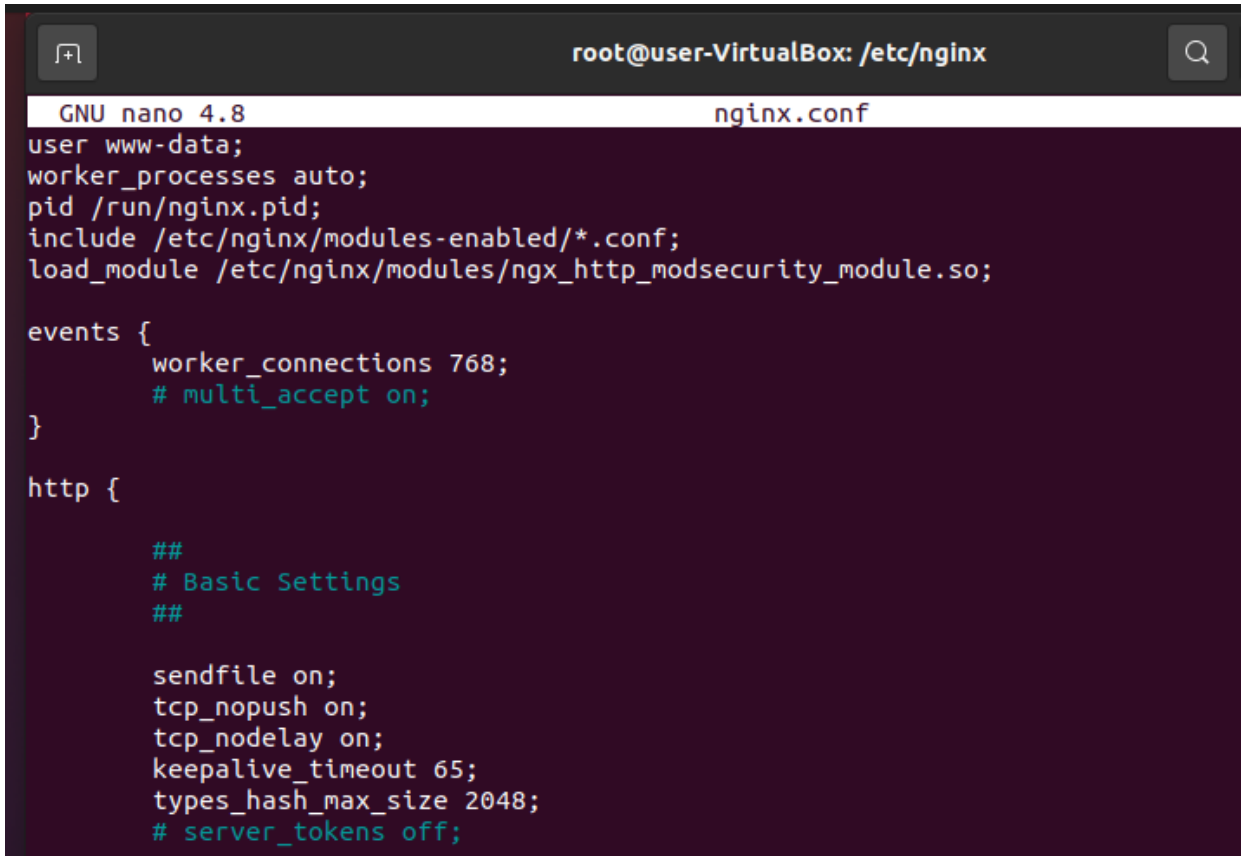


https://coreruleset.org/installation/

Nginx 安裝 modsecurity

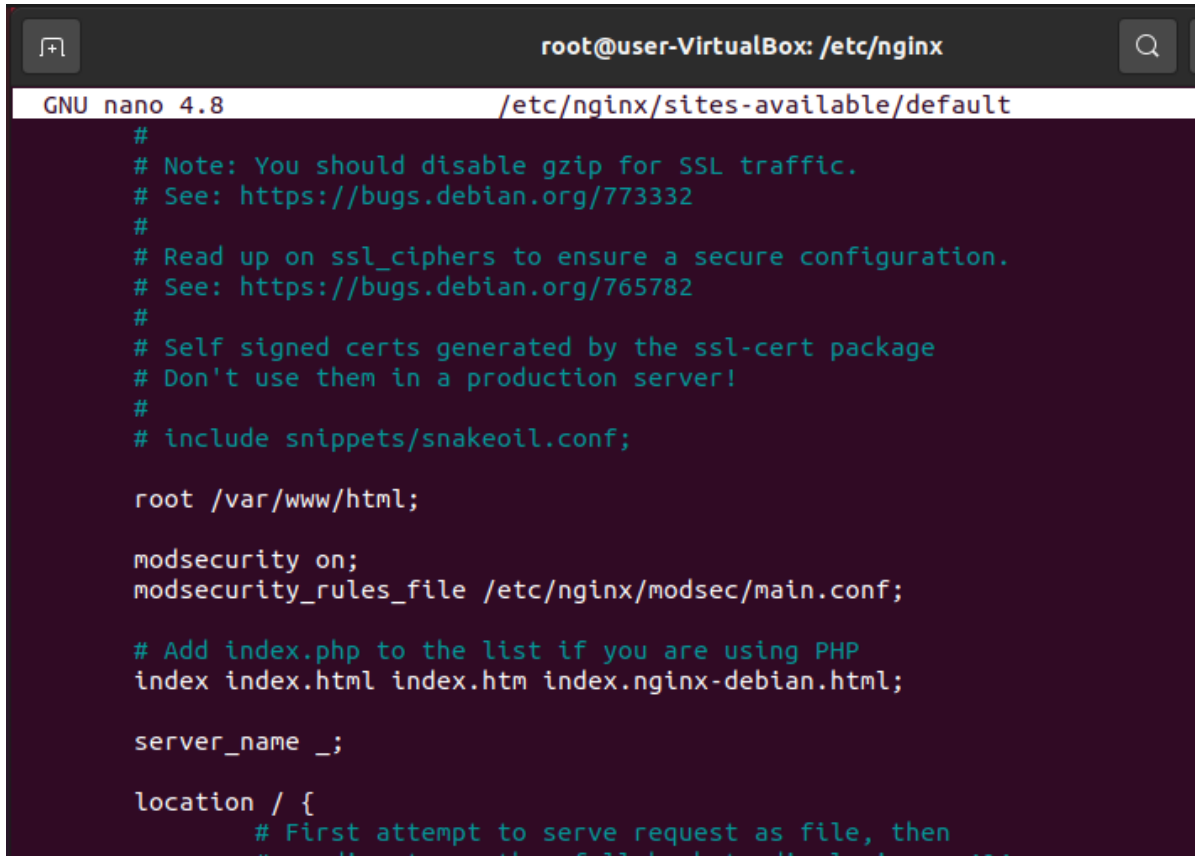
https://www.nginx.com/blog/compiling-and-installing-modsecurity-for-open-source-nginx/

設定- nginx load_module



設定- 啟動WAF

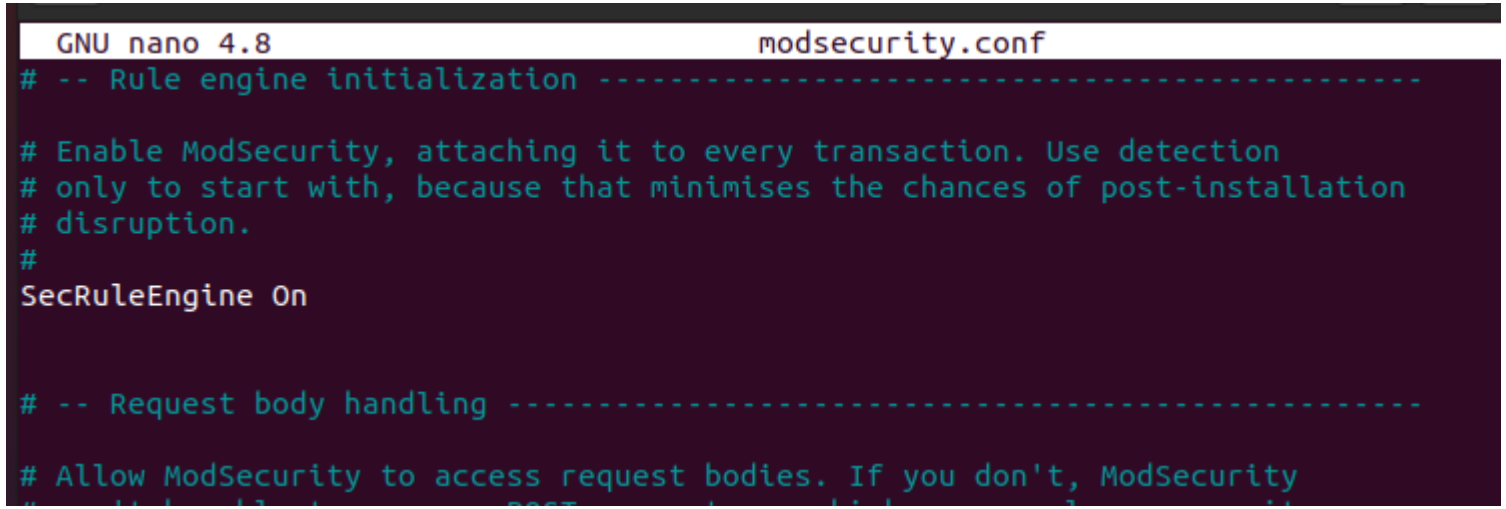
- 可以分別設定於不同 server 的conf
- 或分別啟用不同 rule set



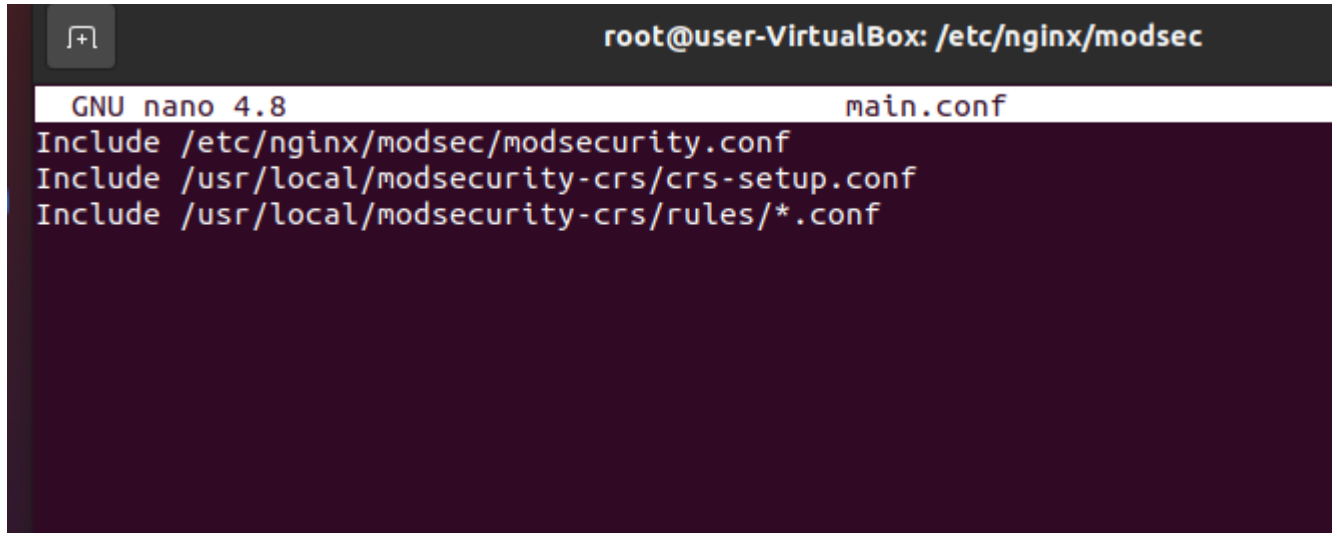
設定- modesecurity conf

SecRuleEngine On|Off|DetectionOnly

DetectionOnly: process rules but never executes any disruptive actions (block, deny, drop, allow, proxy and redirect)



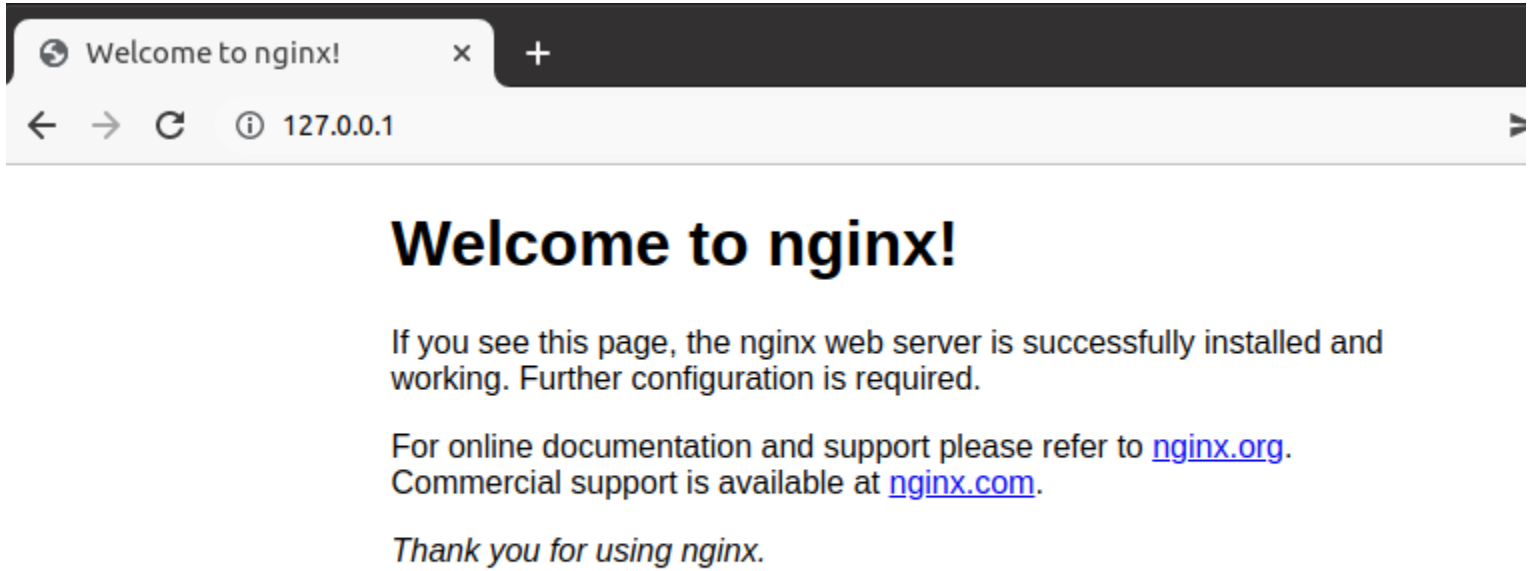
設定- include規則



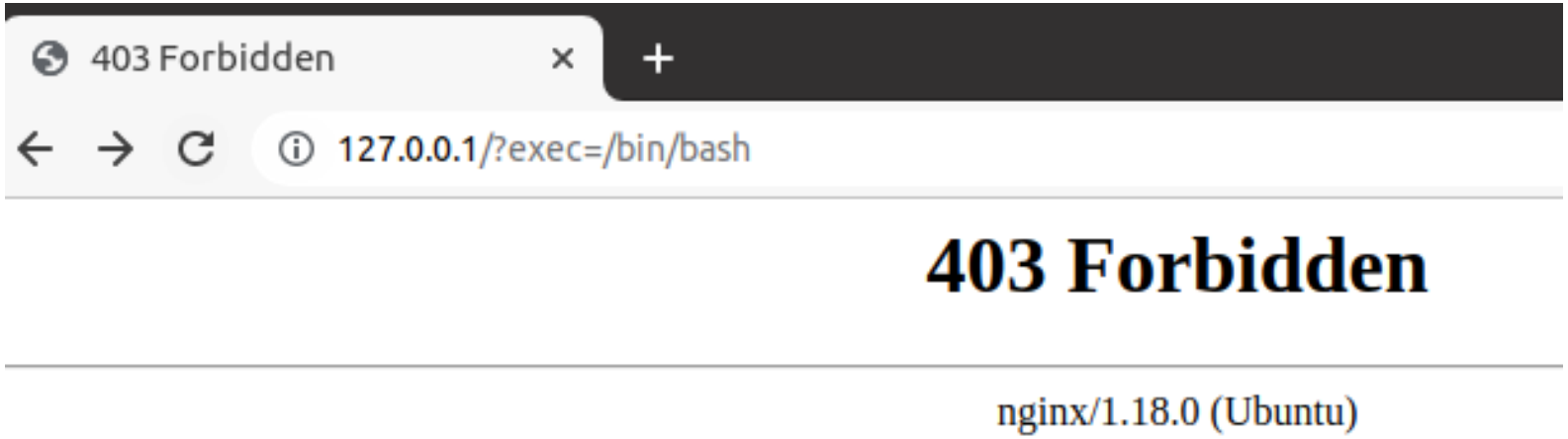
56

Web server & WAF

Nginx & WAF 阻擋


Welcome to nginx!
127.0.0.1
Welcome to nginx!
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.
Thank you for using nginx.

WAF 規則阻擋


403 Forbidden
127.0.0.1/?exec=/bin/bash
403 Forbidden
nginx/1.18.0 (Ubuntu)

Web server - Flask web server

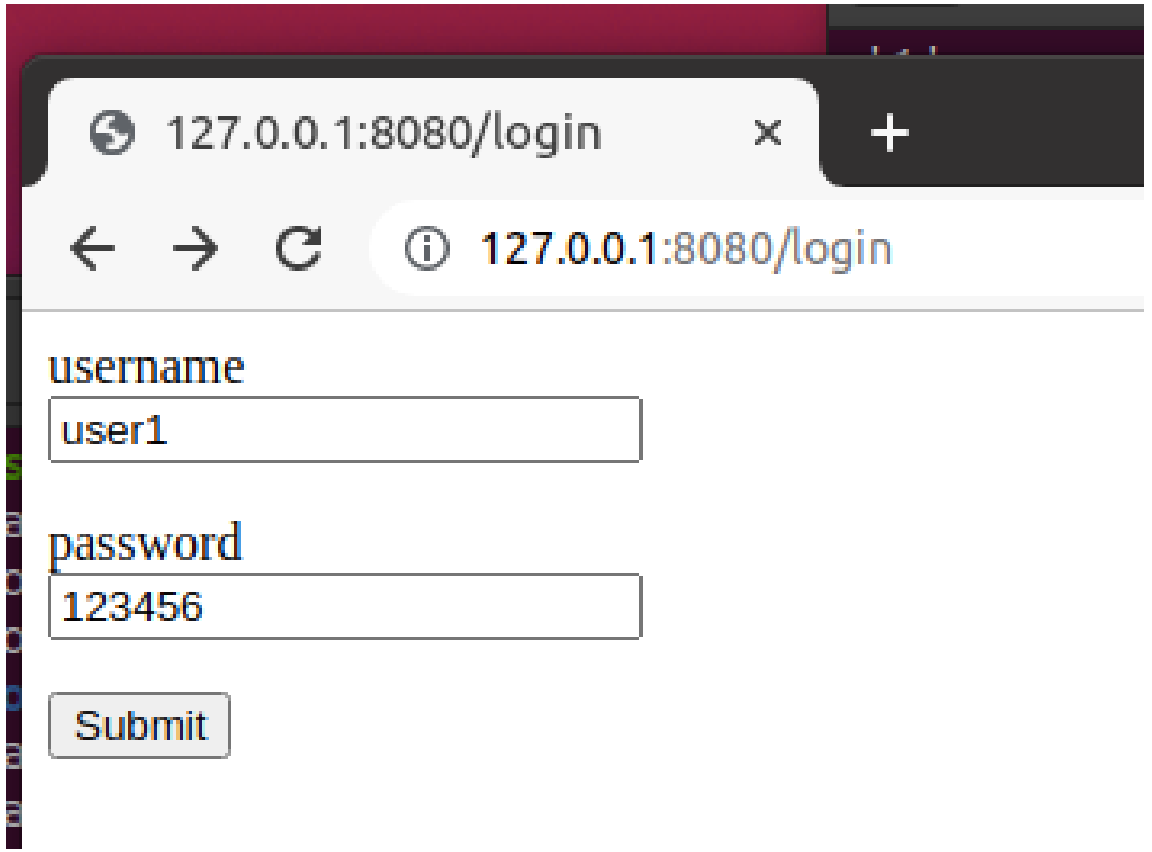
```
(flask-env) user@user-VirtualBox:~/webapp/sqlsev$ python test_submit.py
/home/user/webapp/flask-env/lib/python3.8/site-packages/flask_sqlalchemy/__init__.py:872: FSADeprecationWarning: SQLALC
HEMY_TRACK_MODIFICATIONS adds significant overhead and will be disabled by default in the future.  Set it to True or Fa
lse to suppress this warning.
  warnings.warn(FSADeprecationWarning(
 * Serving Flask app 'test_submit' (lazy loading)
 * Environment: production
   WARNING: This is a development server. Do not use it in a production deployment.
   Use a production WSGI server instead.
 * Debug mode: off
 * Running on all addresses.
   WARNING: This is a development server. Do not use it in a production deployment.
 * Running on http://10.0.2.15:5000/ (Press CTRL+C to quit)
127.0.0.1 - - [10/Dec/2021 12:05:25] "POST /login HTTP/1.0" 200 -
127.0.0.1 - - [10/Dec/2021 12:05:36] "GET /login HTTP/1.0" 200 -
127.0.0.1 - - [10/Dec/2021 12:17:23] "GET /login HTTP/1.1" 200 -
2021-12-10 12:17:28,917 INFO sqlalchemy.engine.Engine SELECT * FROM user WHERE username='' or 1=1 --' and password='';
2021-12-10 12:17:28,917 INFO sqlalchemy.engine.Engine [raw sql] ()
statement :  SELECT * FROM user WHERE username='' or 1=1 --' and password='';
parameters :  ()
duration :  0.0003414154052734375
context :  sqlsev/test_submit.py:36 (login)
127.0.0.1 - - [10/Dec/2021 12:17:28] "POST /login HTTP/1.1" 200 -
127.0.0.1 - - [10/Dec/2021 12:17:48] "GET /login HTTP/1.1" 200 -
127.0.0.1 - - [10/Dec/2021 12:18:20] "GET /login HTTP/1.0" 200 -
(flask-env) user@user-VirtualBox:~/webapp$ pwd
/home/user/webapp
(flask-env) user@user-VirtualBox:~/webapp$
3957  二   4  2019 mime.types
```

Resverse proxy & web server

```
 GNU nano 4.8                                  /etc/nginx/conf.d/flask.conf
server {

    listen 8080 default_server ;
    client_max_body_size 4G;

    # set the correct host(s) for your site
    server_name _ ;

    modsecurity on;
    modsecurity_rules_file /etc/nginx/modsec/main.conf;

    keepalive_timeout 5;

    location / {

      try_files $uri @proxy_to_app;

      #auth_basic "I'm watching you...";
      #auth_basic_user_file /etc/nginx/.servpwd;
    }


    location @proxy_to_app {
      proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
      proxy_set_header X-Forwarded-Proto $scheme;
      proxy_set_header Host $http_host;
      # we don't want nginx trying to do something clever with
      # redirects, we set the Host: header above already.
      proxy_redirect off;
      proxy_pass http://127.0.0.1:5000;

    }
```

Web form query

正常查詢



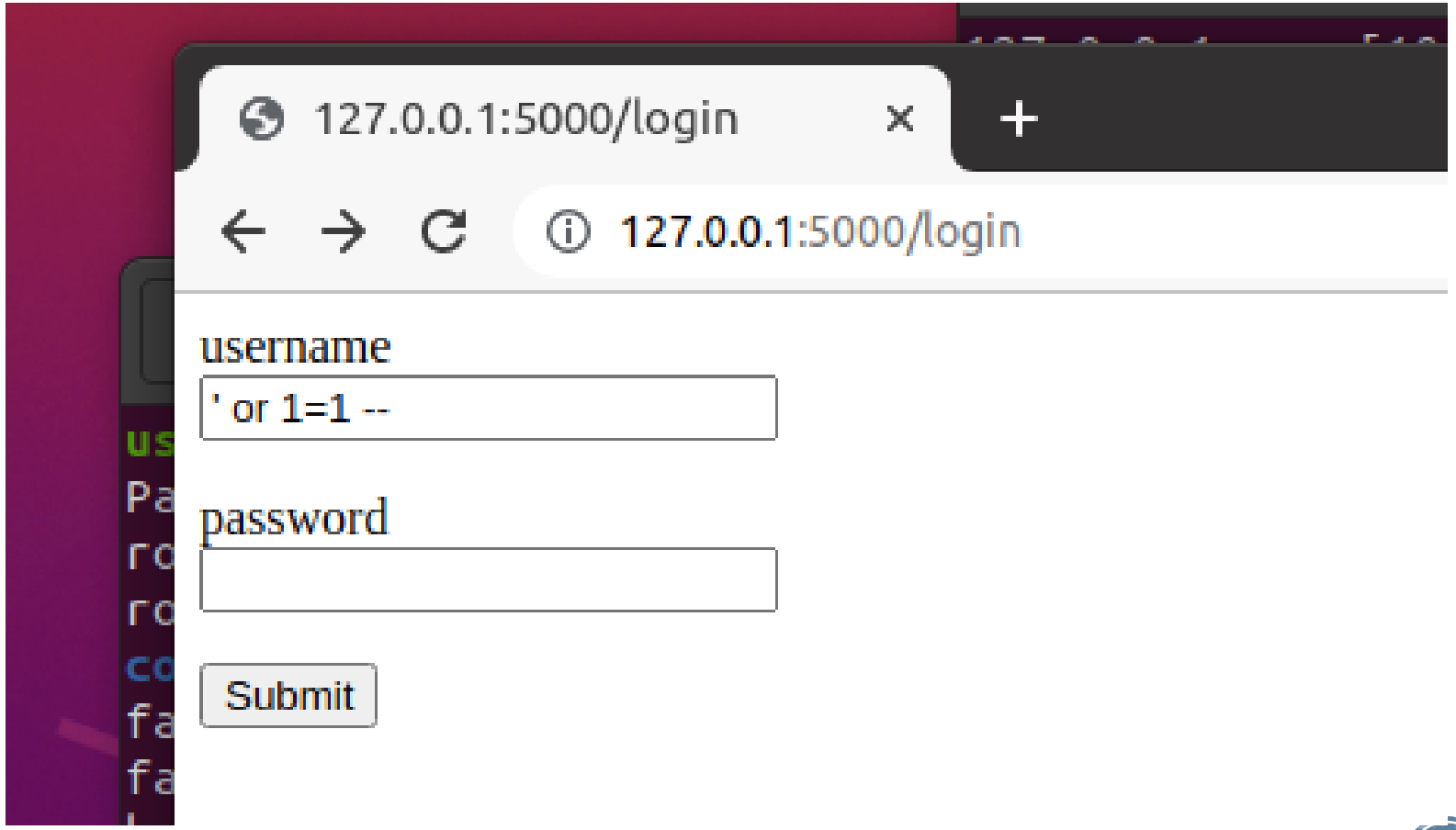
Hello,

Your Information

ID : 2
名字：user1
密碼：123456

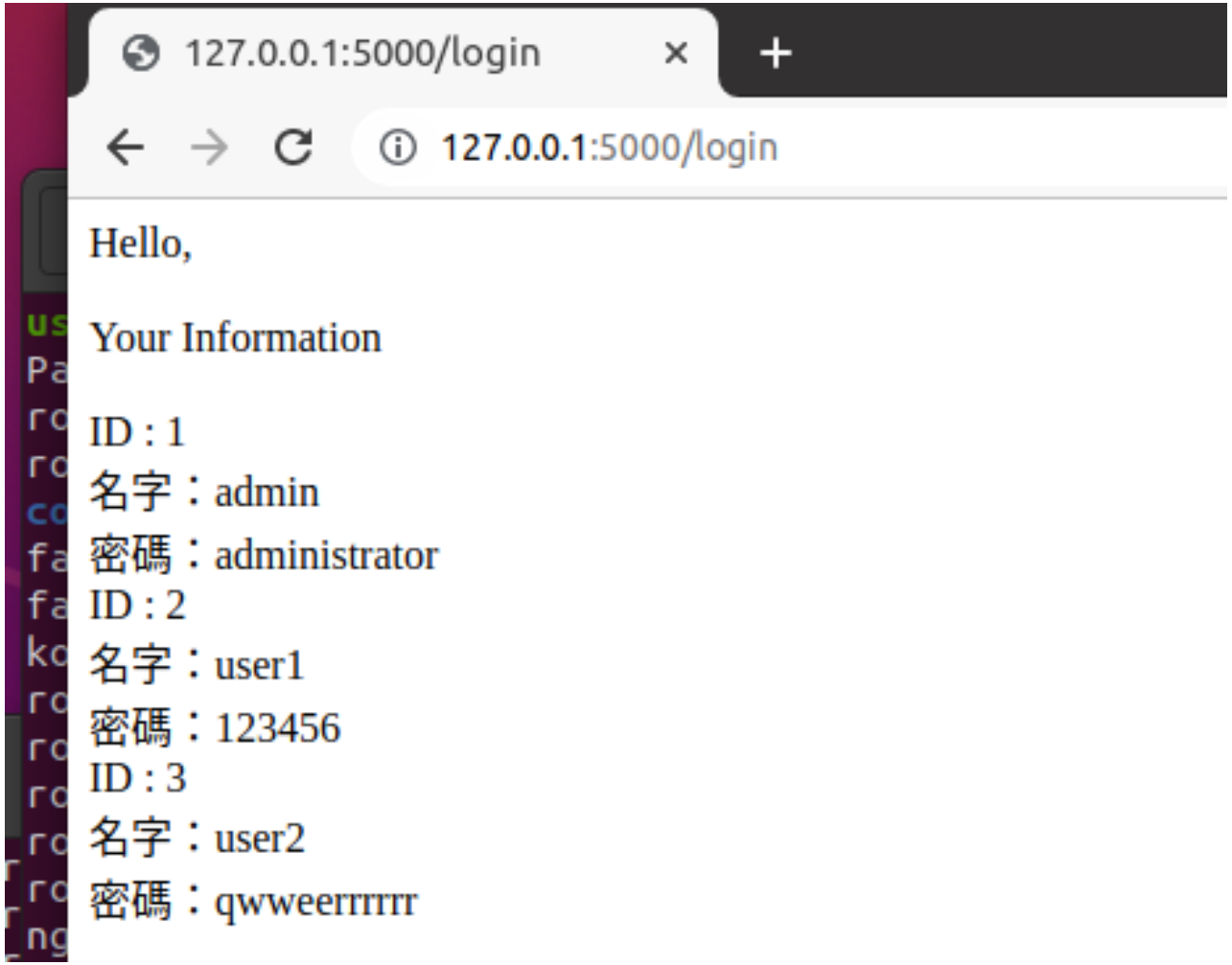
Sql injection 1-1

未啟用 modescurity



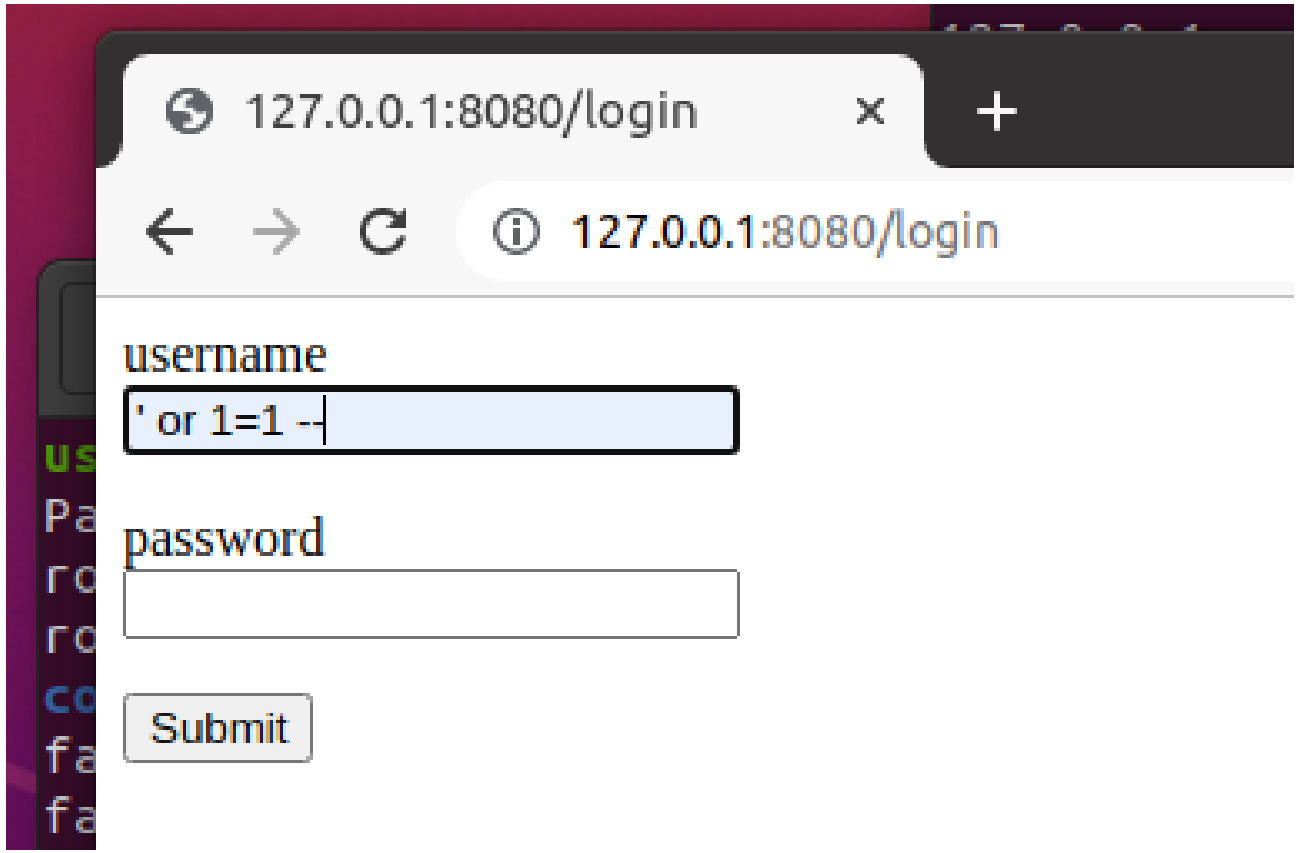
Sql injection 1-2

未啟用 modescurity



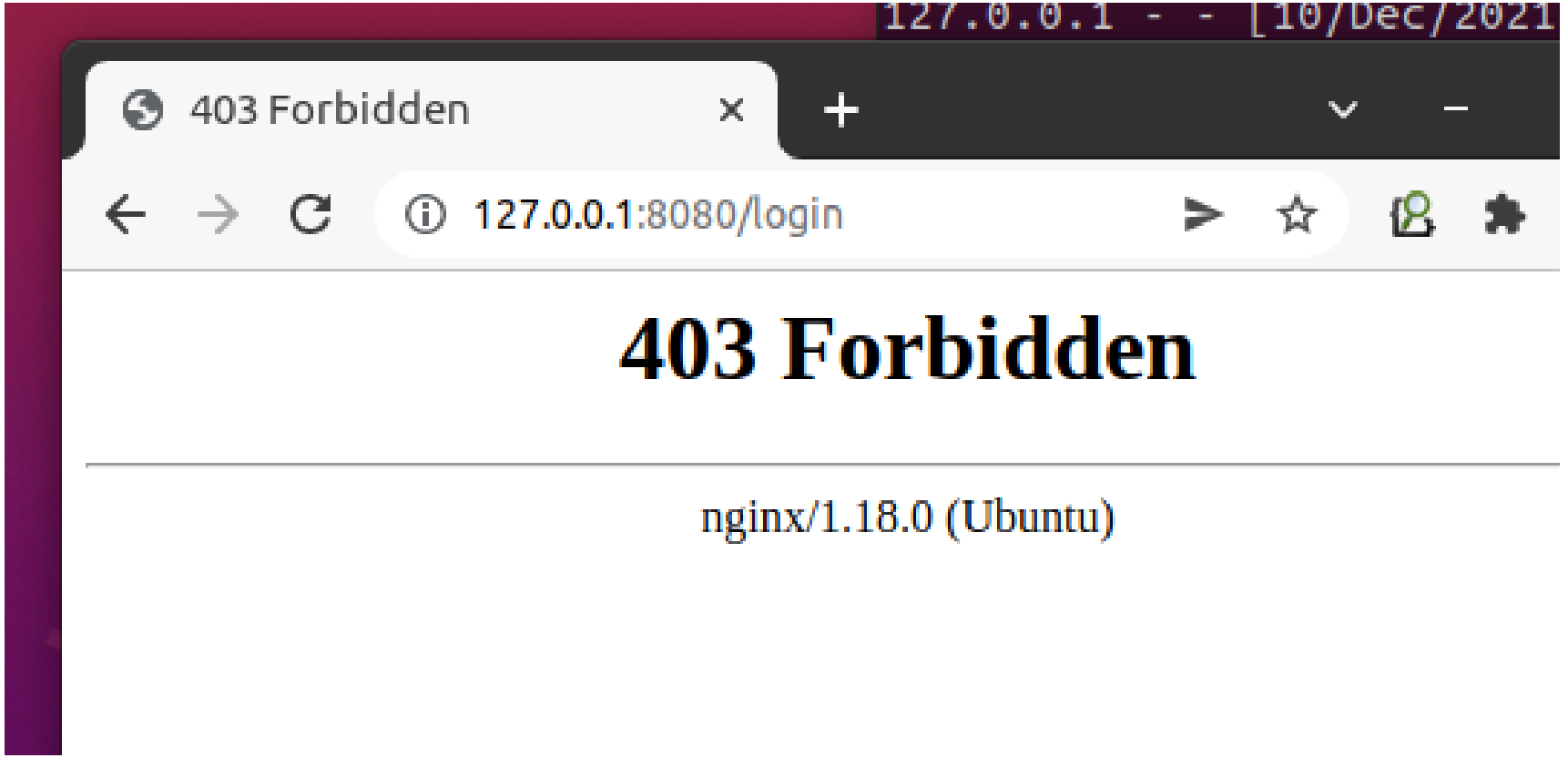
Sql injection 1-3

啟用 modescurity



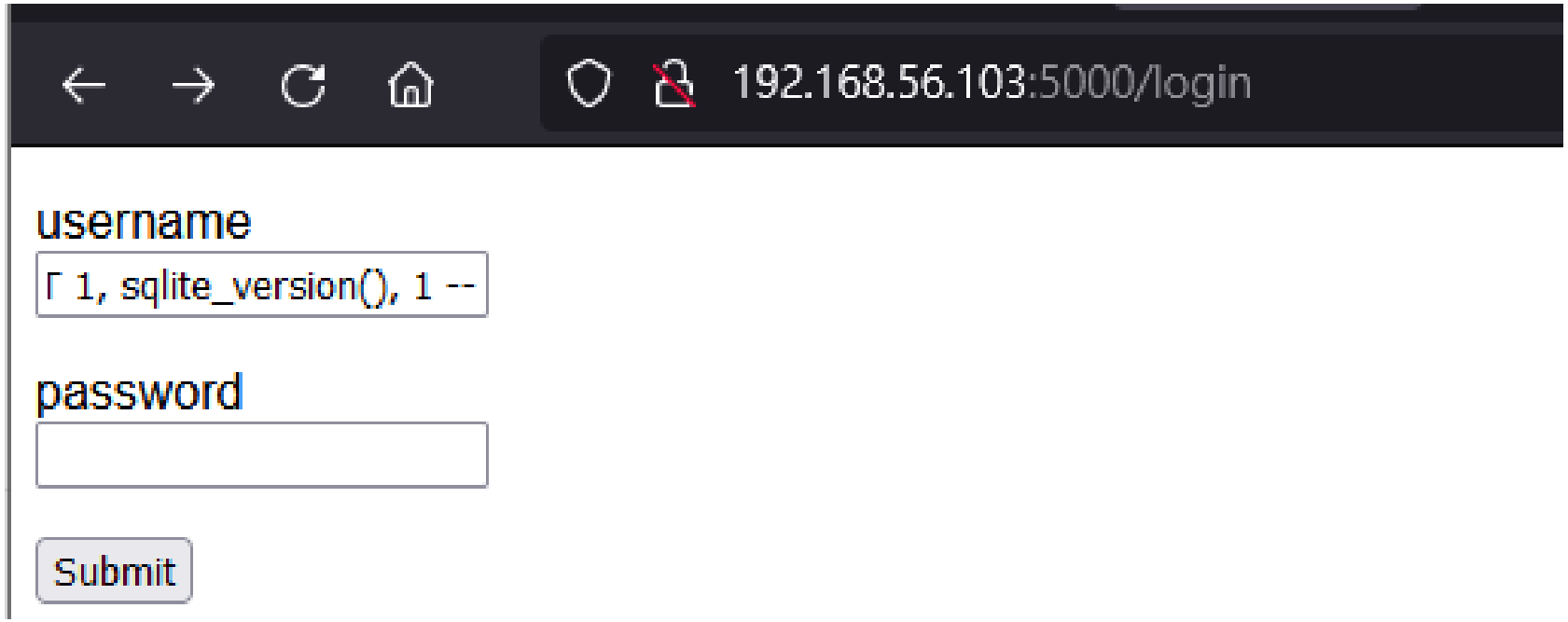
Sql injection 1-4

啟用 modescurity



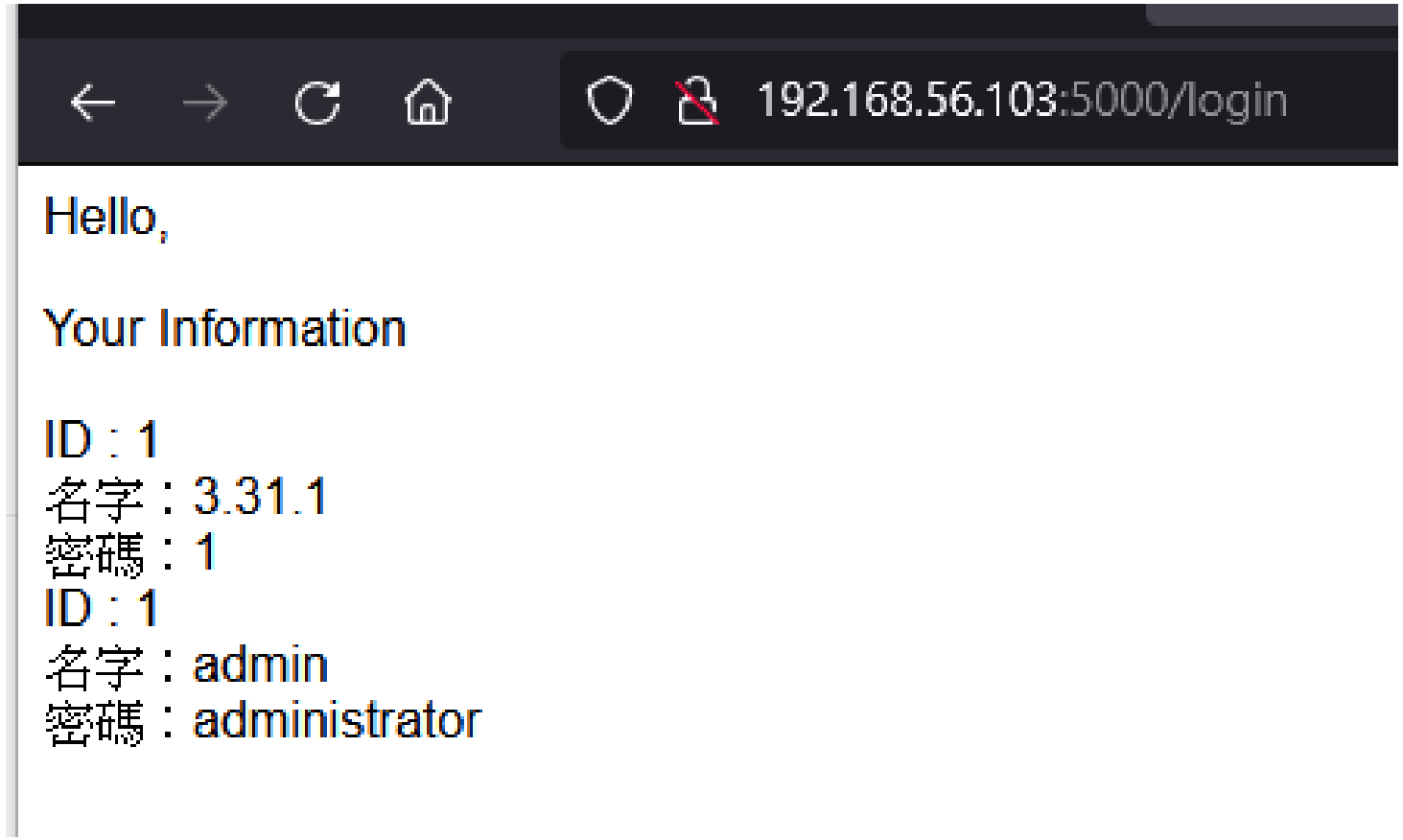
Sql injection 2-1

- 未啟用 modescurity
- 找尋sql版本
- admin' UNION SELECT 1, sqlite_version(), 1 --



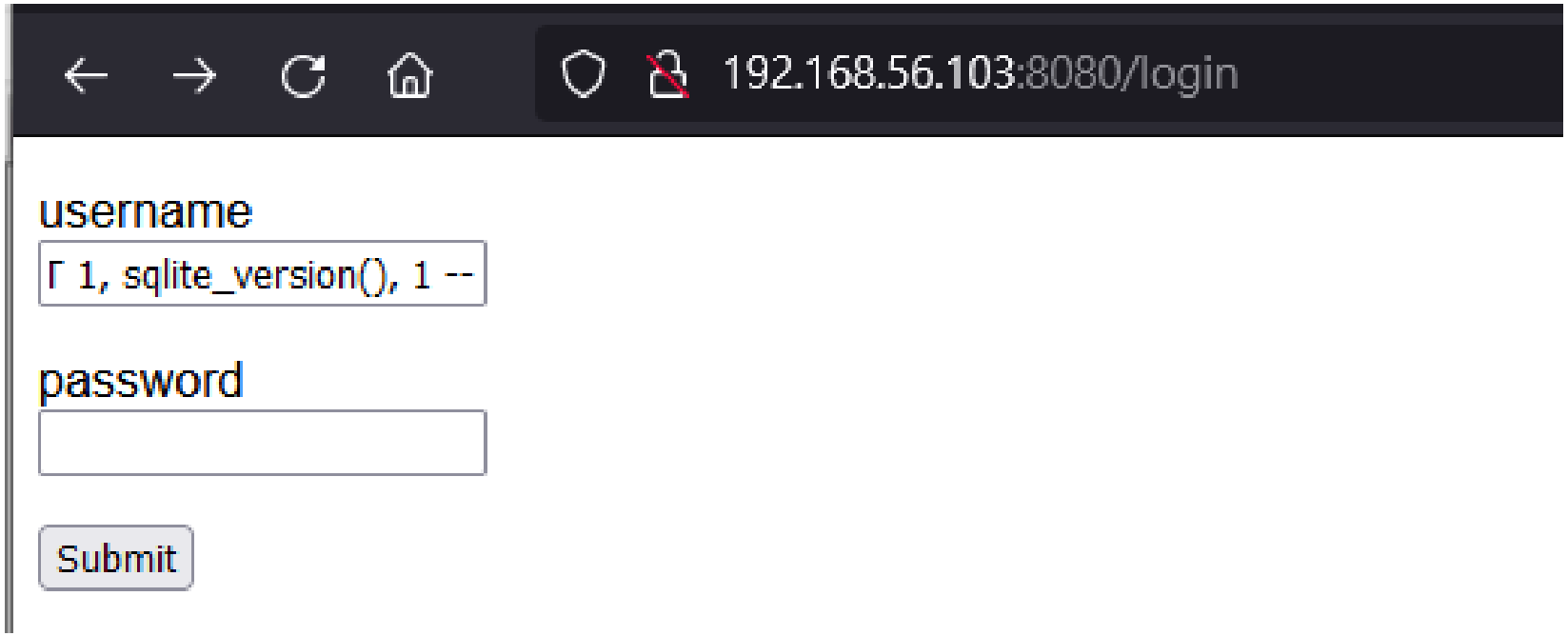
Sql injection 2-2

未啟用 modescurity



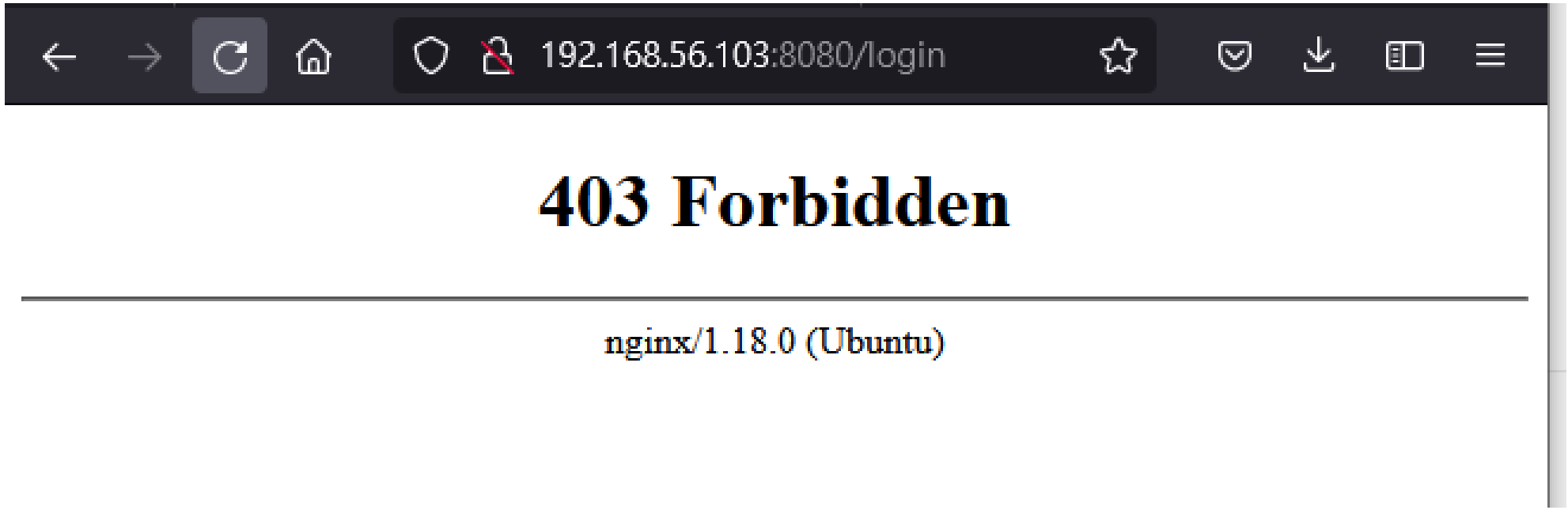
Sql injection 2-3

- 啟用 modescurity
- 找尋sql版本
- admin' UNION SELECT 1, sqlite_version(), 1 --



Sql injection 2-4

啟用 modescurity



WAF log

```
---PR6tTVuP---A--
[10/Dec/2021:12:47:35 +0800] 1639111655 192.168.56.1 3491 192.168.56.103 8080
---PR6tTVuP---B--
POST /login HTTP/1.1
Host: 192.168.56.103:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3
Content-Length: 74
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Origin: http://192.168.56.103:8080
Referer: http://192.168.56.103:8080/login
Connection: keep-alive
Upgrade-Insecure-Requests: 1

---PR6tTVuP---D--

---PR6tTVuP---E--
<html>\x0d\x0a<head><title>403 Forbidden</title></head>\x0d\x0a<body>\x0d\x0a<center><h1>403
Forbidden</h1></center>\x0d\x0a<hr><center>nginx/1.18.0 (Ubuntu)</center>\x0d\x0a</body>\x0d\x0a</html>\x0d\x0a

---PR6tTVuP---F--
HTTP/1.1 403
Server: nginx/1.18.0
Date: Fri, 10 Dec 2021 04:47:35 GMT
Content-Length: 162
Content-Type: text/html
Connection: keep-alive
```

WAF log

```
---PR6tTVuP---H--
ModSecurity: Warning. Matched "Operator `Rx' with parameter `(?:^([\d.]+|\[[\da-f:]+\]|[\da-f:]+)(:[\d]+)?$)' against
variable `REQUEST_HEADERS:Host' (Value: `192.168.56.103:8080' ) [file
"/usr/local/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "760"] [id "920350"] [rev ""] [msg
"Host header is a numeric IP address"] [data "192.168.56.103:8080"] [severity "4"] [ver "OWASP_CRS/3.4.0-dev"]
[maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag
"attack-protocol"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/210/272"] [tag "PCI/6.5.10"] [hostname
"192.168.56.103"] [uri "/login"] [unique_id "1639111655"] [ref "o0,19o0,14o14,5v27,19"]
ModSecurity: Warning. detected SQLi using libinjection. [file
"/usr/local/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "46"] [id "942100"] [rev ""] [msg
""] [data ""] [severity "0"] [ver "OWASP_CRS/3.4.0-dev"] [maturity "0"] [accuracy "0"] [hostname "192.168.56.103"]
[uri "/login"] [unique_id "1639111655"] [ref "y522,45"]
ModSecurity: Warning. Matched "Operator `Rx' with parameter
`(?i)(?:\b(?:(?:c(?:onnection_id|urrent_user)|database)\s*?\([^\)]*?|u(?:nion(?:[\w(\s]*?select| select
@)|ser\s*?\([^\)]*?)|s(?:chema\s*?\([^\)]*?|elect.*?\w?user\()|into[\s+]+(?:dump|out)file\s*?[\"' (201 characters
omitted)' against variable `ARGS:username' (Value: `admin' UNION SELECT 1, sqlite_version(), 1 --' ) [file
"/usr/local/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "173"] [id "942190"] [rev ""] [msg
"Detects MSSQL code execution and information gathering attempts"] [data "Matched Data: ' UNION SELECT 1 found within
ARGS:username: admin' UNION SELECT 1, sqlite_version(), 1 "] [severity "2"] [ver "OWASP_CRS/3.4.0-dev"] [maturity
"0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag
"paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/248/66"] [tag "PCI/6.5.2"] [hostname "192.168.56.103"]
[uri "/login"] [unique_id "1639111655"] [ref "o5,16v522,45t:urlDecodeUni,t:removeCommentsChar"]
ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Ge' with parameter `5' against variable
`TX:ANOMALY_SCORE' (Value: `13' ) [file "/usr/local/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"]
[line "139"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Score: 13)"] [data ""] [severity "2"]
[ver "OWASP_CRS/3.4.0-dev"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag
"platform-multi"] [tag "attack-generic"] [hostname "192.168.56.103"] [uri "/login"] [unique_id "1639111655"] [ref ""]
```

WAF log

```
1 ModSecurity: Warning. Matched "Operator `Rx' with parameter
  `(?i)(?:\b(?:(?:c(?:onnection_id|urrent_user)|database)\s*?\([^\)]*?|u(?:nion(?:[\w(\s]*?select| select
  @)|ser\s*?\([^\)]*?)|s(?:chema\s*?\([^\)]*?|elect.*?\w?user\()|into[\s+]+(?:dump|out)file\s*?[\"' (201 characters
  omitted)' against variable `ARGS:username' (Value: `admin' UNION SELECT 1, sqlite_version(), 1 --' ) [file
  "/usr/local/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "173"] [id "942190"] [rev ""] [msg
  "Detects MSSQL code execution and information gathering attempts"] [data "Matched Data: ' UNION SELECT 1 found within
  ARGS:username: admin' UNION SELECT 1, sqlite_version(), 1 "] [severity "2"] [ver "OWASP_CRS/3.4.0-dev"] [maturity
  "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag
  "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/248/66"] [tag "PCI/6.5.2"] [hostname "192.168.56.103"]
  [uri "/login"] [unique_id "1639111655"] [ref "o5,16v522,45t:urlDecodeUni,t:removeCommentsChar"]
```

防護 Sql injection

- 使用 Parameterized Query (or Parameterized Statement)
  - (X) SELECT * FROM user WHERE username='{username}' and password='{password}'
  - (O) SELECT * FROM user WHERE username=:username and password=:password
- 使用 ORM (Object-Relational Mapping) 套件
  - user.query.filter_by(username= ' {username} ', password= ' {password} ').first()
- 使用 WAF
  - 商用 WAF (F5, Citrix, FortiWeb…etc)
  - ModSecurity

漏洞與更新

OWASP ModSecurity Core Rule Set
THE 1ST LINE OF DEFENSE

Home Blog Videos Installation FAQ Support Donate Sponsors Documentation

CVE-2021-35368 – CRS Request Body Bypass (Update)

By **Christian Folini** / June 30, 2021

There is a severe security issue in our rule set. It has been present since the release of CRS 3.1.0 and was recently brought to our attention.

Here is the official advisory that we are also publishing as CVE-2021-35368 via MITRE (as usual, MITRE will take a few days until they publish this).

Offical Advisory for CVE-2021-35368

30 Jun 2021
lifeforms
v3.3.2
18703f1
Compare

v3.3.2 Latest

This is the OWASP ModSecurity Core Rule Set version 3.3.2

▾ Assets 4

- coreruleset-3.3.2.tar.gz.asc
- coreruleset-3.3.2.zip.asc
- Source code (zip)
- Source code (tar.gz)

2 2 people reacted

https://owasp.org/www-project-modsecurity-core-rule-set/

Reference

- https://news.netcraft.com/archives/category/web-server-survey/
- https://serverguy.com/comparison/apache-vs-nginx/
- http://nginx.org/en/docs/http/ngx_http_auth_request_module.html
- https://www.nginx.com/blog/compiling-and-installing-modsecurity-for-open-source-nginx/
- https://coreruleset.org/installation/