SSRF vs. Developers: A Study of SSRF-Defenses in PHP Applications

Malte Wessels, Simon Koch, Giancarlo Pellegrino, Martin Johns

IAS | INSTITUTE FOR APPLICATION SECURITY

Technische Universität Braunschweig

CISPA | HELMHOLTZ CENTER FOR INFORMATION SECURITY

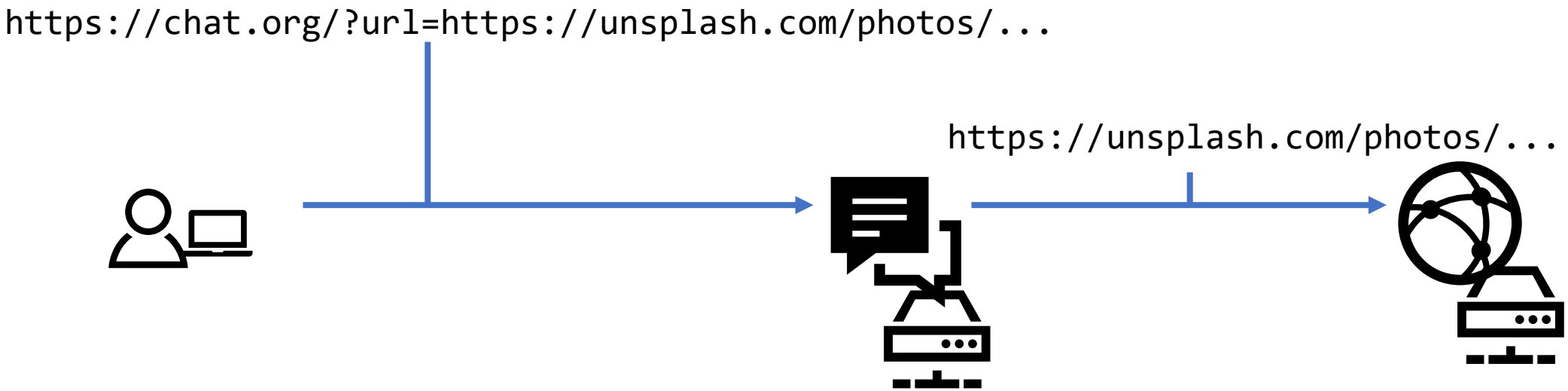
M **Malte Wessels**

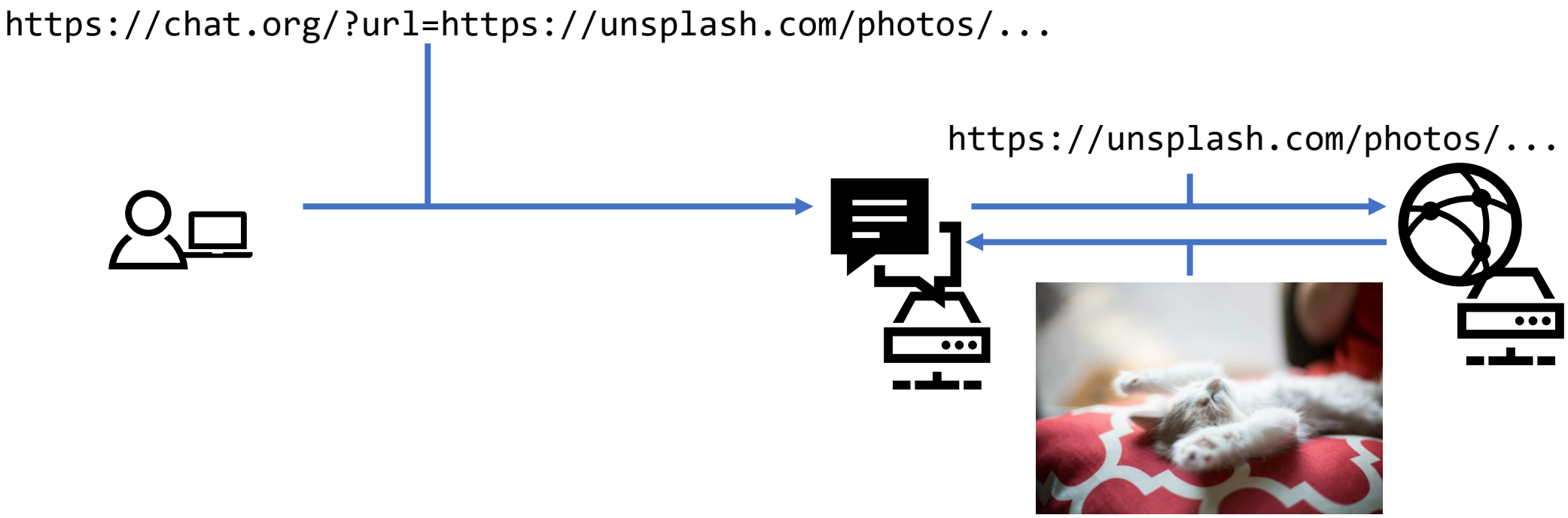
17:19 https://unsplash.com/photos/kitten-lying-on-red-and-white-quatrefoil-textile-Sa1z1pEzjPI

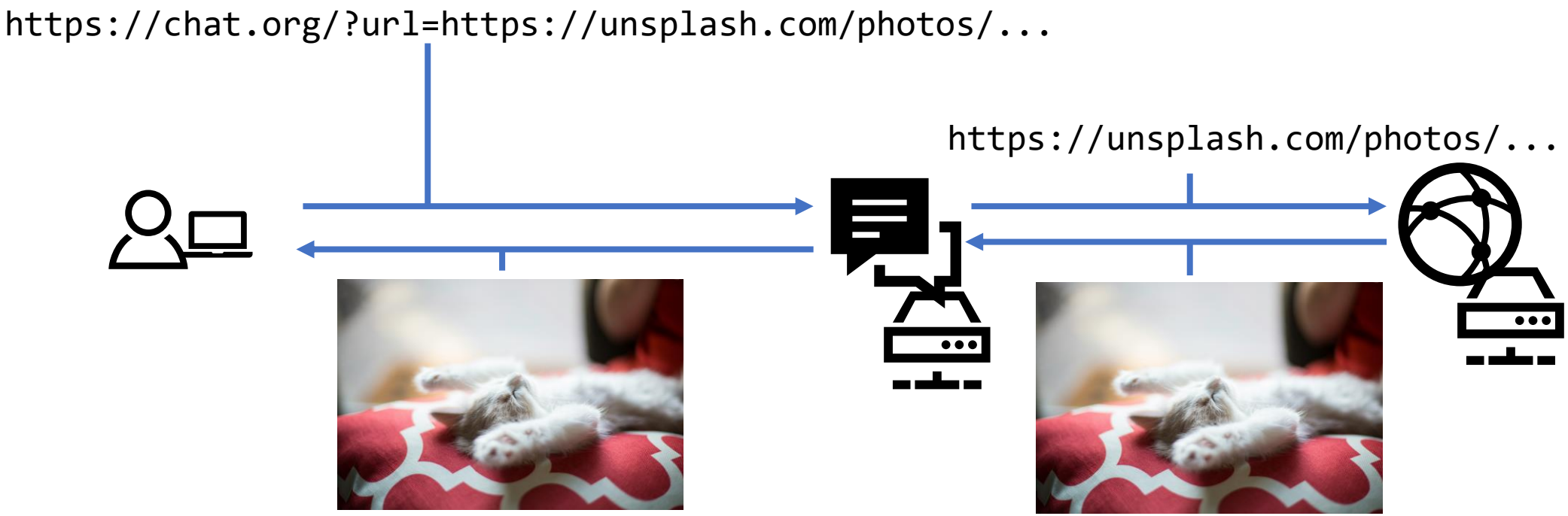
Photo by Jonathan Fink on Unsplash - @unsplash

This is Chip — Chip likes to sleep. We recently got two adorable 6 week old kittens and they absolutely love to wrestle, play and, of course, nap. This photo perfectly captures this young cat's chill personality and encourages us all to take a moment t...

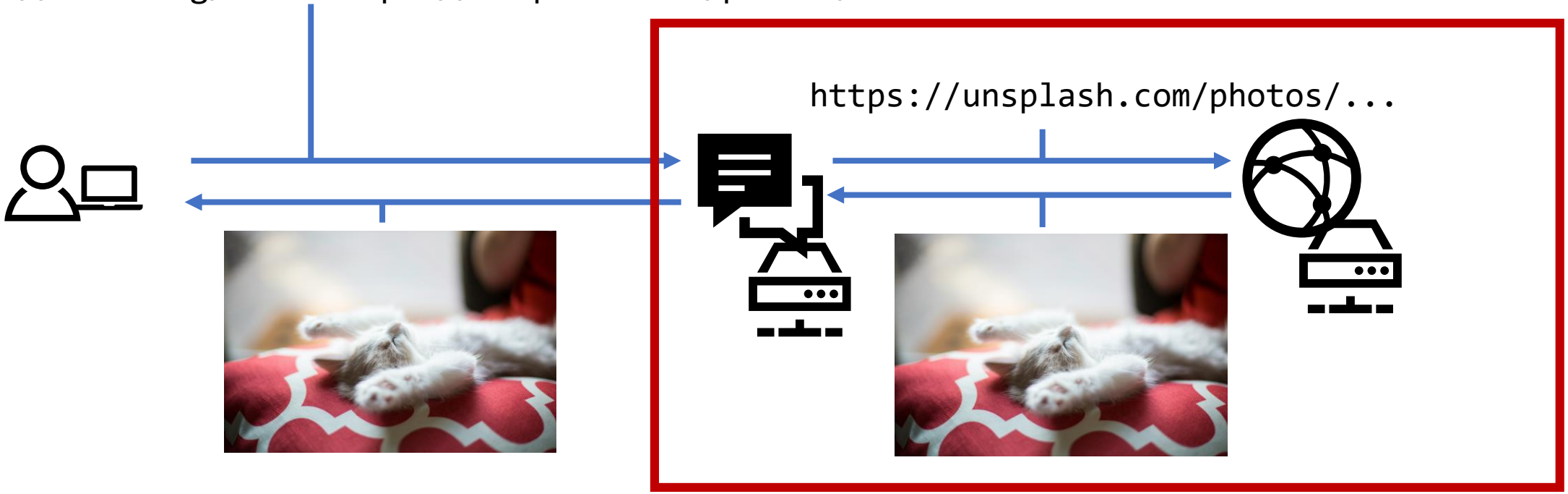
https://chat.org/?url=https://unsplash.com/photos/...


https://chat.org/?url=https://unsplash.com/photos/...
https://unsplash.com/photos/...


https://chat.org/?url=https://unsplash.com/photos/...
https://unsplash.com/photos/...

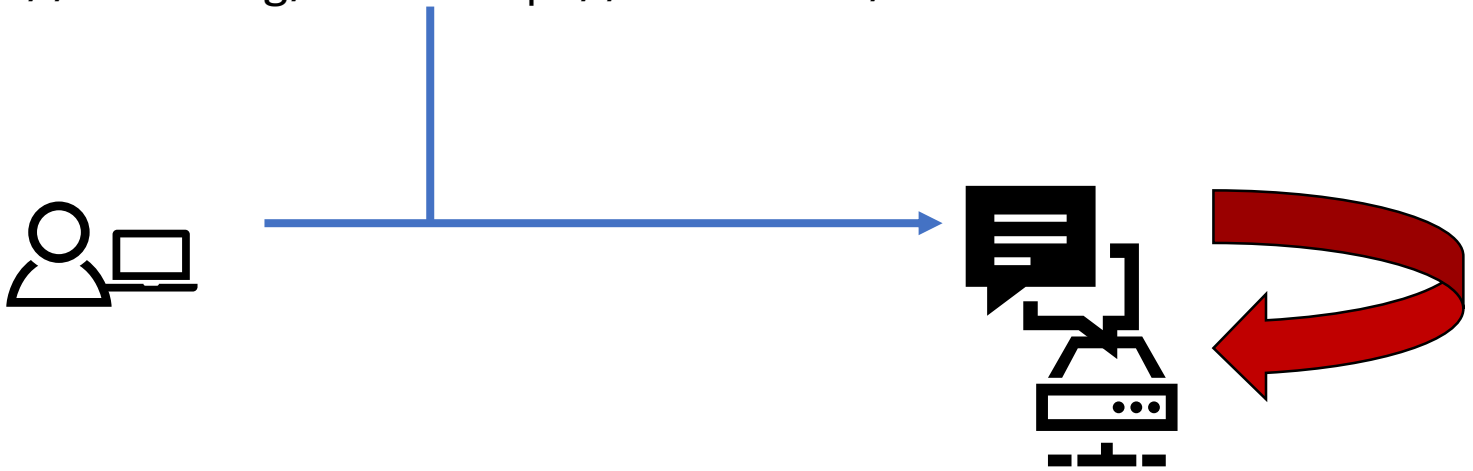

https://chat.org/?url=https://unsplash.com/photos/...
https://unsplash.com/photos/...

https://chat.org/?url=https://unsplash.com/photos/...



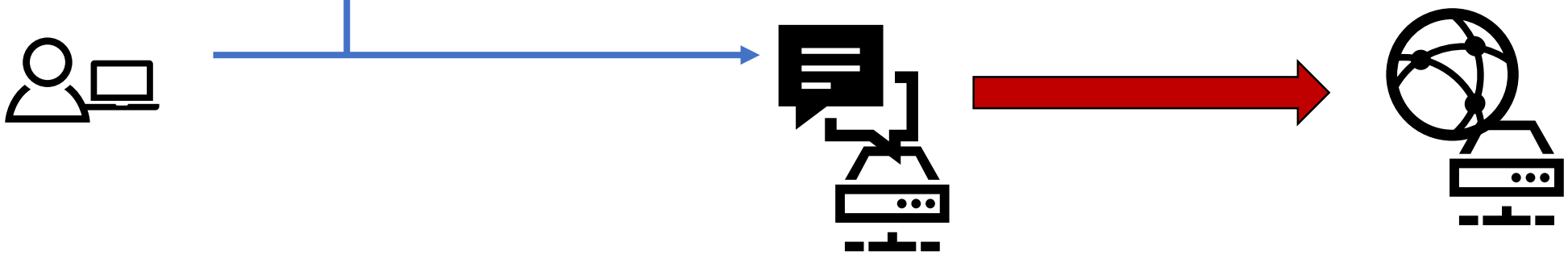
https://chat.org/?url=http://localhost/...

https://chat.org/?url=http://localhost/...

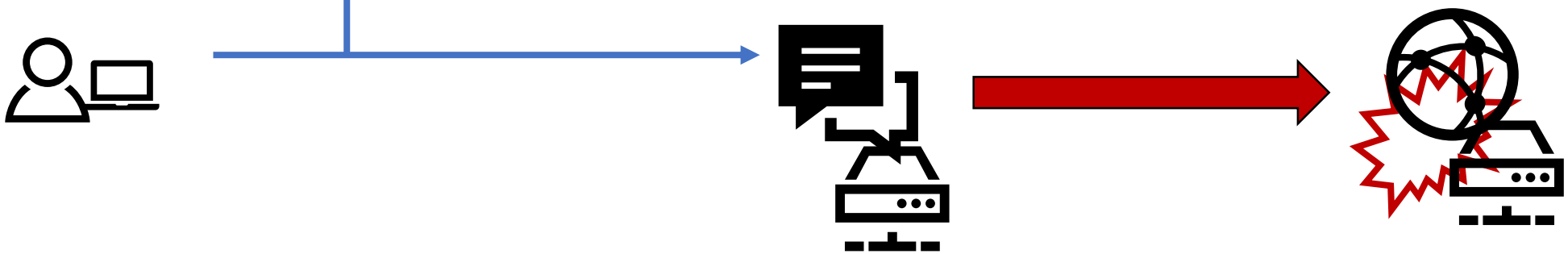


https://chat.org/?url=http://localhost/...

https://chat.org/?url=http://target.tld/attackpayload



https://chat.org/?url=http://target.tld/attackpayload



Literature Survey

Literature Survey

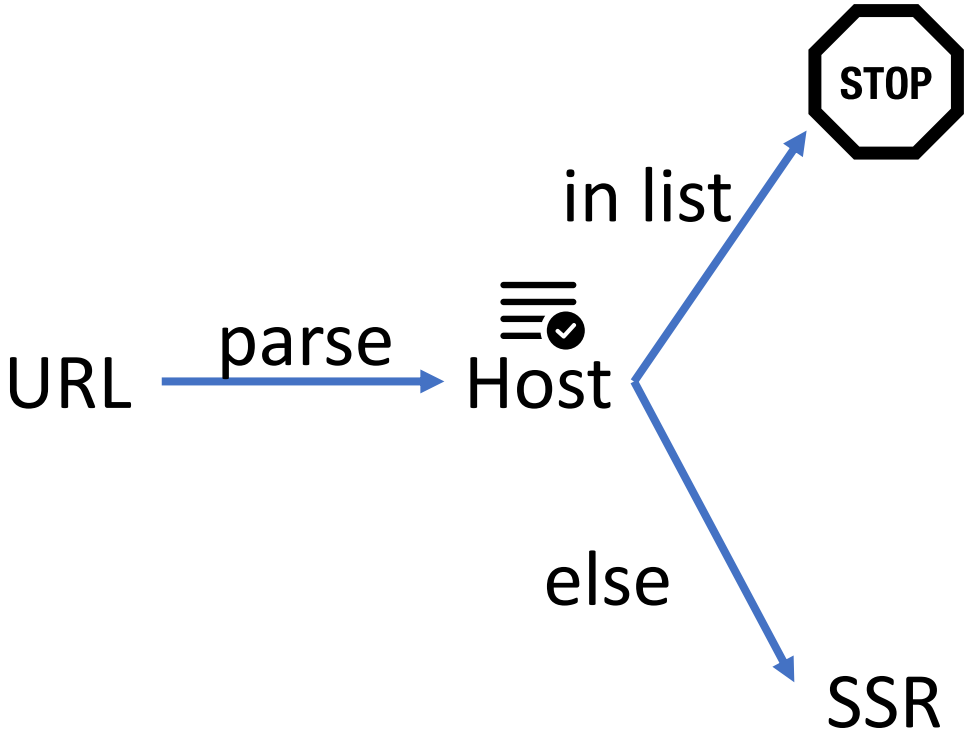
- **Deny/allow list** 
- **Validation** → URL & DNS
- **Configuration** → Redirection, HTTP-only, Rate-Limits, …
- **Response Modification** → Wrap result, …

Literature Survey

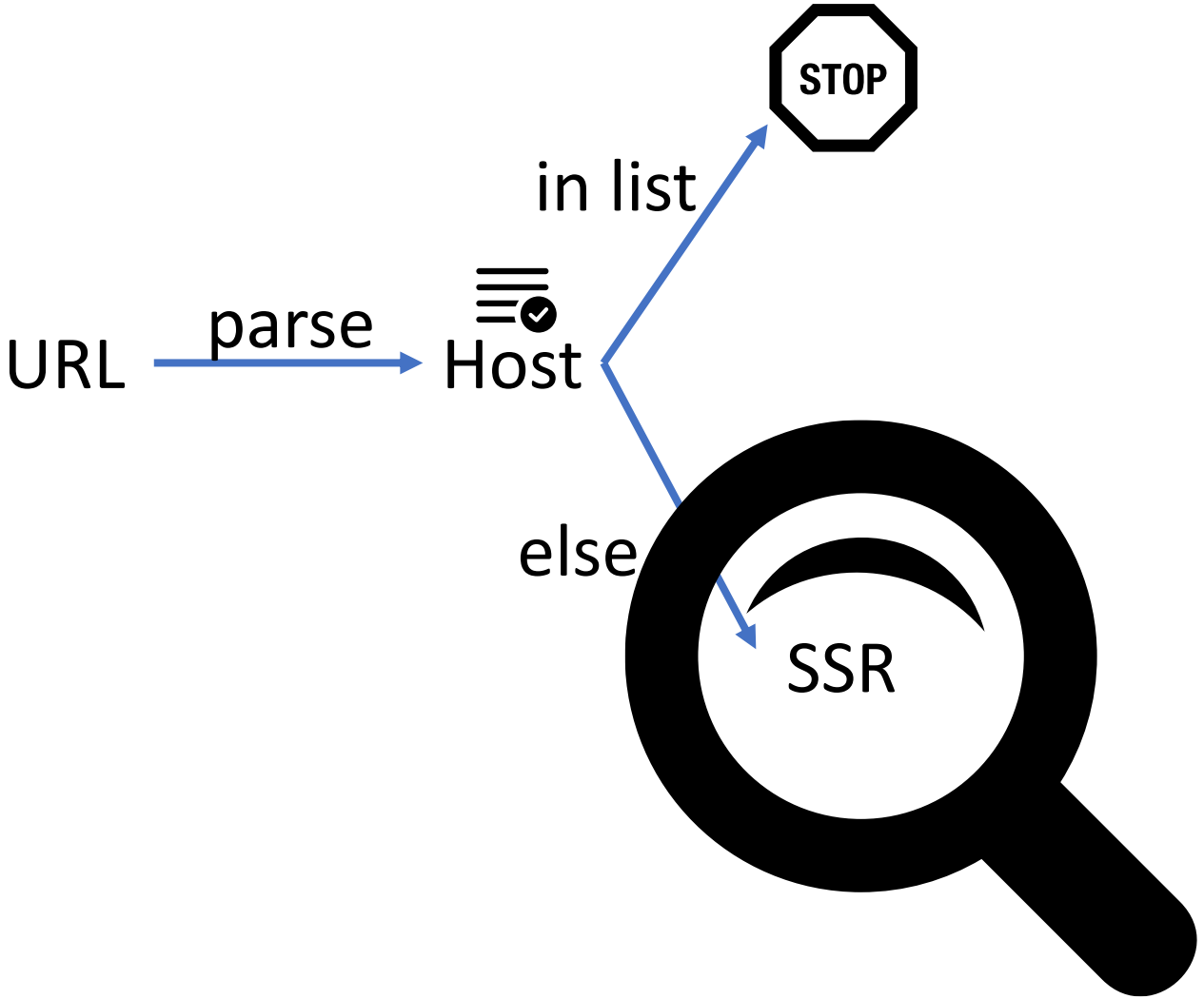
- **Deny/allow list**
- **Validation** → URL & DNS
- **Configuration** → HTTP-only, Rate-Limits, …
- **Response Modification** → Wrap result, …

Host Denylist

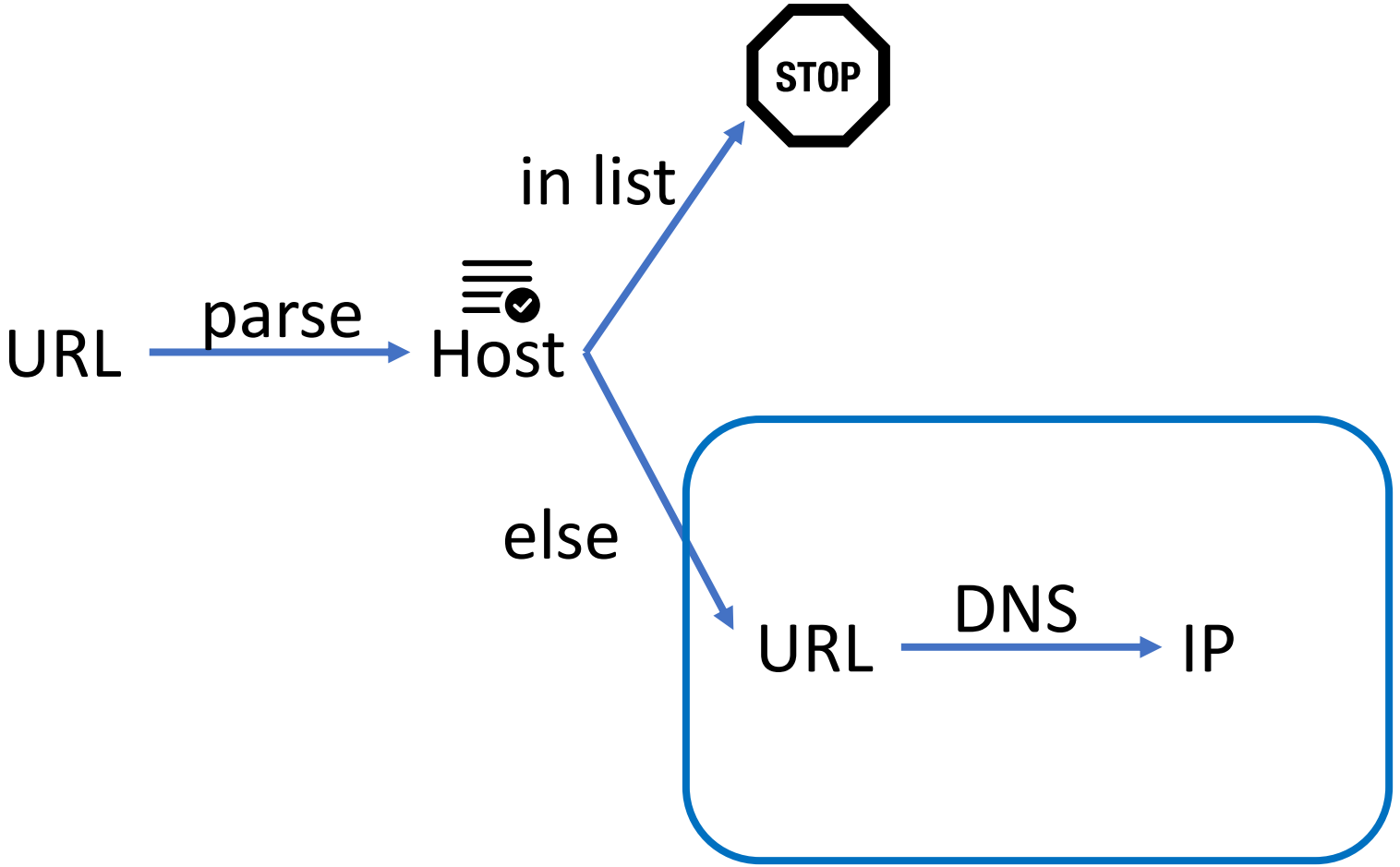
Host Denylist



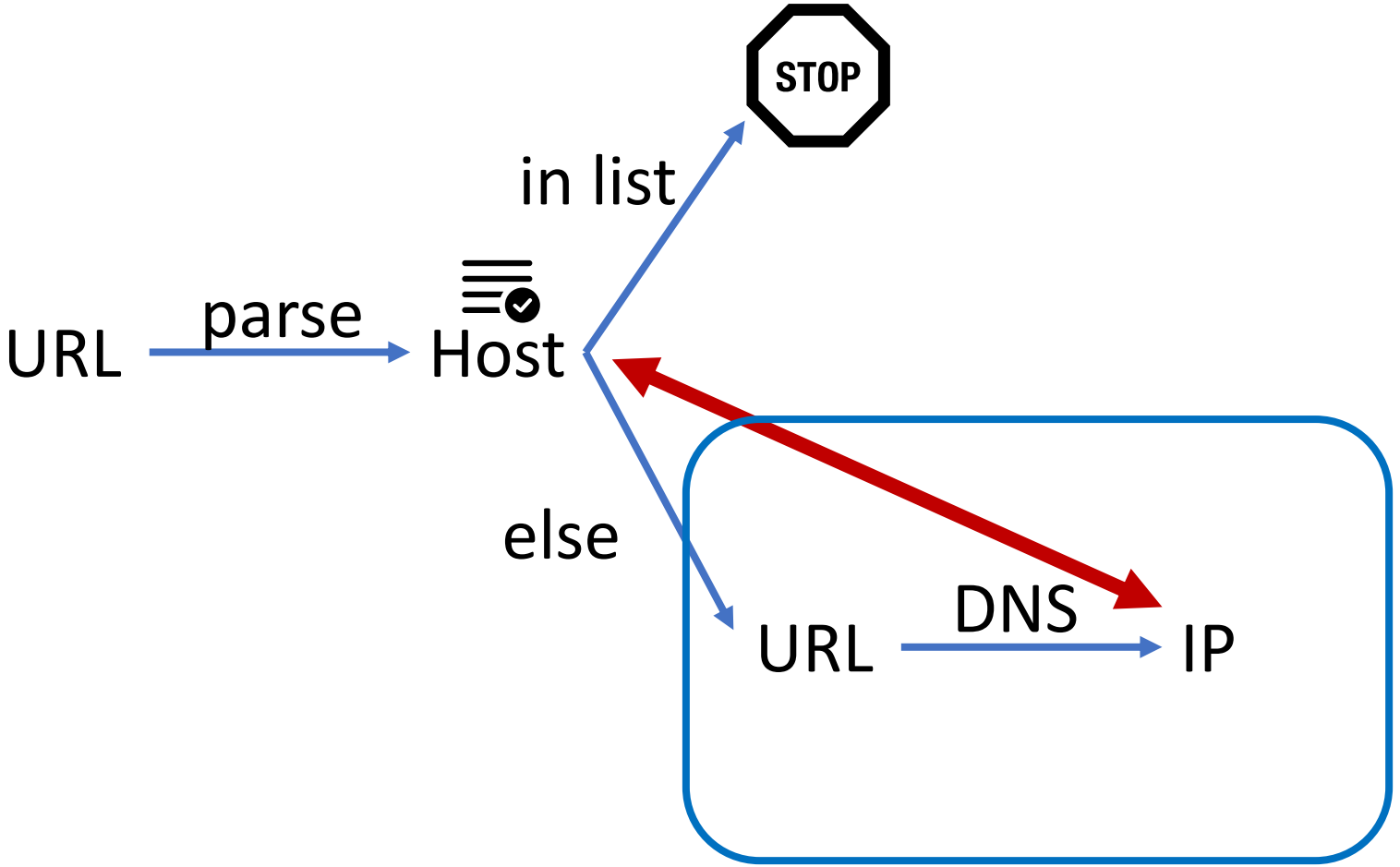
Host Denylist



Host Denylist



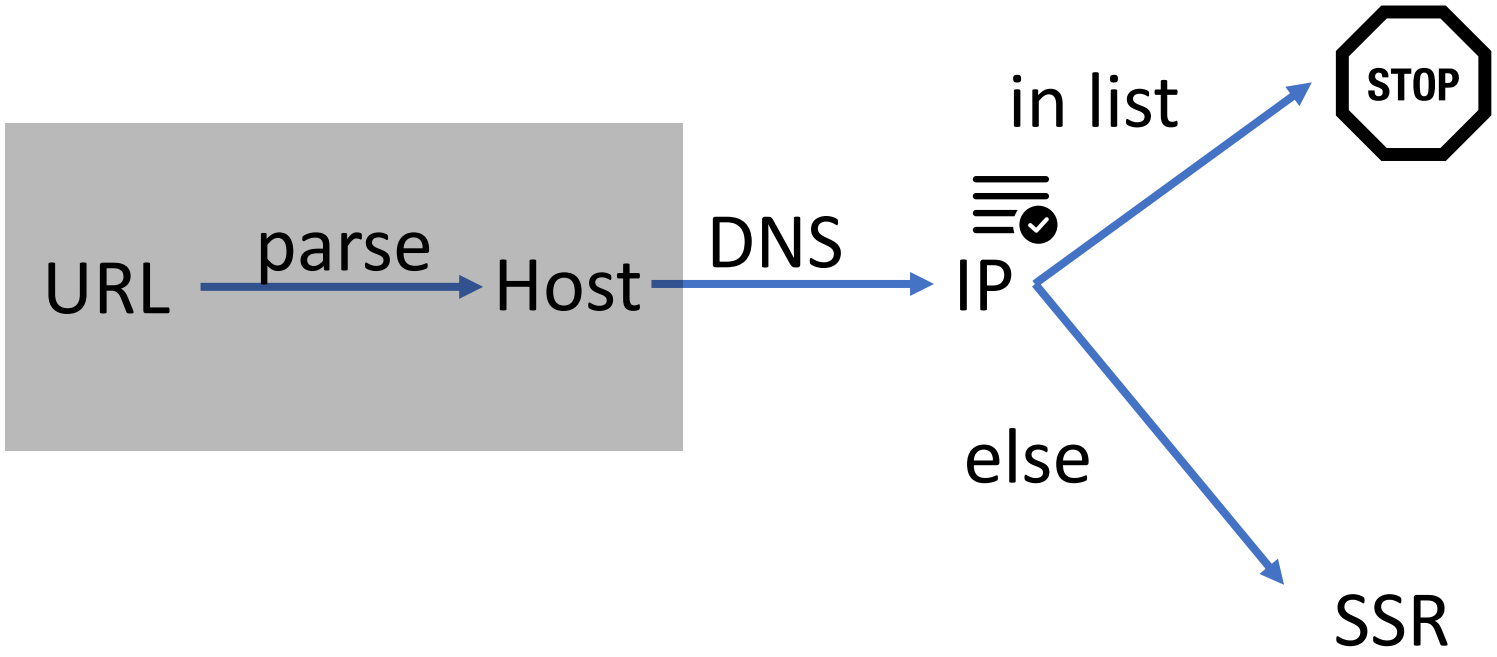
Host Denylist



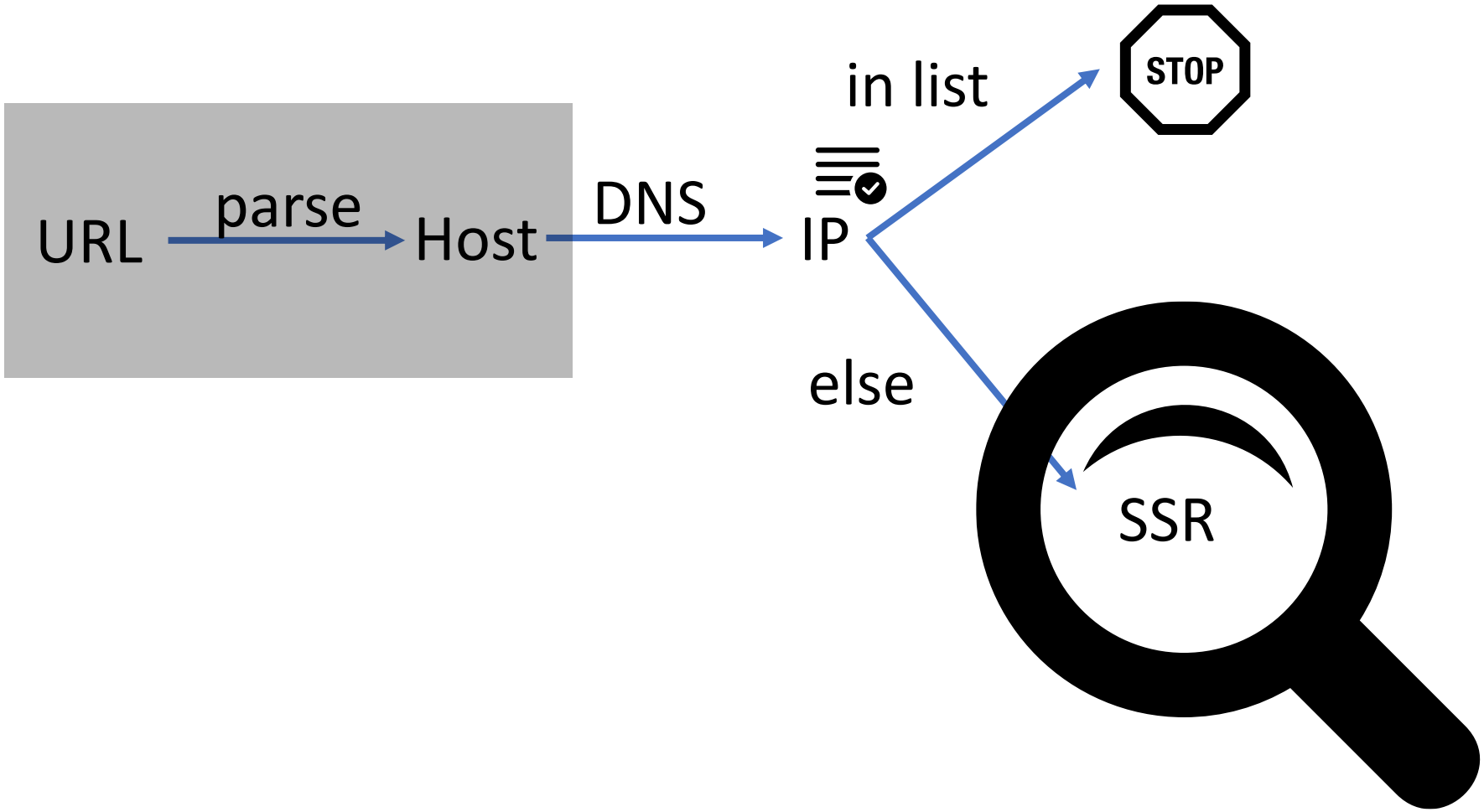
```
sh-5.2$ ping fbi.com
PING fbi.com (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.039 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.034 ms
```

```
sh-5.2$ ping fbi.com
PING fbi.com (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.039 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.034 ms
```

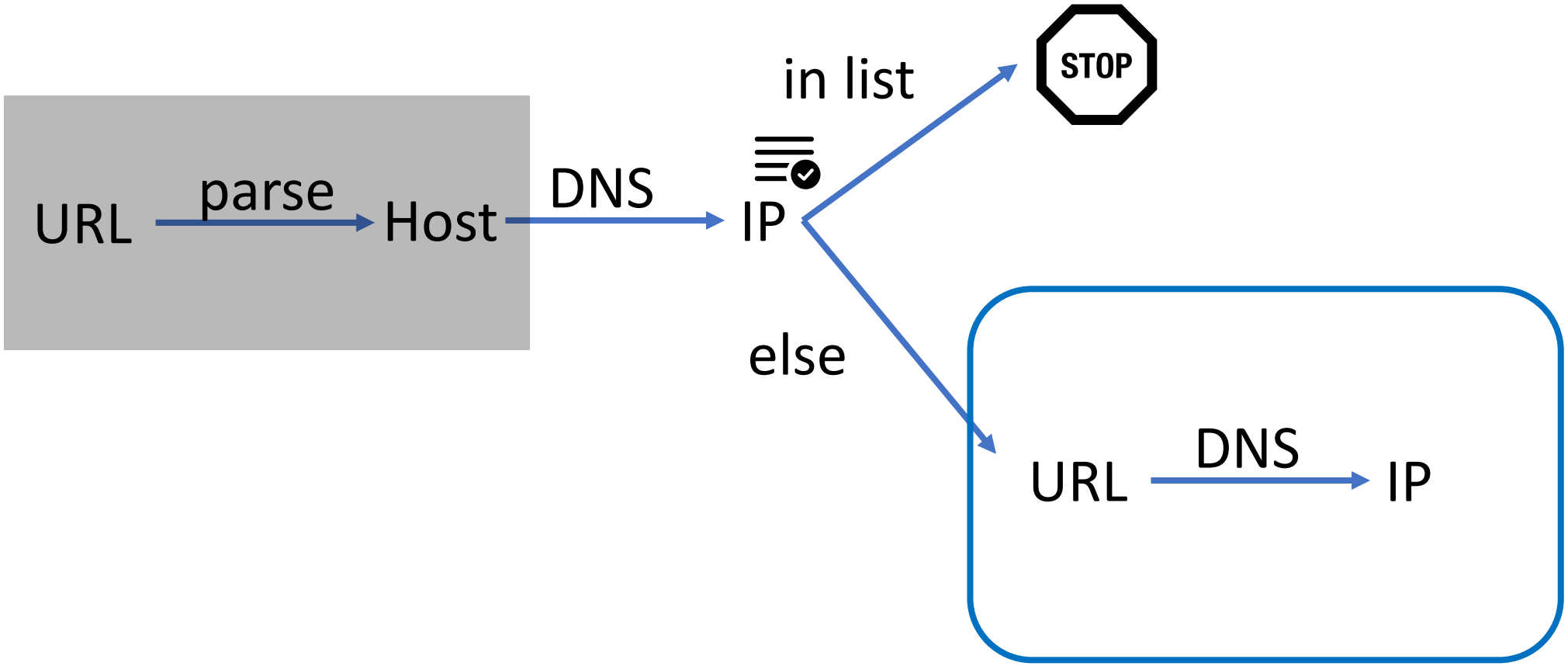
Fix: DNS



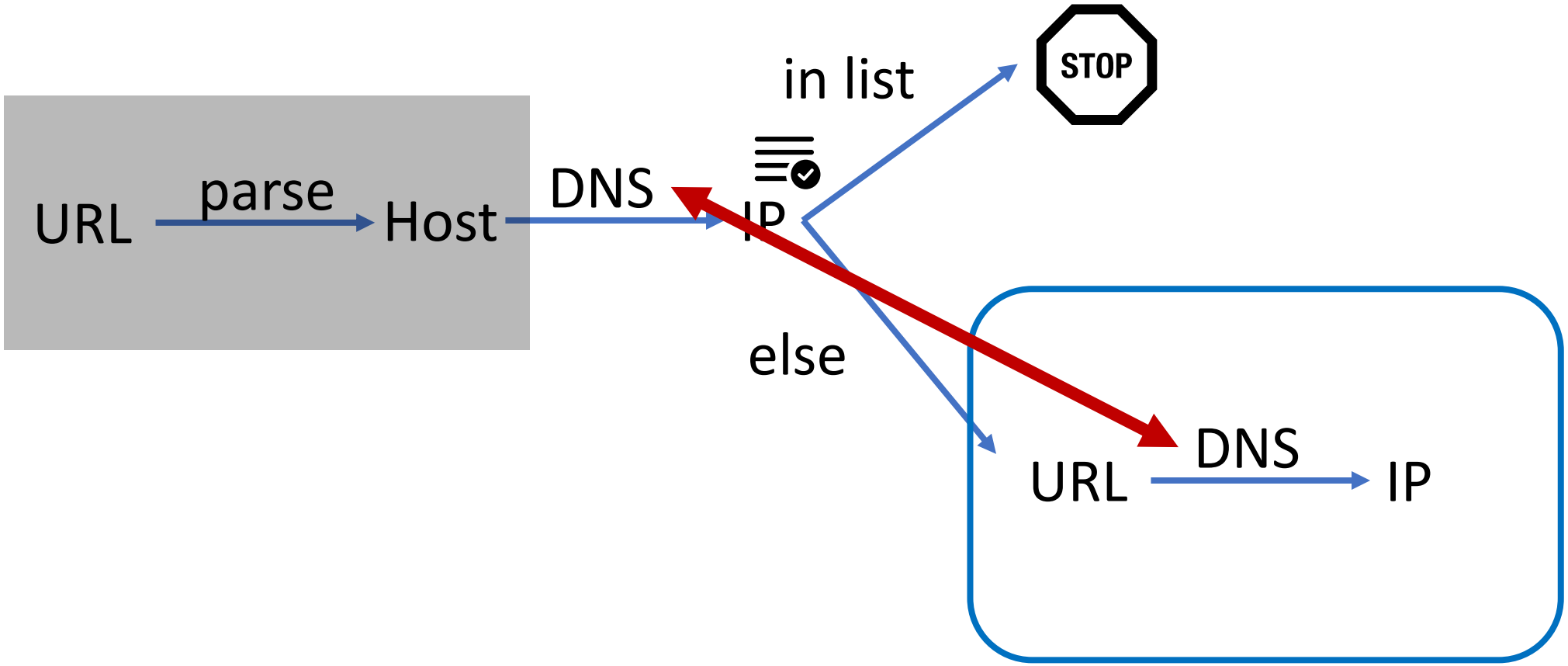
Fix: DNS



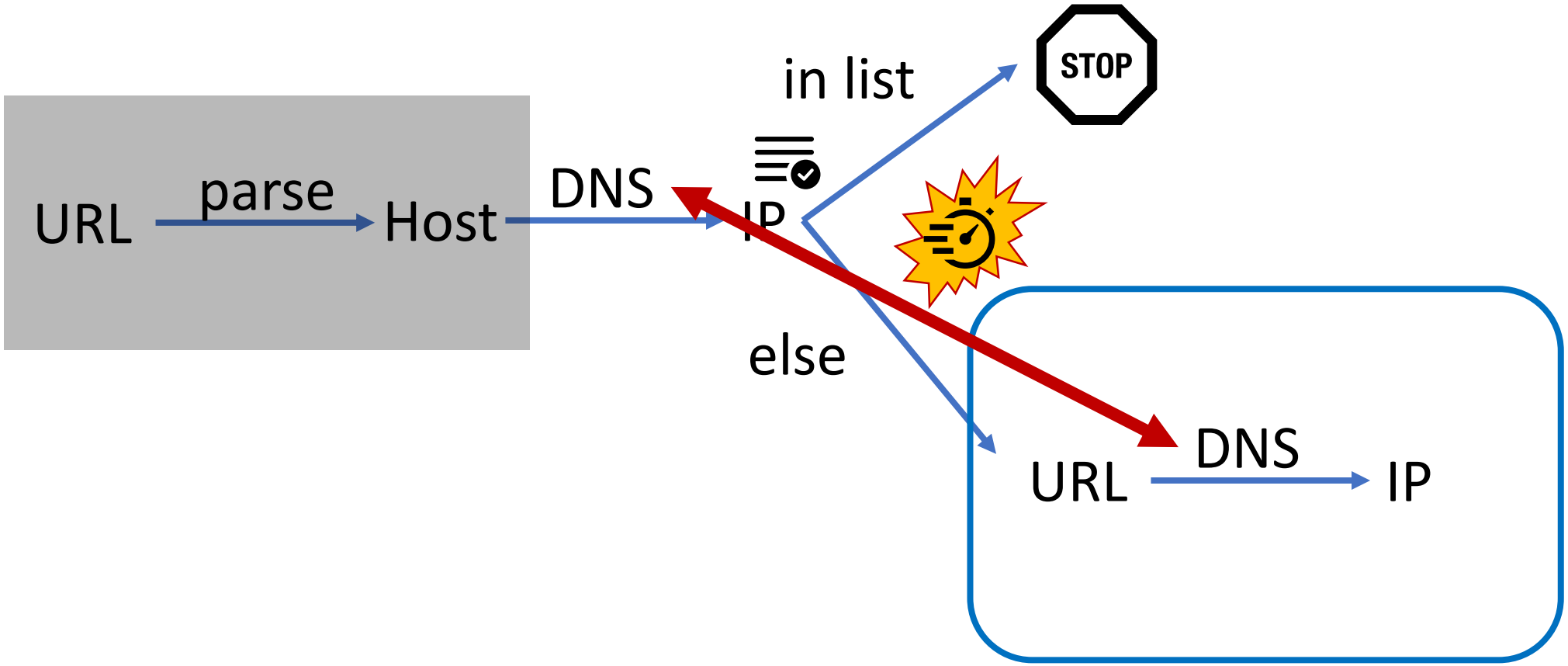
Fix: DNS?



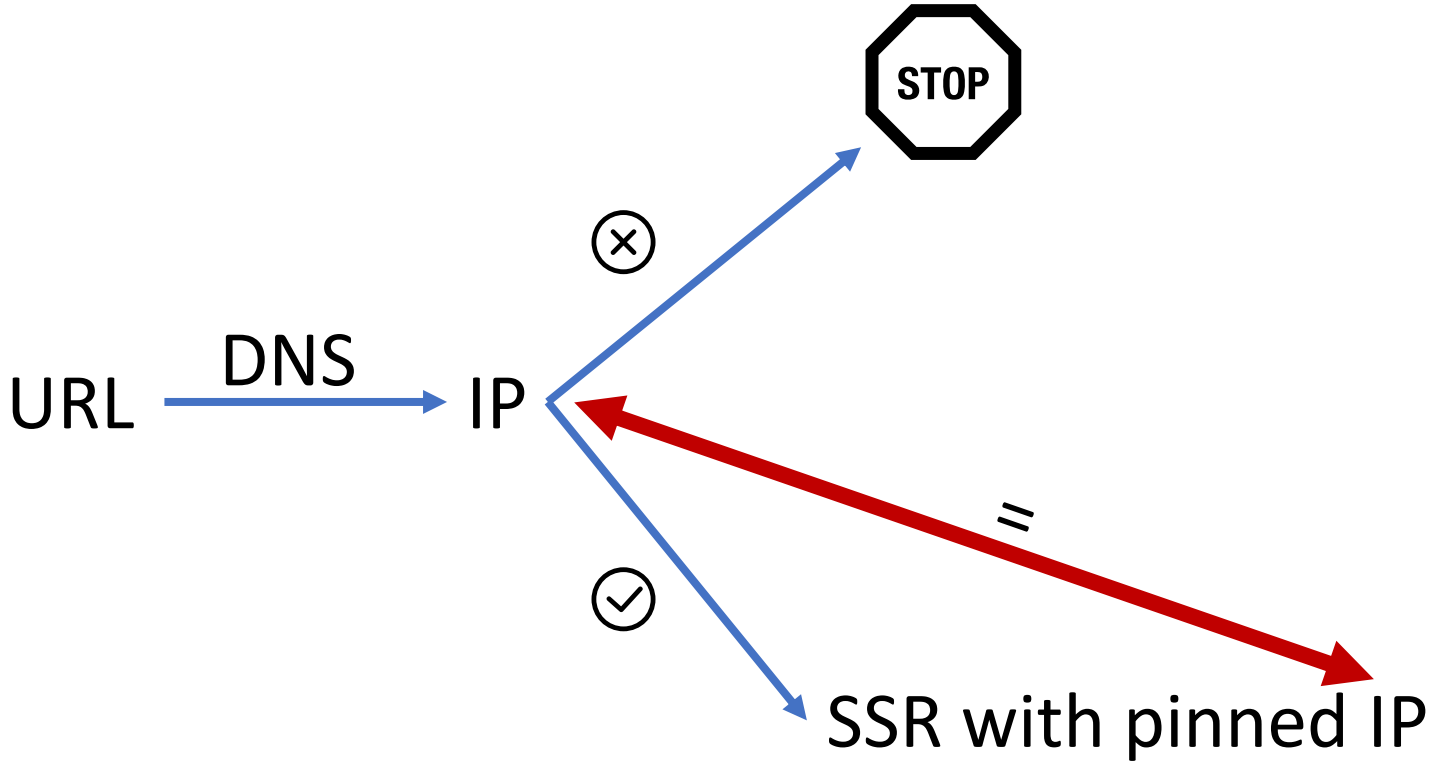
Fix: DNS?



Fix: DNS?



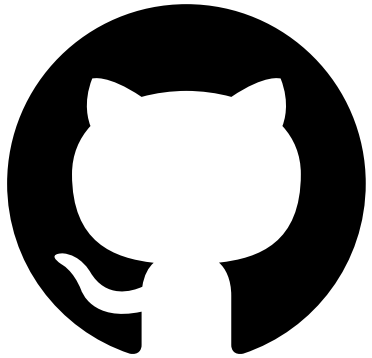
DNS Pinning!



- Defending is hard
- Are developers doing it correctly?
  - I) Are they using off-the-shelf defenses?
  - II) Are they building their own?

Subject

76 % of websites use PHP



30k repositories with PHP

Frameworks

Framework	SSRF-Defense available?
WordPress	**broken**
Laravel	No
Symfony	**Yes**
CakePHP	No
FuelPHP	No
Windwalker	No
Zend	No
Laminas	No
CodeIgnite	No
PHPixie	No

HTTP-Clients

HTTP-Client	Defense available?
PHP std lib	No
PHP curl extension	No
Guzzle	No
PECL HTTP	No
ReactPHP Sockets	No
WordPress Requests	No
Buzz	No
Httpful	No
SafeCurl, SafeURL	**Yes**
HTTPLug	**As Plugin**

Prevalence Study

Prevalence Study

4

Home-Grown Defenses?

Idea

- Static Dataflow Analysis → SSRF candidates
- Check candidates manually
- Which defenses are they using?

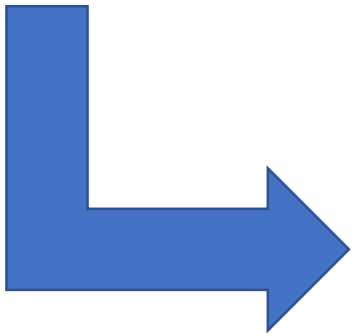
Static Dataflow Analysis

Static Dataflow Analysis

```
<?php
if(isset($x)) {
    file_get_contents($x);
}
echo "ack";
```

Static Dataflow Analysis

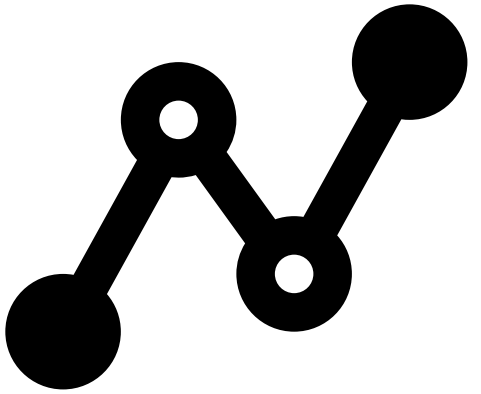
```
<?php
if(isset($x)) {
    file_get_contents($x);
}
echo "ack";
```

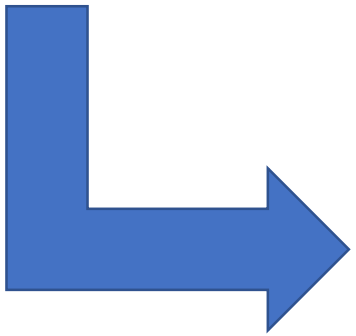


```
$_main:
0000 T1 = ISSET_ISEMPTY_CV (isset)
CV0($x)
0001 JMPZ T1 0005
0002 INIT_FCALL 1 96
string("file_get_contents")
0003 SEND_VAR CV0($x) 1
0004 DO_ICALL
0005 ECHO string("ack")
0006 RETURN int(1)
```

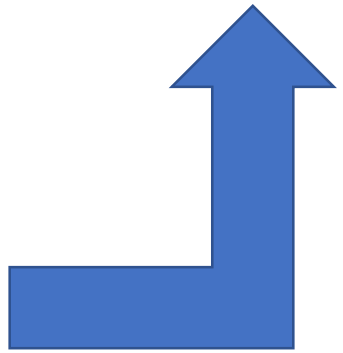
Static Dataflow Analysis

```
<?php
if(isset($x)) {
    file_get_contents($x);
}
echo "ack";
```

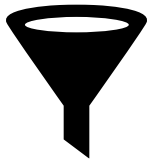




```
$_main:
0000 T1 = ISSET_ISEMPTY_CV (isset)
CV0($x)
0001 JMPZ T1 0005
0002 INIT_FCALL 1 96
string("file_get_contents")
0003 SEND_VAR CV0($x) 1
0004 DO_ICALL
0005 ECHO string("ack")
0006 RETURN int(1)
```

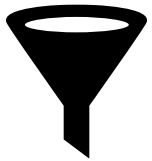


Insights



Only applications

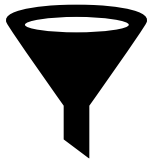
Insights



Only applications

User-input at start

Insights



Only applications

User-input at start

- 104 flows in apps with attacker-controlled domain
- Two apps with proper defense
- No DNS resolution

Take-Aways

We, as a research community, are aware of the risks and solutions.

Take-Aways

But most people do SSRs wrong.

Thank You!

https://github.com/SSRF-vs-Developers

Our tooling, incl. PHP CPG

@maltee:chaos.social

malte.wessels@tu-braunschweig.de

Technische Universität Braunschweig

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

TESTABLE

CASA CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Icons by IconMonstr; Kitten-Photo by Jonathan Fink