Web 安全經驗與案例分享

Speaker: Keniver

$ whoami

王凱慶 Keniver Wang

經歷:

- 中華電信
- 中華資安國際

專長:

- Web/Network/Cloud Security
- Python/PHP

Mail: hi@kaiching.wang

CTF Team: Forx/418/NPC

#興趣使然的資安研究人員 #CTFer

Outline

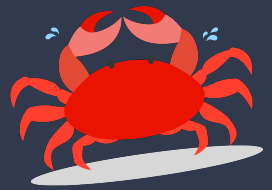
1. 資訊搜集
2. OWASP Top 10
3. 經驗與案例分享

FBI WARNING

Federal Law provides severe civil and criminal penalties for the unauthorized reproduction, distribution, or exhibition of copyrighted motion pictures (Title 17, United States Code, Sections 501 and 508). The Federal Bureau of Investigation investigates allegations of criminal copyright infringement (Title 17, United States Code, Section 506).

本次內容不錄影
你什麼都沒看到

簡報課程後釋出
有些東西會被和諧



在開始之前

- 進行任何行為前，請確保您有獲得授權
- 不小心撿到野生的資料請回報相關廠商
  - (e.g. Hitcon ZeroDay)

~~也可以傳一份給我~~

資訊蒐集

資訊蒐集 - IP 與 Domain

- Domain/IP
- 系統資訊
- 頁面資訊

資訊蒐集 - IP 與 Domain

- IP 列舉
  - 掃描雲服務廠商所有 IP
  - DNS 是個好方向
- 網域列舉
  - 搜尋引擎
  - Crt.sh
  - PassiveDNS
  - dnsdumpster.com
  - Censys, Shodan, Zoomeyes...
  - 暴力破解
  - CSP

資訊蒐集 - IP 與 Domain

- IP 列舉
  - Amazon Web Service
    - https://ip-ranges.amazonaws.com/ip-ranges.json
  - Google Cloud Platform
    - https://cloud.google.com/compute/docs/faq#where_can_i_find_product_name_short_ip_ranges
  - Microsoft Azure
    - https://www.microsoft.com/en-us/download/details.aspx?id=41653

資訊蒐集 - IP 與 Domain

- IP 列舉
  - 掃描雲服務廠商所有 IP **很慢**
  - DNS 是個好方向
- 網域列舉
  - 搜尋引擎
  - Crt.sh
  - PassiveDNS
  - dnsdumpster.com
  - Censys, Shodan, Zoomeyes...
  - 暴力破解
  - CSP

資訊蒐集 - IP 與 Domain

- 網域列舉
  - 搜尋引擎
    - Google
    - Bing
    - Yahoo
    - 百度
    - Yandex

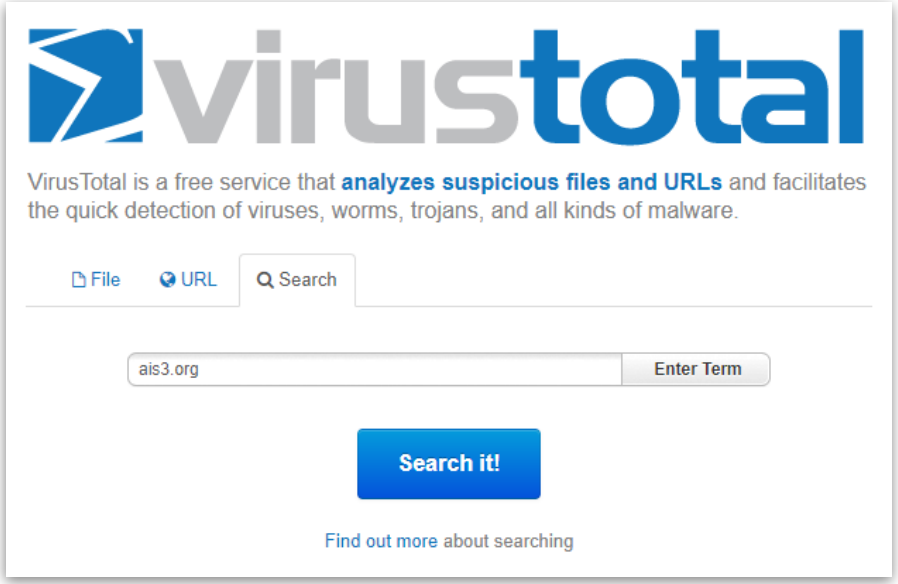
OSINT Resource: https://github.com/jivoi/awesome-osint

資訊蒐集 - IP 與 Domain

- 網域列舉
  - Crt.sh
    - 證書透明度查詢系統
    - 僅有效憑證資訊可供查詢

資訊蒐集 - IP 與 Domain

- 網域列舉
  - PassiveDNS
    - 記錄曾經解析過的網域
    - 分析網域過往行為

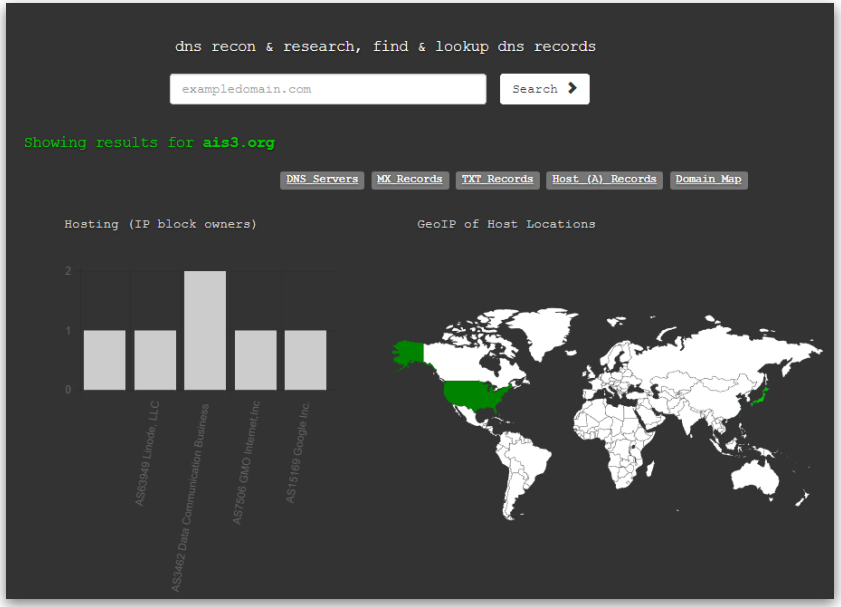


資訊蒐集 - IP 與 Domain

- 網域列舉
  - DNSTable
    - https://dnstable.com/
  - SecurityTrails
    - https://securitytrails.com/dns-trails

資訊蒐集 - IP 與 Domain

- 網域列舉
  - dnsdumpster.com
    - DNS 資訊關聯圖繪製工具
    - 協助分析 DNS 記錄

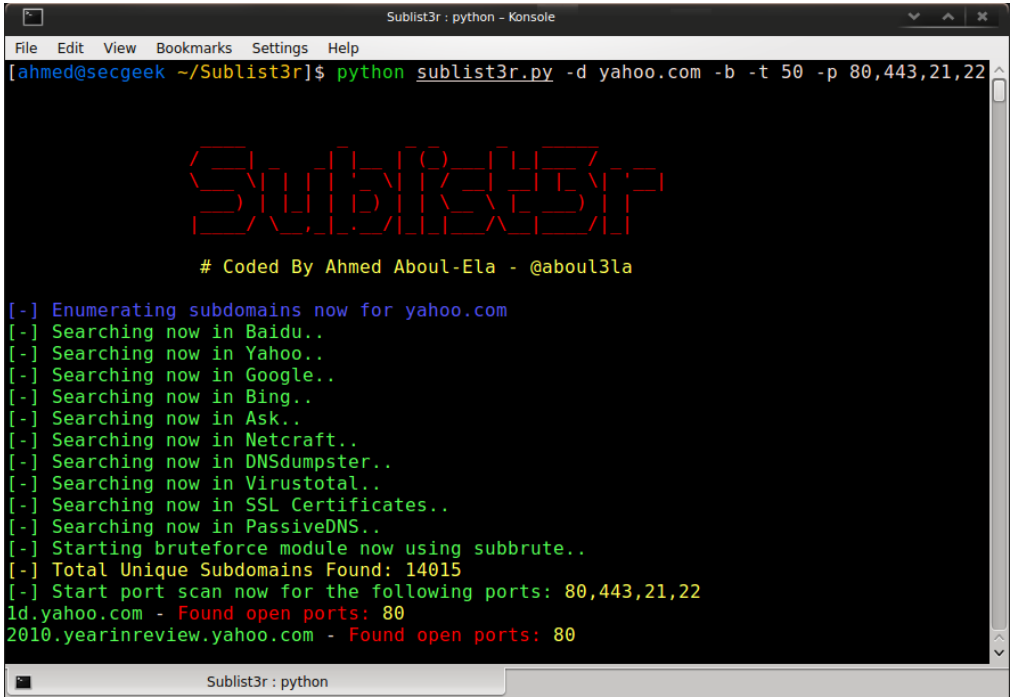


資訊蒐集 - IP 與 Domain

- 網域列舉
  - Censys, Shodan, Zoomeyes…
    - 紀錄網路空間的主機資訊

資訊蒐集 - IP 與 Domain

- 網域列舉
  - 暴力破解
    - 一本好的字典
    - Sublist3r
    - OpenDoor



資訊蒐集 - IP 與 Domain

- 網域列舉
  - CSP (Content Security Policy)
    - CSP 用於指定網站資源的有效域，用於強化 XSS 攻擊的抵抗能力

```
<meta http-equiv="Content-Security-Policy" content="default-src 'self';
img-src https://img.ais3.org; child-src 'none';">
```

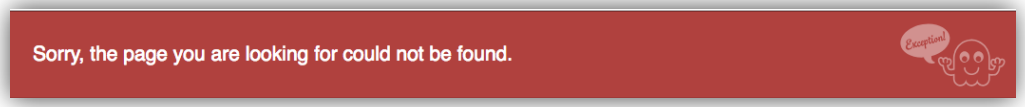
資訊蒐集 - 系統資訊

- 觀察HTTP 資訊
  - Header
  - Cookie

資訊蒐集 - 系統資訊

- 錯誤訊息特徵
  - HTTP 403/404
  - HTTP 500

資訊蒐集 - 系統資訊


Sorry, the page you are looking for could not be found.
Exception!


A Database Error Occurred
Error Number: 1064
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'LEFT JOIN SELECT room_number FROM new_reservation WHERE star' at line 6
SELECT room_number FROM rooms WHERE room_type = 'Econ_25000' ORDER BY room_number ASC LEFT JOIN SELECT room_number FROM new_reservation WHERE start_date >= '2013-07-16' AND end_date <= '2013-07-18' ORDER BY room_number ASC
Filename: C:\xampp\htdocs\bit\system\database\DB_driver.php
Line Number: 330

資訊蒐集 - 系統資訊

- 考古？
  - https://zeroday.hitcon.org/

資訊蒐集 - 系統資訊

- 自動識別工具
  - Wappalyzer

資訊蒐集 - 特徵辨識

- 測試檔案結構
  - Wordpress
    - /wp-content/
  - Codeigniter
    - https://codeigniter.org.tw/system
    - https://codeigniter.org.tw/application
  - 還有 ...

資訊蒐集 - 頁面調查

- 目錄爆破
  - dirb
  - OpenDoor
- 回跳

資訊蒐集 - 頁面調查

看 Code!!!!!!!!

OWASP Top 10

OWASP

1 2001年成立至今

開放Web應用程式安全計畫（OWASP，Open Web Application Security Project）是一個組織，它提供有關電腦和互聯網應用程式的公正、實際、有成本效益的資訊。其目的是協助個人、企業和機構來發現和使用可信賴軟體。

2 公開非營利組織

OWASP是一個開放社群、非營利性組織，全球目前有130個分會近萬名會員，其主要目標是研議協助解決Web軟體安全之標準、工具與技術文件，長期致力於協助政府或企業了解並改善網頁應用程式與網頁服務的安全性。

3 致力於推動網路安全

美國聯邦貿易委員會（FTC）強烈建議所有企業務必遵循OWASP所發佈的十大網路弱點防護守則，美國國防部亦將此守則列為最佳實務，就連國際信用卡資料安全技術PCI標準更將其列為必要元件。

4 旗下有多項相關計畫

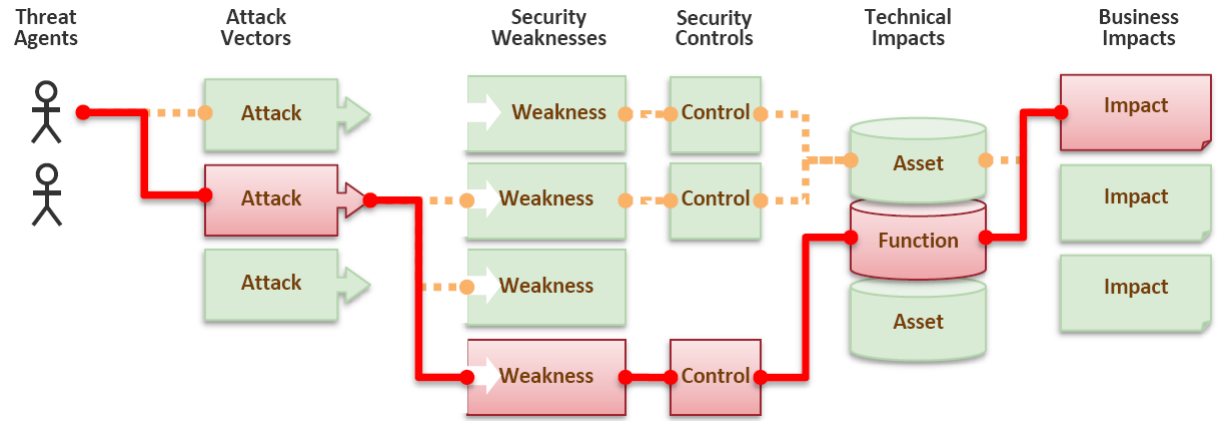
目前OWASP有30多個進行中的計畫，包括最知名的OWASP Top 10（OWASP十大網路應用系統安全弱點）、WebGoat（代罪羔羊）練習平台、安全函式庫（ESAPI）等計畫，針對不同的軟體安全問題進行討論與研究。

OWASP


系統分級
需求
設計
實作
測試
部署與維運
Top 10 risks
Application Security Verification Standard
Enterprise Security API
Developer Guide
Code Review Guide
Testing Guide
Dependency check
Appsensor
Modsecurity

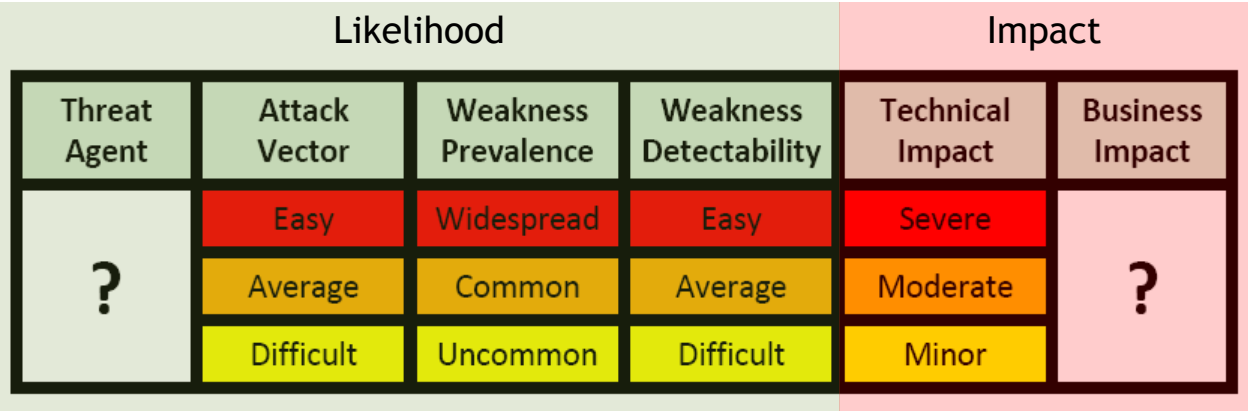
OWASP Risk Rating Methodology

- 威脅對系統進行攻擊。
- 若系統存在有弱點，則攻擊成功並藉此控制系統。
- 技術上可對系統造成影響，進而對組織利益造成影響。



OWASP Risk Rating Methodology

- Risk = Likelihood * Impact (機率 * 影響)。
- 機率：攻擊難度、弱點常見率、弱點被發現率。
- 影響：考量弱點對機密性、一致性、可用性、可歸責性等造成的影響。



OWASP TOP 10
Application Security Risks 2017

A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)-New
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization-New
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging&Monitoring-New

OWASP TOP 10
Application Security Risks 2017

2017 年 OWASP 十大 Web 弱點			
A1	注入攻擊 Injection	A6	不安全的的組態設定 Security Misconfiguration
A2	無效的身分認證 Broken Authentication	A7	跨網站腳本攻擊 Cross-Site Scripting (XSS)
A3	機敏資料外洩 Sensitive Data Exposure	A8	不安全的反序列化漏洞 Insecure Deserialization

2017 年 OWASP 十大 Web 弱點			
A4	XML 外部處理器漏洞 XML External Entities (XXE)	A9	使用已知漏洞元件 Using Components with Known Vulnerabilities
A5	無效的存取控管 Broken Access Control	A10	紀錄與監控不足風險 Insufficient Logging&Monitoring

資料來源：OWASP(http://www.owasp.org.tw/)

A1-Injection

新　聞
新 聞 專 題
即 時 新 聞
新 聞 簡 訊
技　術
產 品 報 導
技 術 專 題
IT 書 訊
IT管理
CIO
IT 人 物
專 欄
新聞總覽
業界動態

訂 閱 電 子 報
iThome Online提供免費電

Mass SQL Injection來襲，百萬網址受駭

文/黃彥棻 (記者) 2011-04-19

Like 118　Share　+1 0　我要收藏

資安公司Wensense發布資安報告顯示，LizaMoon惡意連結植入全球超過百萬個網址，臺灣受駭網址也從原本千個暴增為6萬多個，名列全球受害第7名

資安廠商Websense在3月29日於該公司部落格發布一則資安通報，有一個名為LizaMoon.com的惡意網址，透過SQL Injection手法被植入許多網站中。根據Websense持續更新的資安報告，透過Google查詢被植入該惡意連結的網址數量，從原本的2萬8千多個，暴增為全球受害遭植入該惡意連結的網址數量超過百萬個的Mass SQL Injection攻擊。

根據統計，臺灣此次在全球受駭國家排名中，名列亞洲第2名、全球第7名；從Google查詢臺灣受感染的網址數量，也從原本的1千個暴增到6萬3千個。

研討會訊息
- 《IBM x VMware 智慧虛擬化論壇》
- 資安零死角為您打造最完善的資安環境
- 加密自動化 保障機密資料生命週期無憂慮
- Big Data , Big Power , Big Opportunity

+更多研討會

▼ ADVERTISEMENT ▼

保障機密資料
生命週期無憂慮 研討會

檔案生成時即由系統自動加密，確保資料從生成到廢止都受到充分的保護，進而保障機密文件內容的安全性

A1-Injection

- **Prepare Statements**
  - $ps = $db->prepareStatement("SELECT * FROM NEWS WHERE id = :id")
  - $ps->bindParam("id", $id);
  - $ps->execute();

正確

  - $ps = $db->prepareStatement(“SELECT * FROM NEWS WHERE id = ” + $id)
  - $ps->execute();

錯誤

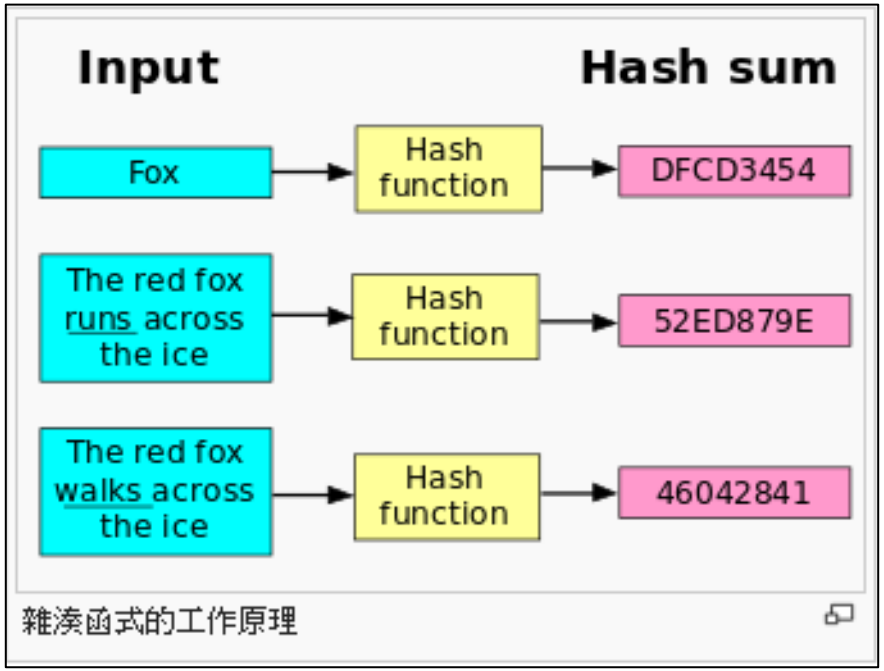
A2-Broken Authentication and Session Management

- 驗證碼繞過
- 登入/登出 Session ID 未更新或失效
- 暴力破解

A3-Sensitive Data Exposure

- Google Hacking 到機敏資訊
- 目錄列舉看到其他人上傳的資料
- 資料庫密碼明文儲存 (未使用 Hash 與 salt)

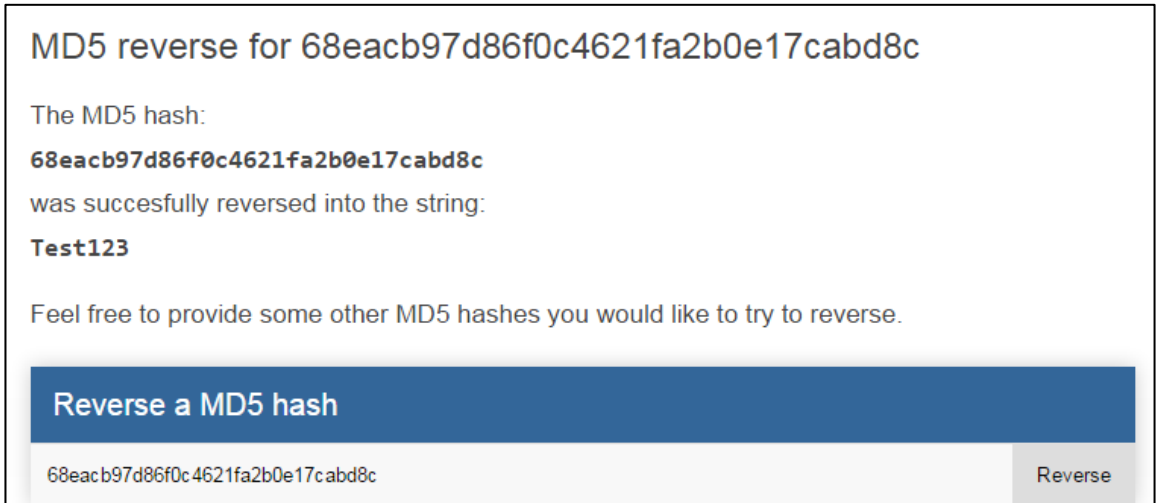
Hash



雜湊函式的工作原理

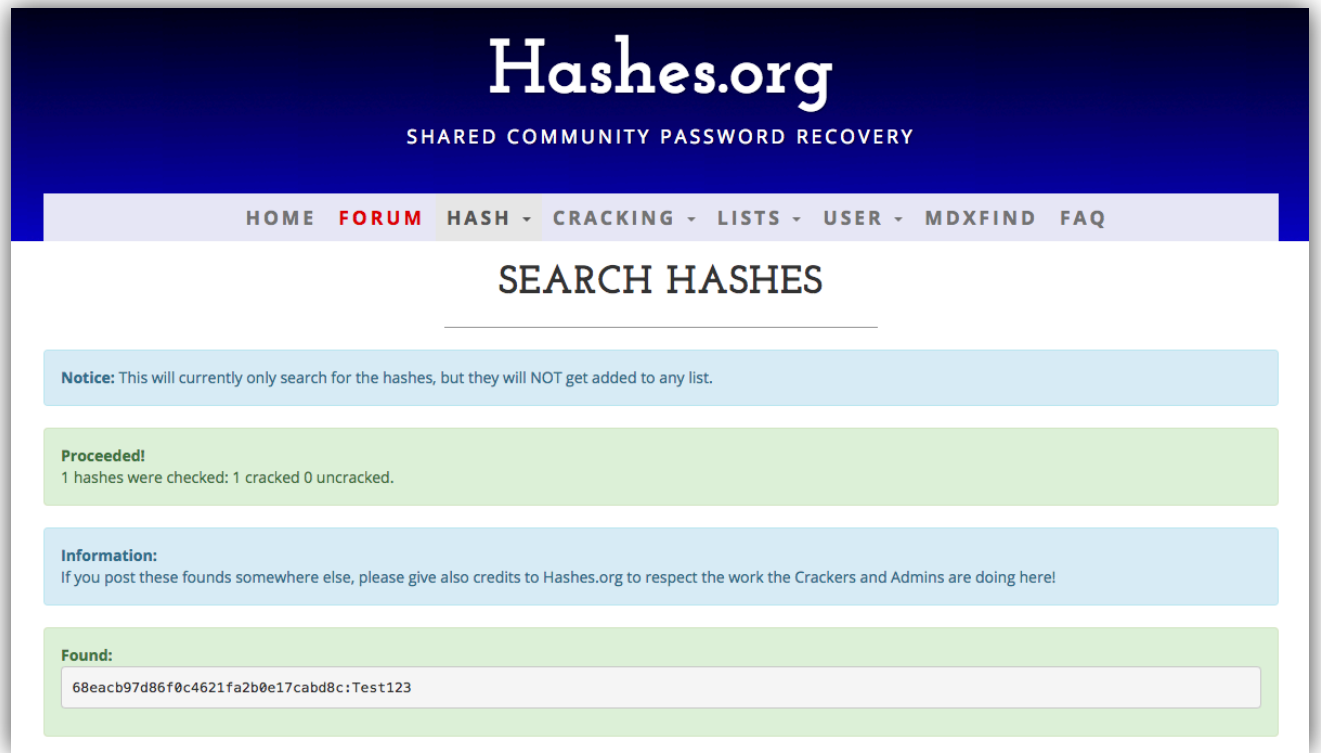
Hash

Test123 ➔ 68EACB97D86F0C4621FA2B0E17CABD8C
Test1234 ➔ 2C9341CA4CF3D87B9E4EB905D6A3EC45
Test12345➔ 662AF1CD1976F09A9F8CECC868CCC0A2



Hash - 查詢服務: CMD5

Hash - 查詢服務: Hashes.org



Hash - 破解工具

- 字典檔案
  - rockyou

- HashCat 客製化破解服務
  - Mask-1: ?l?u
  - Mask: ?1?d?d?d?d?d?d?d?d?d?d

  - 密碼變形

Hash - 施鹽

- test + aksuw285
  - 原始長度: 4
  - 加鹽長度: 12

- 7777777 + kj3485jkfv
  - 原始長度: 7
  - 加鹽長度: 17

A3-Sensitive Data Exposure

- .git
  - .git/config
  - 調查作者
  - 調查遠端資源

```
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
        precomposeunicode = true
[remote "origin"]
        url = https://github.com/sensepost/reGeorg.git
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "master"]
        remote = origin
        merge = refs/heads/master
```

A4-XXE

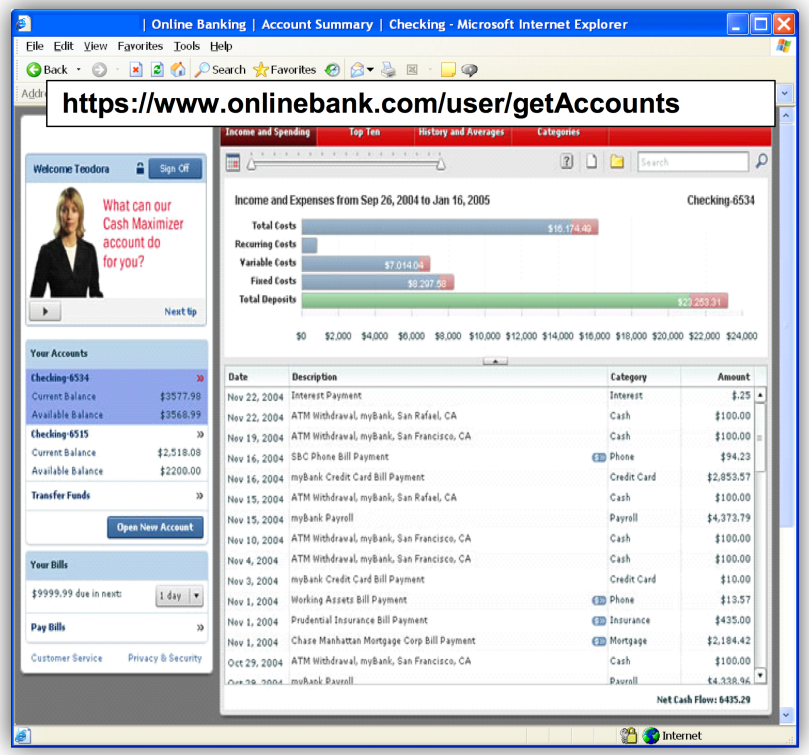
A4-XXE

- 時常出沒於
  - WebService (WSDL)
  - JSP
  - 政府機關
  - SAML (SSO)

- 特殊狀況
  - A4 + A8
  - 導致 XXE 被重新啟動

A5-Broken Access Control

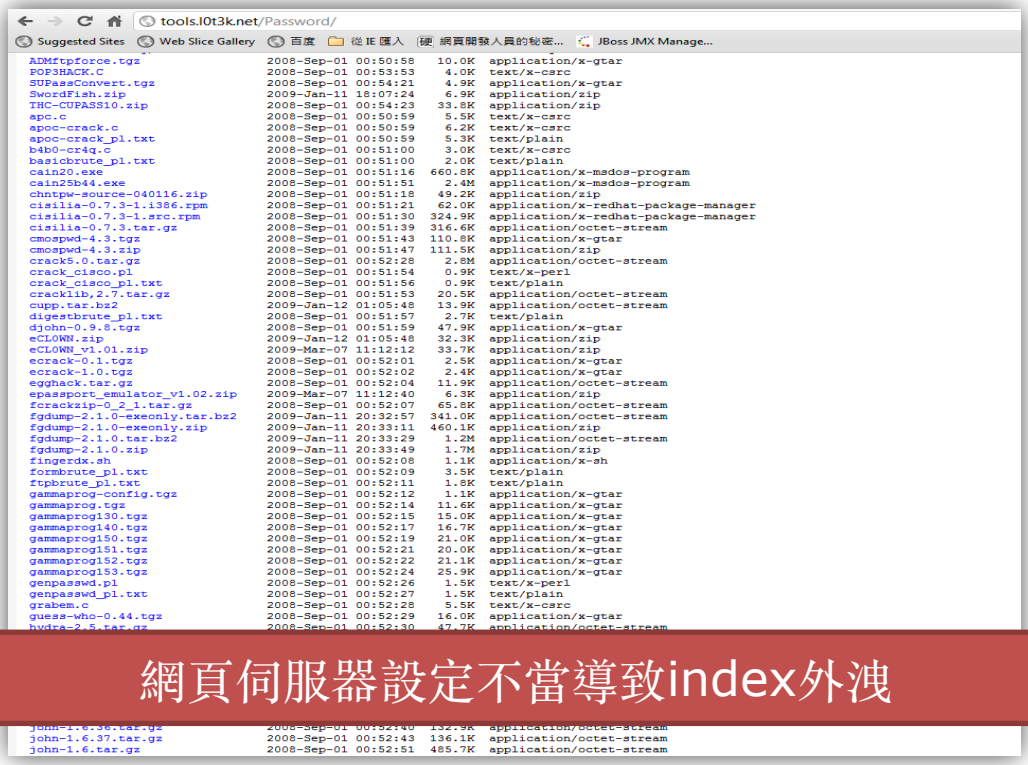
- 攻擊者 注意到 URL 指出他的角色
  - /user/getAccounts
- 試圖修改角色 (role)
  - /admin/getAccounts
  - /manager/getAccounts
- 猜測可能存在路徑
  - /sz1199/sz1199_list.jsp (原始連結)
  - /sz1199/sz1199_update.jsp (推測)
-



A5-Broken Access Control

人員角色/ 系統功能	案件新增	案件處理	案件管理	員工管理	項目管理	統計報表	FAQ
系統管理者	●	●	●	●	●	●	●
客服主管	●	●	●			●	●
機關受理窗口	●						●
客服人員		●	●				●
無權限的使用者	●			●			

A6-Security Misconfiguration



網頁伺服器設定不當導致index外洩

A7-XSS

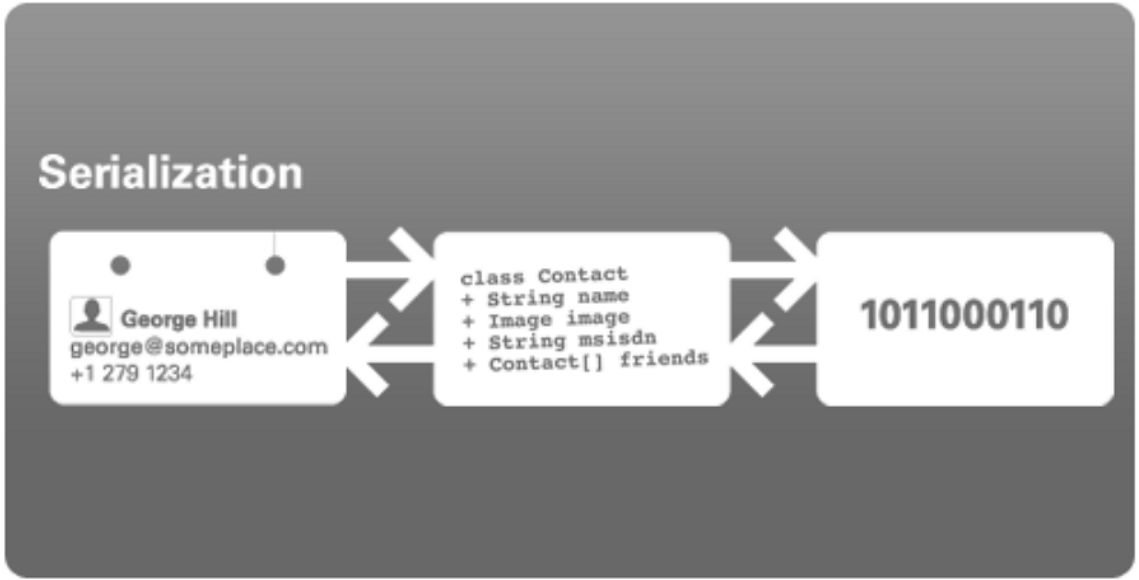
- 相信大家都很會，看個 XSS 的例子吧

A8-Insecure Deserialization

- 什麼是「序列化」和反序列化
  - 將物件轉化為可儲存的資料型態
  - 將資料重新轉化為原來物件型態
  - 常見的程式語言皆有實做此功能

- 程式語言中使用序列化的方法
  - ASP.NET: ISerializable
  - PHP: serialize()
  - Java: java.io.Serializable
  - Python: pickle

A8-Insecure Deserialization

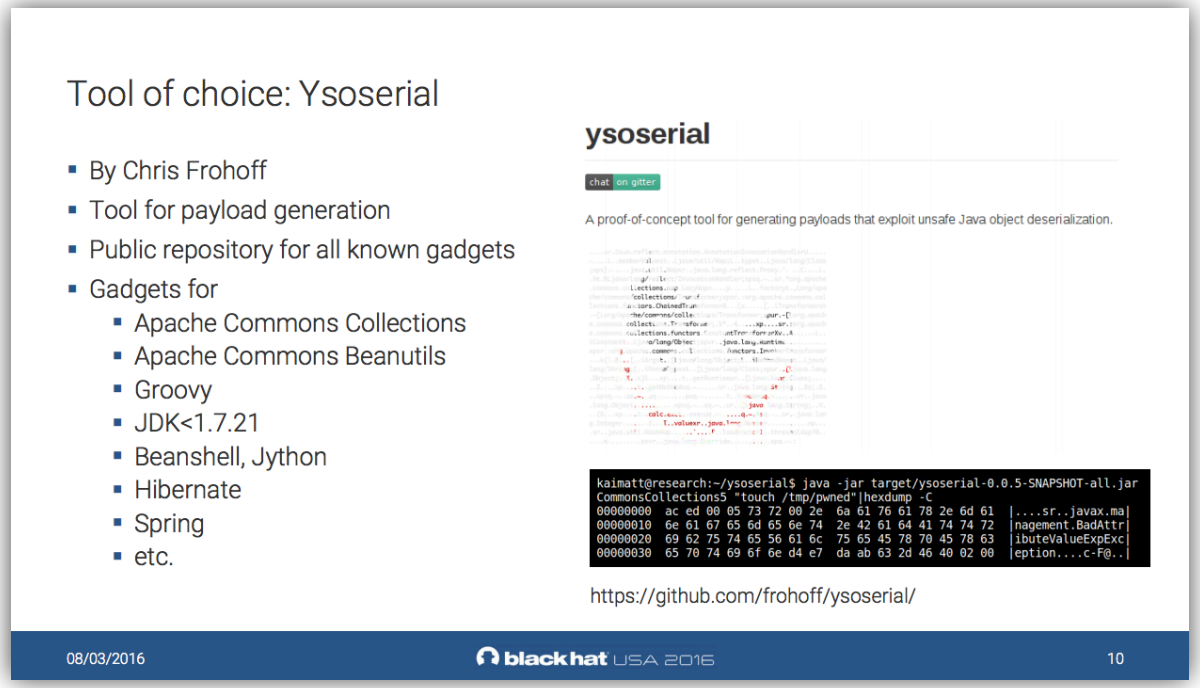


圖片來源：*http://ppt.cc/PHtAe*

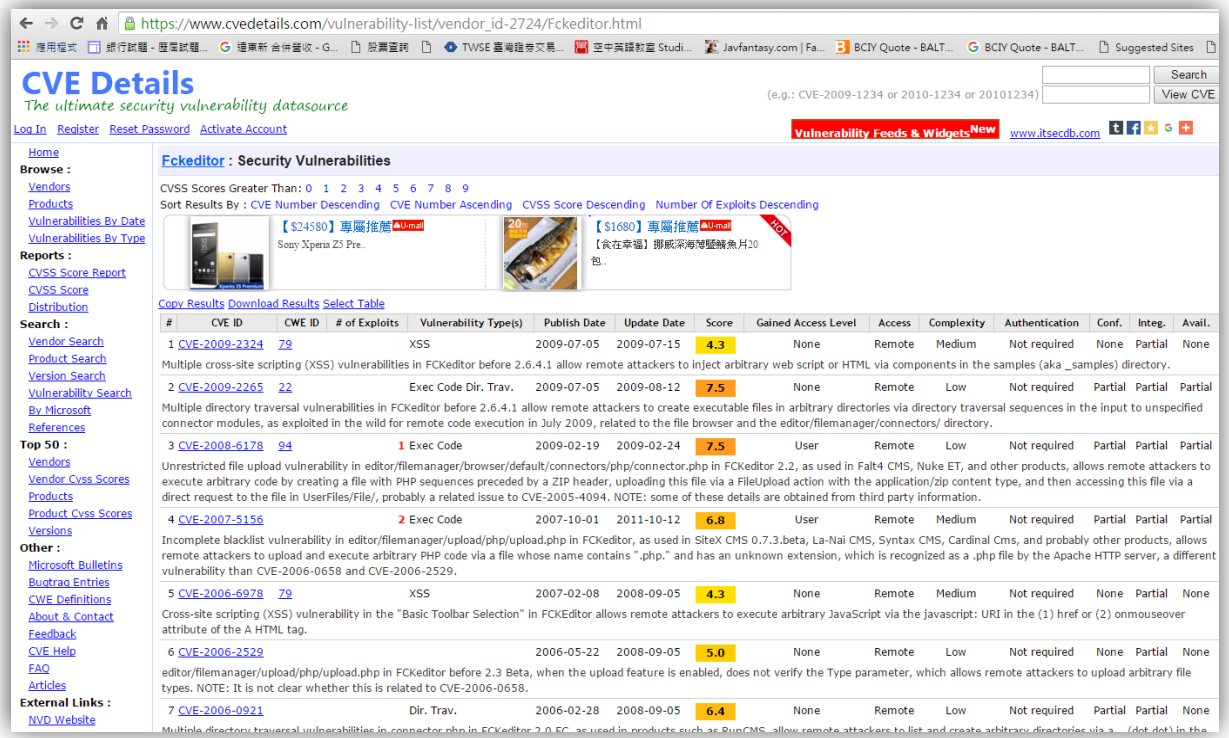
A8-Insecure Deserialization

A8-Insecure Deserialization

- 利用工具
  - ysoserial
- RPC 非常仰賴序列化
- 不是所有物件都可以序列化
  - 注意客製化



A9-Using Components with Known Vulnerabilities



A9-Using Components with Known Vulnerabilities

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(ms17_010_eternalblue) > show targets
    ...targets...
msf exploit(ms17_010_eternalblue) > set TARGET <target-id>
msf exploit(ms17_010_eternalblue) > show options
    ...show and set options...
msf exploit(ms17_010_eternalblue) > exploit
```

Related Vulnerabilities

- Microsoft CVE-2017-0143: Windows SMB Remote Code Execution Vulnerability
- Microsoft CVE-2017-0144: Windows SMB Remote Code Execution Vulnerability
- Microsoft CVE-2017-0145: Windows SMB Remote Code Execution Vulnerability
- Microsoft CVE-2017-0146: Windows SMB Remote Code Execution Vulnerability
- Microsoft CVE-2017-0147: Windows SMB Information Disclosure Vulnerability
- Microsoft CVE-2017-0148: Windows SMB Remote Code Execution Vulnerability

CVE-2016-5195 Like

Home Twitter Wiki Shop

DIRTY COW

Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel

View Exploit Details

供應鏈攻擊

供應鏈攻擊


iThome 新聞 產品&技術 專題 AI & 大數據 區塊鏈 Cloud DevOps GDPR 資安 研討會 社群 搜尋
新聞
軟體供應鏈攻擊再現! 熱門函式庫Event-Stream遭植入比特幣竊取程式
Event-Stream易手後，被發現植入了可竊取比特幣的惡意程式，會竊取比特幣錢包Copay內私鑰等機密訊息，並將錢包內的比特幣轉至駭客的帳號。
文/ 陳曉莉 | 2018-11-27 發表
按讚加入iThome粉絲團
圖片來源: 維基共享資源；作者：AntanaCoins
iThome Security
iThome 按讚追蹤 iThome 最新報導
熱門新聞
Chrome及Firefox都不想再支援用了超過40年的FTP
2018-11-27
研究：大多數ATM只要不到20分鐘就能攻陷
2018-11-26
印度銀行遭駭4億元，駭客不

A10-Insufficient Loggin&Monitoring

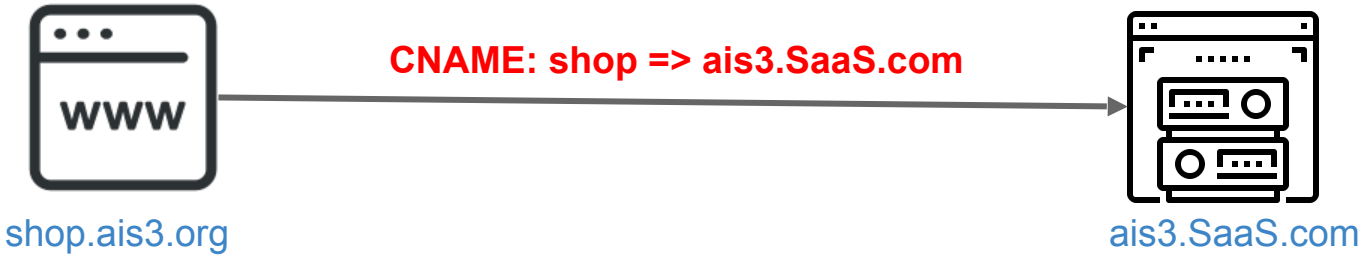
- 沒有適當的監視機制
- 沒有 Log 或者 沒有紀錄關鍵資訊
- Log 紀錄無效
  - 時間有誤
  - 紀錄資訊錯誤
  - 過多垃圾資訊

其他常見資安問題

網域劫持

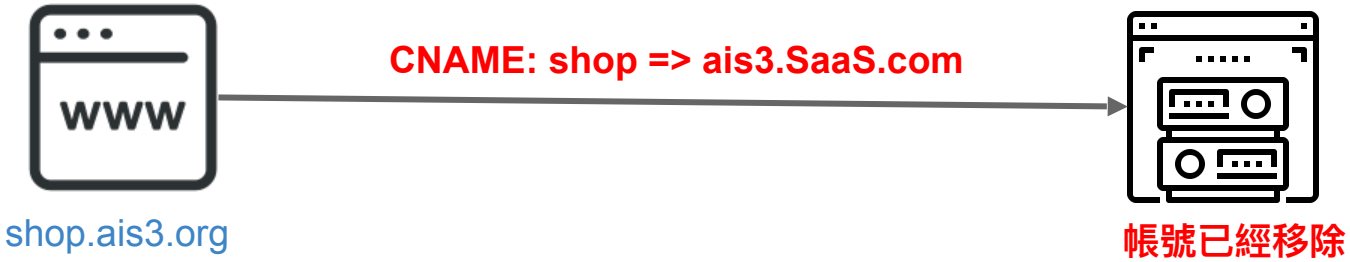
網域劫持

- 使用第三方服務(SaaS)，使用 CNAME 綁定自家網域



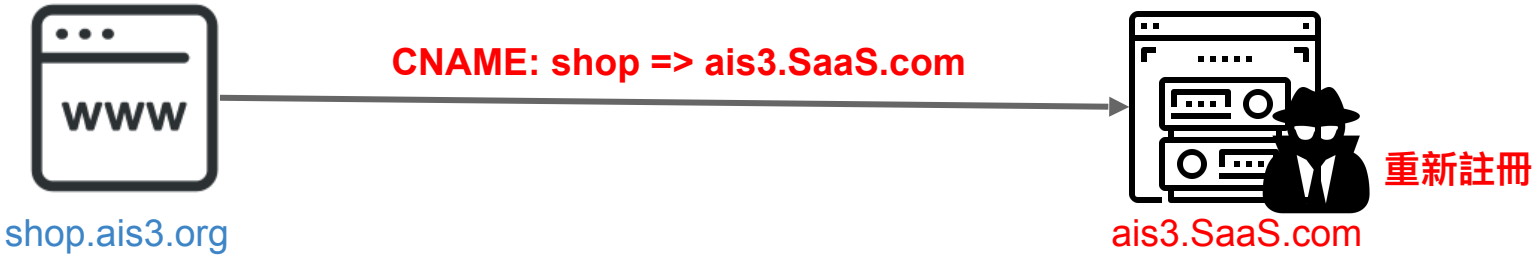
網域劫持

- 停用服務後，僅刪除第三方服務(SaaS)帳號，未清除CNAME



網域劫持

- 忘記移除 DNS 指向紀錄，但目標服務已經移除
  - 攻擊者重新註冊該服務，獲取網域內容控制權



CDN

好像有東西擋在前面

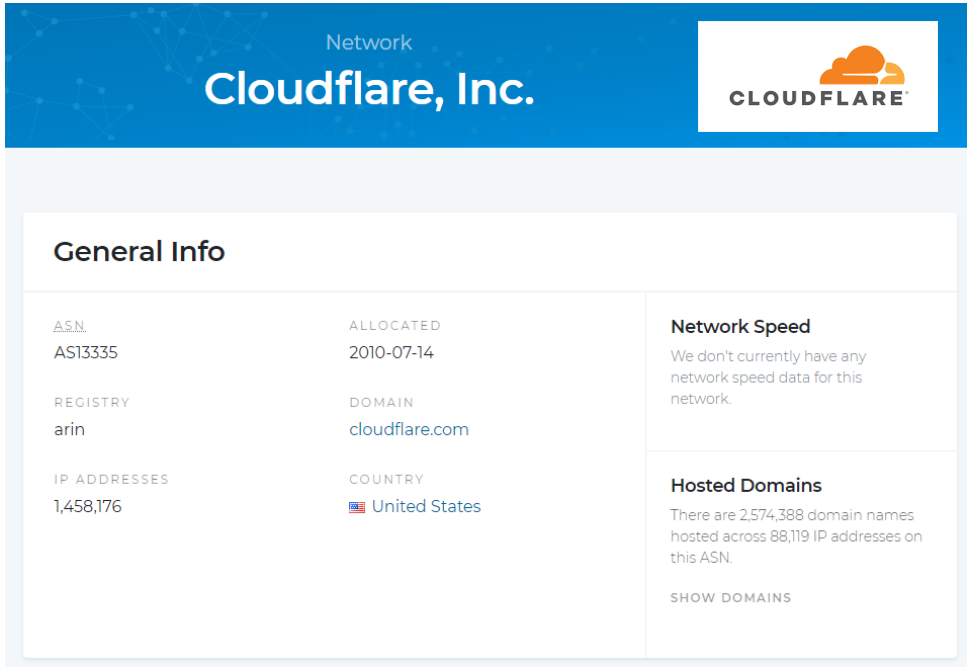
```
root@localhost:~# dig sploot.tw

; <<>> DiG 9.10.3-P4-Debian <<>> sploot.tw
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16432
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sploot.tw.                     IN      A

;; ANSWER SECTION:
sploot.tw.              300     IN      A       104.24.117.234
sploot.tw.              300     IN      A       104.24.116.234
```

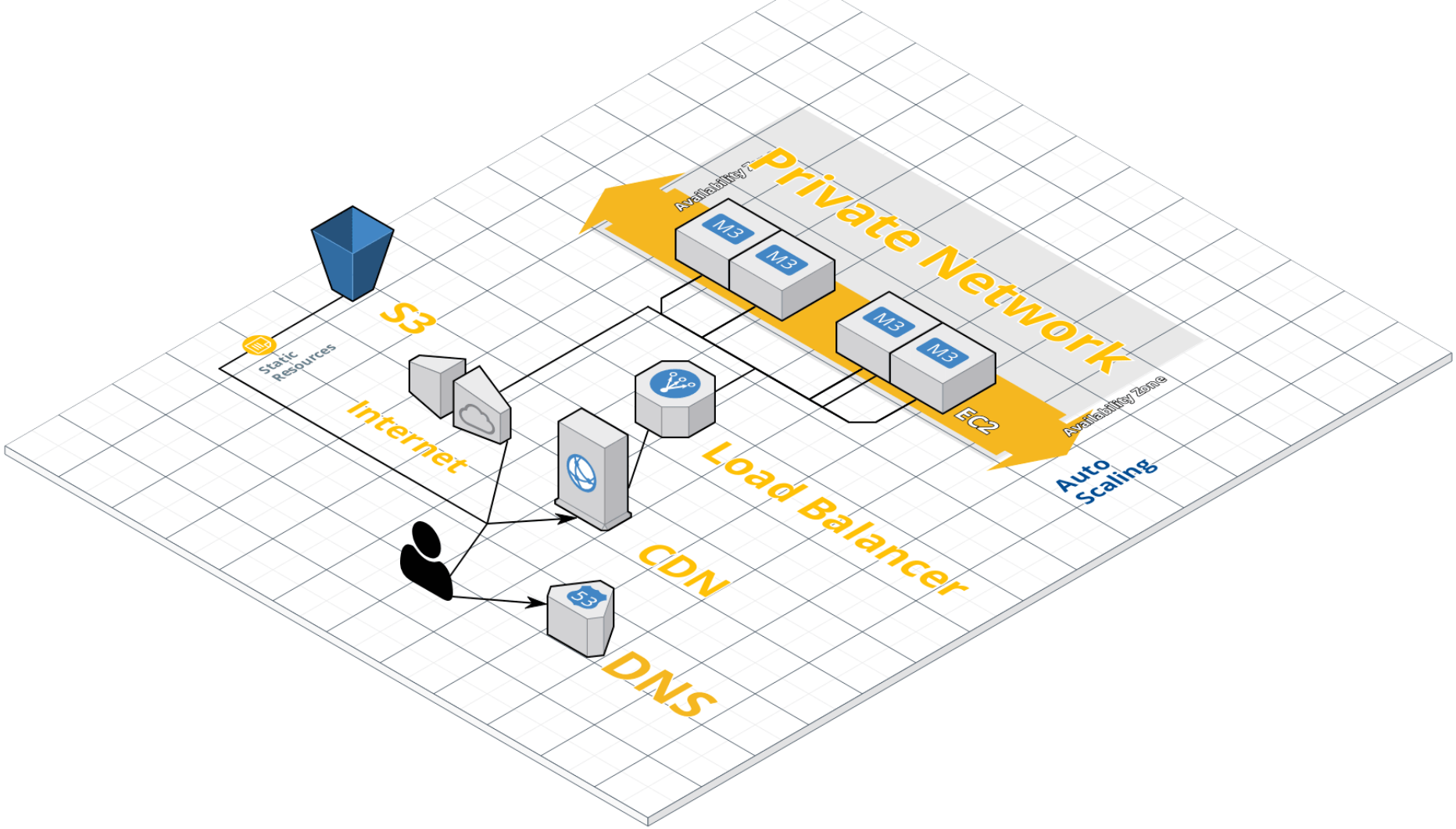
好像有東西擋在前面

```
root@localhost:~# dig 0x61697333.cf

; <<>> DiG 9.10.3-P4-Debian <<>> 0x61697333.cf
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39764
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;0x61697333.cf.                 IN      A

;; ANSWER SECTION:
0x61697333.cf.          300     IN      A       104.28.11.231
0x61697333.cf.          300     IN      A       104.28.10.231
```

原來是 CDN 啊 (Content Delivery Network)

- CDN 服務
  - 快取
  - 存取控制
  - WAF
  - 抗 DDOS




Private Network
Availability Zone
M3
M3
M3
M3
EC2
Availability Zone
Auto Scaling
S3
Static Resources
Internet
Load Balancer
CDN
DNS

繞過 CDN

- 為什麼要繞過?
  - 沒了 CDN 就沒了 WAF
  - DDOS 就打的到?
  - 容易 Debug

額外的注入機會

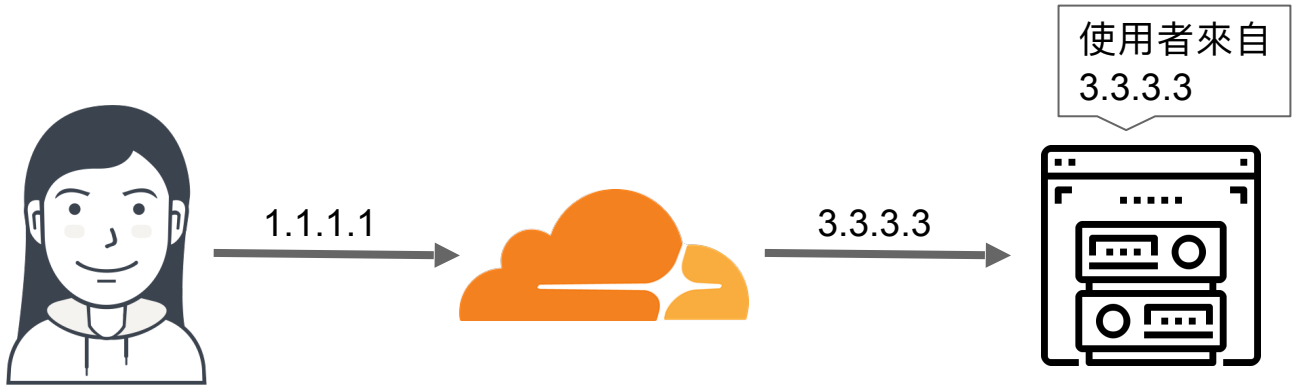
- AP 通常是如何獲取使用者的 IP?

```php
<?php
if(!empty($_SERVER['HTTP_CLIENT_IP'])){
   $ip = $_SERVER['HTTP_CLIENT_IP'];
}else if(!empty($_SERVER['HTTP_X_FORWARDED_FOR'])){
   $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
}else{
   $ip = $_SERVER['REMOTE_ADDR'];
}
echo $ip;
?>
```

錯誤示範，好孩子不要學

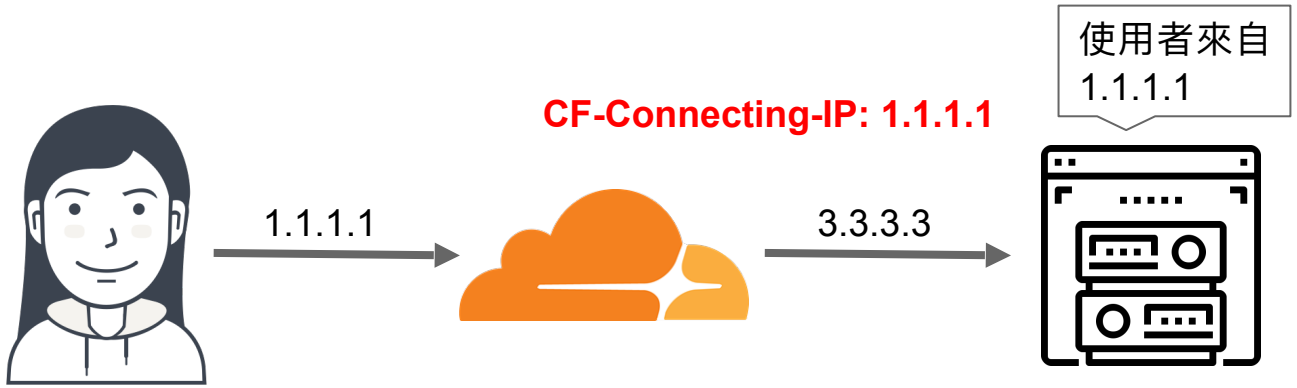
額外的注入機會

- 使用 CDN 的 AP 要如何獲取使用者真實 IP?



額外的注入機會

- 使用 CDN 的 AP 要如何獲取使用者真實 IP?



繞過 CDN

- 怎麼繞過?
  - 嘗試找到舊 IP
  - 找尋暴露在網路上的真實IP
  - 尋找沒有受 CDN 保護的子網域
  - 調整 HTTP Referer
  - 觀察 Header

使用 CDN 的正確姿勢

- 使用安全通道
  - GRE Tunnel
  - VPN
- 僅允許 CDN 與 AP 進行連線
  - https://www.cloudflare.com/ips/

Cloud Storage Service

Cloud Storage Service

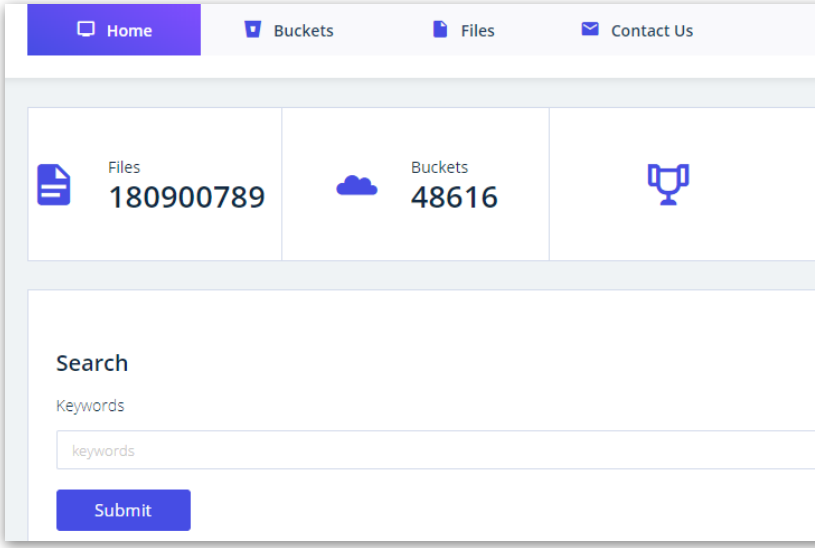
- 資料儲存服務
- 透過 API 進行操作
- 雲端環境中的角色
  - 資料長時間儲存
  - 資料交換
  - 儲存備份資料

Cloud Storage Service

- 最常見的安全問題
  - 權限配置錯誤
  - 被意外存取
  - 網域劫持

AWS S3

- 尋找公開的儲存空間
  - https://buckets.grayhatwarfare.com
  - 嘗試列舉
- 外洩事件
  - https://github.com/nagwww/s3-leaks



AWS S3

- 如何列舉目標的 S3 Bucket
  - 使用字典檔
- 如何生成字典檔
  - 手動產生
    - 公司名稱
    - 參考實際使用名稱
    - 參考 DevOps 的命名方式
  - 自動產生
    - Smeegescrape
    - CeWL

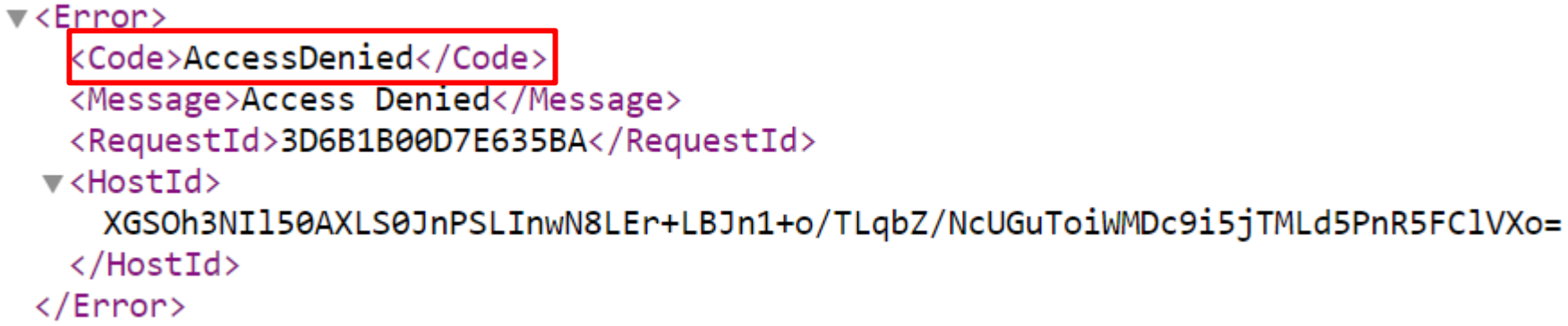
AWS S3

- Bucket Name 具有唯一性
- 網址格式
  - [bucket name].地區.amazonaws.com
  - 地區.amazonaws.com/[bucket name]
- 範例網址
  - ais3-sample.s3-ap-northeast-1.amazonaws.com
- 地區列表
  - https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region

AWS S3


▼<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<Name>ais3-sample.s3-ap-northeast-1.amazonaws.com</Name>
<Prefix/>
<Marker/>
<MaxKeys>1000</MaxKeys>
<IsTruncated>false</IsTruncated>
▼<Contents>
<Key>01.jpg</Key>
<LastModified>2018-07-26T08:10:09.000Z</LastModified>
<ETag>"b29de3abb6fb8aaf1713c52b0145dace"</ETag>
<Size>185419</Size>
<StorageClass>STANDARD</StorageClass>
</Contents>
</ListBucketResult>

AWS S3


<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>3D6B1B00D7E635BA</RequestId>
<HostId>
XGSOh3NIl50AXLS0JnPSLInwN8LEr+LBJn1+o/TLqbZ/NcUGuToiWMDc9i5jTMLd5PnR5FClVXo=
</HostId>
</Error>

AWS S3

- 自訂網域
  - 使用 img.ais3.org 而不是 ais3.s3.amazonaws.com

- 對應方法
  - img.ais3.org.地區.amazonaws.com

AWS S3

▼ **Response Headers** view source

CF-RAY: 440fd551245d78f8-LAX

Connection: keep-alive

Content-Encoding: gzip

Content-Type: application/xml

Date: Fri, 27 Jul 2018 14:35:34 GMT

Server: cloudflare

Transfer-Encoding: chunked

x-amz-bucket-region: ap-northeast-1

x-amz-id-2: oULEHxW79ZWb2lM/pc9NgK/fh1cJhm34SDhyzKT35aY/eaYs77I5UBC5I8vBc+bfCm/9j66rQZY=

x-amz-request-id: 1CF34231987E8803

AWS S3

- 訪問某網址出現下列回應

AWS S3

好麻煩，有沒有給懶人的方法

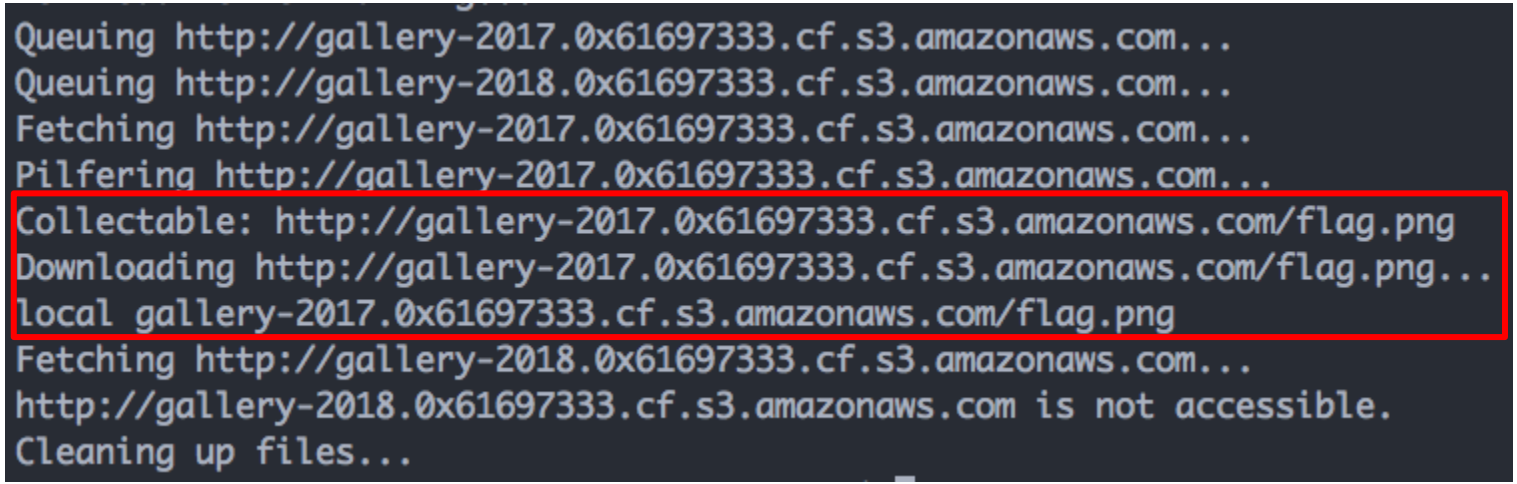
AWS S3

- AWSBucketDump
  - 全自動列舉公開的 AWS S3
  - 自動下載有興趣的檔案

- python AWSBucketDump.py -l 字典檔 -g 關鍵字列表 -D -m 檔案尺寸限制 -t 執行緒 (建議 2 以上)

AWSBucketDump: https://github.com/jordanpotti/AWSBucketDump

AWS S3

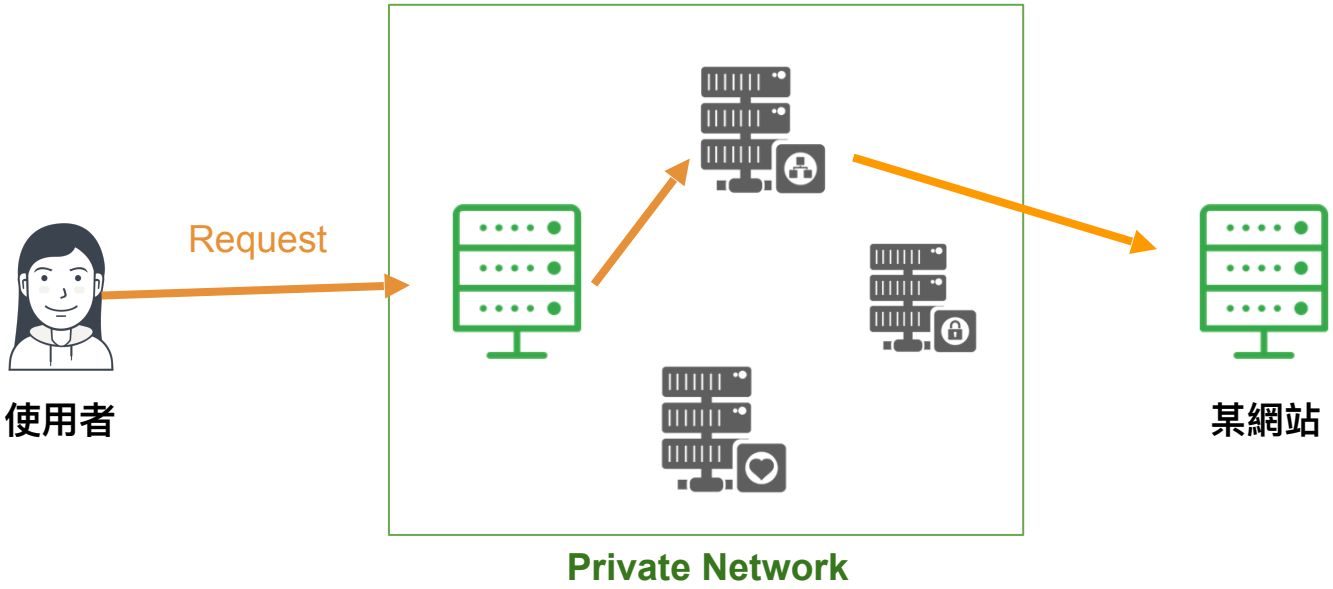

Queuing http://gallery-2017.0x61697333.cf.s3.amazonaws.com...
Queuing http://gallery-2018.0x61697333.cf.s3.amazonaws.com...
Fetching http://gallery-2017.0x61697333.cf.s3.amazonaws.com...
Pilfering http://gallery-2017.0x61697333.cf.s3.amazonaws.com...
Collectable: http://gallery-2017.0x61697333.cf.s3.amazonaws.com/flag.png
Downloading http://gallery-2017.0x61697333.cf.s3.amazonaws.com/flag.png...
local gallery-2017.0x61697333.cf.s3.amazonaws.com/flag.png
Fetching http://gallery-2018.0x61697333.cf.s3.amazonaws.com...
http://gallery-2018.0x61697333.cf.s3.amazonaws.com is not accessible.
Cleaning up files...

Server-Side Request Forgery (SSRF)

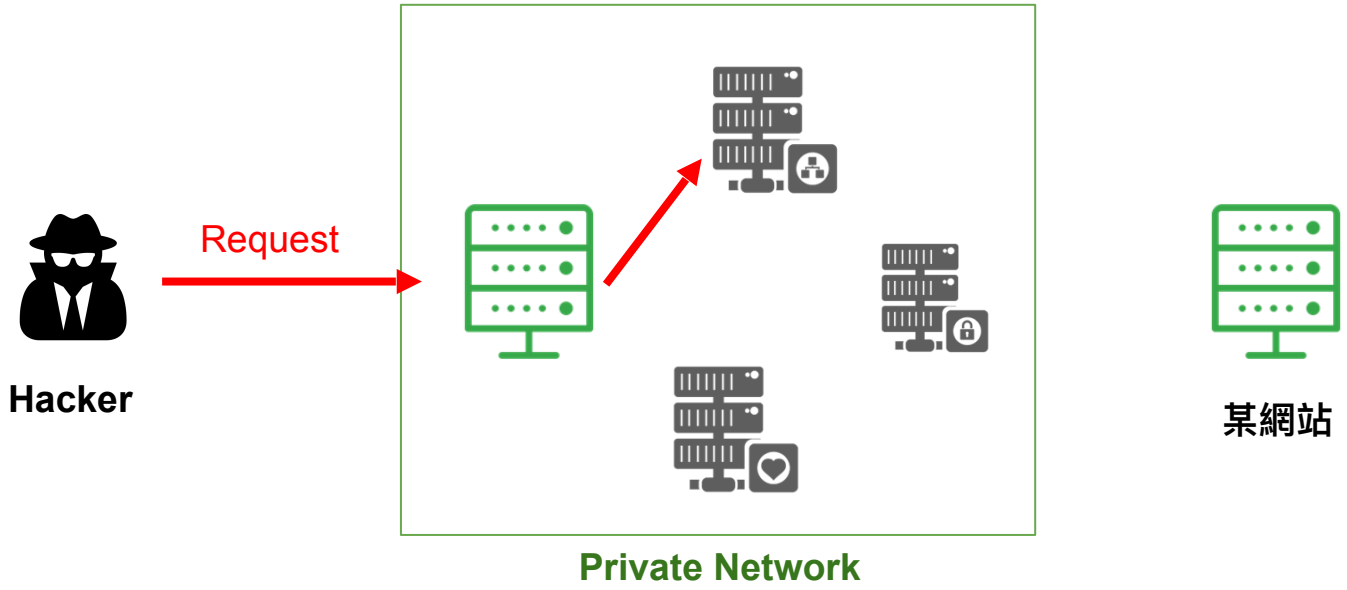
SSRF

- 什麼是 SSRF?
  - SSRF 服務請求偽造, 攻擊者構造特殊請求, 透過伺服器端發起請求的攻擊手段
- 漏洞成因
  - 沒有對輸入進行過濾

SSRF



SSRF



SSRF

- SSRF 的攻擊面
  - 借刀殺人
  - 探索內部服務 (Port Scan)
  - 攻擊內部服務 (Struct2, Redis, ElasticSearch...)
  - 讀取本機端檔案 (/etc/passwd...)
  - 識別服務框架/架構 (Banner)

SSRF

- 什麼地方會出現 SSRF?
  - 能夠發起網路請求的地方
  - 呼叫其他服務
  - 請求遠端資源 (下載檔案, 快取...)
  - 服務內建功能 (Oracle、MSSQL、CouchDB...)
  - 文件處理 (ffmpeg、ImageMagic、Doc、Xlsx、PDF、XML)
  - 其他漏洞利用 (Command Injection、SQLi、XSS、SSTI)

SSRF

- 神奇服務
  - Splash: Javascript Render Service
  - 爬蟲會用到的工具
  - 可以 GET/POST 還可以修改 Header
- 運行方法
  - docker run -p 8050:8050 -p 5023:5023 scrapinghub/splash

Splash: https://github.com/scrapinghub/splash

SSRF

- 可利用協議
  - Http/Https
    - http://127.0.0.1:8080
  - Gopher
    - gopher://127.0.0.1:6378/_get
  - File
    - file:///etc/passwd
  - Dict
    - dict://127.0.0.1:8379/hello:world

SSRF

- 常見可利用服務
  - ElasticSearch
  - CouchDB
  - Redis

SSRF

- 保護繞過
  - HTTP 302 重新導向
  - IP 變形
  - DNS Rebind
  - 解析不一致

SSRF

- 保護繞過
  - HTTP 302 重新導向
    - Location: scheme://IP:Port/Path

SSRF

- 保護繞過
  - IP 變形
    - 127.0.1
    - 127.0x0.0x00.1
    - 127.0.0.1 => http://2130706433
    - http://0/
    - http://[::]
    - http://0000::1
    - nip.io

SSRF

- 保護繞過
  - DNS Rebind
    - 檢查與請求結果不一致

```php
<?php
$domain = 'xxxx.com';
$ip = gethostbyname($domain); // 1.1.1.1
if ( !in_blacklist( $ip ) ){
    $content = file_get_contents( $domain ); // 127.0.0.1
}
```

SSRF

- 保護繞過
  - DNS Rebind
    - A.1.1.1.1.1time.127.0.0.1.1times.repeat.rebind.network

SSRF

```
; <<>> DiG 9.10.3-P4-Debian <<>> A.1.1.1.1.1time.127.0.0.1.1times.repeat.rebind.network
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25306
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;A.1.1.1.1.1time.127.0.0.1.1times.repeat.rebind.network.        IN A

;; ANSWER SECTION:
A.1.1.1.1.1time.127.0.0.1.1times.repeat.rebind.network. 5 IN A 1.1.1.1
```

SSRF

```
; <<>> DiG 9.10.3-P4-Debian <<>> A.1.1.1.1.1time.127.0.0.1.1times.repeat.rebind.network
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18660
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;A.1.1.1.1.1time.127.0.0.1.1times.repeat.rebind.network.        IN A

;; ANSWER SECTION:
A.1.1.1.1.1time.127.0.0.1.1times.repeat.rebind.network. 5 IN A 127.0.0.1
```

SSRF

- 保護繞過
  - 解析不一致 (一個網址各自表述)

http://1.1.1.1 &@2.2.2.2# @3.3.3.3/

urllib2 requests browsers urllib

SSRF

- 該保護哪些 IP 禁止存取?
  - 127.0.0.1
  - Private network
  - 還有嗎?

SSRF

- 該保護哪些 IP 禁止存取?
  - 127.0.0.1
  - Private network
  - 169.254.169.254

MetaData Service

- 什麼是 MetaData Service?
  - 提供機制將設定資訊注入 instance 中
- 裡面有些什麼？
  - hostname
  - host-ID, host-IP
  - SSH Public key
  - Startup script

MetaData Service

- Meta Data Service 的 IP 位置
  - AWS/GCP/Azure/Digital Ocean/Helion/OpenStack
    - 169.254.169.254
  - Oracle
    - 192.0.0.192
  - Alibaba
    - 100.100.100.200

MetaData Service

- 存取方式 (AWS/OpenStack)
  - http://169.254.169.254/latest/user-data
  - http://169.254.169.254/latest/meta-data/
  - http://169.254.169.254/latest/meta-data/iam/security-credentials/

MetaData Service

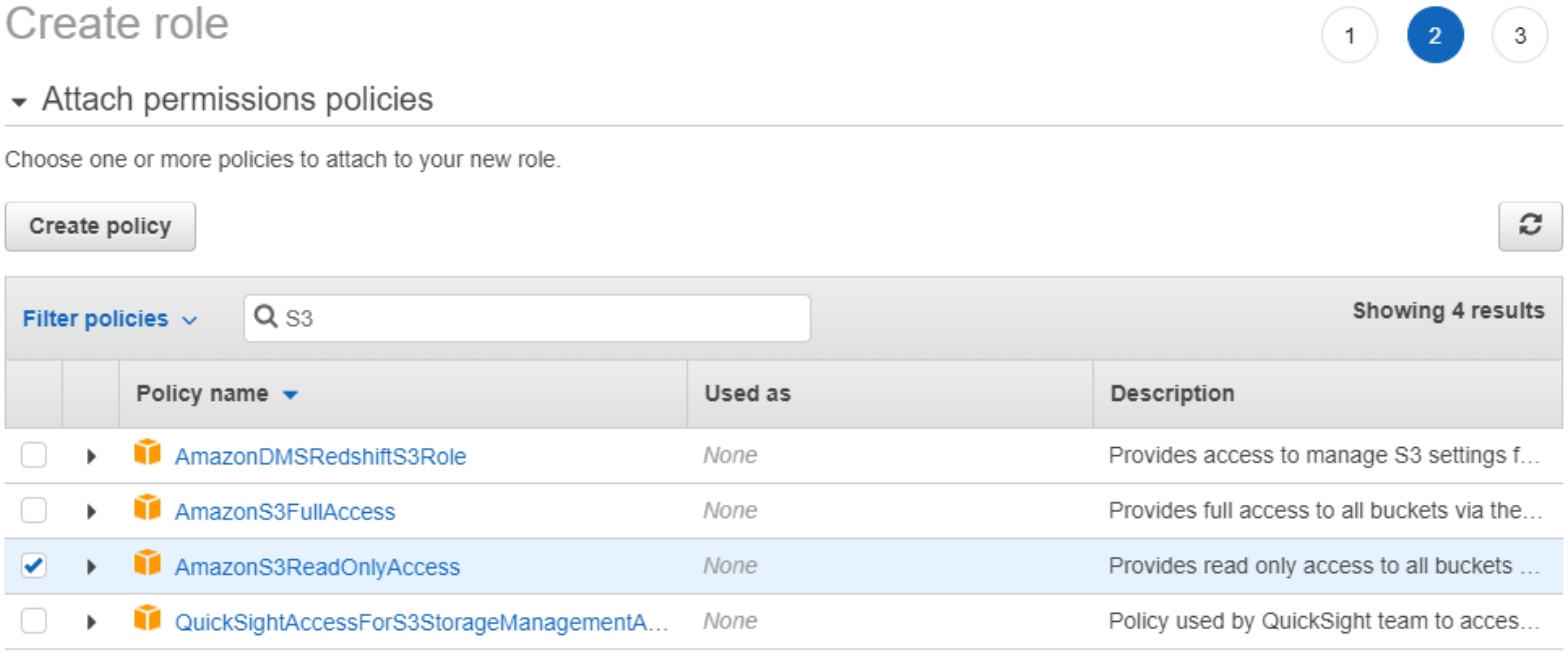
- 存取方式 (Google)
  - 要設定 Header: X-Google-Metadata-Request: True
  - http://169.254.169.254/computeMetadata/v1/
- 不用設定 Header
  - http://metadata.google.internal/computeMetadata/v1beta1/

MetaData Service

- 敏感內容
  - http://169.254.169.254/latest/meta-data/iam/security-credentials/RoleName


```
  "Code" : "Success",
  "LastUpdated" : "2018-07-30T13:39:38Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAIBYL2HB22R4KW52A",
  "SecretAccessKey" : "RTWGwT0EZe2IXFgb1RzDrrQUUOWsSwFTqQp5fQJc",
  "Token" : "FQoDYXdzEBcaDNEBogdVOnOp6CIrHCLBA1Qdc7pyPKJVy/Jsw6gqpZdcQf/mE9+CmoWmX7Ow
M4lZxag3BCiGbRfRAyzQUeogkbIE7QNcwS4HFeT3y68Cf+Yh4DjRrte2rb5b1impflEOwe63tYtNbGJeK0RMS
+NyFtg13c9hnRYcBsJzv2gKZYY1BlE5KIf2EP7qCXFnnD0P2PSBZrKlkuvzcgqqKViw5lB5eHXWJmA5Nos0Th
A5jK7w0PbqLvUkDepZ5f7LlI8UBOeHPIqGghQfCg7VtQxBOAMuC6GgxnY30WSTz5wIaDCqOLGMmOM0EF3aFLC
U1ZStOmB0ZS6ssPYhzLKvg9oMAxku+GDKRAEUOxCqTG7oC61wlm4VbDzHVnGIsWXSNSjd2sh0/7btG2LstgezZ
x/F12ODPFNWlfceMwig3nGAu03r+APZSXGCskVNgEhOty0w2Dh3DKZH8hH26ZToksoa10+xtVVy3UCWs5PVhE
nZHT3IfgoqnyTM8J0HhklRUln0HnZEOV5s/Hgzv45bJzi3uwIQ11LQtVQwTKfYMLRMWmPmrZJ+kRz8UedMGMT
khFbPXPz9dY5cH1b1w5fKNcwXReuK0M3/GMP0whqs/am7kdwdIKIOq/NoF",
  "Expiration" : "2018-07-30T19:57:56Z"
```

MetaData Service



MetaData Service

- 事實沒有那麼美好
  - Role 的權限是沒有 API 可以查詢的
  - 只能每一個 API 都試試看

MetaData Service

好麻煩，有沒有給懶熊的方法

WeirdAAL (AWS Attack Library)

- 專門設計來攻擊 AWS Service
- 全自動測試所有API
- 提供 API 呼叫模組

WeirdAAL: https://github.com/carnal0wnage/weirdAAL

WeirdAAL (AWS Attack Library)

- 使用方法
  - python3 weirdAAL.py -m recon_all -t MyTarget

```
### Enumerating Simple Notification Service (SNS) Permissions ###
An error occurred (AuthorizationError) when calling the ListPlatformApplications operation: User: arn:aws:sts::332449
734084:assumed-role/EC2/i-0044c0766ab7def95 is not authorized to perform: SNS:ListPlatformApplications on resource: a
rn:aws:sns:us-east-1:332449734084:*
An error occurred (AuthorizationError) when calling the ListPhoneNumbersOptedOut operation: User: arn:aws:sts::332449
734084:assumed-role/EC2/i-0044c0766ab7def95 is not authorized to perform: SNS:ListPhoneNumbersOptedOut on resource: a
rn:aws:sns:us-east-1:332449734084:*
An error occurred (AuthorizationError) when calling the ListSubscriptions operation: User: arn:aws:sts::332449734084:
assumed-role/EC2/i-0044c0766ab7def95 is not authorized to perform: SNS:ListSubscriptions on resource: arn:aws:sns:us-
east-1:332449734084:*
An error occurred (AuthorizationError) when calling the ListTopics operation: User: arn:aws:sts::332449734084:assumed
-role/EC2/i-0044c0766ab7def95 is not authorized to perform: SNS:ListTopics on resource: arn:aws:sns:us-east-1:3324497
34084:*
An error occurred (AuthorizationError) when calling the GetSMSAttributes operation: User: arn:aws:sts::332449734084:a
ssumed-role/EC2/i-0044c0766ab7def95 is not authorized to perform: SNS:GetSMSAttributes on resource: arn:aws:sns:us-ea
st-1:332449734084:*

[-] No sns actions allowed [-]
```

WeirdAAL (AWS Attack Library)

- 發現可用 API

```
#### Trying to list s3 bucketsfor ASIAJ2Y3W4C47DRNE4GA ####

ais3-sample.0x61697333.cf
gallery-2017.0x61697333.cf
```

WeirdAAL (AWS Attack Library)

- 列舉 Bucket 內的檔案
  - python3 weirdAAL.py -m s3_list_bucket_contents -a 'bucket' -t yolo

```
#### Attempting to list s3 bucket contents for gallery-2017.0x61697333.cf ####
01.jpg
flag.png
```

- 嘗試下載 S3 File
  - python3 weirdAAL.py -m s3_download_file -a 'bucket','file' -t yolo

```
ubuntu@ip-172-31-3-100:/tmp/weirdAAL$ python3 weirdAAL.py -m s3_download_file -a 'gallery-2017.0x6
1697333.cf','01.jpg' -t yolo
file downloaded to: /tmp/weirdAAL/loot/01.jpg
```

Q & A

Mail: hi@kaiching.wang