

SSRF – Server-side Request Forgery

Exploração de vulnerabilidades SSRF

Segurança Web – Aula / CTF

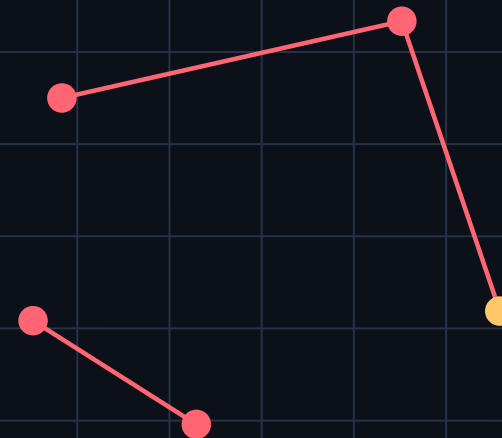
Állan Rocha Pereira

RED TEAM



Tópicos que iremos abordar

- 01 Comunicação HTTP
- 02 Command Injection
- 03 DevTools
- 04 SSRF – Conceitos e exploração
- 05 Atividade Prática PortSwigger



PROTOCOLO HTTP

Comunicação HTTP

Protocolo da camada de aplicação (modelo TCP/IP) que define as regras e o formato da troca de mensagens na web, além disso, ele estrutura não apenas os dados transmitidos, o corpo da mensagem, mas todo o contexto da sessão, como métodos de ação, cabeçalhos, parâmetros e códigos de estado.

FLUXO DE COMUNICAÇÃO



EXEMPLO TÉCNICO

Requisição e Resposta HTTP



HTTP/Requisição

POST /product/stock HTTP/1.1

Host: shop.example

Content-Type: application/x-www-form-urlencoded

Cookie: session= ...

Content-Length: ...

stockApi=https://stock.example/check?id=7



HTTP/Resposta

HTTP/1.1 200 OK

Content-Type: application/json

Cache-Control: no-store

Set-Cookie: session=...; Secure; HttpOnly

{"stock": 18}

PROTOCOLO HTTP

Fluxo de requisição



CLIENT-SIDE

Client decide os dados!

interface / navegador

FORMULÁRIO EXIBIDO

País

Brasil ▼

user_id = 42 readonly

role = user hidden

ENVIAR

HTTP / requisição alterada

POST /profile/update HTTP/1.1
Content-Type: application/x-www-form-urlencoded

country=XX&user_id=99&role=admin

A interface pode limitar valores, mas o servidor recebe qualquer valor

COMMAND INJECTION

Dados virando comandos!

O servidor espera um valor, o shell interpreta de outra forma.



backend / comando

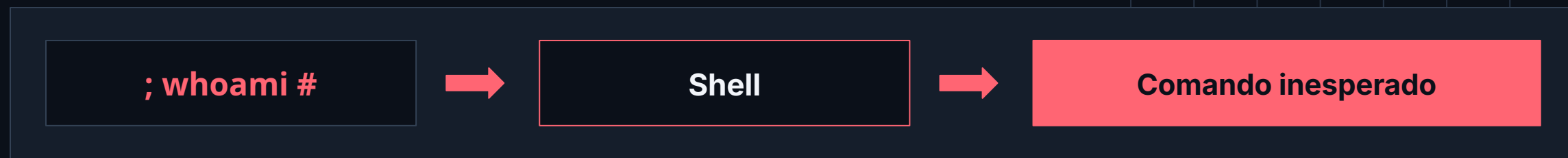
```
Entrada esperada: UTC  
Código:          system("TZ=" + input + " date")  
Entrada alterada: ; whoami #  
Resultado:       TZ=; whoami # date
```

01 Dado controlado**02** Shell interpreta**03** Comando inesperado

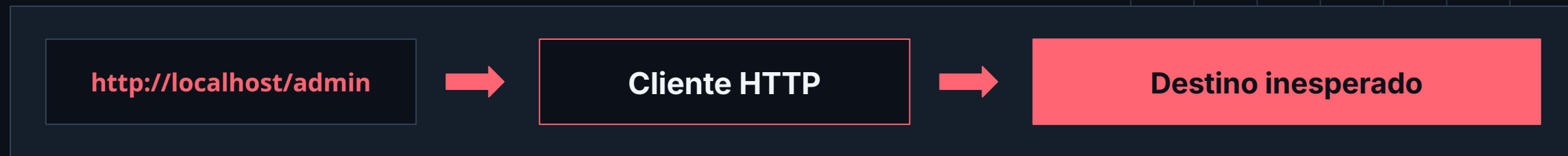
MODELO MENTAL

Injeção e SSRF

COMMAND INJECTION



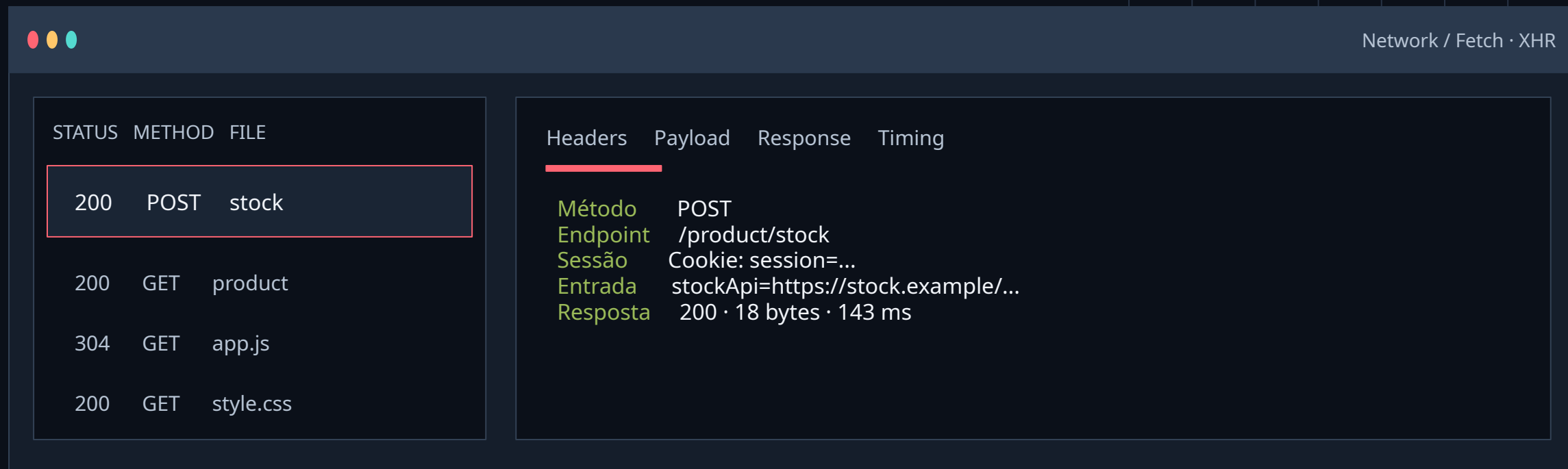
SERVER-SIDE REQUEST FORGERY



A entrada atravessa a aplicação e executa algo indevido!

DEVTOOLS

Lendo uma requisição



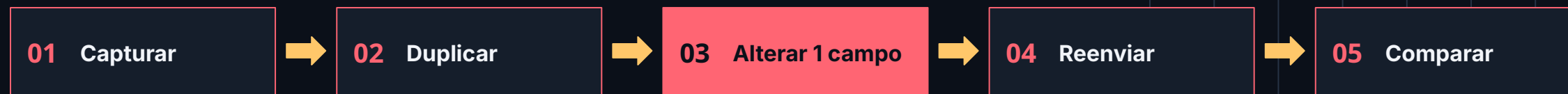
The screenshot shows the Chrome DevTools Network tab. The top bar indicates 'Network / Fetch · XHR'. The left pane displays a list of requests with columns for STATUS, METHOD, and FILE. The first request, a POST to 'stock', is highlighted with a red box. The right pane shows the details for this request, with tabs for Headers, Payload, Response, and Timing. The 'Método' (Method) is POST, the 'Endpoint' is /product/stock, the 'Sessão' (Session) is Cookie: session=..., the 'Entrada' (Input) is stockApi=https://stock.example/..., and the 'Resposta' (Response) is 200 · 18 bytes · 143 ms.

STATUS	METHOD	FILE
200	POST	stock
200	GET	product
304	GET	app.js
200	GET	style.css

Headers	Payload	Response	Timing
Método	POST		
Endpoint	/product/stock		
Sessão	Cookie: session=...		
Entrada	stockApi=https://stock.example/...		
Resposta	200 · 18 bytes · 143 ms		

DEVTOOLS

Editar e reenviar



requisição / original

```
POST /product/stock HTTP/1.1
stockApi=https://stock.example/check?id=7
```

requisição / editada

```
POST /product/stock HTTP/1.1
stockApi=http://localhost/admin
```

Matenha o contexto (Headers) → Mude algo (Payload) → Compare as respostas

PRÓXIMO PASSO

DevTools e Burp Suite

DEVTOOLS

Entender a requisição

- Ver método, URL e cabeçalhos
- Ler corpo e resposta
- Editar e reenviar manualmente



BURP SUITE

Escalar o teste

- Interceptar antes do envio
- Repetir e organizar tentativas
- Variar entradas com controle

Mesma ideia: observar, formular uma possível falha e testar.

SSRF

Server-Side Request Forgery

O atacante induz a aplicação a fazer uma requisição para um destino não indevido!



Alcance do ataque:

ORIGEM DA REQUISIÇÃO



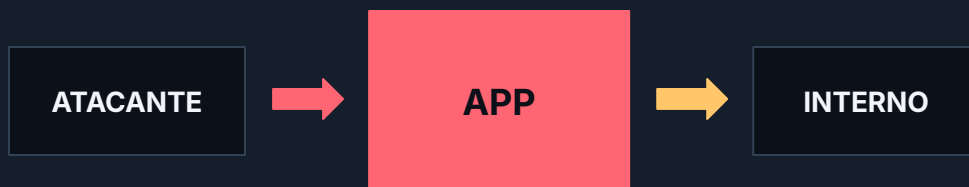
O SSRF se passa pelo servidor mantendo conexões que a aplicação já podia realizar.

TIPOS DE SSRF

Basic SSRF e Blind SSRF

BASIC SSRF

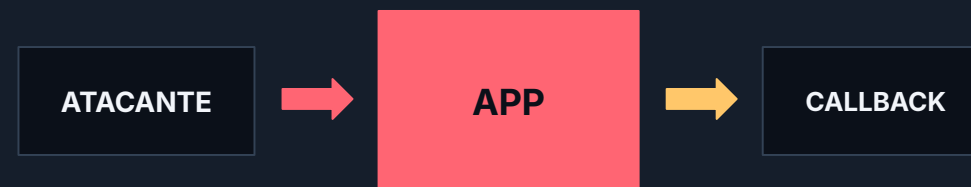
A resposta fica visível no retorno



HTML · JSON · status · efeito observado

BLIND SSRF

A resposta não retorna para o client



OAST · DNS · tempo · erro indireto

RISCO E MITIGAÇÃO

Sinais, impactos e defesas

SINAIS

01 Entrada contém URL ou host

02 Backend busca recursos

03 Resposta ou tempo varia

04 Erros citam conexão

IMPACTOS

01 Leitura de dados internos

02 Ações administrativas

03 Acesso À credenciais

04 Falsificação de origem

DEFESAS

01 Allowlist de destinos

02 Bloqueio após resolução DNS

03 Revalidar redirecionamentos

04 Restringir saída e autenticar

Atividade Prática

CTF no PortSwigger + Extra HTB

LAB 01

SSRF contra a própria
aplicação
EASY

LAB 02

SSRF contra outro
sistema
EASY

LAB 03

Blind SSRF com chamada
externa
MEDIUM

LAB 04

SSRF contra filtro
Blacklist
MEDIUM

LAB 05

SSRF com falha de
OpenRedirect
MEDIUM

LAB 06

SSRF com Whitelist Block
AVANÇADO

LAB HTB

NomadNotes
MONSTER