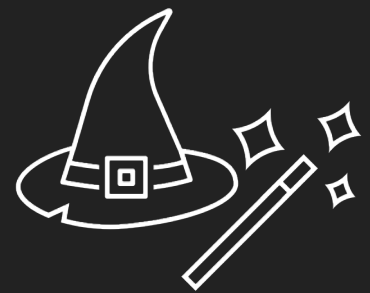


DEV✓CORE

SECURITY
CONSULTING



黑魔法、大壞蛋、大壞蛋
得崩

Crystal & Cyku

戴夫寇爾股份有限公司

contact@devco.re

2023.03.11

DEVCORE Conference



- 為了紅隊的 Initial Access 而研究
- 軟體提供 80、443 網頁介面
- 軟體整合可以設定作業系統
- 數十萬台機器暴露在外網

聲明：

為保護當事人，

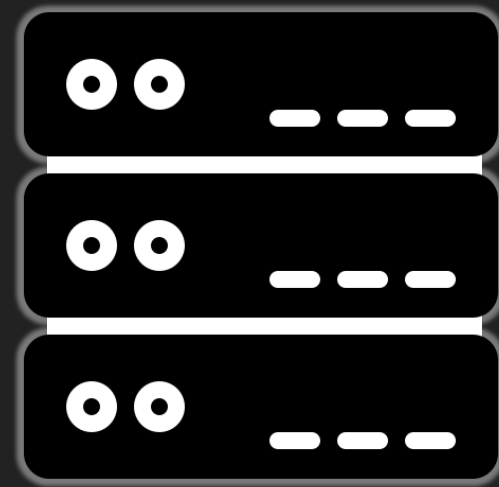
API 路徑與參數名稱均已混淆，

僅保留利用思路

與 exploit chain 邏輯。



Internet IP



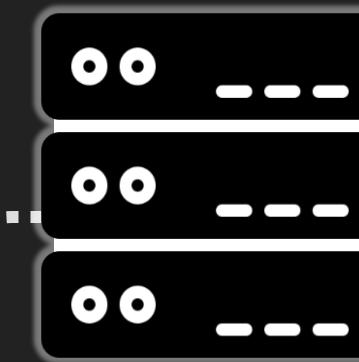
Reverse Proxy

/api1/*



Component α

127.0.0.1:1234/cgi-bin/



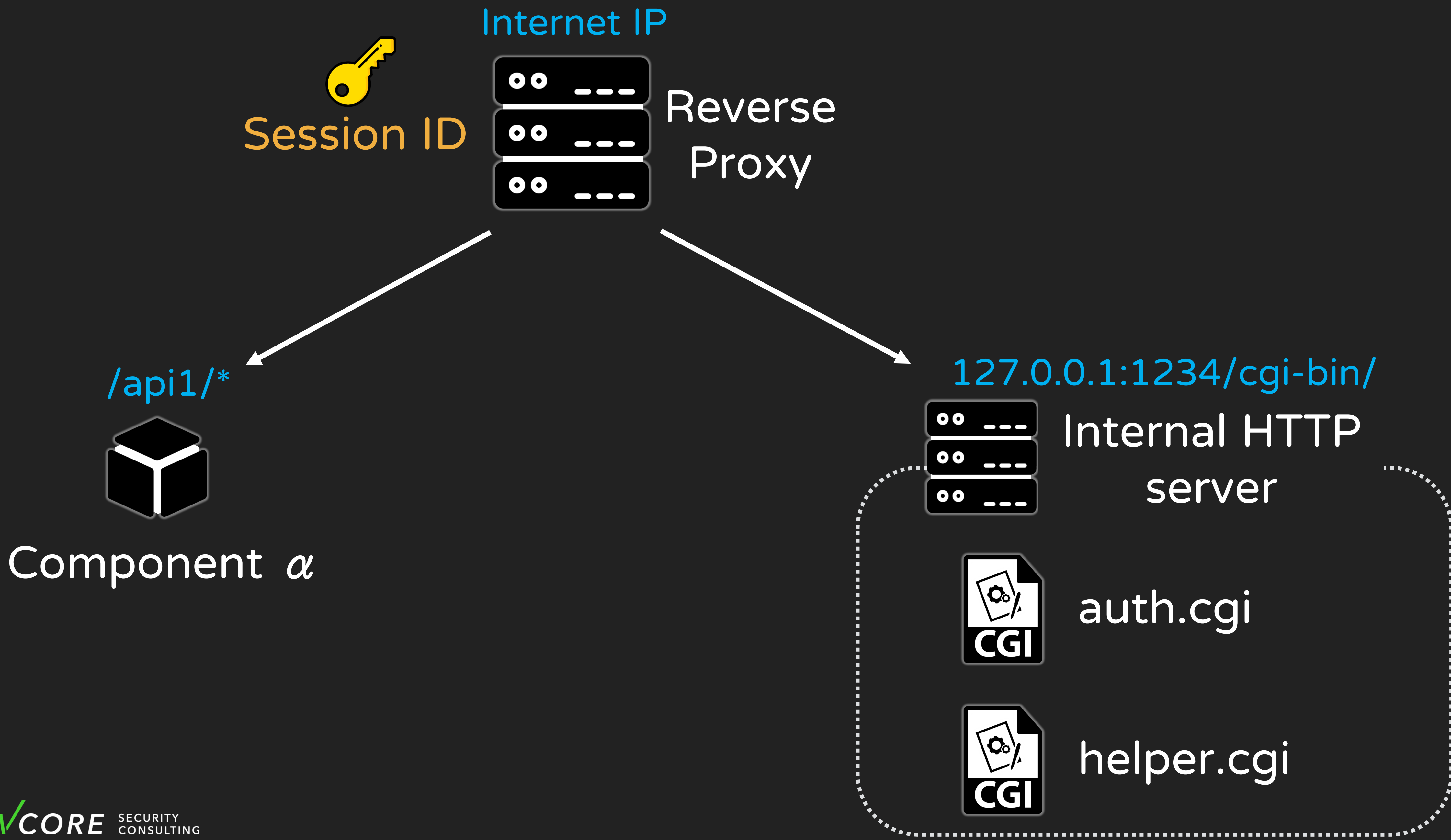
Internal HTTP server



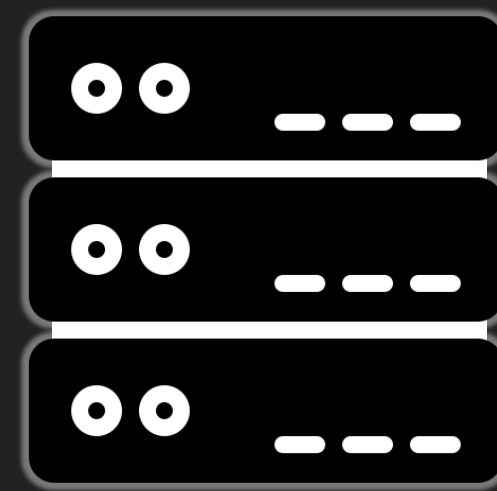
auth.cgi



helper.cgi



Internet IP



Reverse Proxy

/api1/*

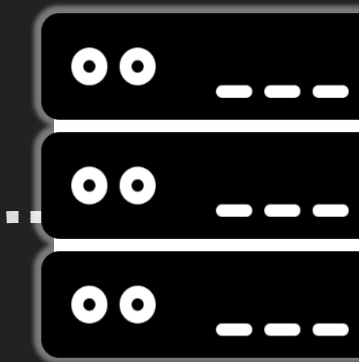


Component α



Session ID

127.0.0.1:1234/cgi-bin/



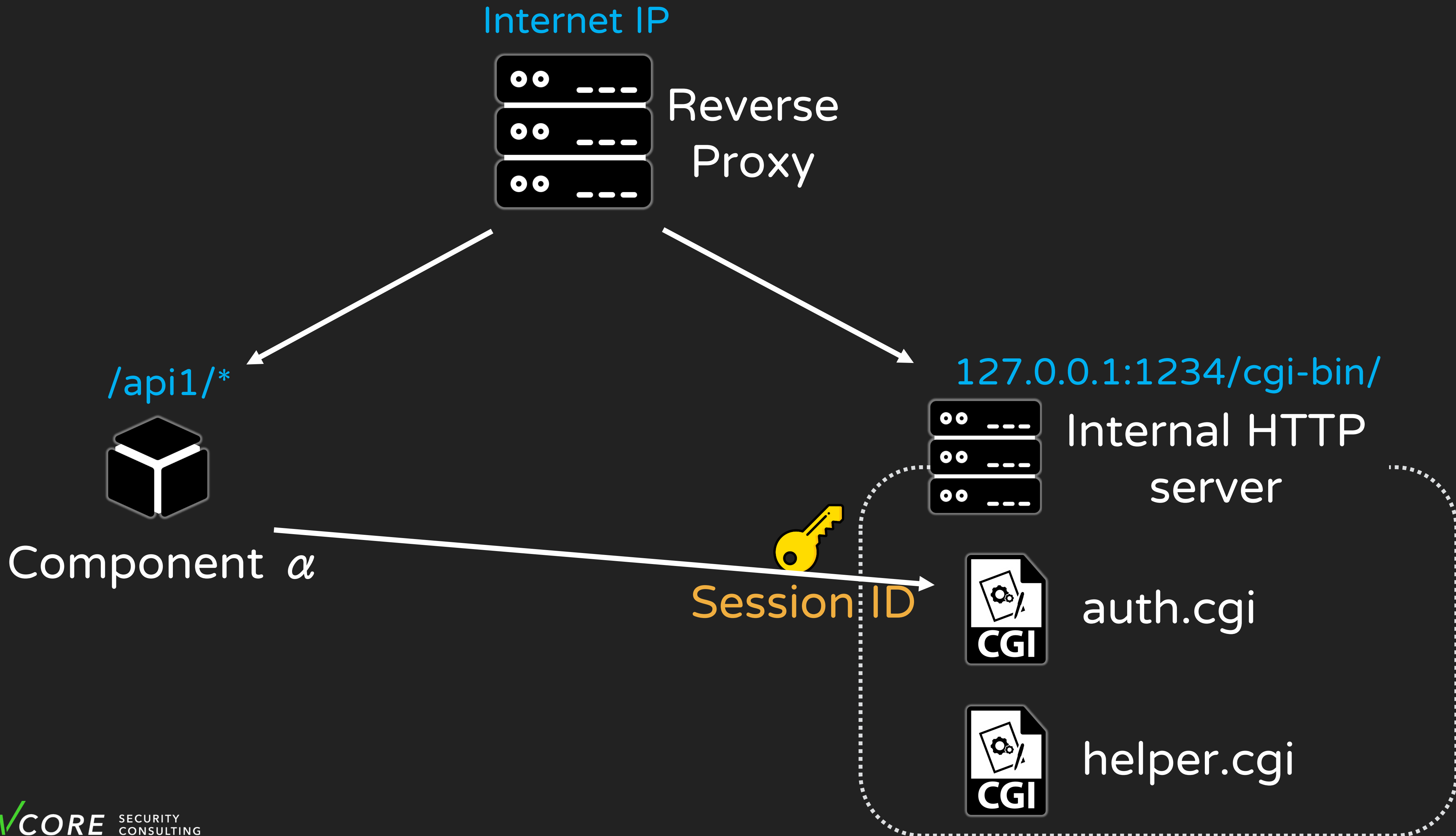
Internal HTTP server



auth.cgi



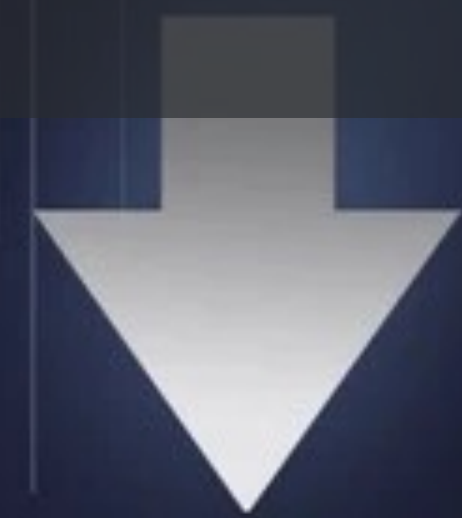
helper.cgi



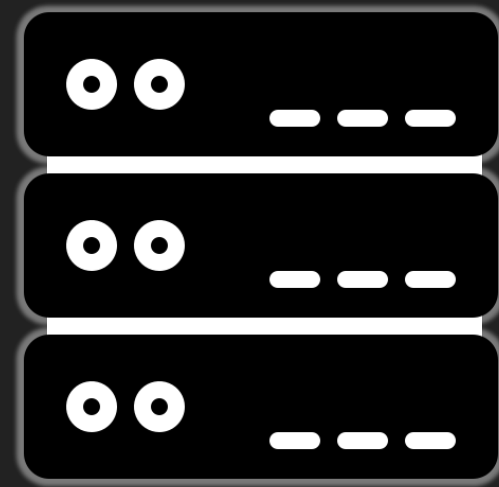
Let's talk about the 4 bugs.



Bug 1 :
Path Traversal



Internet IP



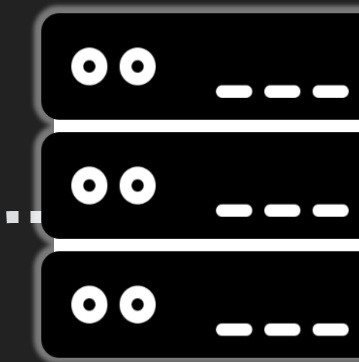
Reverse Proxy

/api1/*



Component α

127.0.0.1:1234/cgi-bin/



Internal HTTP server

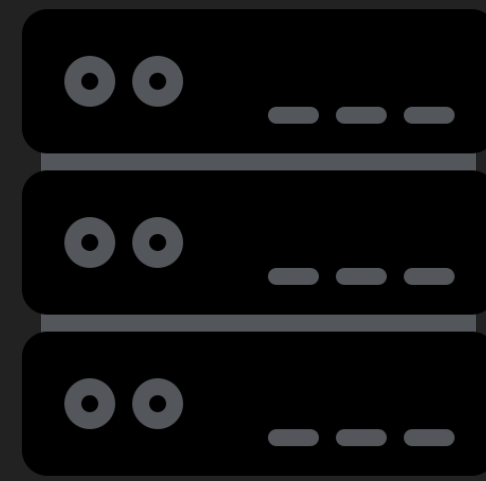


auth.cgi



helper.cgi

Internet IP



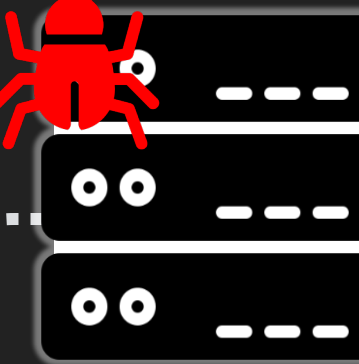
Reverse Proxy

/api1/*



Component α

127.0.0.1:1234/cgi-bin/



Internal HTTP server



auth.cgi



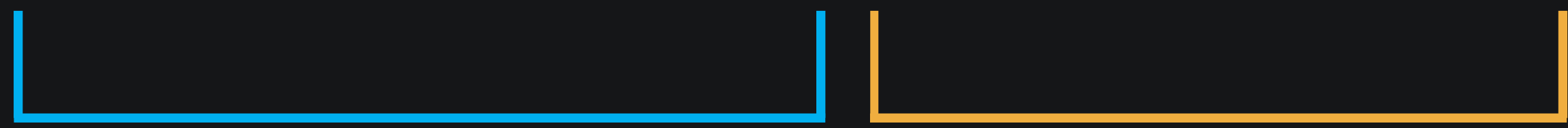
helper.cgi

Internet IP
Reverse



Original API

http://127.0.0.1:1234
/cgi-bin/auth.cgi?sid=abcdefgh

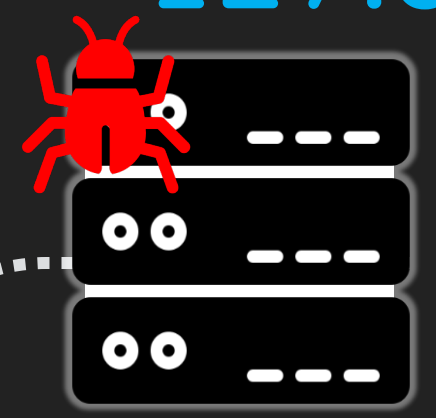


Path

Query String

Component α

127.0.0.1:1234/cgi-bin/



Internal HTTP server

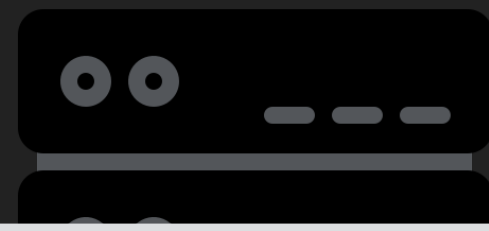


auth.cgi



helper.cgi

Internet IP

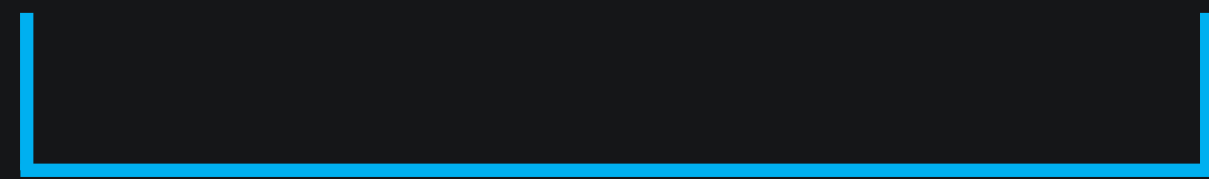


Reverse

Intended

http://127.0.0.1:1234

/cgi-bin/auth.cgi?sid=ab/../../index.cgi

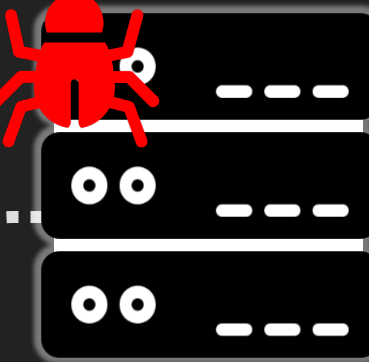


Path



Query String

127.0.0.1:1234/cgi-bin/



Internal HTTP server

Component α

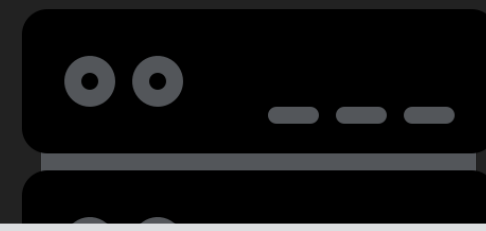


auth.cgi



helper.cgi

Internet IP



Reverse

Unintended

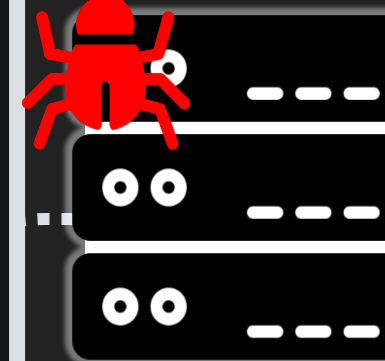
http://127.0.0.1:1234

/cgi-bin/auth.cgi?sid=ab/../../index.cgi



Path

127.0.0.1:1234/cgi-bin/



Internal HTTP server

Component α

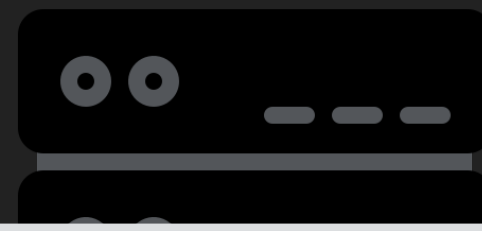


auth.cgi



helper.cgi

Internet IP

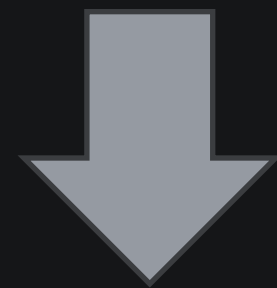


Reverse

Unintended

http://127.0.0.1:1234

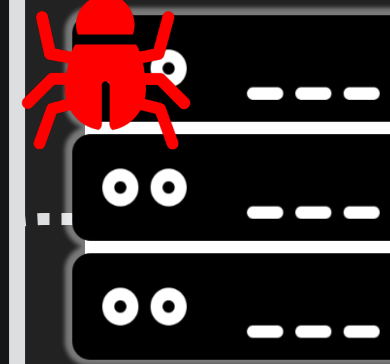
~~/cgi-bin/auth.cgi?sid=ab~~ /../index.cgi



http://127.0.0.1:1234

/cgi-bin/index.cgi

127.0.0.1:1234/cgi-bin/



Internal HTTP
server



CGI

auth.cgi



CGI

helper.cgi

那 Attacker 可以做什麼？

X 破壞機密性 Confidentiality

X 破壞完整性 Integrity

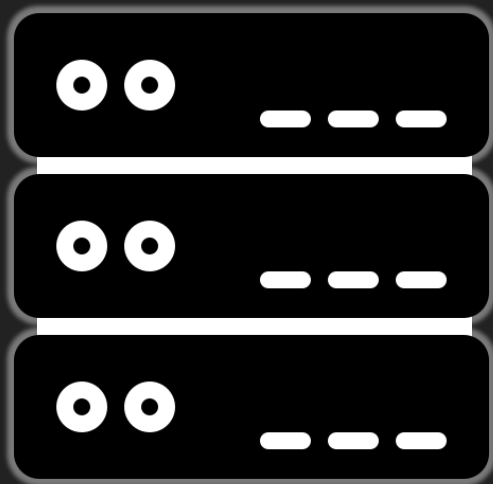
X 破壞可用性 Availability

CVSS 0.0 (None)



Bug 2 :
Parameter Pollution

Internet IP



Reverse Proxy

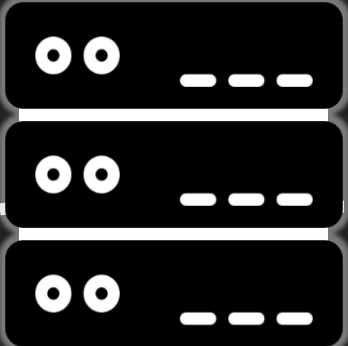


/api1/*



Component
α

127.0.0.1:1234/cgi-bin/



Internal HTTP server

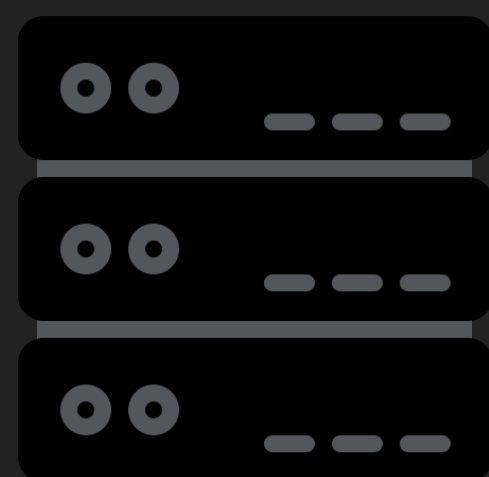


auth.cgi



helper.cgi

Internet IP



Reverse Proxy

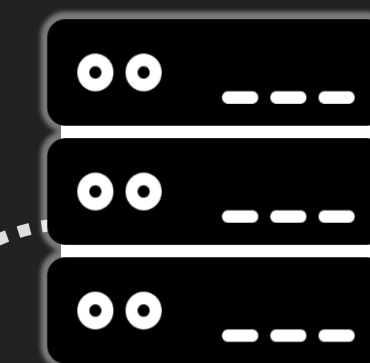


/api1/*



Component
 α

127.0.0.1:1234/cgi-bin/



Internal HTTP
server



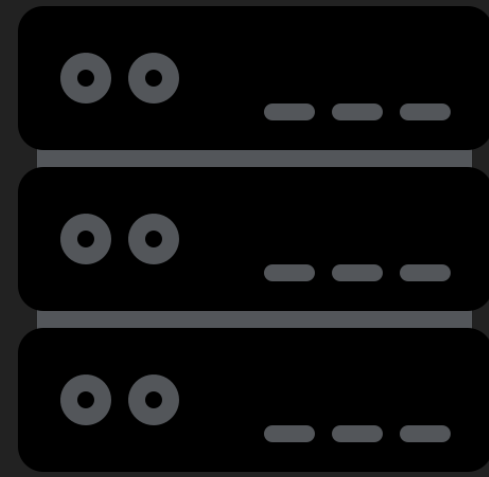
auth.cgi



helper.cgi

```
GET /api1/ HTTP/1.1
Host: internet_ip
Cookie: sid=aa&bb=cc
```

Internet IP



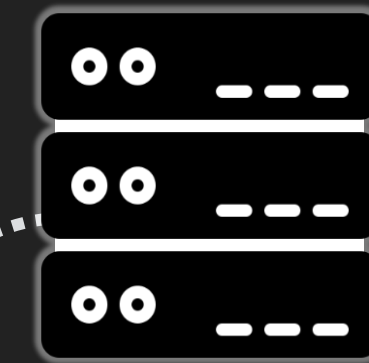
Reverse Proxy

/api1/*



Component
 α

127.0.0.1:1234/cgi-bin/



Internal HTTP
server



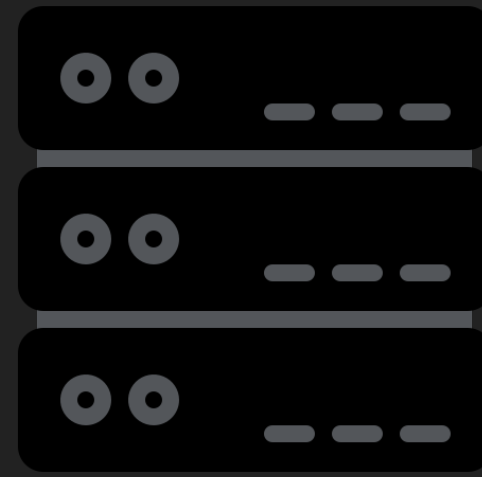
auth.cgi



helper.cgi

```
GET /api1/ HTTP/1.1
Host: internet_ip
Cookie: sid=aa&bb=cc
```

Internet IP



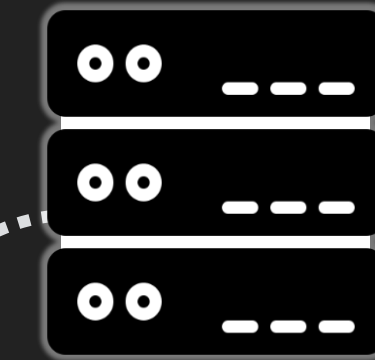
Reverse Proxy

/api1/*



Component
 α

127.0.0.1:1234/cgi-bin/



Internal HTTP server



auth.cgi



helper.cgi

```
GET /cgi-bin/auth.cgi?sid=aa&bb=cc
HTTP/1.1
Host: 127.0.0.1:1234
```

Internet IP

Expectation

```
GET /cgi-bin/auth.cgi?sid=aa&bb=cc
HTTP/1.1
Host: 127.0.0.1:1234
```

/api1/*

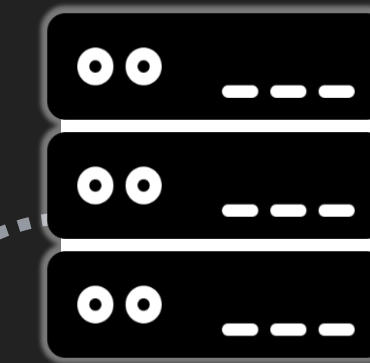


Component
 α

Reality

```
GET /cgi-bin/auth.cgi?sid=aa&bb=cc
HTTP/1.1
Host: 127.0.0.1:1234
```

127.0.0.1:1234/cgi-bin/



Internal HTTP
server



auth.cgi



helper.cgi

那 Attacker 可以做什麼？

X 破壞機密性 Confidentiality

X 破壞完整性 Integrity

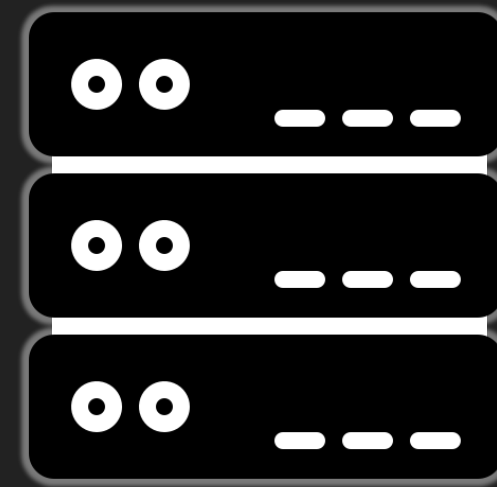
X 破壞可用性 Availability

CVSS 0.0 (None)

Bug 3 : CRLF Injection



Internet IP



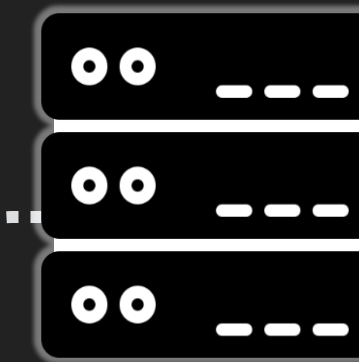
Reverse Proxy

/api1/*



Component α

127.0.0.1:1234/cgi-bin/



Internal HTTP server

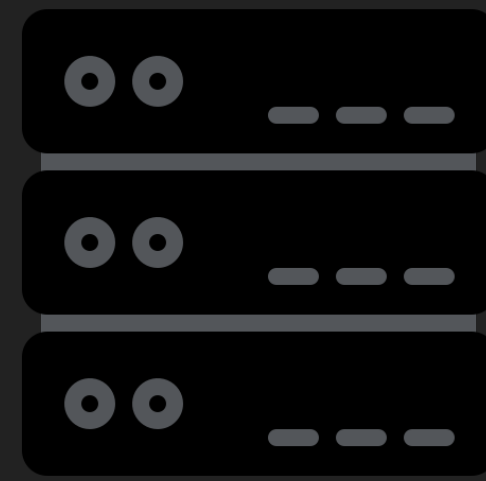


auth.cgi



helper.cgi

Internet IP



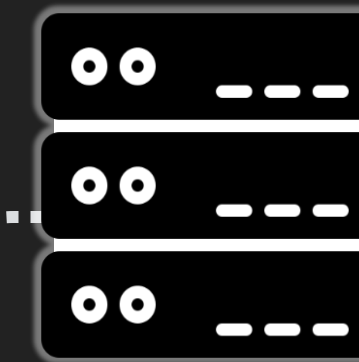
Reverse Proxy

/api1/*



Component α

127.0.0.1:1234/cgi-bin/



Internal HTTP server



auth.cgi



helper.cgi

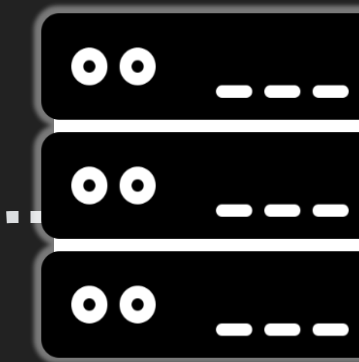
Internet IP

```
GET /cgi-bin/helper.cgi?f=backup&sid=abc HTTP/1.1  
Host: 127.0.0.1:1234
```



```
HTTP/1.1 302 Found  
Location: /cgi-bin/login.cgi?sid=abc  
Connection: close
```

127.0.0.1:1234/cgi-bin/



Internal HTTP
server



auth.cgi



helper.cgi

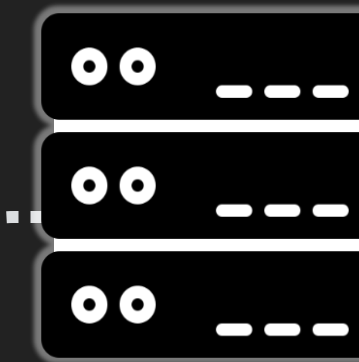
Internet IP

```
GET /cgi-bin/helper.cgi?f=backup&sid=a%0ax-b:c%0a HTTP/1.1  
Host: 127.0.0.1:1234
```



```
HTTP/1.1 302 Found  
Location: /cgi-bin/login.cgi?sid=a  
x-b:c  
Connection: close
```

127.0.0.1:1234/cgi-bin/



Internal HTTP
server

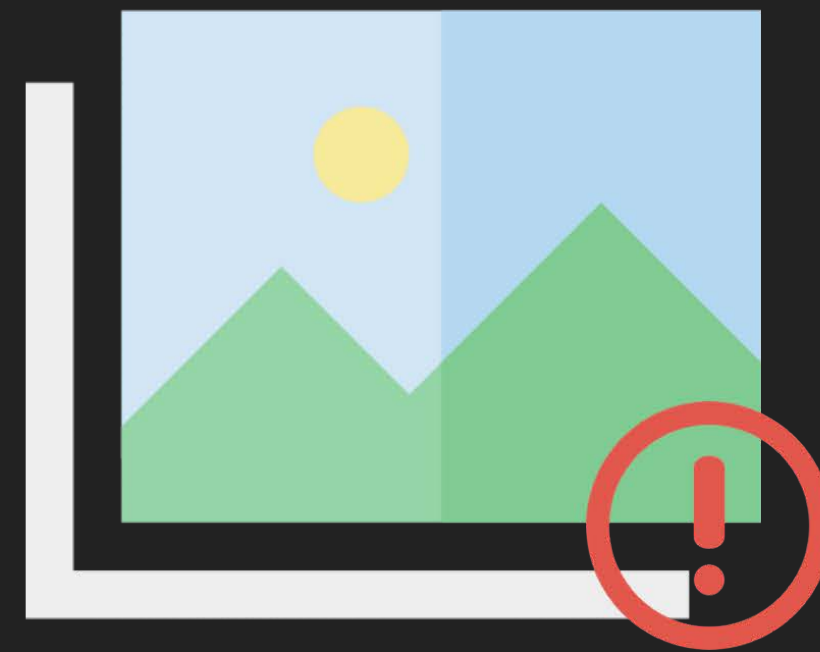


auth.cgi



helper.cgi

我們可以用來串 XSS ？



內部演練畫面
僅公布於研討會

有料ㄟ！



says :



所以 Attacker 可以做 ..

X 破壞機密性 Confidentiality

X 破壞完整性 Integrity

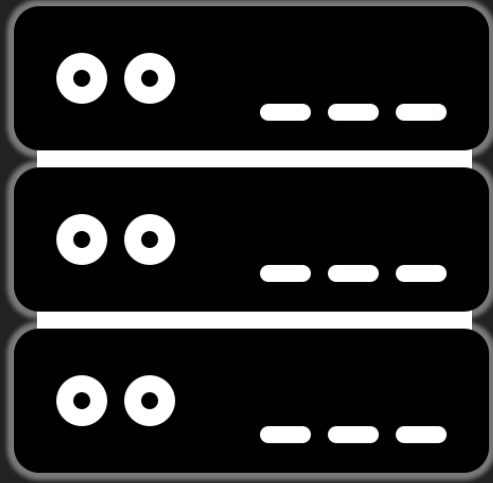
X 破壞可用性 Availability

CVSS 0.0 (None)

Bug 4 : “Impossible” Command Injection



Internet IP



Reverse Proxy



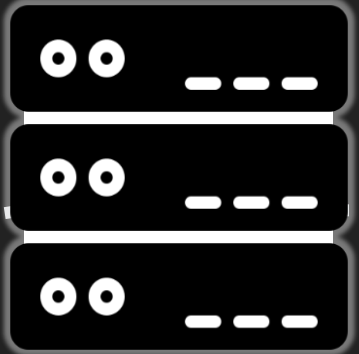
/api1/*



Component

α

127.0.0.1:1234/cgi-bin/



Internal HTTP server

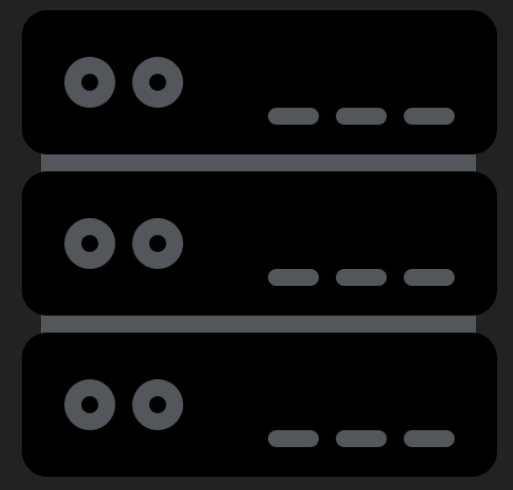


auth.cgi



helper.cgi

Internet IP



Reverse Proxy

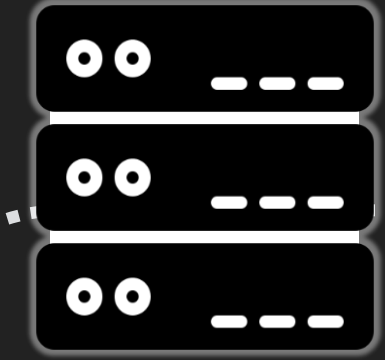


/api1/*



Component
α

127.0.0.1:1234/cgi-bin/



Internal HTTP server



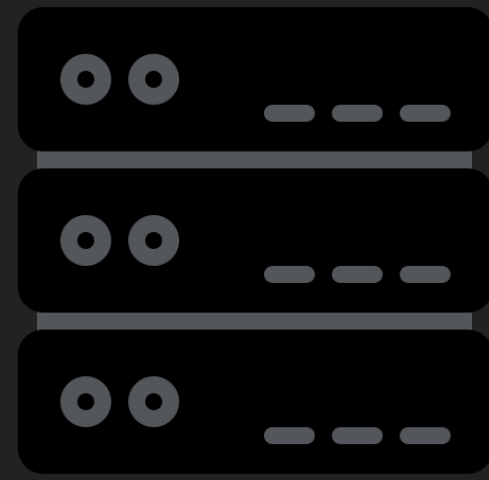
auth.cgi



helper.cgi

```
GET /api1/ HTTP/1.1
Host: internet_ip
Cookie: sid=a
```

Internet IP



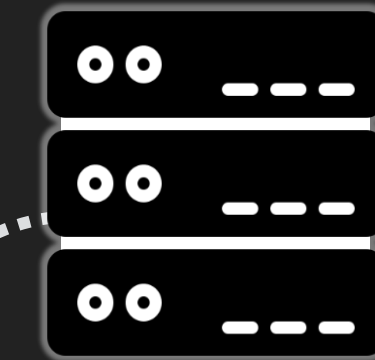
Reverse Proxy

/api1/*



Component
 α

127.0.0.1:1234/cgi-bin/



Internal HTTP
server



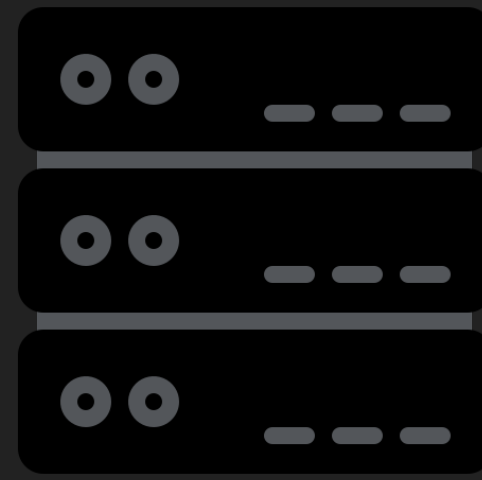
auth.cgi



helper.cgi

```
GET /api1/ HTTP/1.1
Host: internet_ip
Cookie: sid=a
```

Internet IP



Reverse Proxy

/api1/

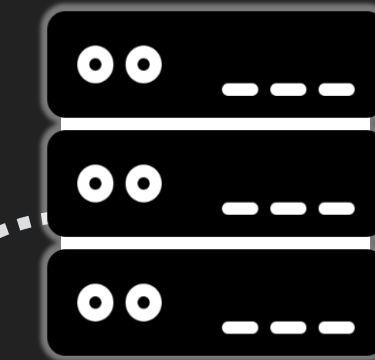


Component

α

```
GET /cgi-bin/auth.cgi?sid=a
```

127.0.0.1:1234/cgi-bin/



Internal HTTP server

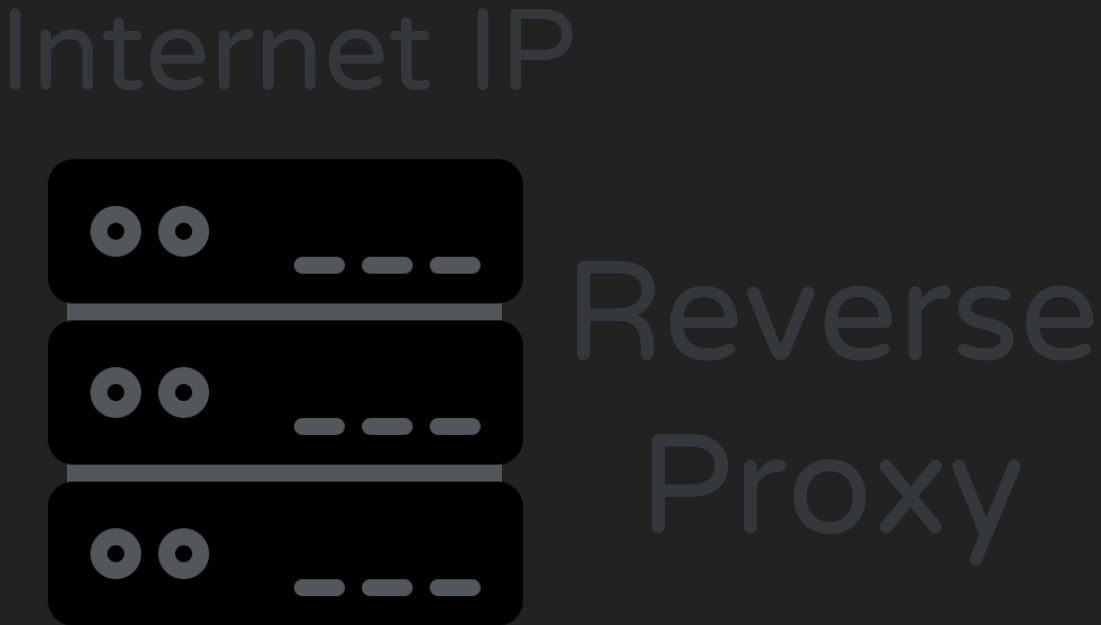


auth.cgi

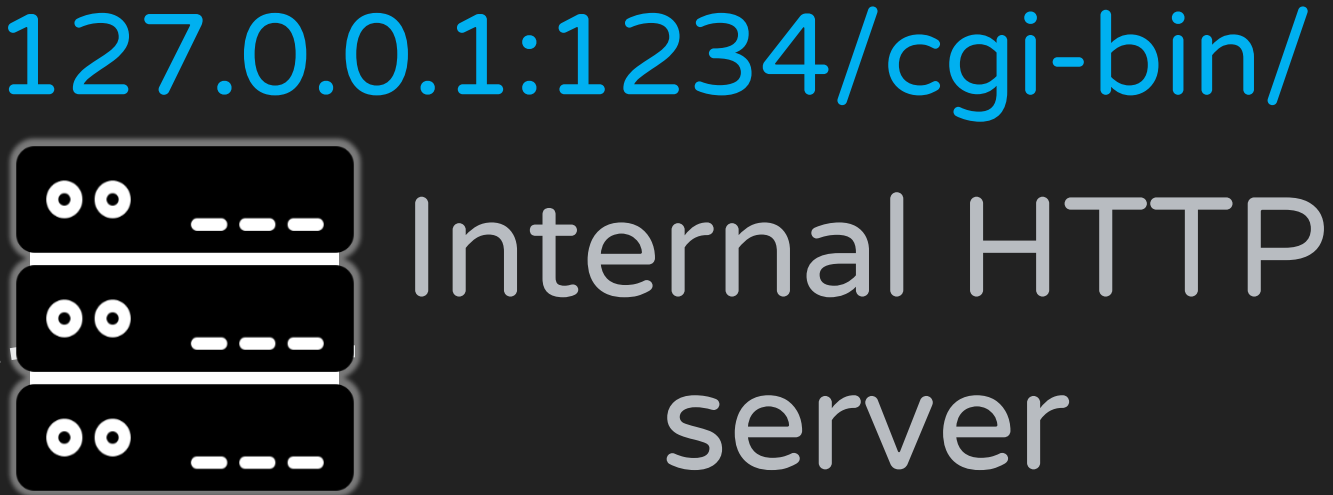


helper.cgi

```
GET /api1/ HTTP/1.1
Host: internet_ip
Cookie: sid=a
```

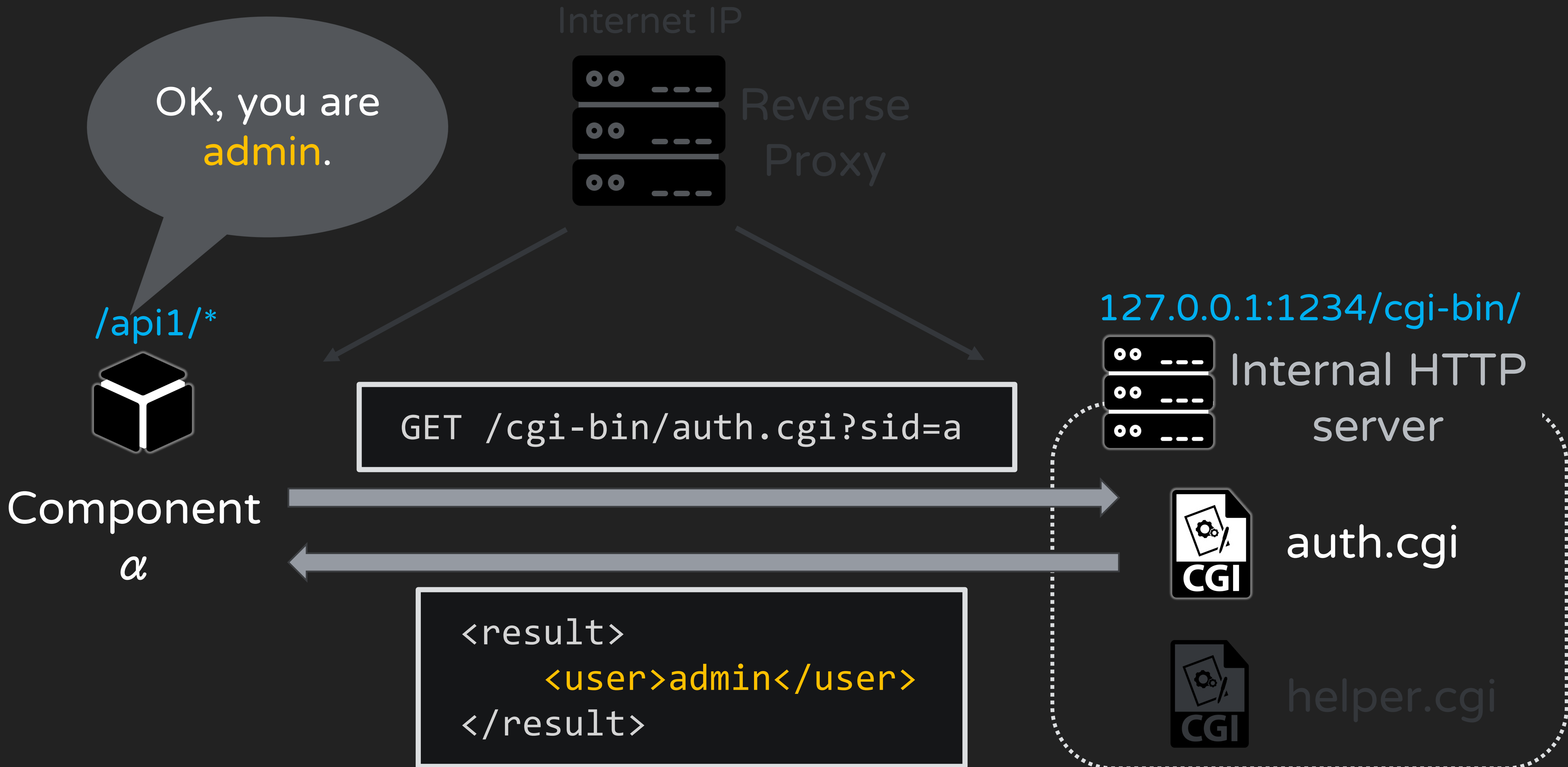


```
GET /cgi-bin/auth.cgi?sid=a
```

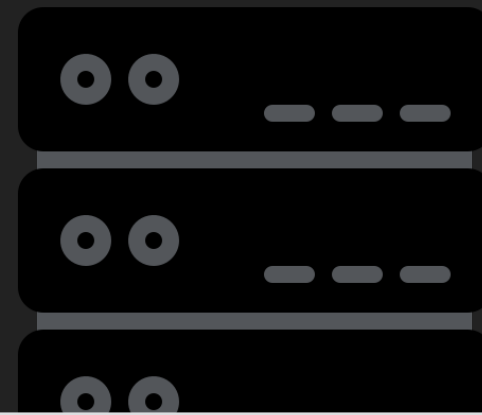


Component α

```
<result>
  <user>admin</user>
</result>
```



Internet IP

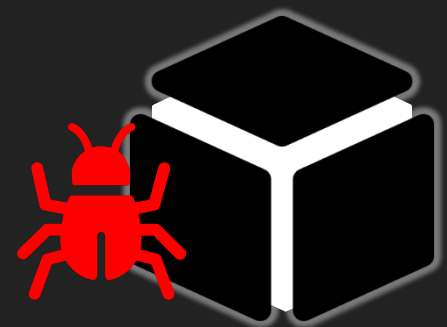


Reverse
Proxy

username = 'admin'

```
@app.route('/fakeapi')  
def config():  
    ...  
    command = "safecmd -u '{}' commit".format(current_user.username)  
    proc = subprocess.Popen(command, shell=True, stdout=subprocess.PIPE)
```

/api1/*



Component

α



auth.cgi



helper.cgi

如果我們有低權限帳號，或許可以改自己的名稱！

internet_ip 顯示

使用者名稱不可以包含特殊字元。



經過測試發現，
想在使用者名稱插入特殊字元，
我們需要這麼做：

1. 以 root 身分透過 SSH 登入設備
2. 用 useradd 指令新增使用者
3. 編輯 /etc/passwd 修改使用者名稱

CVSS 8.8 (High)

經過測試發現，
想在使用者名稱插入特殊字元，
我們需要這麼做：

1. 以 root 身分透過 SSH 登入設備
2. 用 useradd 指令新增使用者
3. 編輯 /etc/passwd 修改使用者名稱

RCE

CVSS 8.8 (High)



WAIT A MINUTE

經過測試發現，
想在使用者名稱插入特殊字元，
我們需要這麼做：

1. 以 root 身分透過 SSH 登入設備
2. 用 useradd 指令新增使用者
3. 編輯 /etc/passwd 修改使用者





CVSS 0.0 (None)

Turning Harmless Bugs into Vulnerability



Bug 1 :
Path Traversal



Bug 2 :
Parameter Pollution

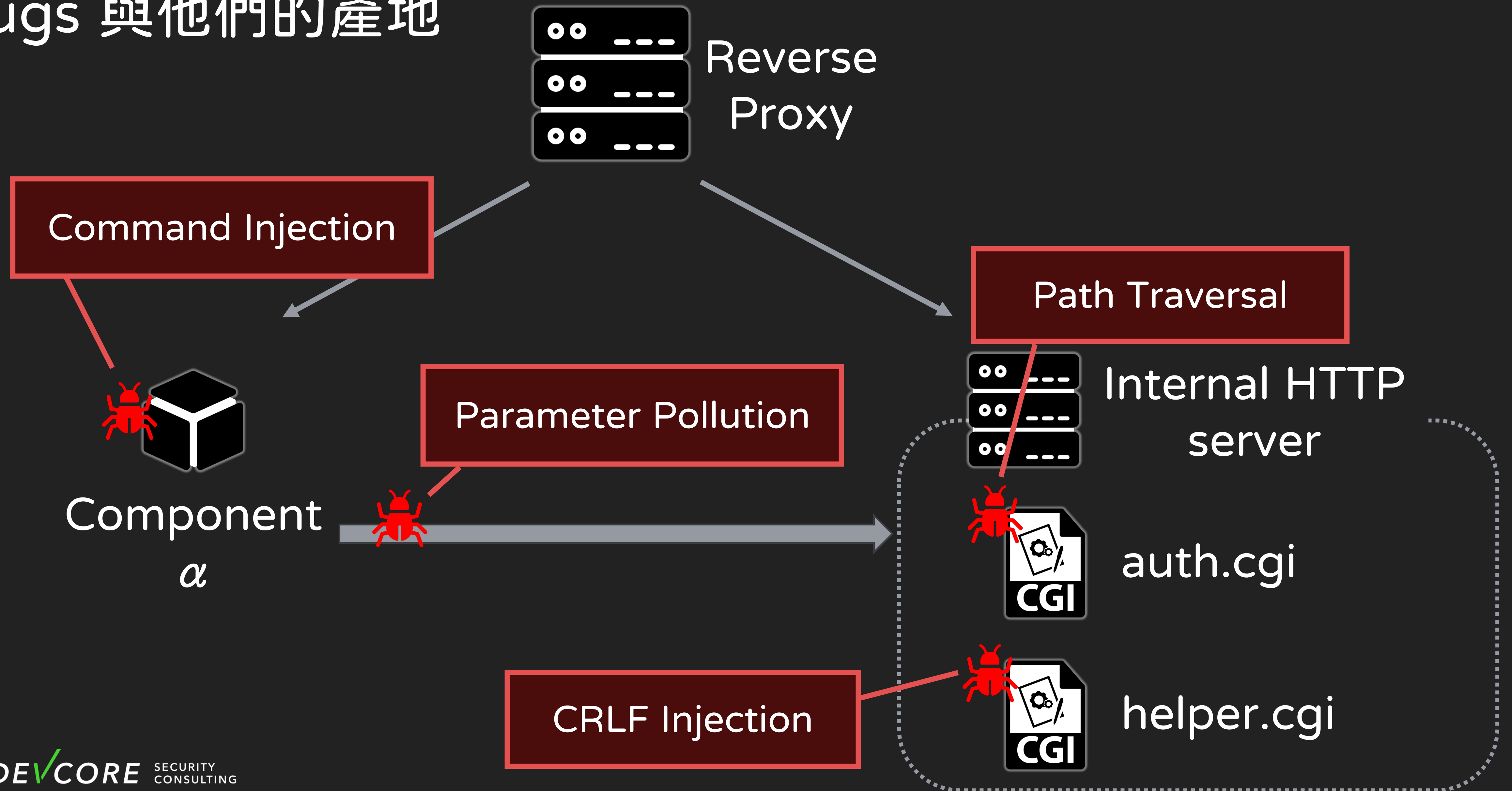


Bug 4 :
"Impossible"
Command Injection

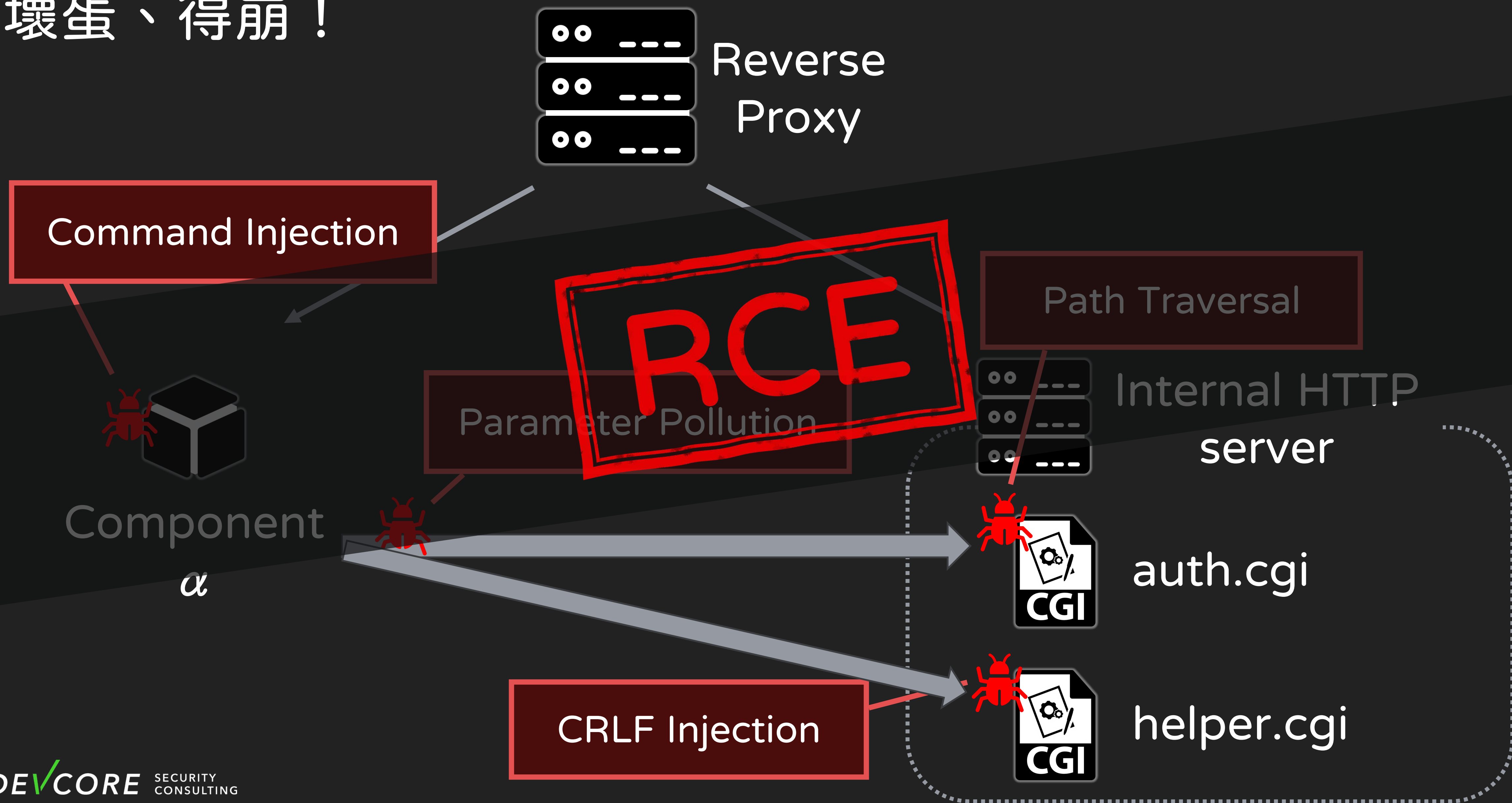
Bug 3 :
CRLF Injection



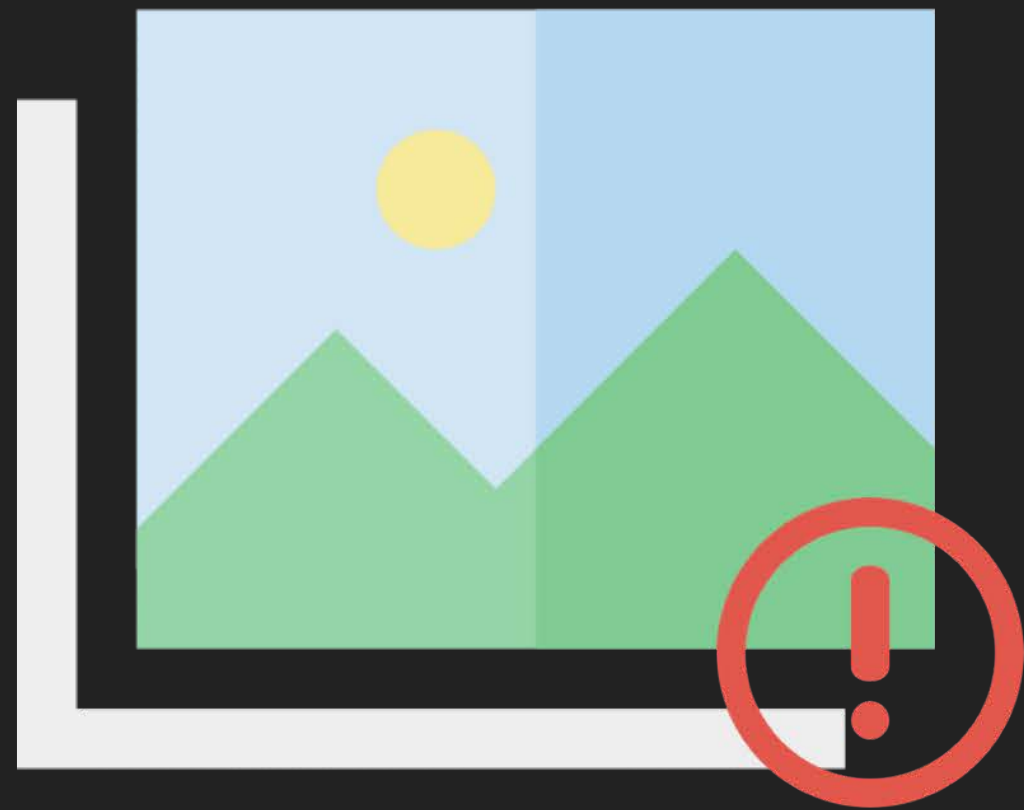
Bugs 與他們的產地



大壞蛋、得崩！

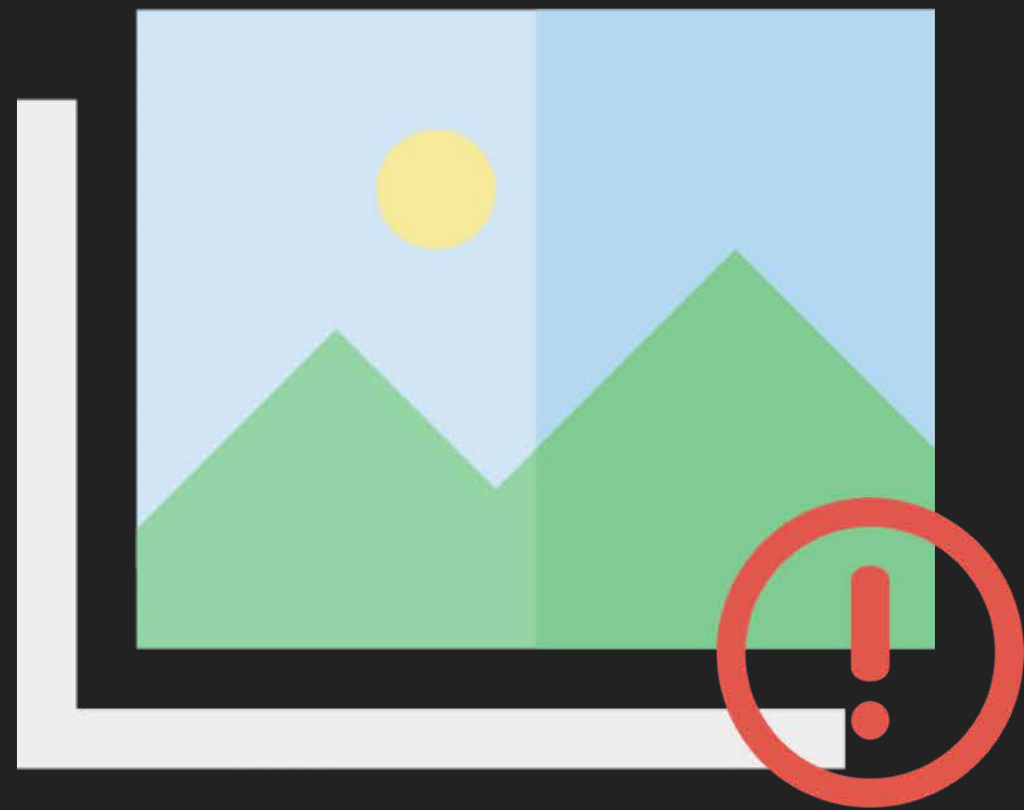


Step 1 : From auth.cgi to helper.cgi



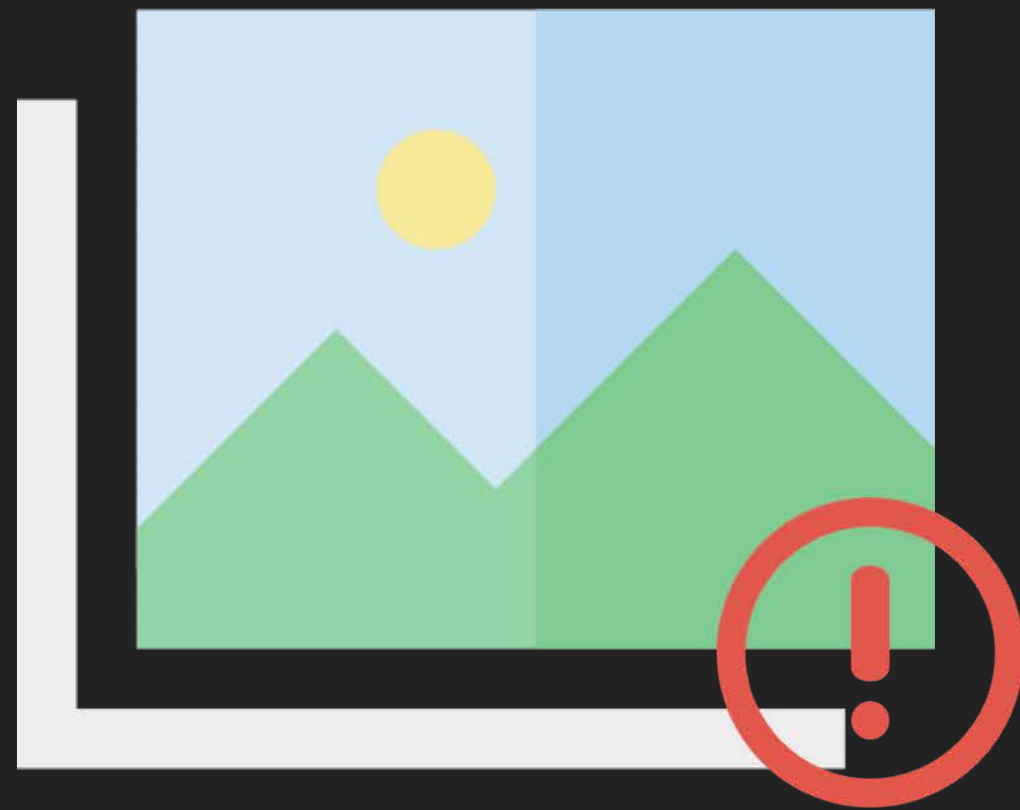
內部演練畫面
僅公布於研討會

Step 2 : Inject parameter for helper.cgi



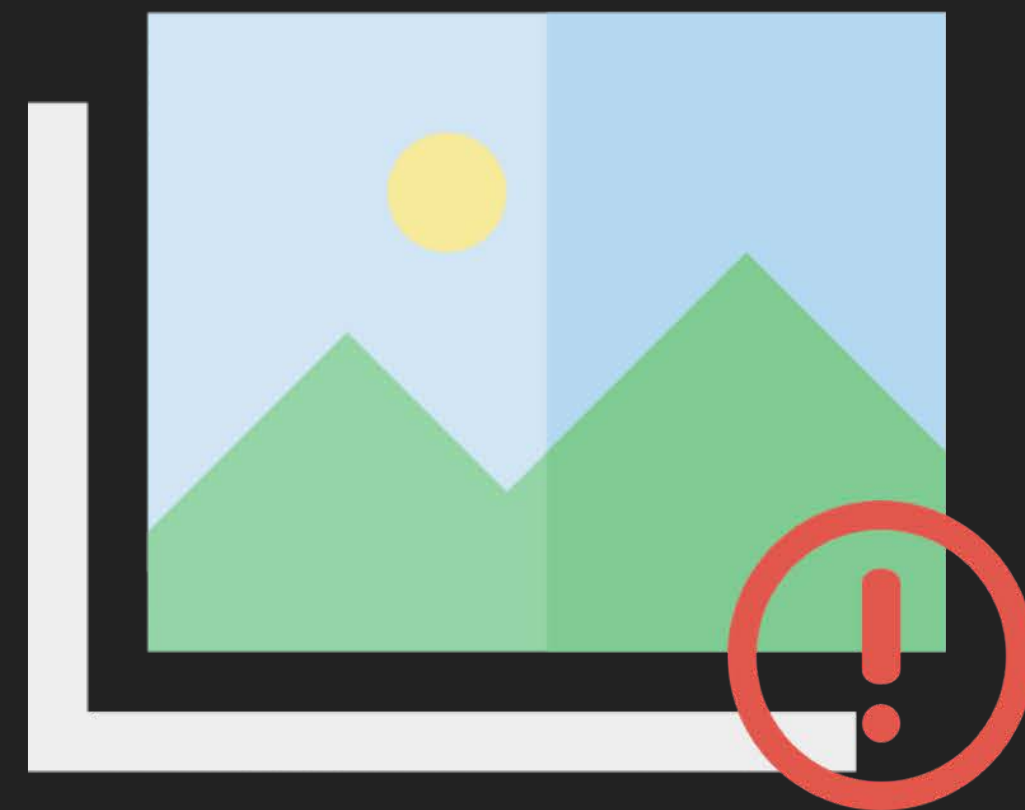
內部演練畫面
僅公布於研討會

Step 3 : Inject CRLF to fake response



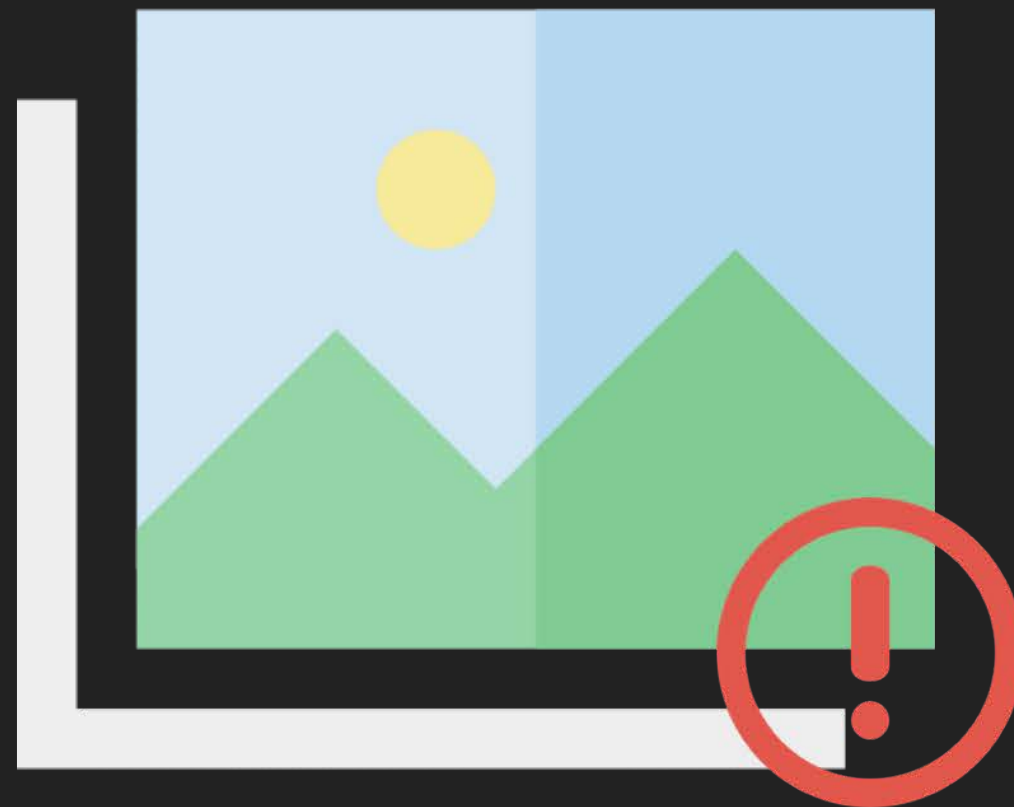
內部演練畫面
僅公布於研討會

Fix path



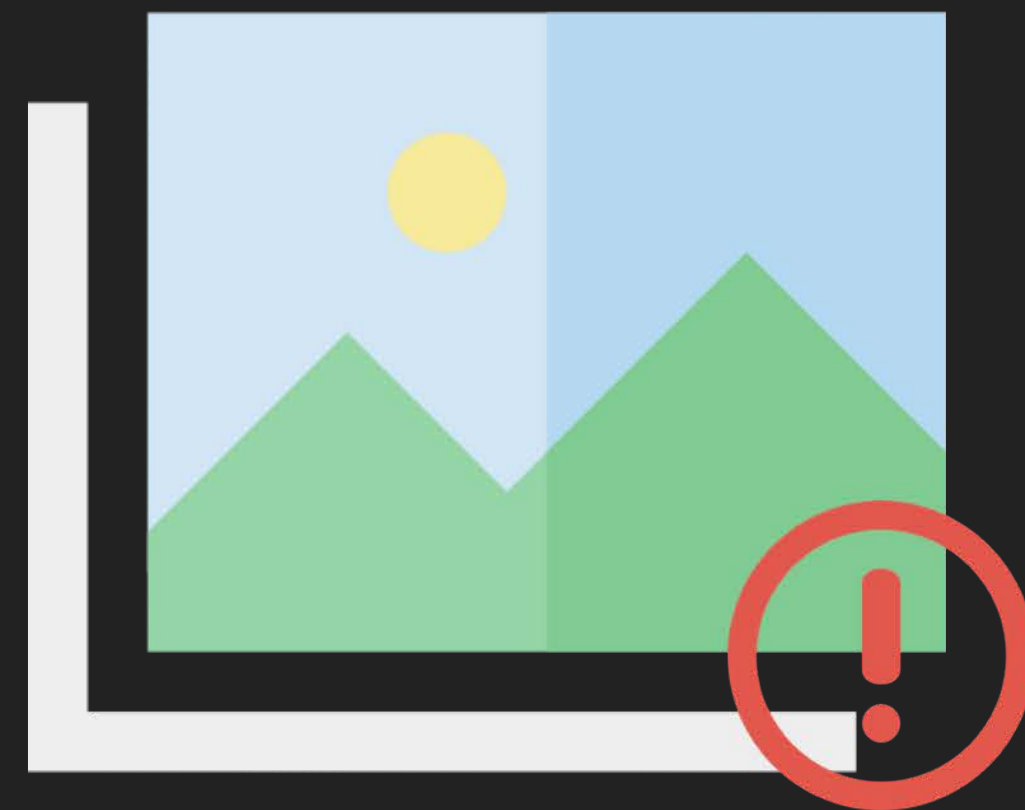
內部演練畫面
僅公布於研討會

Step 4 : Inject malicious command



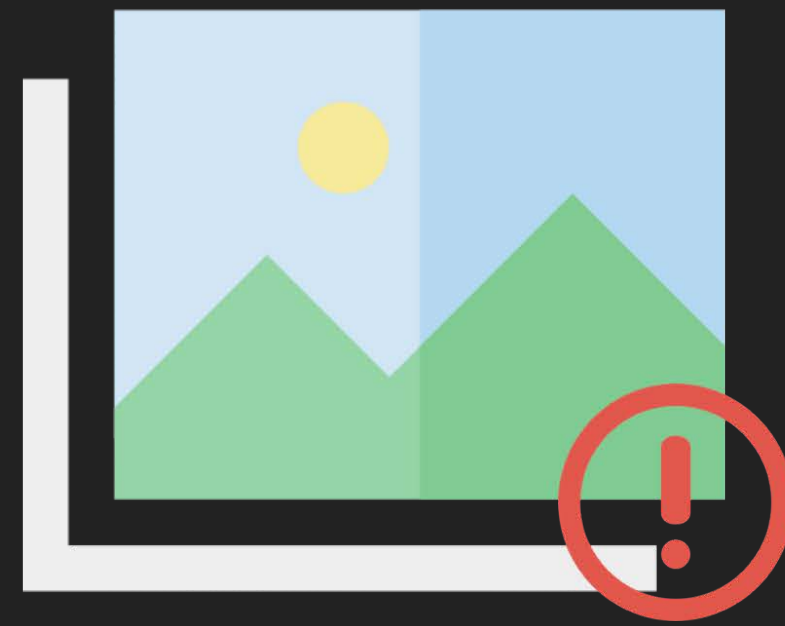
內部演練畫面
僅公布於研討會

Fix Content-Length



內部演練畫面
僅公布於研討會

We got RCE !!



內部演練畫面
僅公布於研討會

《來賓請掌聲鼓勵》

更多更詳盡漏洞在※ 127.0.0.1

Pre-Auth RCE !!

≡

- ✓ 破壞機密性 Confidentiality
- ✓ 破壞完整性 Integrity
- ✓ 破壞可用性 Availability



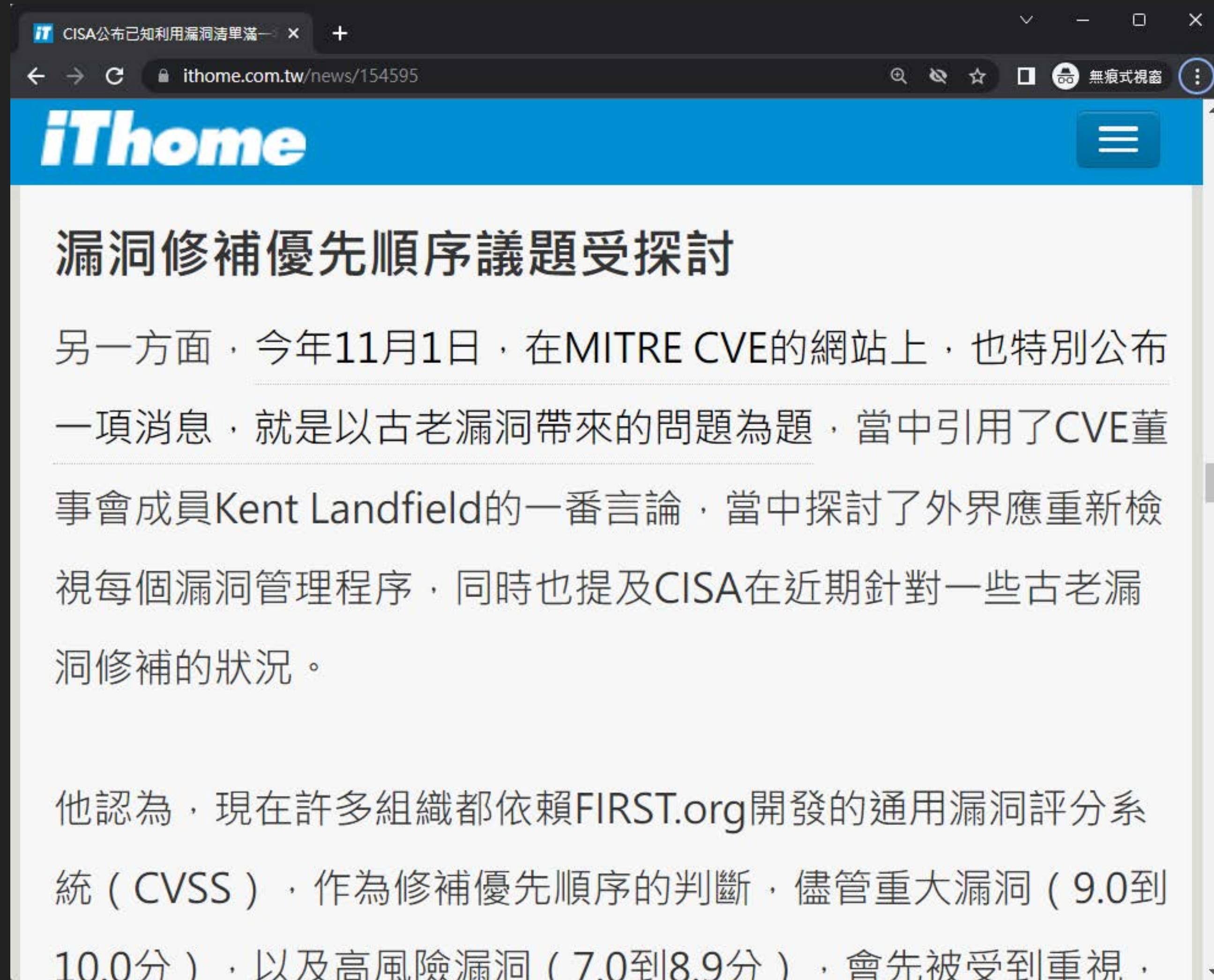
CVSS 8.8 (High)

引申思考

漏洞修補順序議題

- 企業資源有限，人力不足
- CVE 這麼多，怎麼修得完？
- 中風險不急，低風險不用修？





The image is a screenshot of a web browser displaying a news article on the iThome website. The browser's address bar shows the URL [ithome.com.tw/news/154595](https://www.ithome.com.tw/news/154595). The article's title is "漏洞修補優先順序議題受探討" (Vulnerability Patch Priority Issue Discussed). The main text discusses a report from MITRE CVE dated November 1st, focusing on the challenges of patching old vulnerabilities. It quotes Kent Landfield, a member of the CVE Board, who suggests that organizations should re-evaluate their patch management processes. The text also mentions that CISA has recently addressed some of these old vulnerabilities. The article notes that many organizations rely on the CVSS (Common Vulnerability Scoring System) from FIRST.org to determine patch priority, with high-risk vulnerabilities (7.0 to 8.9) and critical ones (9.0 to 10.0) receiving the most attention.

CISA公布已知利用漏洞清單

ithome.com.tw/news/154595

漏洞修補優先順序議題受探討

另一方面，今年11月1日，在MITRE CVE的網站上，也特別公布一項消息，就是以古老漏洞帶來的問題為題，當中引用了CVE董事會成員Kent Landfield的一番言論，當中探討了外界應重新檢視每個漏洞管理程序，同時也提及CISA在近期針對一些古老漏洞修補的狀況。

他認為，現在許多組織都依賴FIRST.org開發的通用漏洞評分系統（CVSS），作為修補優先順序的判斷，儘管重大漏洞（9.0到10.0分），以及高風險漏洞（7.0到8.9分），會先被受到重視，

Reference: <https://www.ithome.com.tw/news/154595>

Known Exploited Vulnerabilities

Known Exploited Vulnerabilities Catalog

Download CSV version
Download JSON version
Download JSON schema
Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin
Back to previous page for background on known exploited vulnerabilities

Show 10 entries Search:

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date
CVE-2022-21587	Oracle	E-Business Suite	Oracle E-Business Suite Unspecified Vulnerability	2023-02-02	Oracle E-Business Suite contains an unspecified vulnerability that allows an unauthenticated attacker with network access via HTTP to compromise Oracle Web Applications	Apply updates per vendor instructions.	2023-02-23

Reference: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

自家開發的服務怎麼辦

- 也只能做滲透跟紅隊了
- 企業可預先規劃修復時程
- 利用駭客經驗評估弱點潛在利用機會
- 有機會找出攻擊鏈，代表漏洞可利用



一起來施展黑魔法吧！



Q&A

