DEVCORE
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

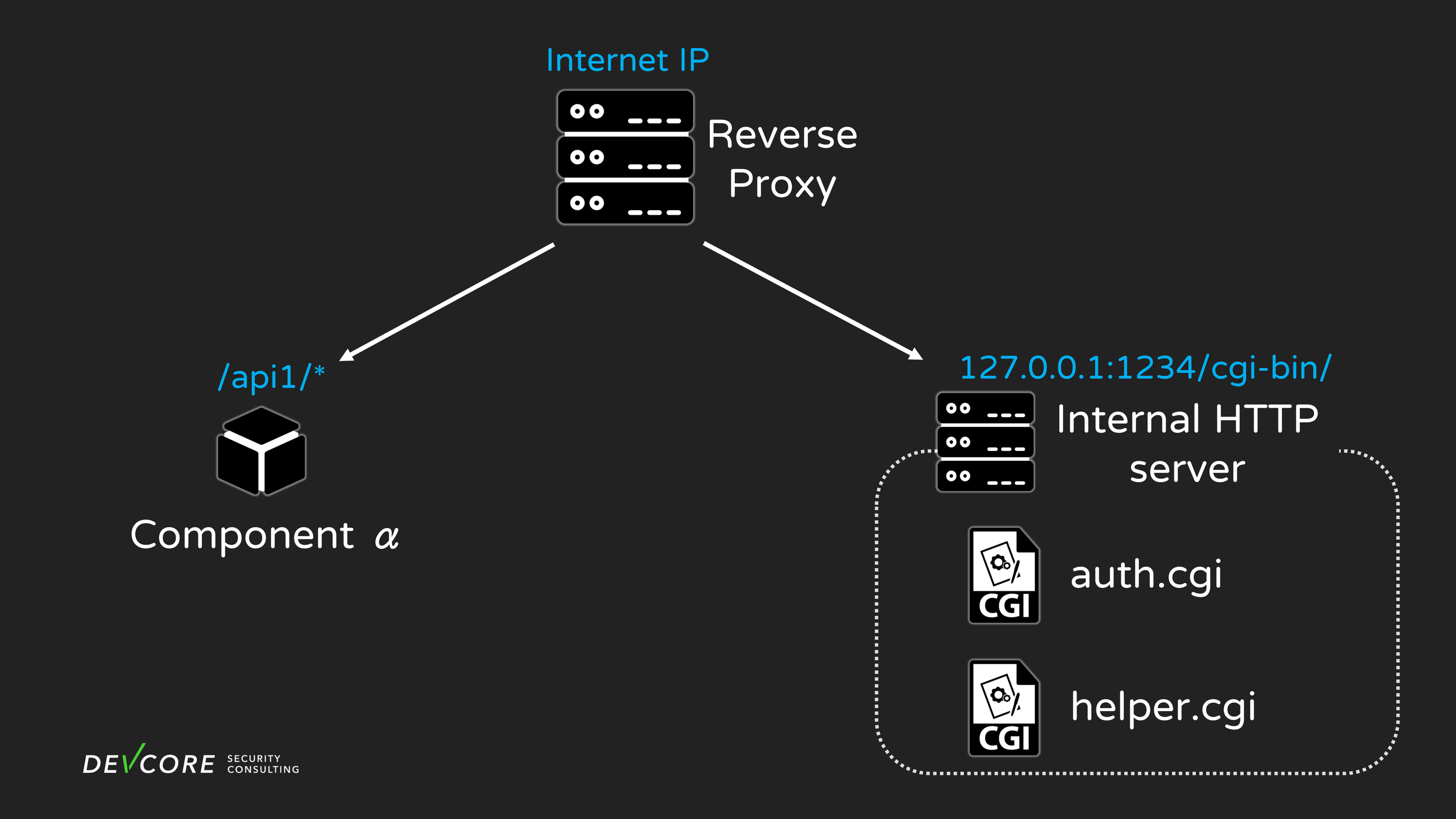
聲明：

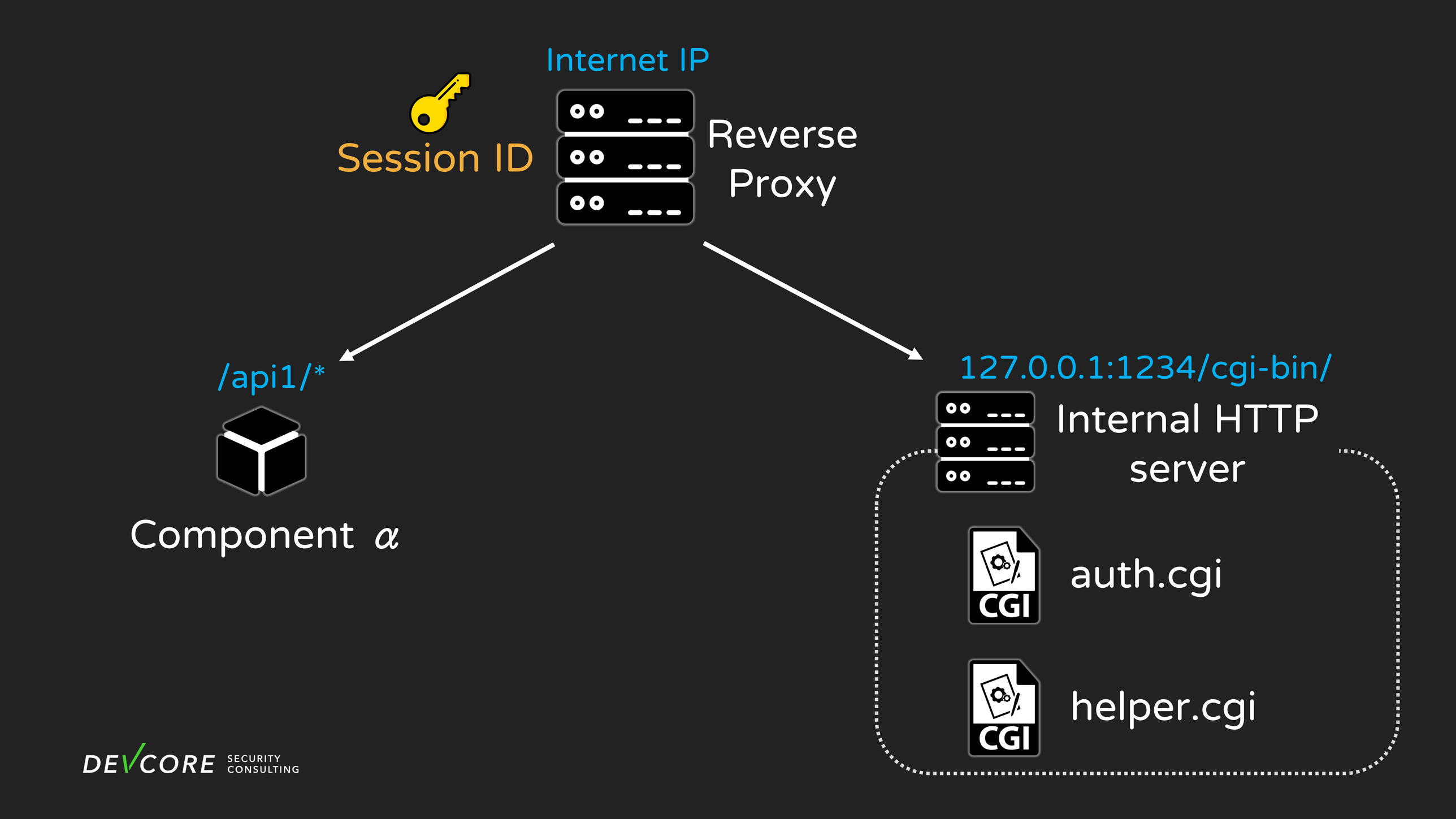
為保護當事人，

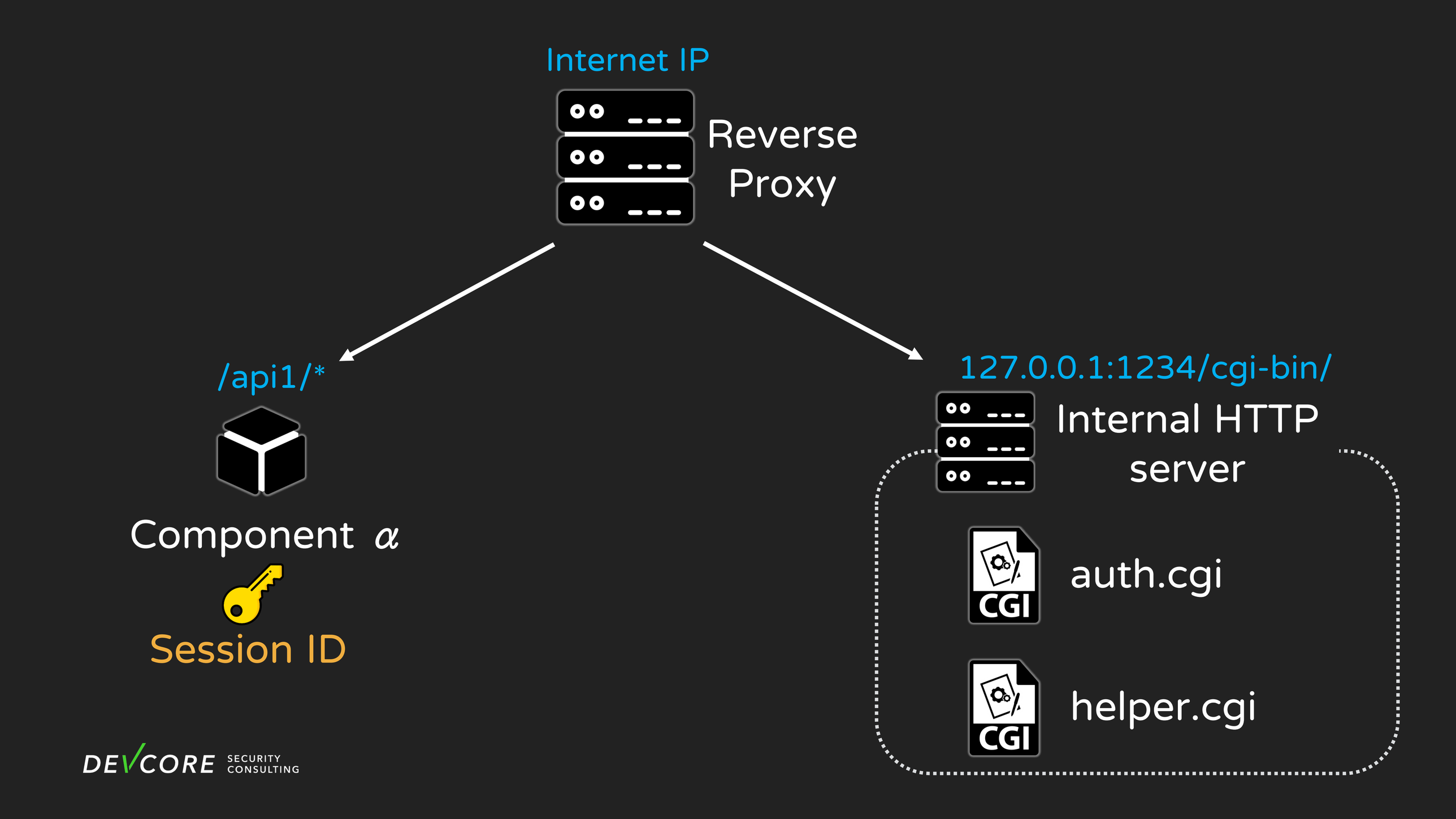
API 路徑與參數名稱均已混淆，

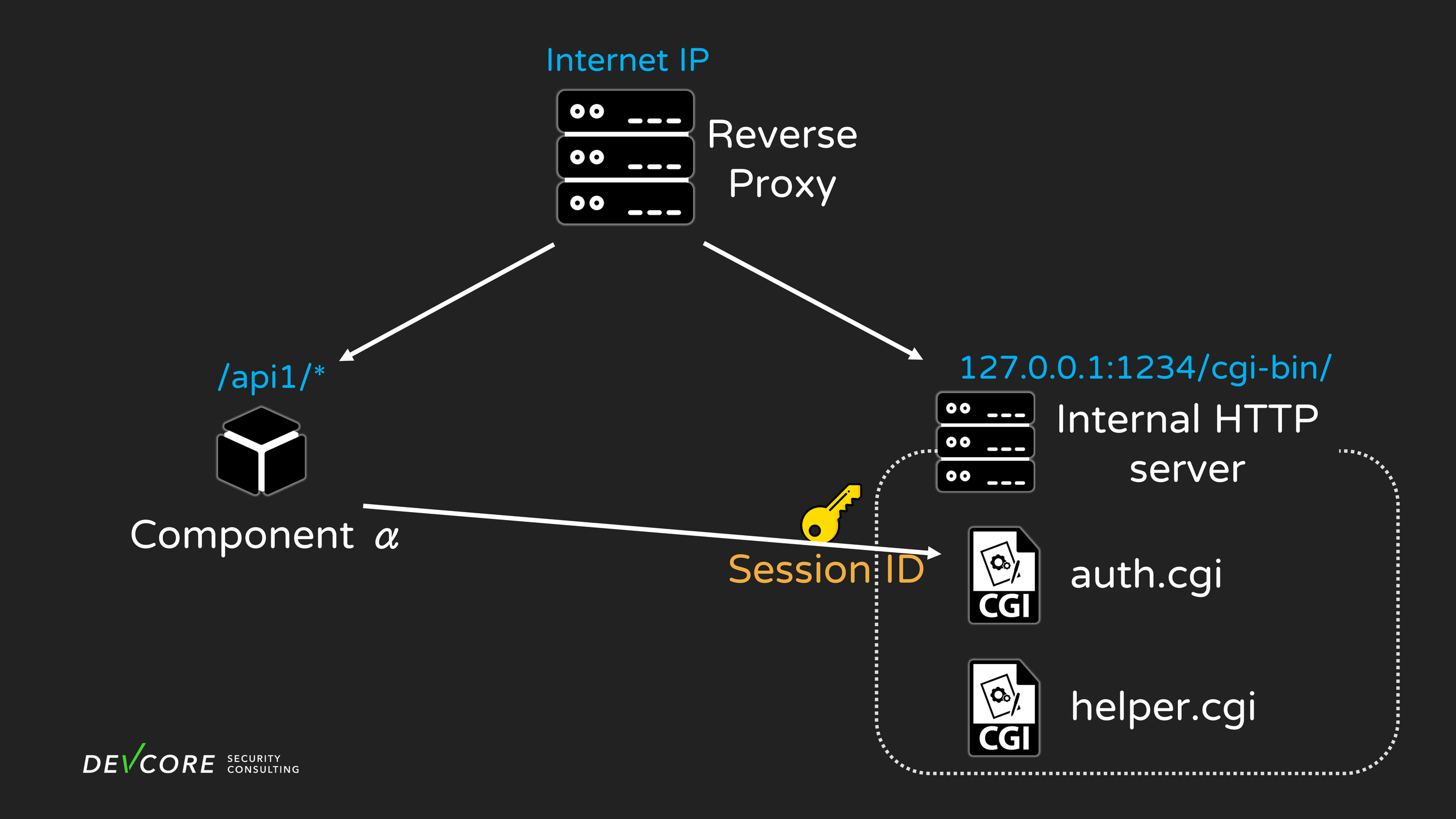
僅保留利用思路

與 exploit chain 邏輯。


Internet IP
Reverse Proxy
/api1/*
Component α
127.0.0.1:1234/cgi-bin/
Internal HTTP server
CGI
auth.cgi
CGI
helper.cgi

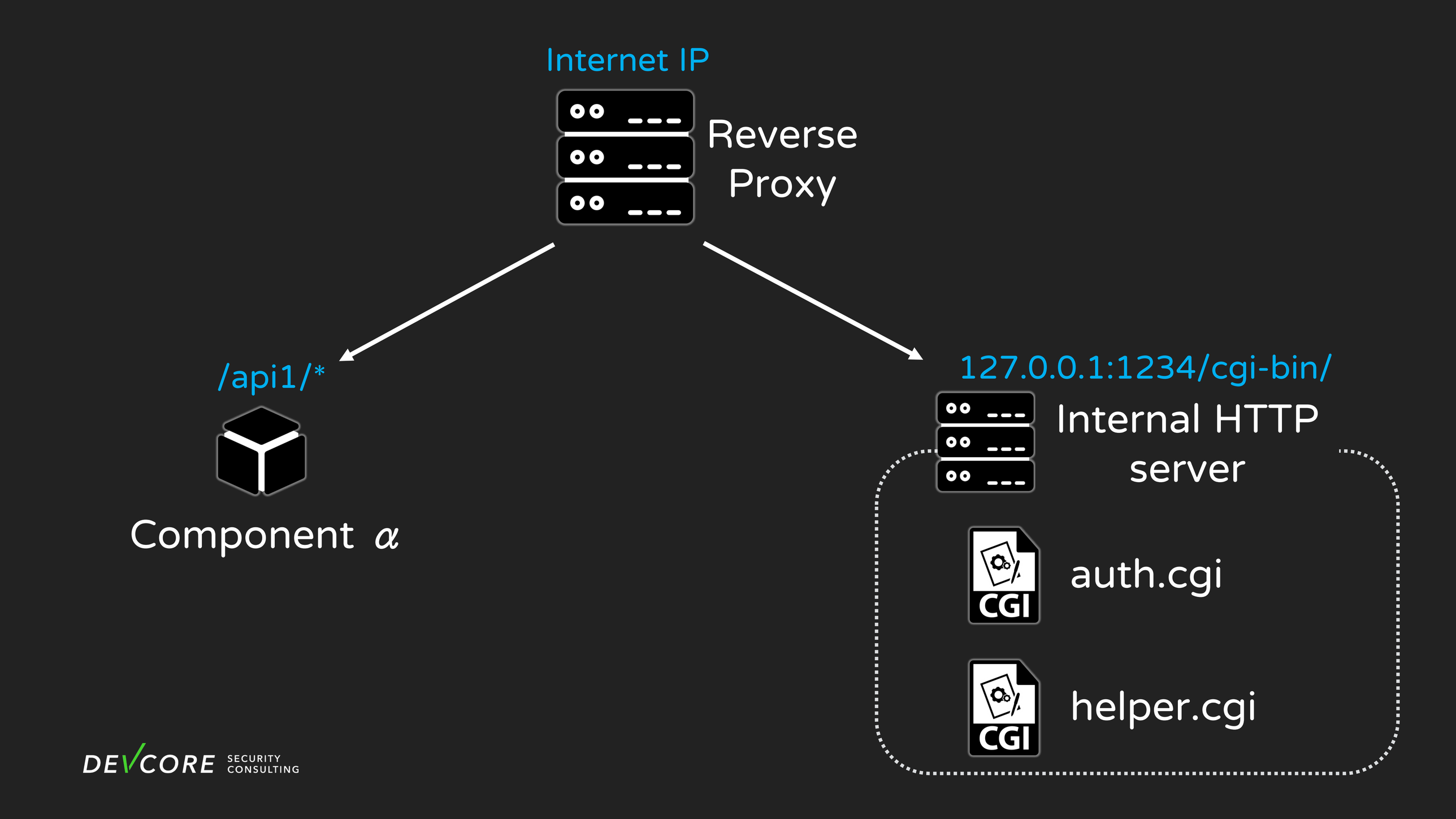

Internet IP
Session ID
Reverse Proxy
/api1/*
Component α
127.0.0.1:1234/cgi-bin/
Internal HTTP server
CGI
auth.cgi
CGI
helper.cgi

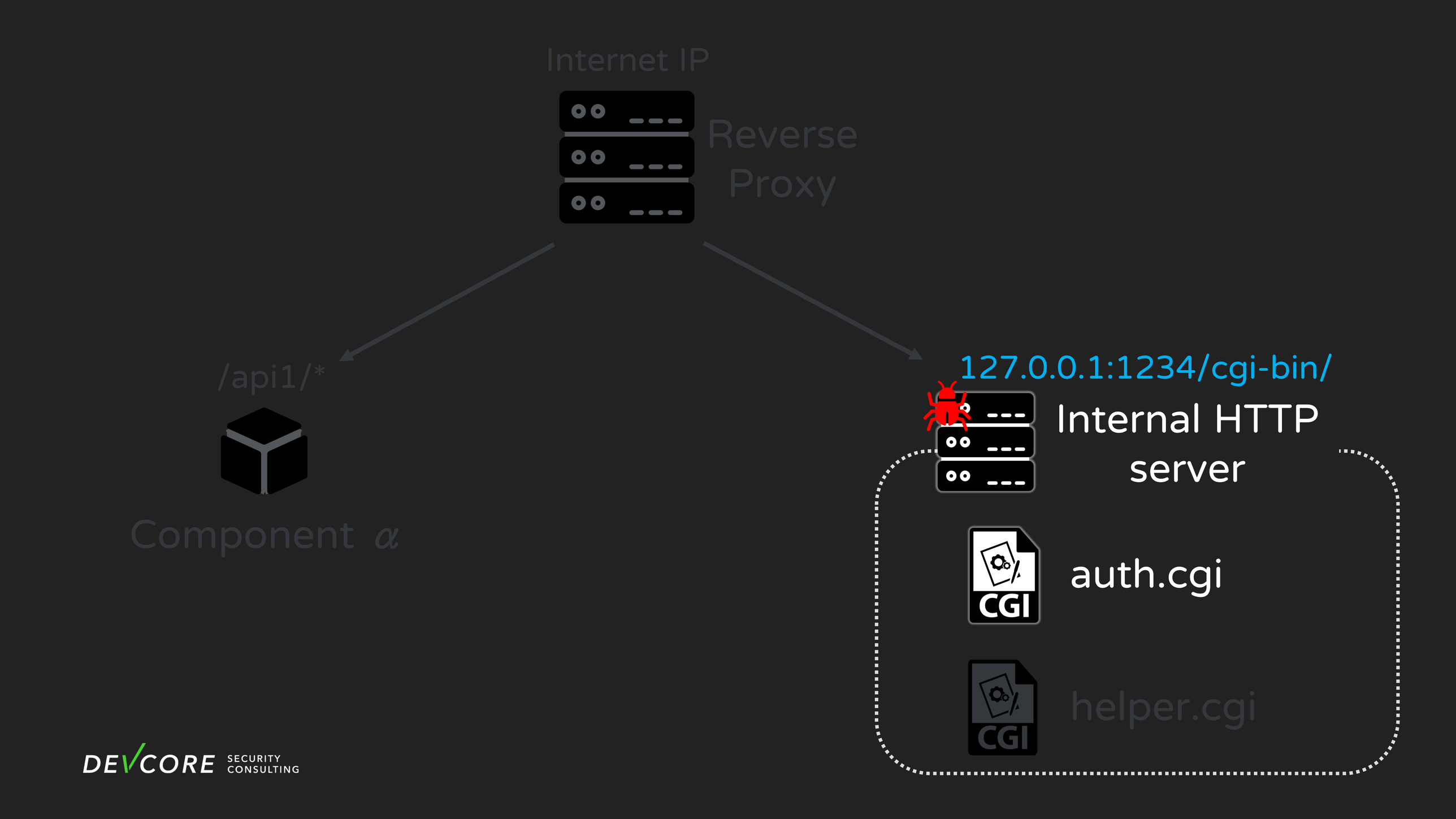

Internet IP
Reverse Proxy
/api1/*
Component α
Session ID
127.0.0.1:1234/cgi-bin/
Internal HTTP server
auth.cgi
helper.cgi
CGI
CGI


Internet IP
Reverse Proxy
/api1/*
Component α
127.0.0.1:1234/cgi-bin/
Internal HTTP server
Session ID
CGI
auth.cgi
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
CGI
auth.cgi
CGI
helper.cgi


Internet IP
Reverse Proxy
/api1/*
Component α
127.0.0.1:1234/cgi-bin/
Internal HTTP server
auth.cgi
helper.cgi
CGI
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

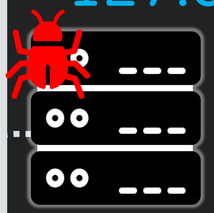
http://127.0.0.1:1234
/cgi-bin/auth.cgi?sid=ab/../index.cgi

Path

Query String

Component α

127.0.0.1:1234/cgi-bin/



Internal HTTP server

auth.cgi

helper.cgi

DEVCORE SECURITY CONSULTING

Internet IP

Reverse

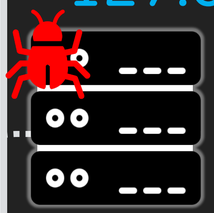
Unintended

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

Path

Component α

127.0.0.1:1234/cgi-bin/



Internal HTTP server

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

auth.cgi

helper.cgi

DEVCORE SECURITY CONSULTING

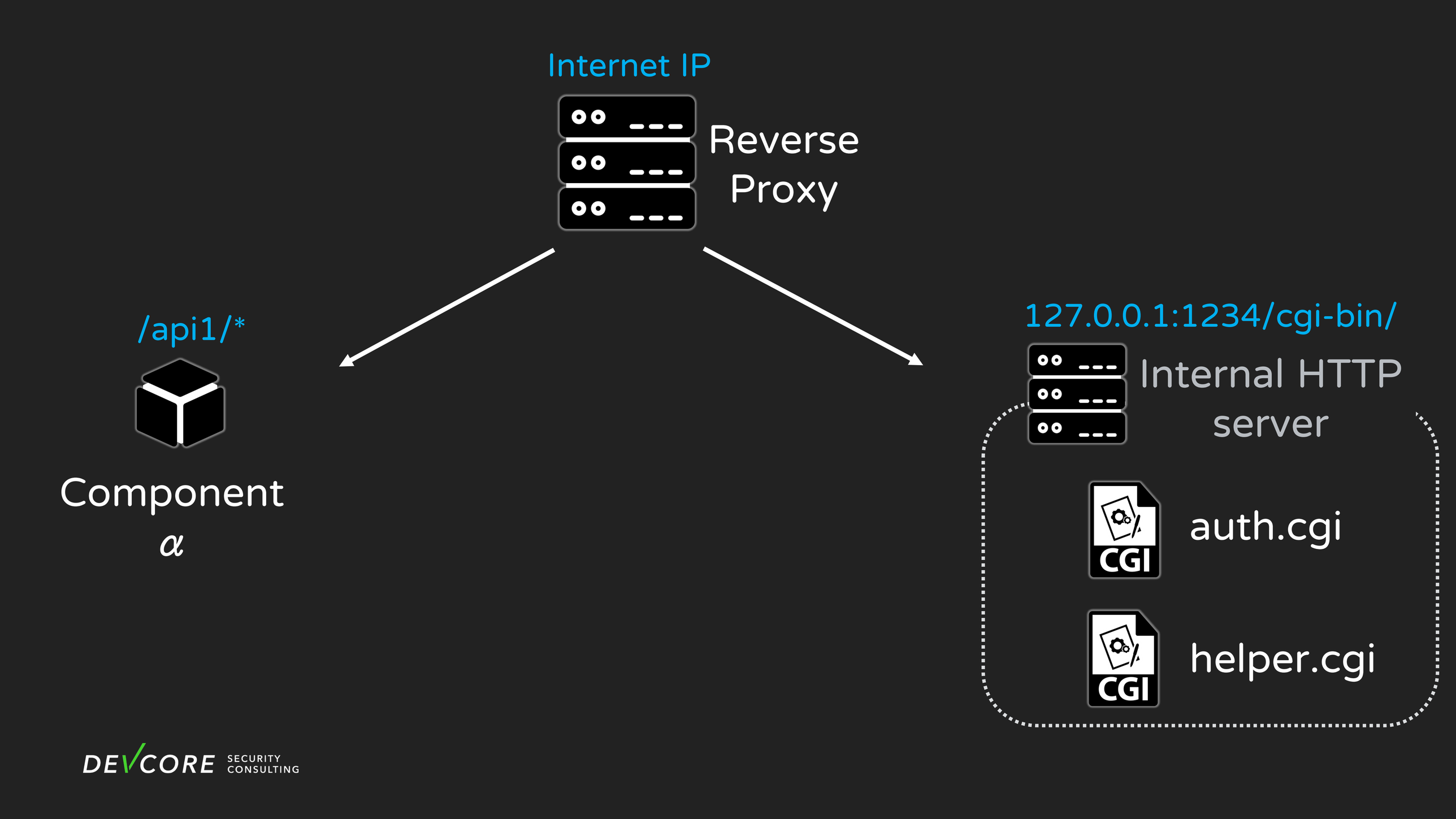
那 Attacker 可以做什麼？

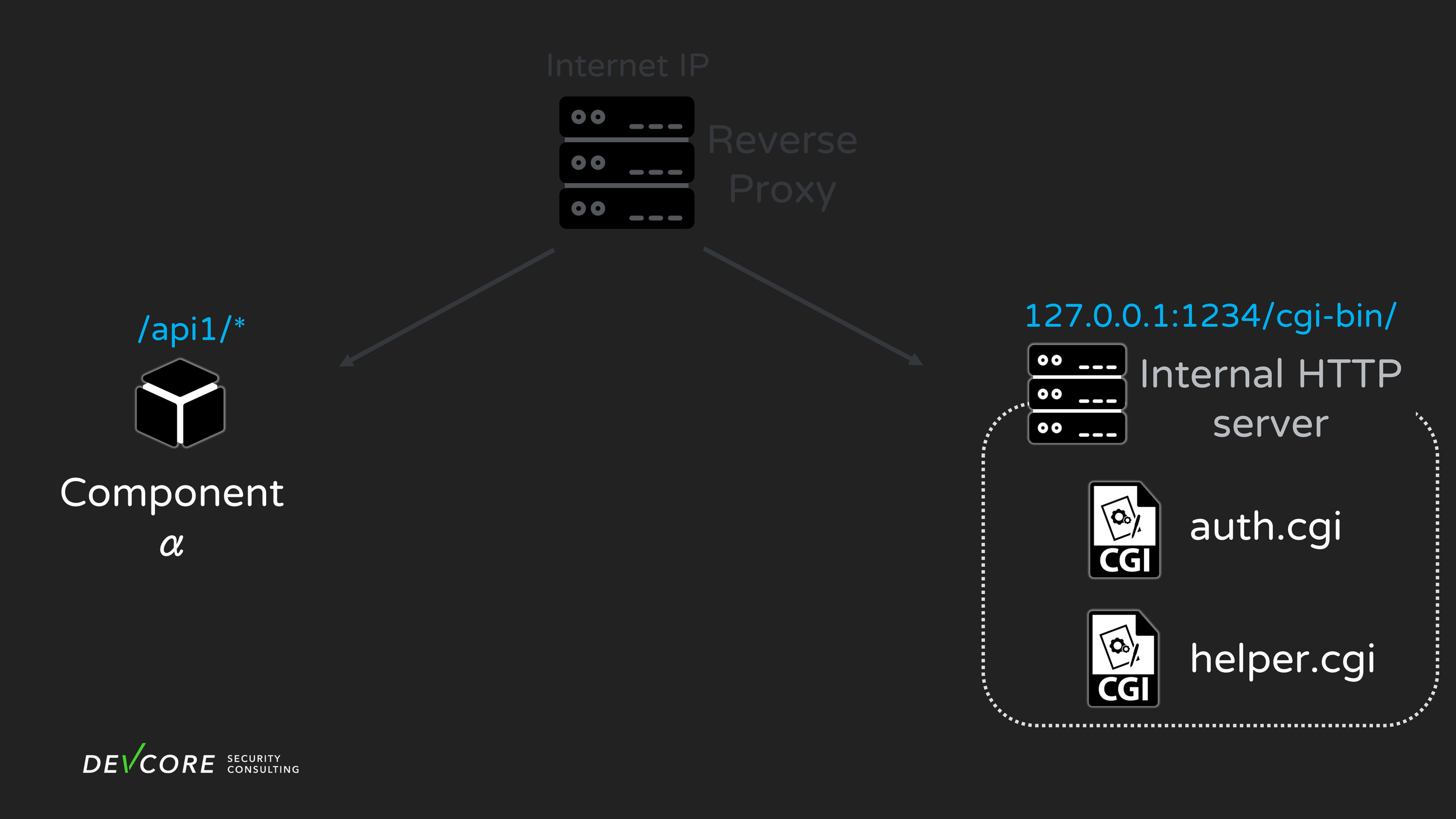
✗ 破壞機密性 Confidentiality

✗ 破壞完整性 Integrity

✗ 破壞可用性 Availability


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
CGI
CGI


Internet IP
Reverse Proxy
/api1/*
Component α
127.0.0.1:1234/cgi-bin/
Internal HTTP server
auth.cgi
helper.cgi
CGI
CGI

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

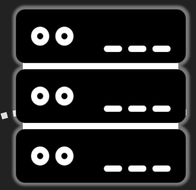
Internet IP

Reverse Proxy

/api1/*

Component
α

127.0.0.1:1234/cgi-bin/



Internal HTTP server

auth.cgi

helper.cgi

DEVCORE SECURITY CONSULTING

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

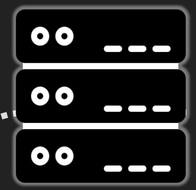
Internet IP

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
```

DEVCORE SECURITY CONSULTING

Internet IP

Expectation

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

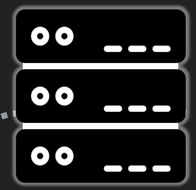
/api1/*

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

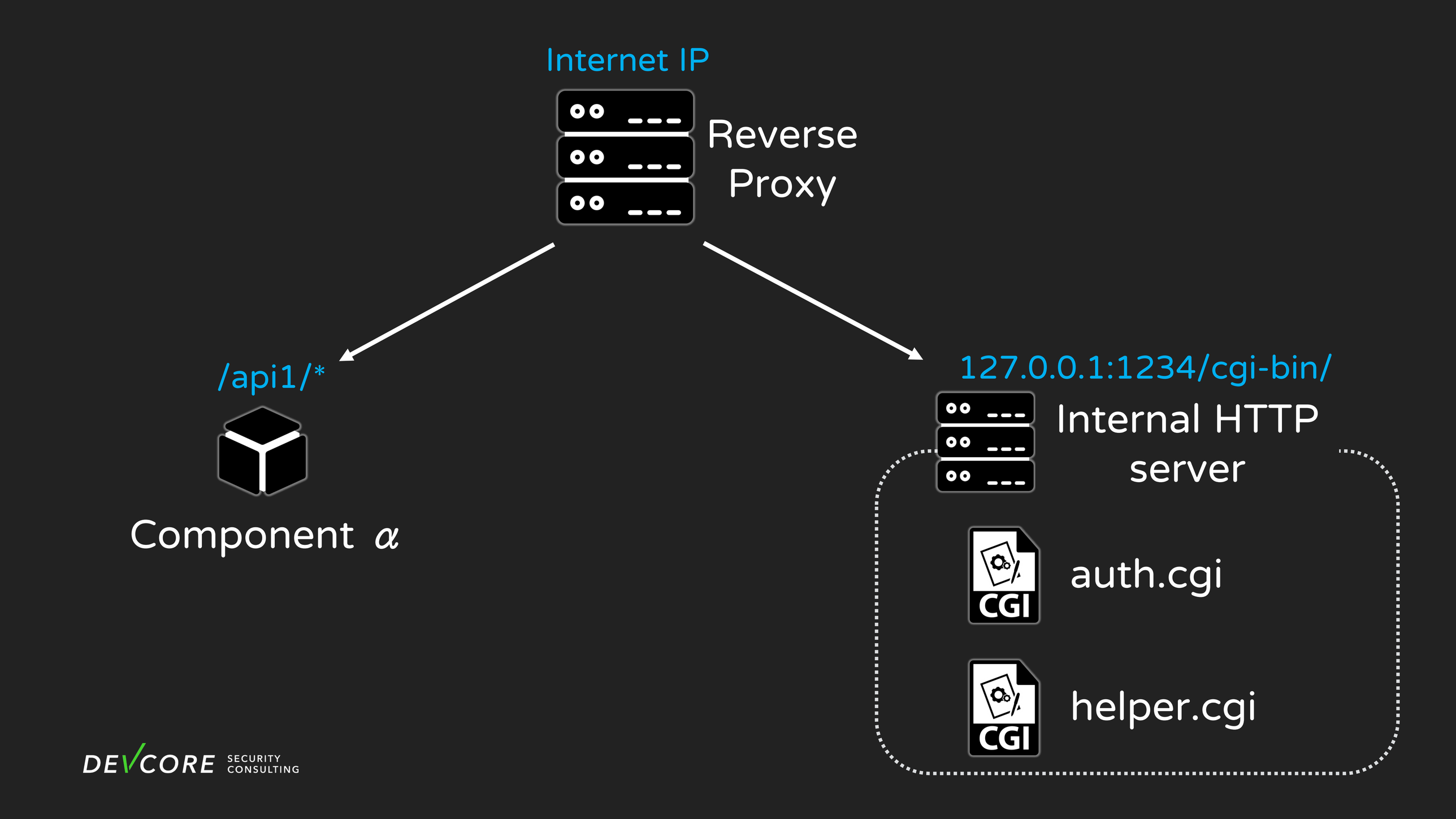
那 Attacker 可以做什麼？

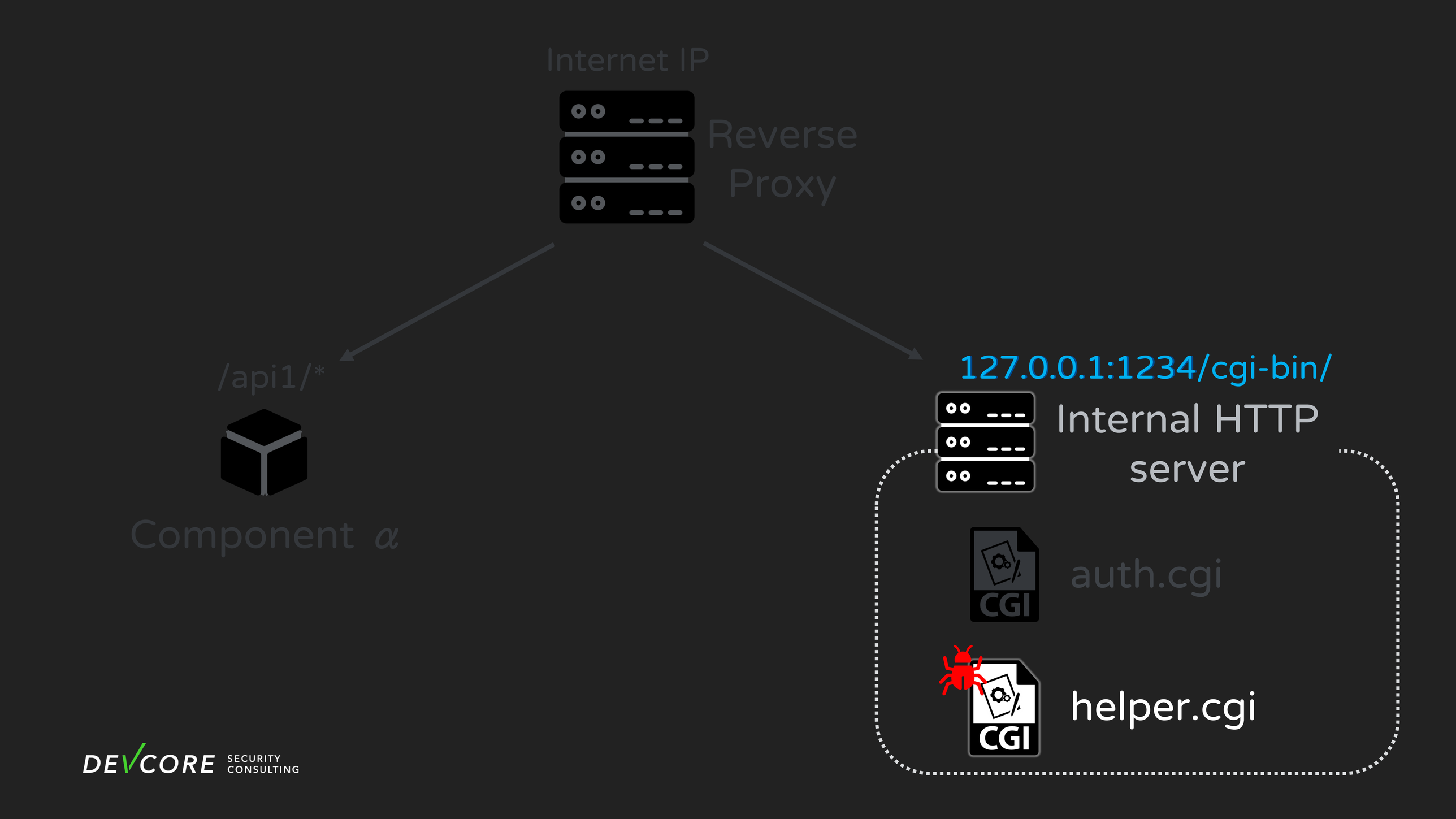
✗ 破壞機密性 Confidentiality

✗ 破壞完整性 Integrity

✗ 破壞可用性 Availability

Bug 3 :
CRLF Injection


Internet IP
Reverse Proxy
/api1/*
Component α
127.0.0.1:1234/cgi-bin/
Internal HTTP server
CGI
auth.cgi
CGI
helper.cgi


Internet IP
Reverse Proxy
/api1/*
Component α
127.0.0.1:1234/cgi-bin/
Internal HTTP server
CGI
auth.cgi
CGI
helper.cgi

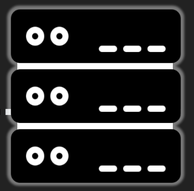
Internet IP

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

/api1/*

```
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

DEVCORE SECURITY CONSULTING

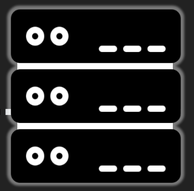
Internet IP

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

/api1/*

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

127.0.0.1:1234/cgi-bin/

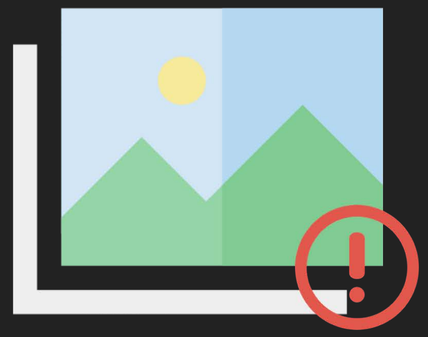


Internal HTTP server

auth.cgi

helper.cgi

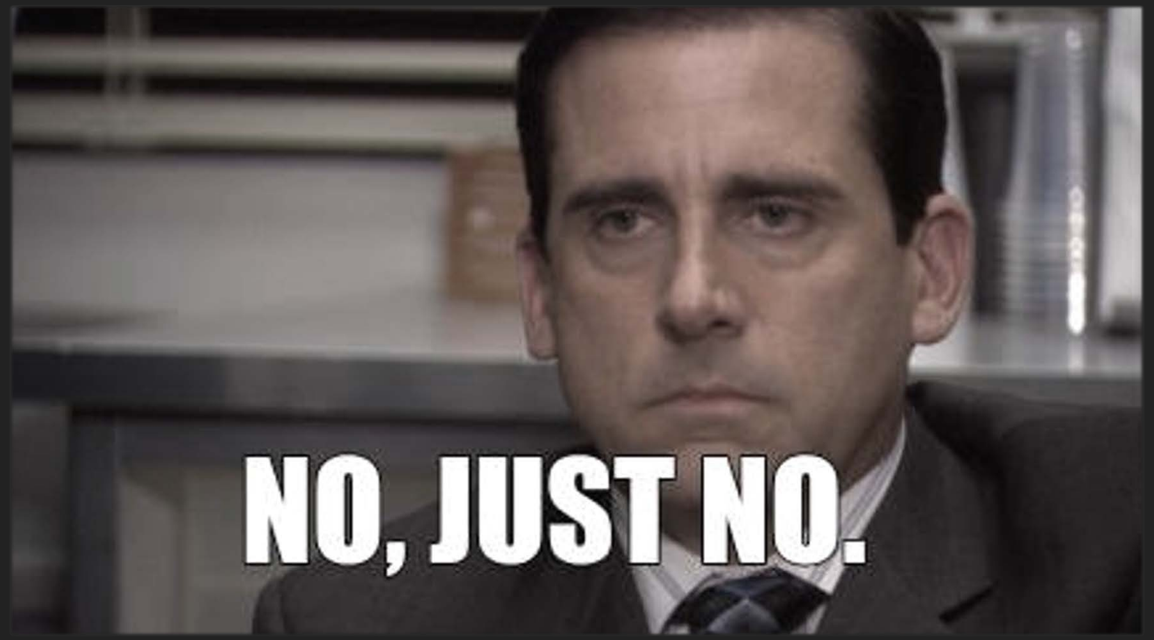
我們可以用來串 XSS？



內部演練畫面
僅公布於研討會

有料ㄛ！

says :



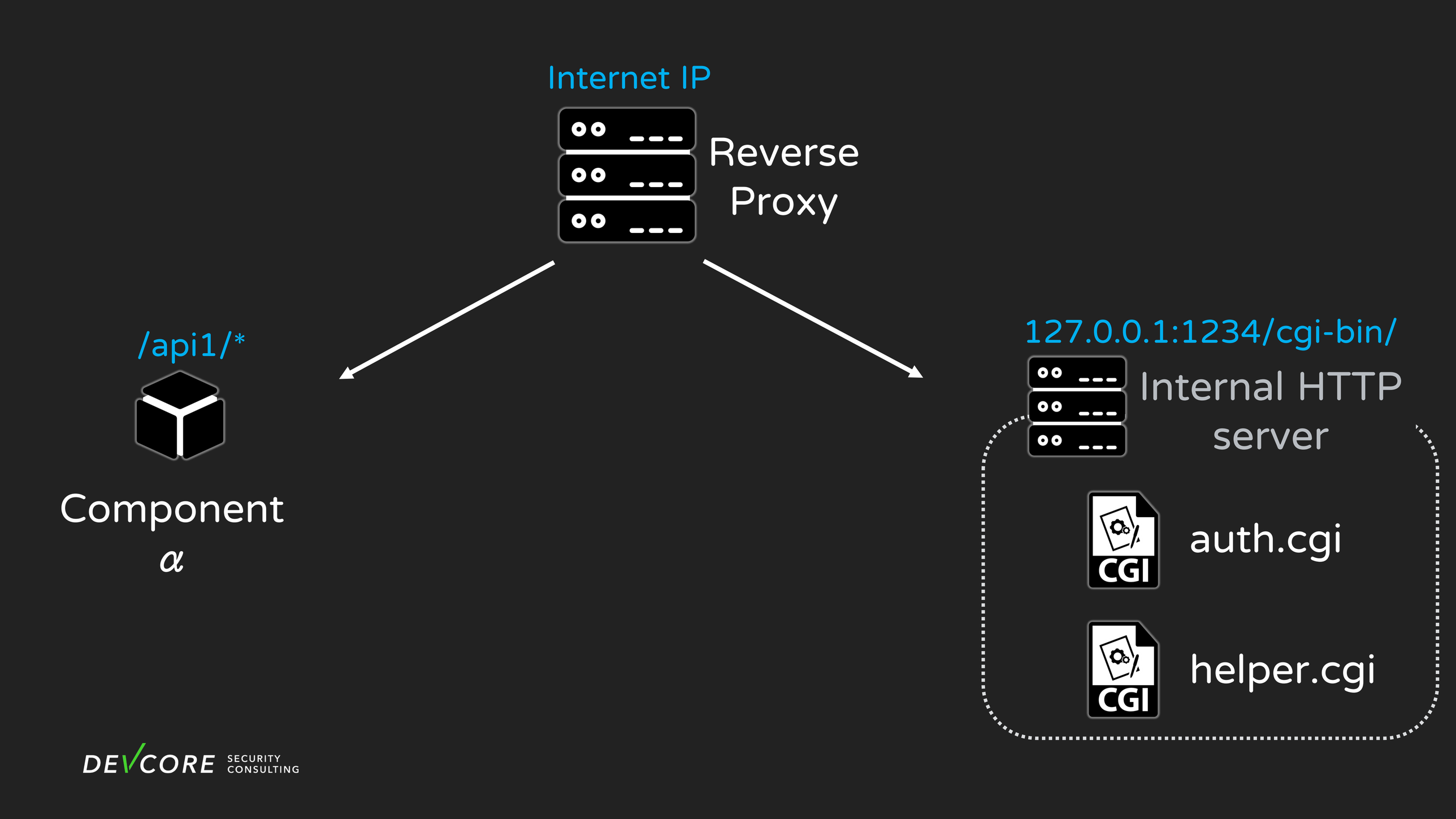
所以 Attacker 可以做 ..

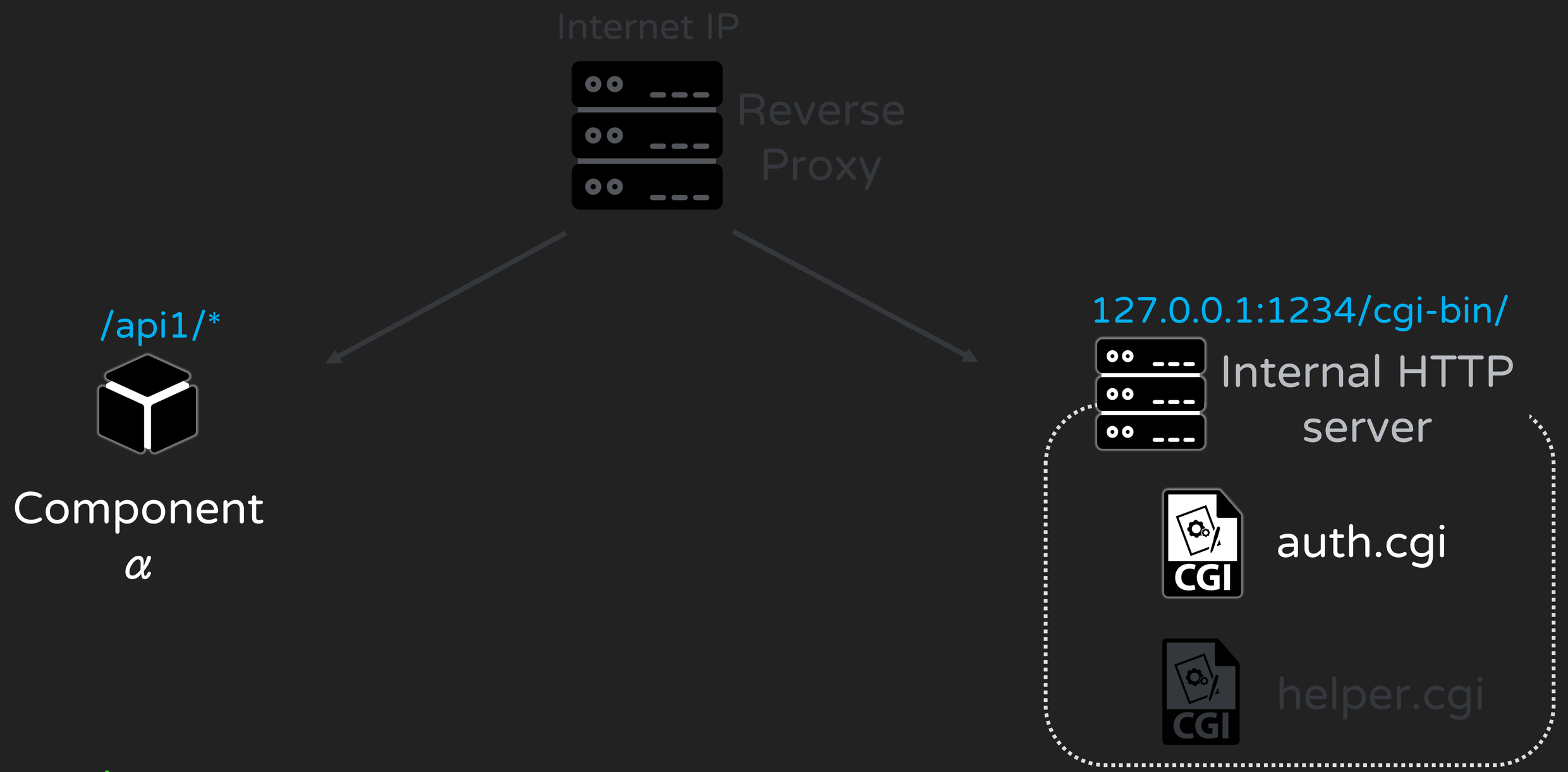
✗ 破壞機密性 Confidentiality

✗ 破壞完整性 Integrity

✗ 破壞可用性 Availability

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
CGI
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
```

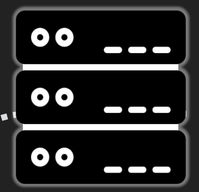
Internet IP

Reverse Proxy

/api1/*

Component
α

127.0.0.1:1234/cgi-bin/

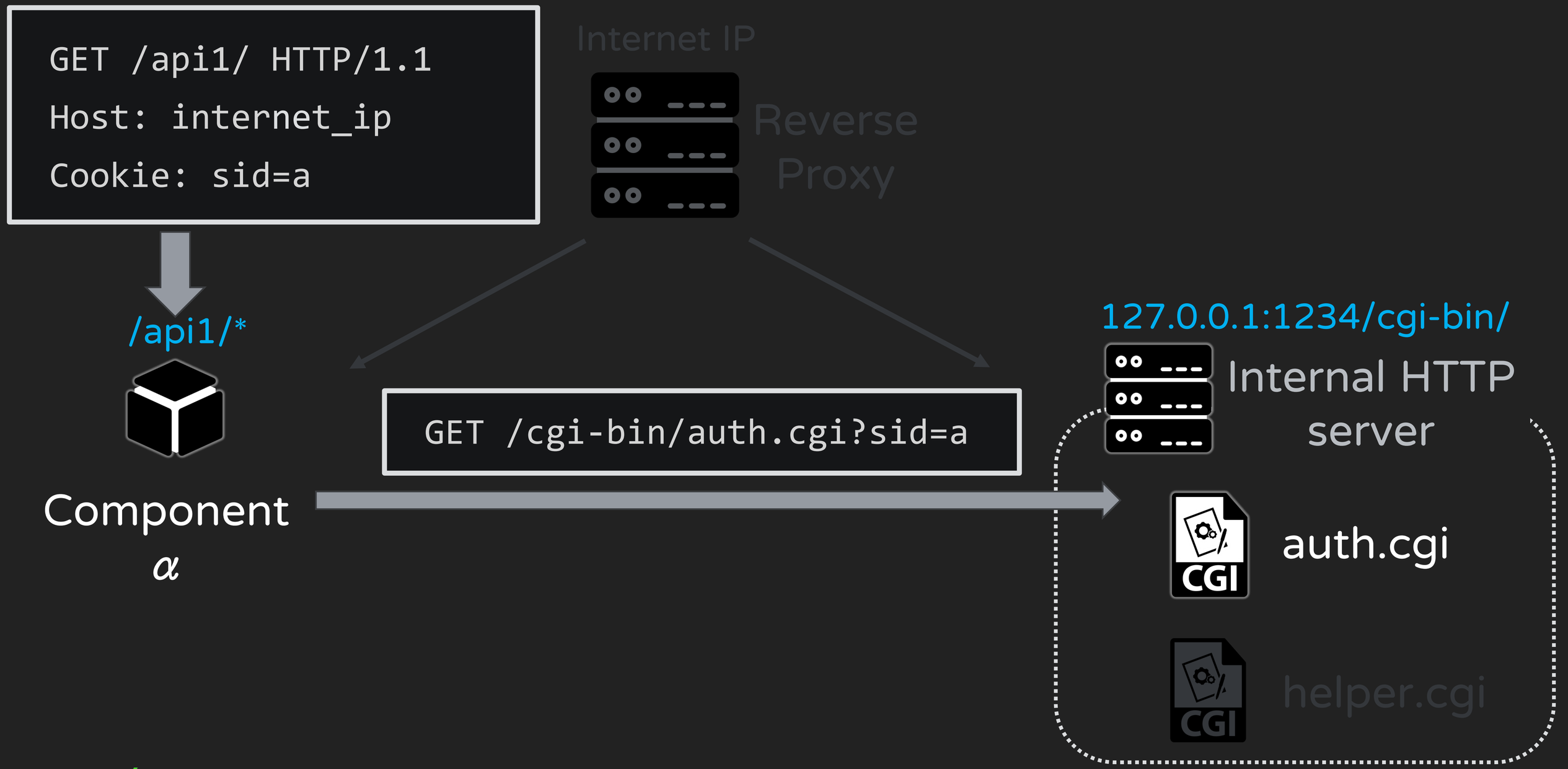


Internal HTTP server

auth.cgi

helper.cgi

DEVCORE SECURITY CONSULTING


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
CGI
CGI

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

Internet IP

Reverse Proxy

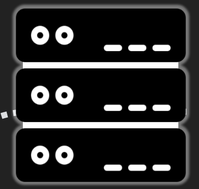
/api1/*

Component
α

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

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

127.0.0.1:1234/cgi-bin/

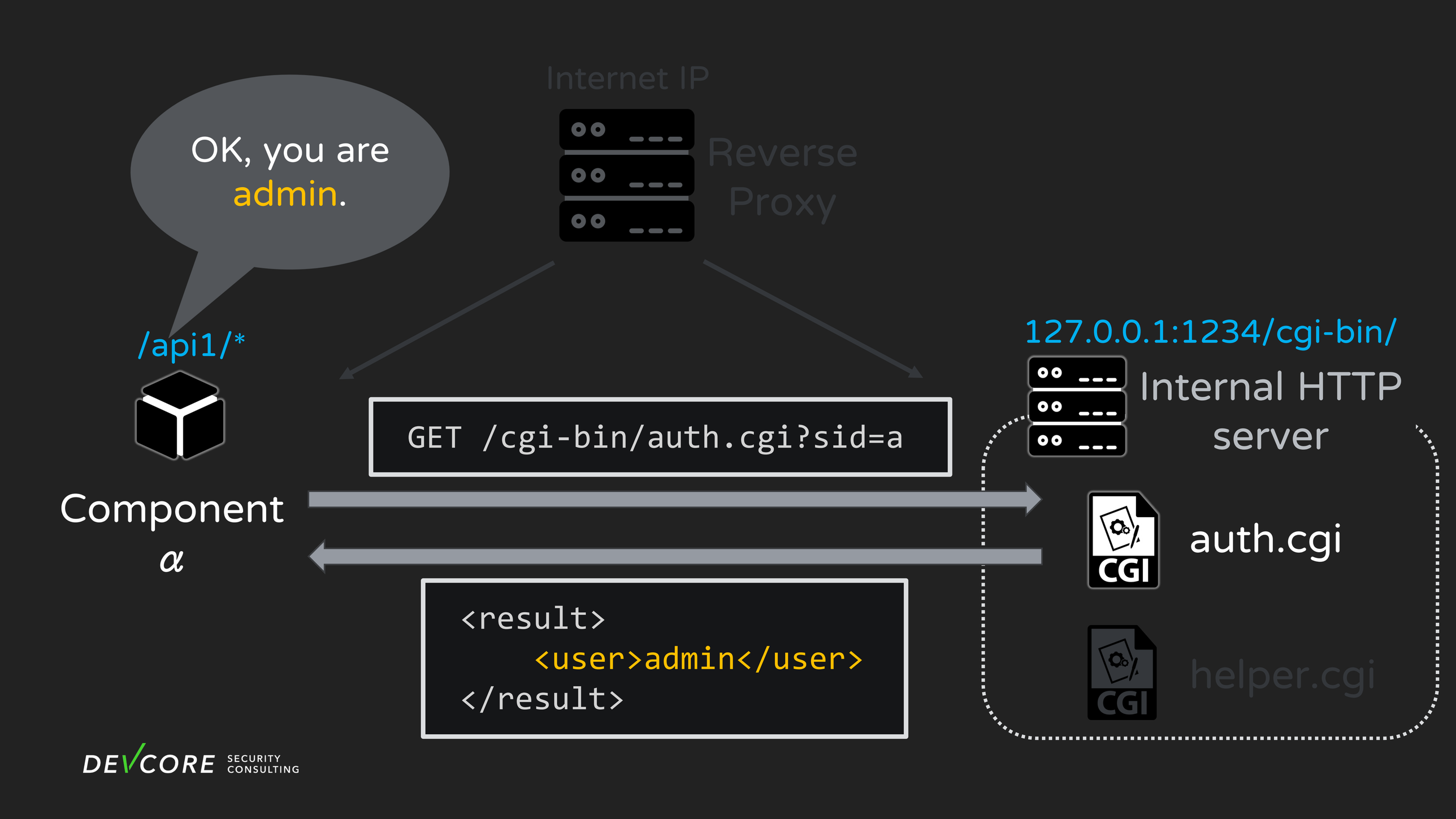


Internal HTTP server

auth.cgi

helper.cgi

DEVCORE SECURITY CONSULTING


Internet IP
Reverse Proxy
OK, you are admin.
/api1/*
Component α
GET /cgi-bin/auth.cgi?sid=a
<result>
<user>admin</user>
</result>
127.0.0.1:1234/cgi-bin/
Internal HTTP server
auth.cgi
helper.cgi
CGI
CGI

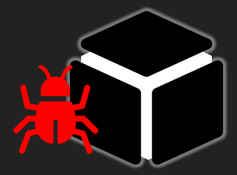
Internet IP

Reve
Prox

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！

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

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)


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)

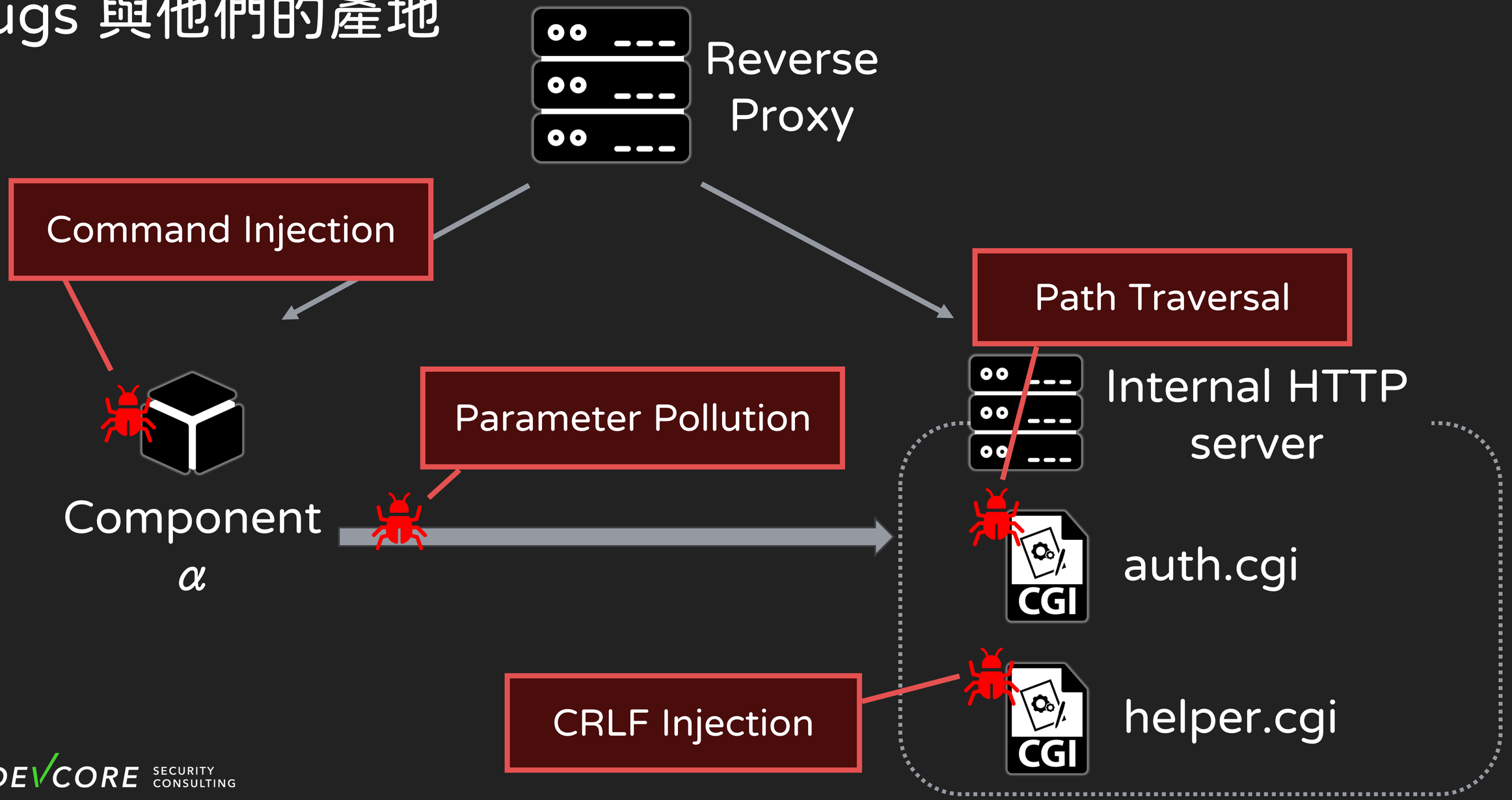
Turning Harmless Bugs into Vulnerability

DEVCORE SECURITY CONSULTING

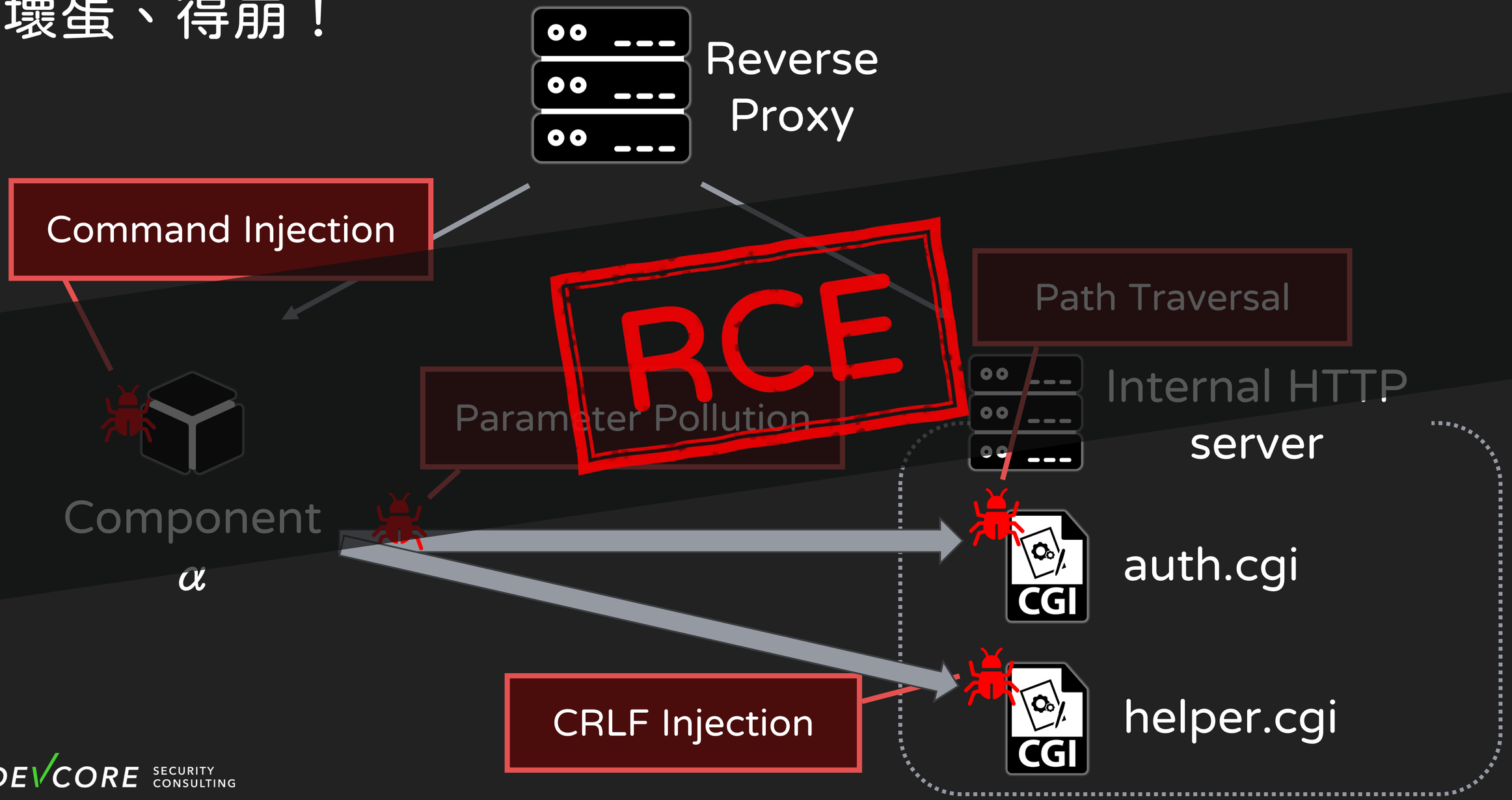
Bug 3 :
CRLF Injection

Bug 4 :
Impossible”
mand Injection

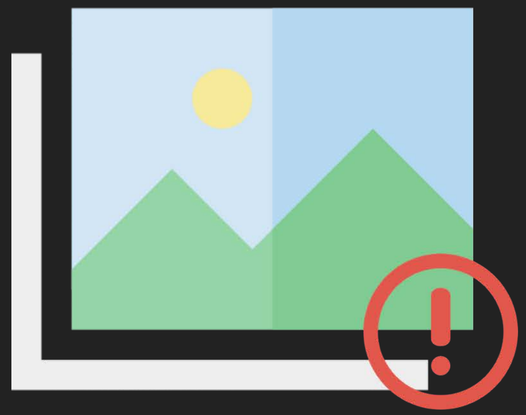
Bugs 與他們的產地


Reverse Proxy
Command Injection
Path Traversal
Parameter Pollution
Internal HTTP server
Component α
auth.cgi
CRLF Injection
helper.cgi
CGI
CGI

大壞蛋、得崩！

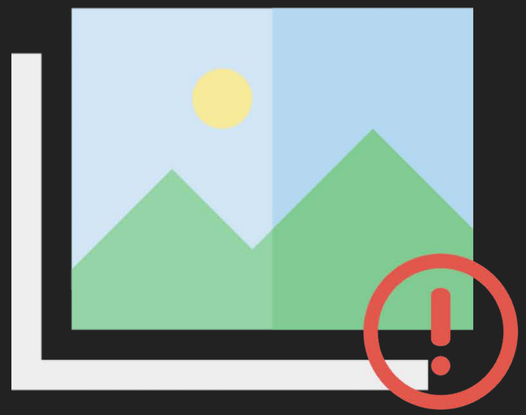

Reverse Proxy
Command Injection
RCE
Path Traversal
Parameter Pollution
Internal HTTP server
Component α
auth.cgi
CRLF Injection
helper.cgi
CGI
CGI

Step 1 : From auth.cgi to helper.cgi



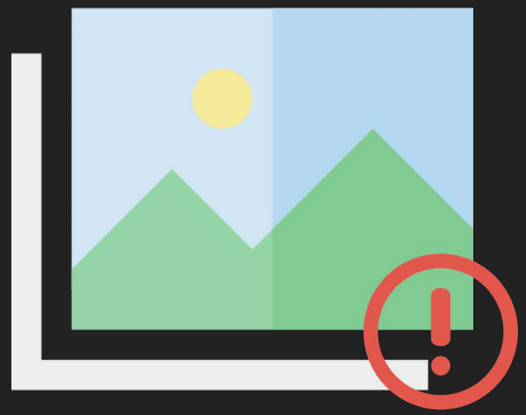
內部演練畫面
僅公布於研討會

Step 2 : Inject parameter for helper.cgi



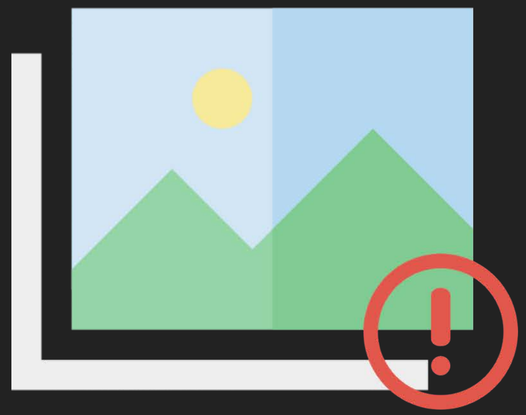
內部演練畫面
僅公布於研討會

Step 3 : Inject CRLF to fake response



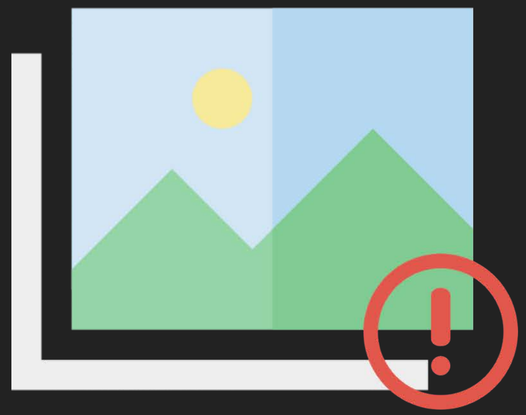
內部演練畫面
僅公布於研討會

Fix path



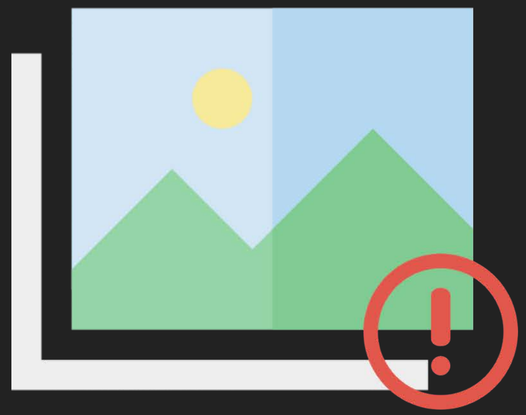
內部演練畫面
僅公布於研討會

Step 4 : Inject malicious command



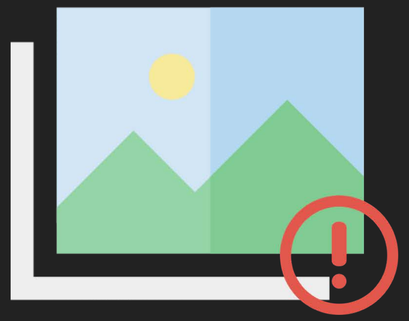
內部演練畫面
僅公布於研討會

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

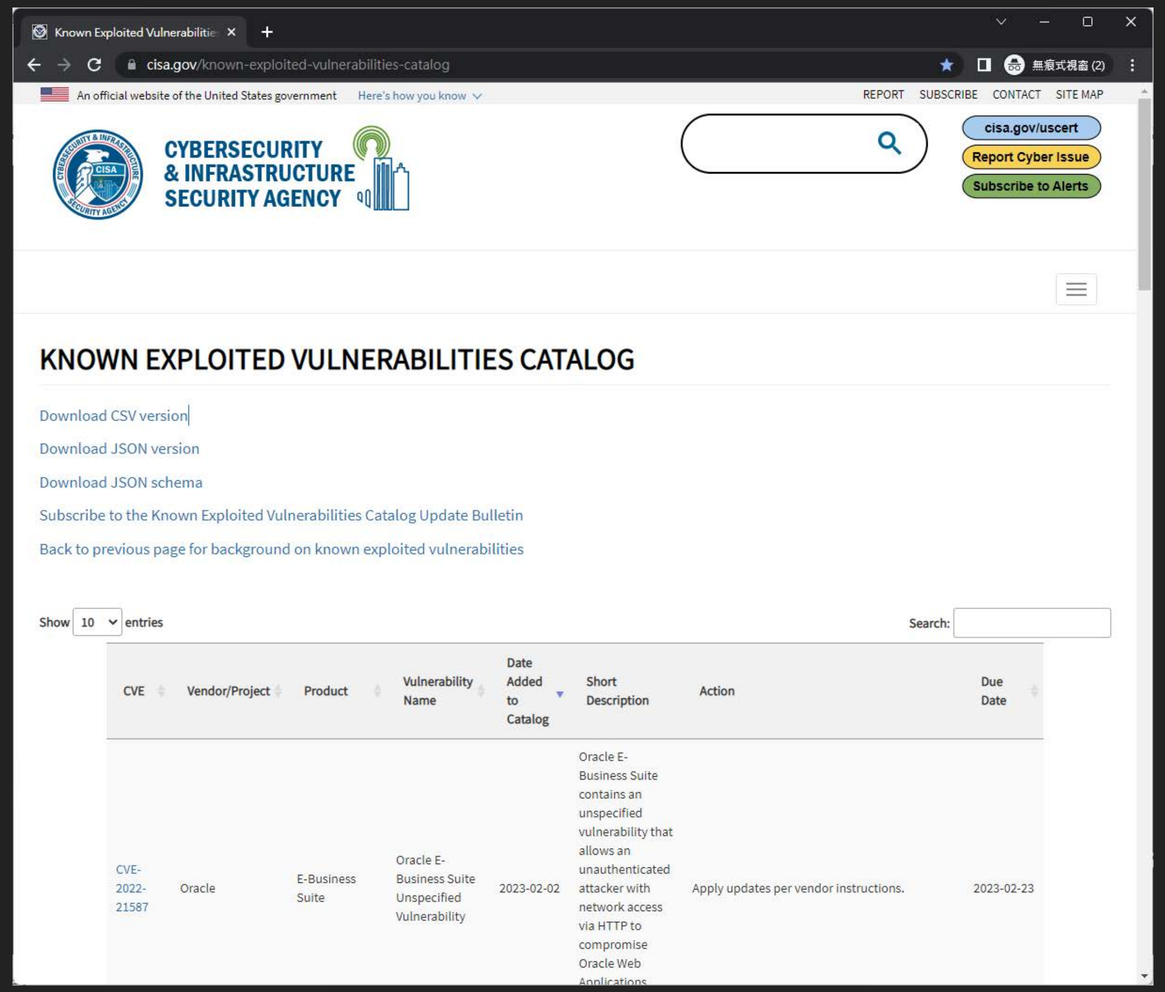
漏洞修補順序議題

- 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？

DEVCORE SECURITY CONSULTING

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

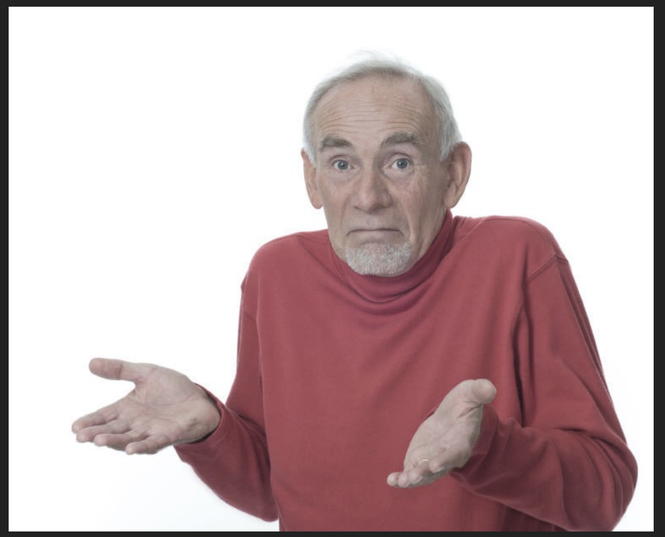
Known Exploited Vulnerabilities



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！

DEVCORE SECURITY CONSULTING

DEVCORE
SECURITY
CONSULTING

Q&A