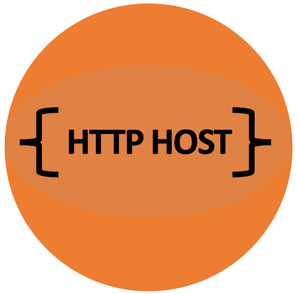
HTTP HOST

HTTP Host Header Attacks

Agenda



WHAT IS THE HTTP HOST HEADER?

WHAT ARE HOST HEADER VULNERABILITIES?

HOW DO YOU FIND AND EXPLOIT THEM?

HOW DO YOU PREVENT THEM?

WHAT IS THE HTTP HOST HEADER?

HTTP Host Header

The **HTTP Host header** is a mandatory request header that specifies the domain name that the client wants to access.

```
GET / HTTP/1.1
Host: ranakhalil.com
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
...
```

The purpose of the HTTP Host header is to help identify which back-end component the client wants to communicate with.

HTTP Host Header

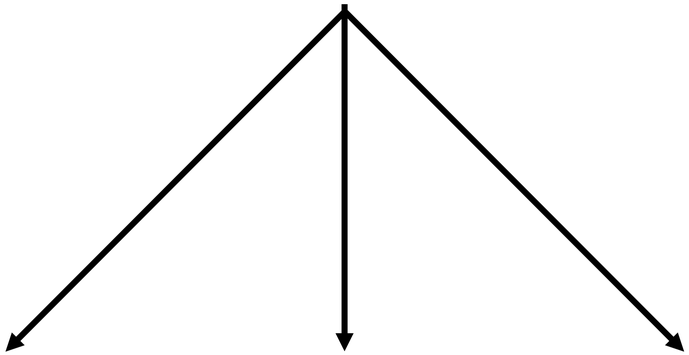
BEFORE

140.7.140.195

ranakhalil.com

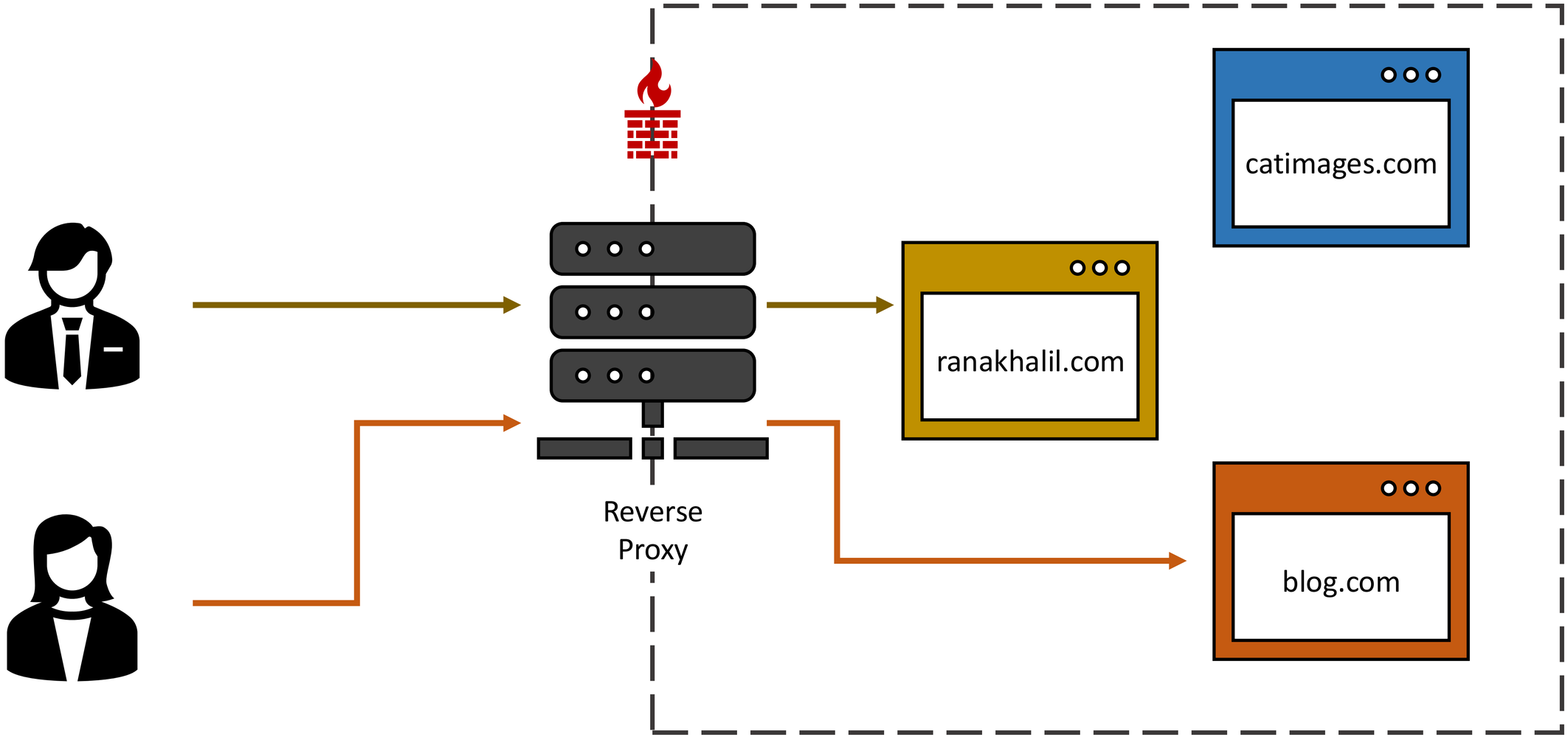
NOW

140.7.140.195



catimages.com ranakhalil.com blog.com

HTTP Host Header



WHAT ARE HTTP HOST HEADER VULNERABILITIES?

Host Header Vulnerabilities

Host header vulnerabilities occur when a web application trusts the value of the Host header without properly validating or restricting it.

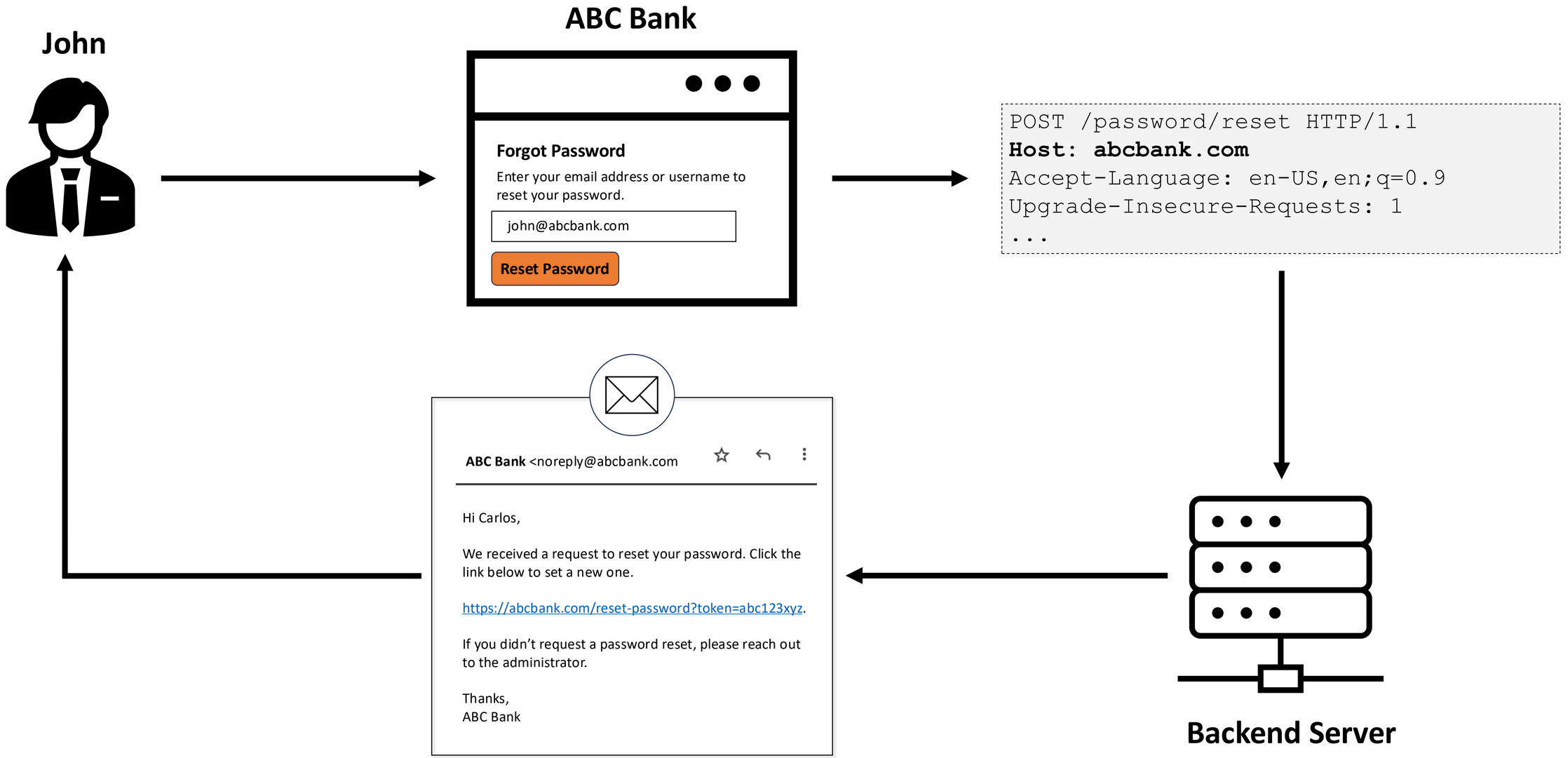
HTTP Request

```
GET / HTTP/1.1
Host: ranakhalil.com
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
...
```

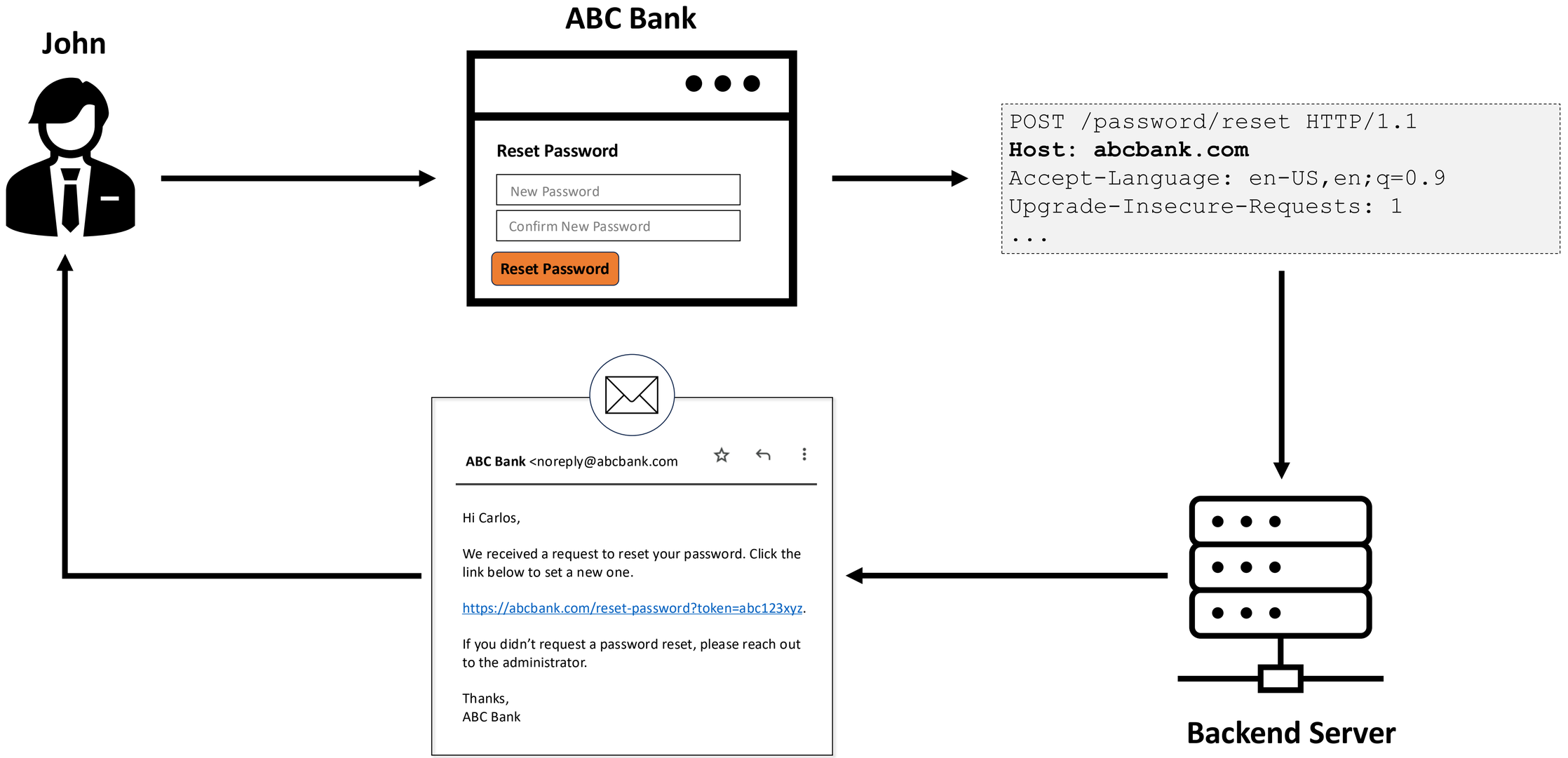
User Controllable

Potential vector for exploiting a range of vulnerabilities – Web cache poisoning, business logic flaws, SSRF, password reset poisoning.

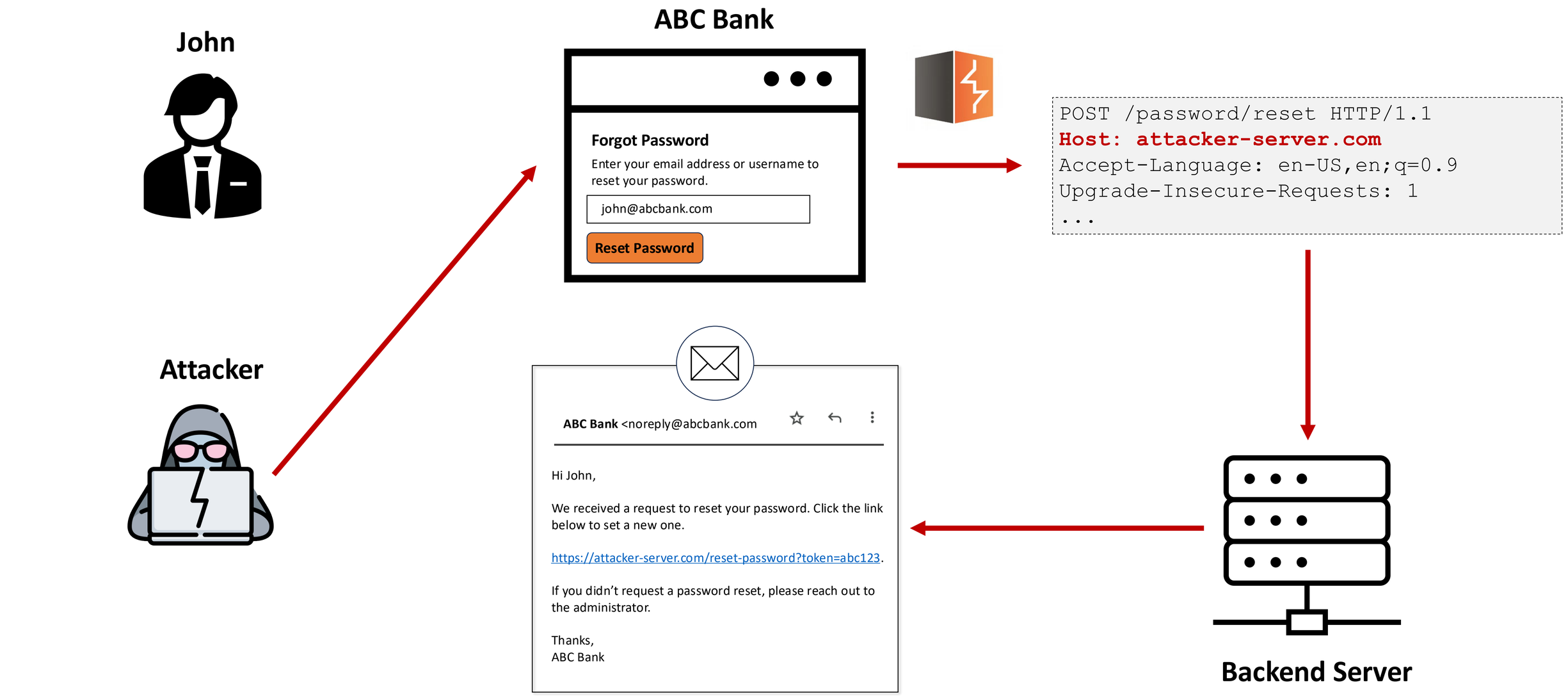
Password Reset Poisoning



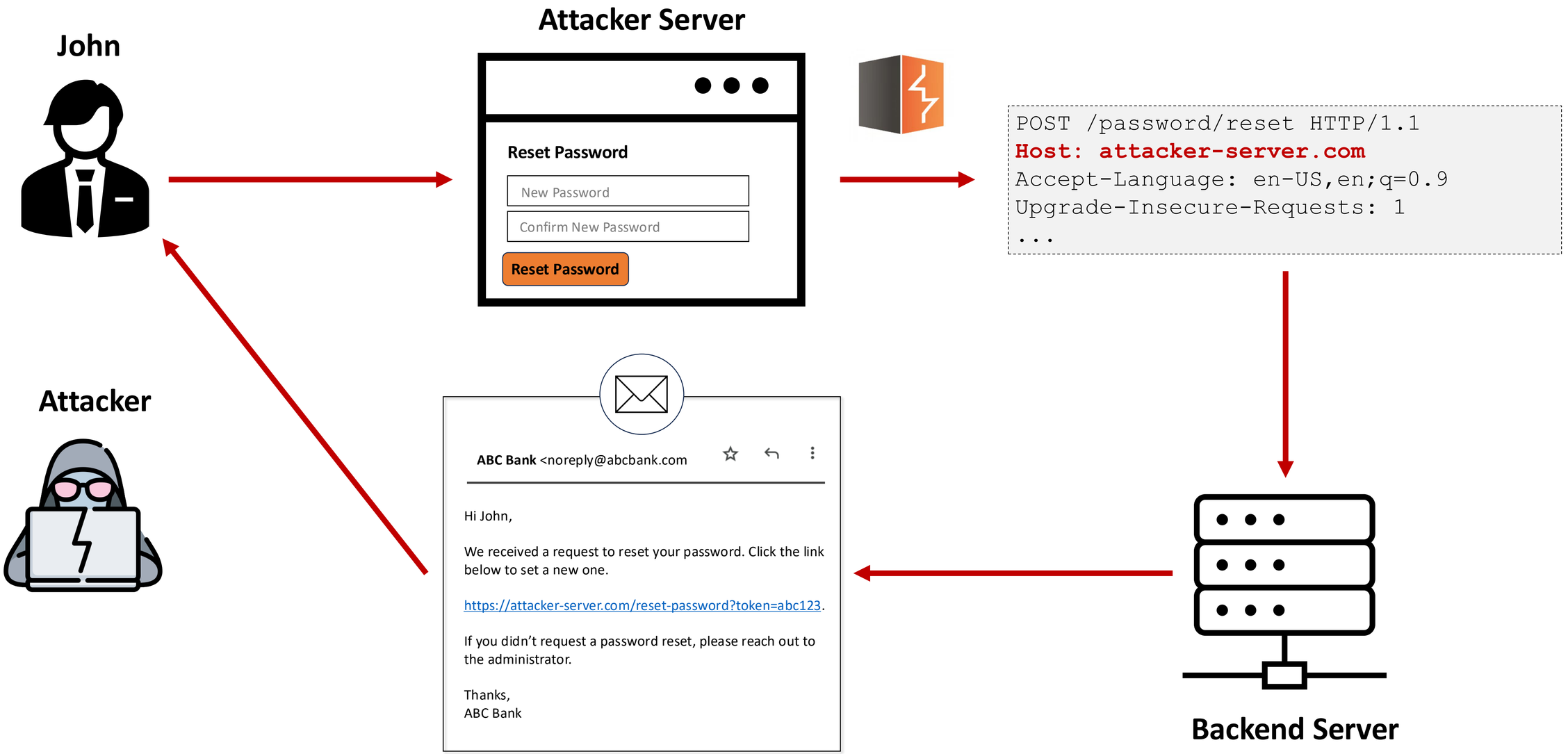
Password Reset Poisoning



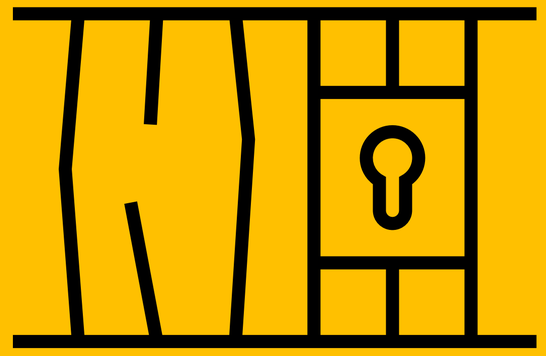
Password Reset Poisoning



Password Reset Poisoning



HOW TO FIND & EXPLOIT HTTP HOST HEADER VULNERABILITIES?



How to Identify Host Header Vulnerabilities

- Supply an arbitrary Host header.

Original Request

```
GET / HTTP/1.1
Host: abcbank.com
...
```

Modified Request

```
GET / HTTP/1.1
Host: ranakhalil.com
...
```

How to Identify Host Header Vulnerabilities

- Check for flawed validation
  - Allows the addition of a port.

```
GET / HTTP/1.1
Host: abcbank.com:bad-stuff-here
...
```

  - Flawed validation to allow subdomains.

```
GET / HTTP/1.1
Host: notabcbank.com
...
```

```
GET / HTTP/1.1
Host: hacked-subdomain.abcbank.com
...
```

How to Identify Host Header Vulnerabilities

- Send ambiguous requests.
  - Inject duplicate Host headers.

```
GET / HTTP/1.1
Host: abcbank.com
Host: ranakhalil.com
...
```

  - Supply an absolute URL.

```
GET https://abcbank.com/ HTTP/1.1
Host: ranakhalil.com
...
```

  - Add a line wrapping.

```
GET / HTTP/1.1
  Host: ranakhalil.com
Host: abcbank.com
...
```

How to Identify Host Header Vulnerabilities

- Inject host override headers. For example:
  - `X-Forwarded-Host`
  - `X-Host`
  - `X-Forwarded-Server`
  - `X-HTTP-Host-Override`
  - `Forwarded`

```
GET / HTTP/1.1
Host: abcbank.com
X-Forwarded-Host: ranakhalil.com
...
```

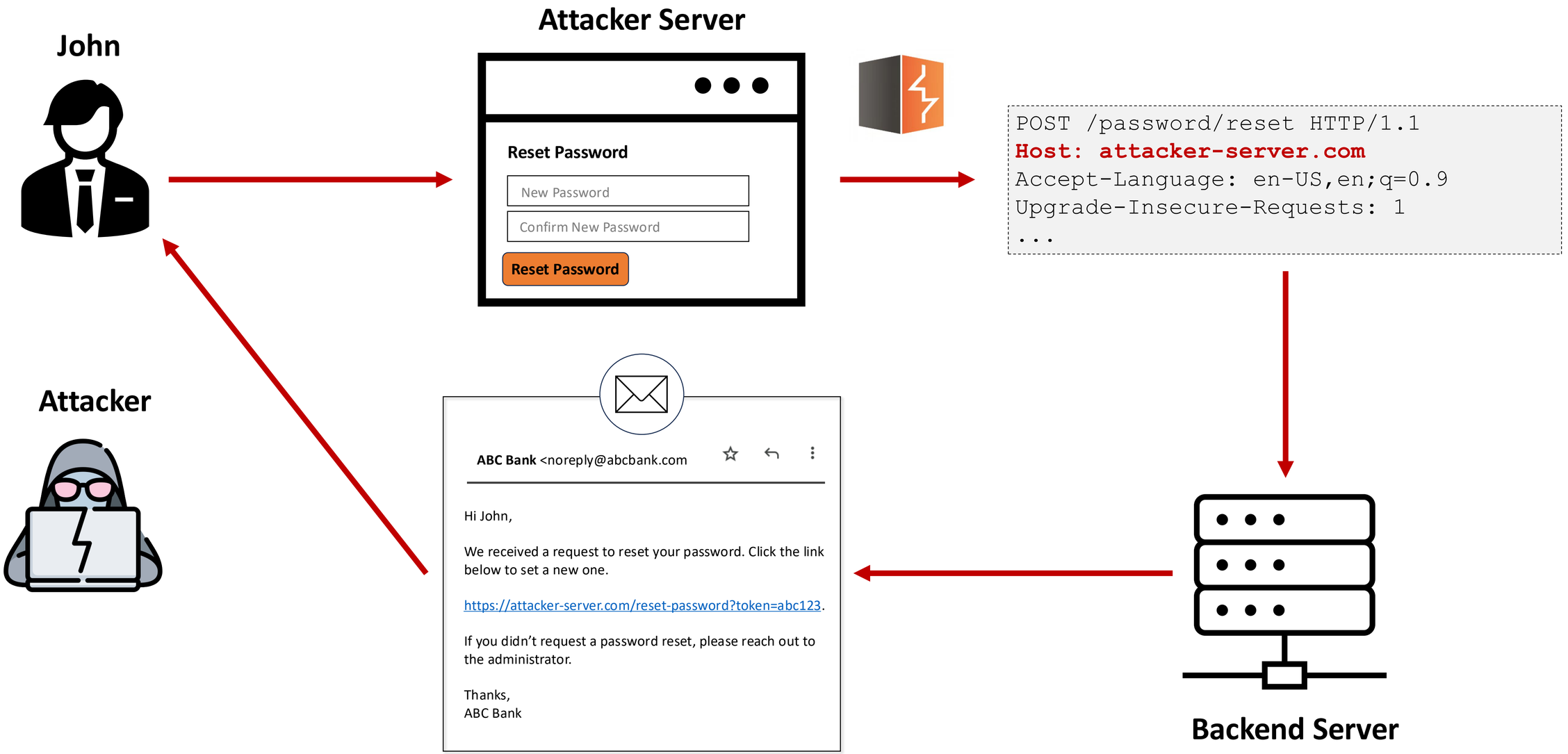
How to Exploit the HTTP Host Header

Once you identify that the application accepts arbitrary hostnames, you need to look for ways to exploit it based on how the header is utilized by the application.

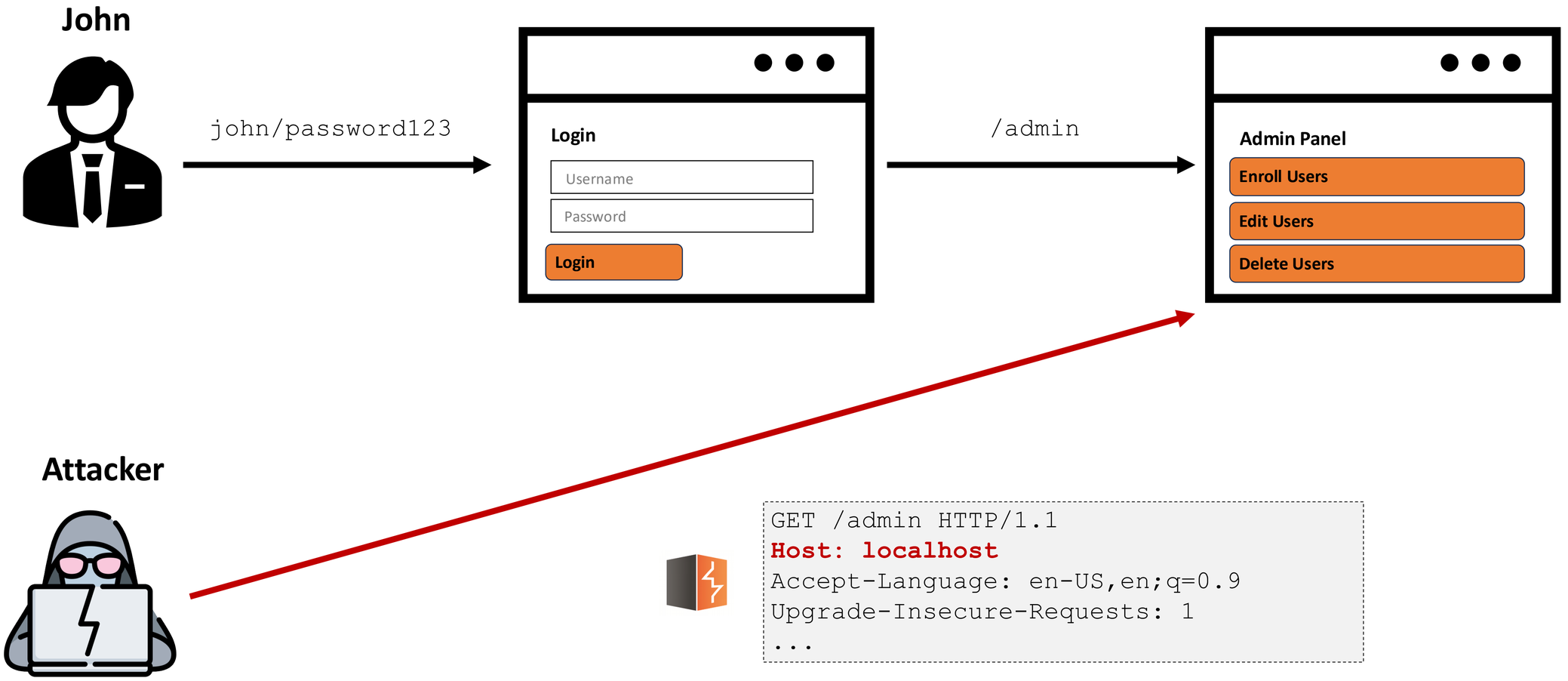
Common attacks:

- Password reset poisoning
- Web cache poisoning
- Exploiting classic server-side vulnerabilities
- Bypassing authentication
- Virtual host brute-forcing
- Routing-based SSRF
- …

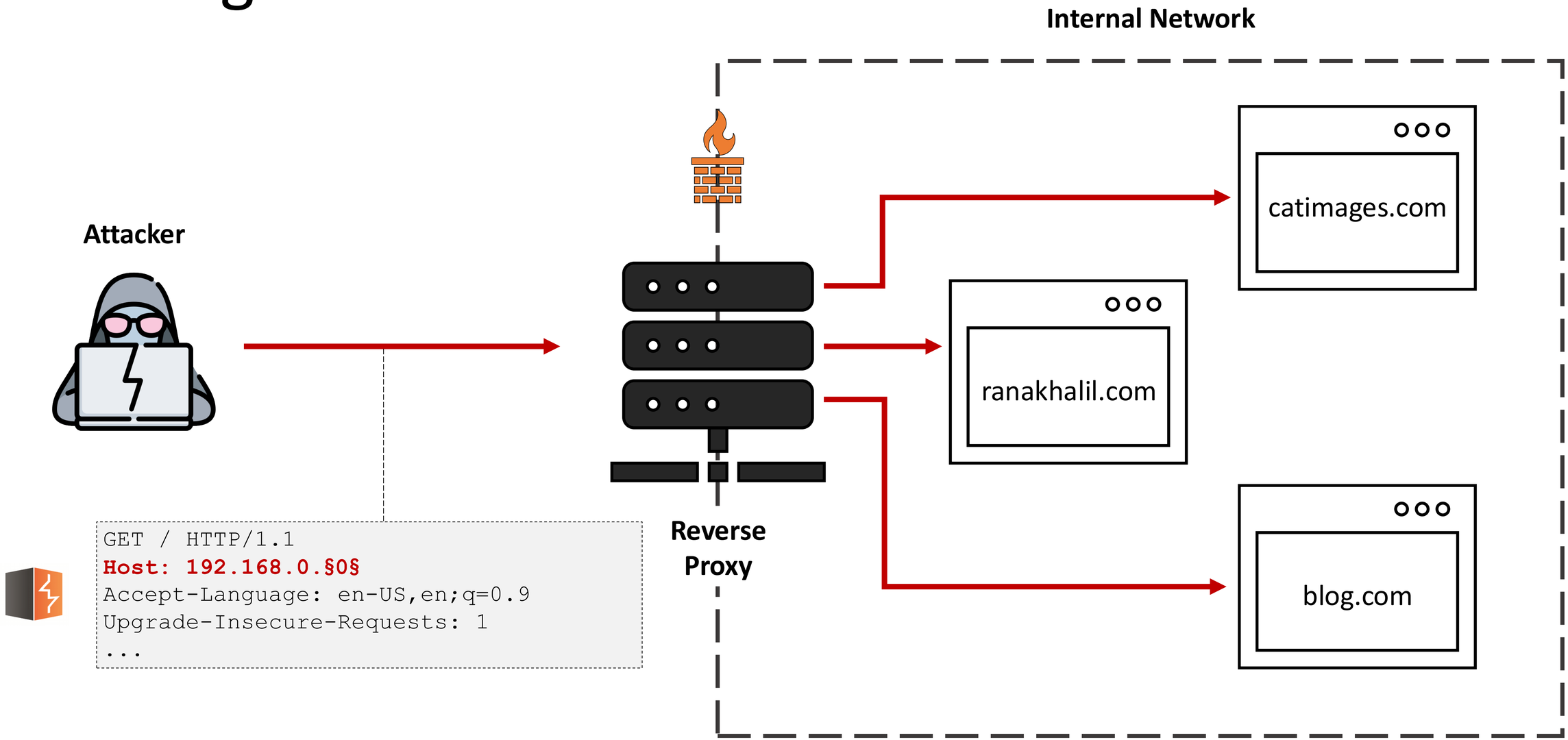
Password Reset Poisoning



Host Header Authentication Bypass



Routing-based SSRF



HTTP Host Header Attacks Labs

LAB APPRENTICE
Basic password reset poisoning →

LAB APPRENTICE
Host header authentication bypass →

LAB PRACTITIONER
Web cache poisoning via ambiguous requests →

LAB PRACTITIONER
Routing-based SSRF →

LAB PRACTITIONER
SSRF via flawed request parsing →

LAB PRACTITIONER
Host validation bypass via connection state attack →

LAB EXPERT
Password reset poisoning via dangling markup →

HOW TO SECURE THE HOST HEADER?

Best Practices to Secure the HTTP Host Header

- If possible, avoid using the Host header altogether in server-side code.
- If you must use the host header, make sure to validate it properly against a whitelist of permitted domains.
- Ensure that Host override headers are not supported.
- When you must use absolute URLs, you should require the current domain to be manually specified in a configuration file and refer to this value instead of the Host header.
- When using virtual hosting, you should avoid hosting internal-only websites and applications on the same server as public-facing content.

Resources

- Web Security Academy – HTTP Host Header Attacks
  - *https://portswigger.net/web-security/host-header*
- Web Security Academy – HTTP Host Header Attacks Labs
  - *https://portswigger.net/web-security/all-labs#http-host-header-attacks*