Práticas de Programação Segura

Aula 2

Tiago Lage Payne de Pádua

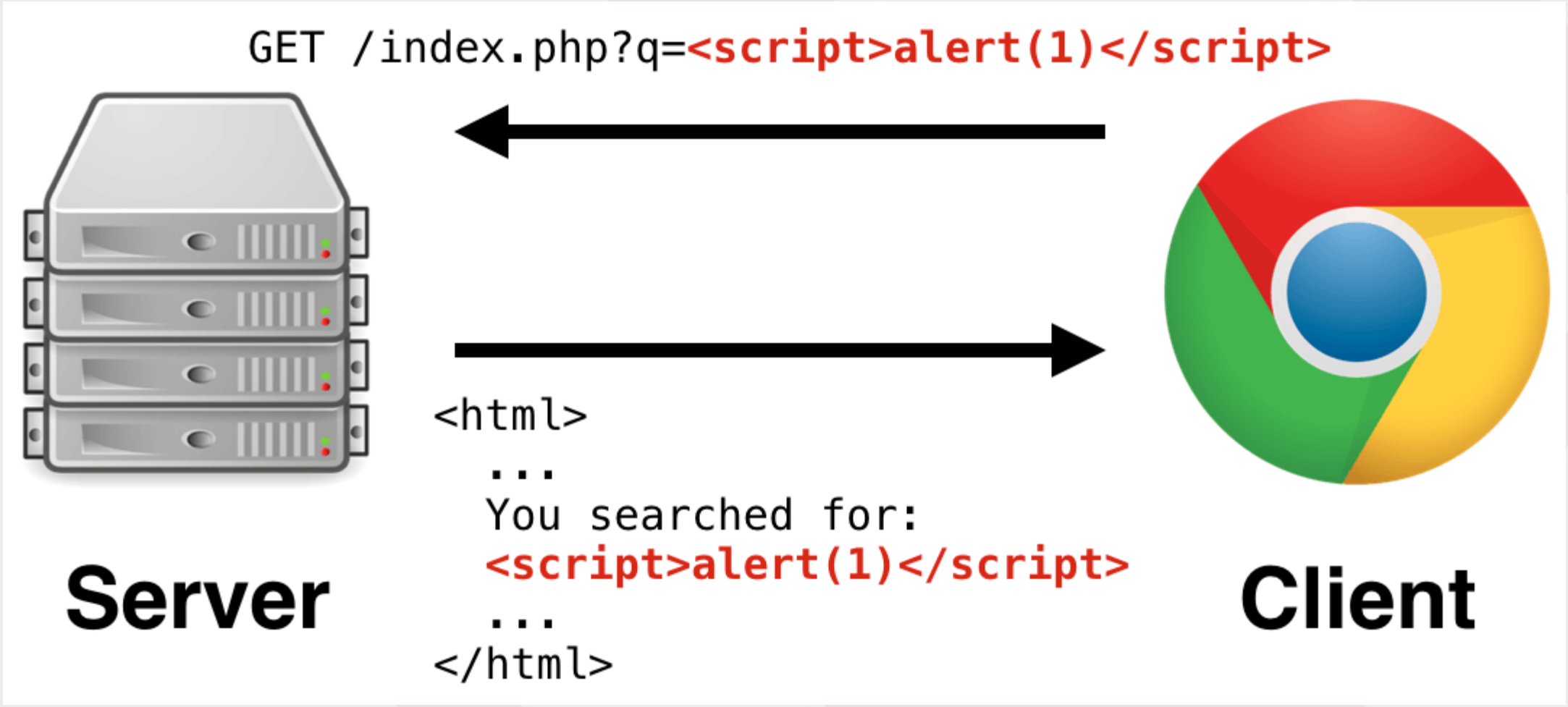
❑ Validação dos Dados de Entrada

```
<div>
        <label for="email">Email: </label>
        <input type="email" name="email" id="email">
</div>
<div>
        <label for="url">Website: </label>
        <input type="url" name="url" id="url">
</div>
<div>
        <label for="number">Number: </label>
        <input type="number" name="number" id="number" min="0" max="100" step="10" value="0">
</div>
<div>
        <label for="range">Range: </label>
        <input type="range" name="range" id="range" min="0" max="100" step="10" value="0">
</div>
<div>
        <label for="date">Date: </label>
        <input type="date" name="date" id="date">
</div>
<div>
        <label for="time">Time: </label>
        <input type="time" name="time" id="time">
</div>
```

❑ Validação dos Dados de Entrada

- Realização de validação de dados em sistemas confiáveis;
- Validação de condução e identificação de dados em termos de fontes confiáveis e não confiáveis;
- Validação de dados com base no tipo de dados, intervalo e comprimento de entrada em relação a uma lista de caracteres permitidos;
- Verificar e validar se os valores nos cabeçalhos de solicitações e respostas estão apenas em caracteres ASCII;
- Validar todos os dados fornecidos pelo cliente/usuário antes que os dados sejam processados, incluindo URLs, cabeçalhos HTTP, código incorporado, etc;

❑ Codificação de Dados de Saída



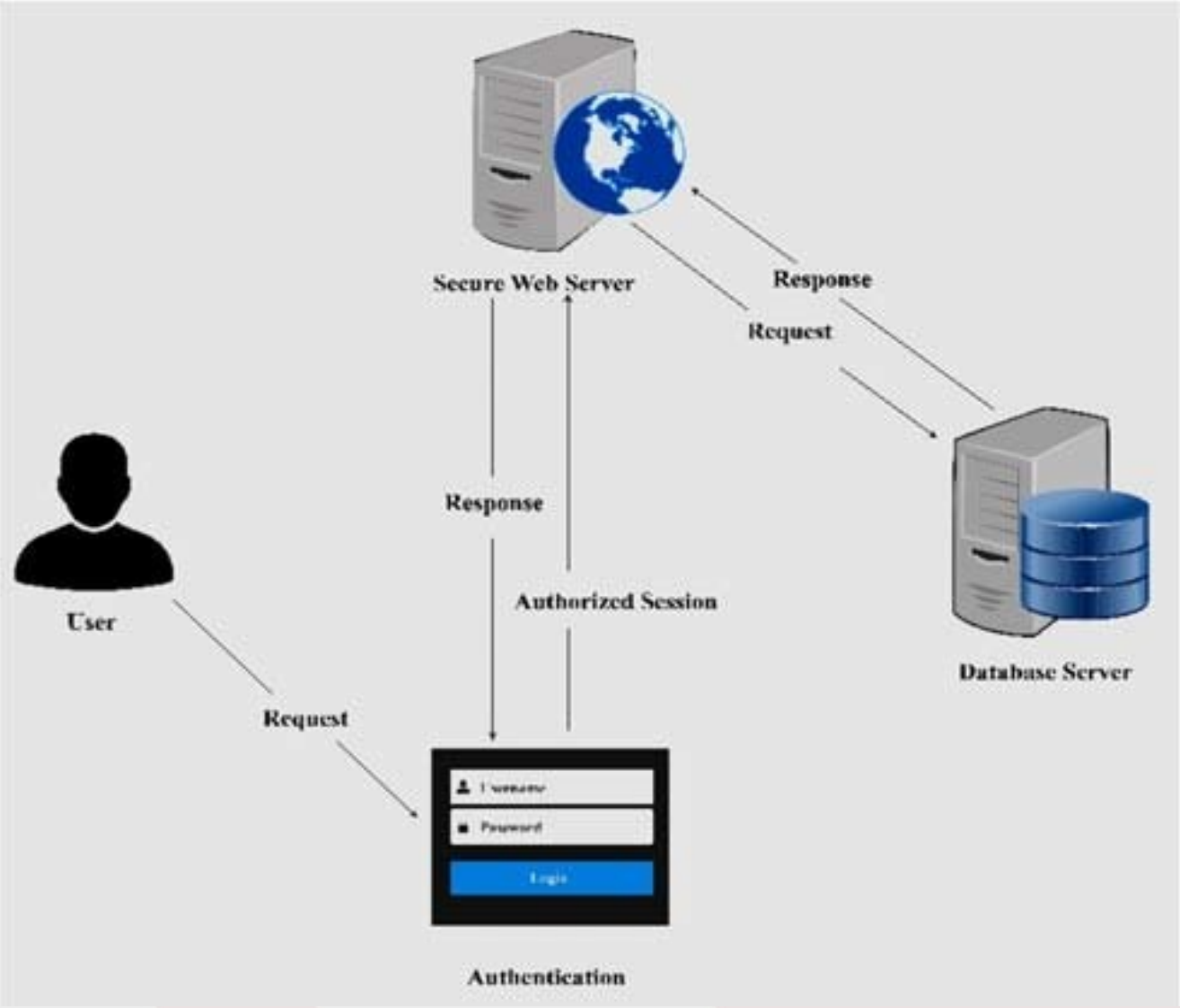
❑ Codificação de Dados de Saída

- Validar dados em um sistema confiável;
- Codificar todos os caracteres, a menos que sejam considerados seguros para o interpretador de destino;
- Sanitização de saída de dados não confiáveis usando comandos do SO;

❑ Autenticação e Gerenciamento de Credenciais

- Requerer autenticação para todas as páginas e recursos, exceto para aqueles que são intencionalmente públicos;
- Impedir a reutilização de senhas;
- Notificar os usuários quando ocorrer uma redefinição de senha;
- Relatar o número de falhas de login ao usuário no próximo login bem-sucedido;
- Manter um tempo de expiração curto para senhas temporárias que precisam ser alteradas no próximo login;
- Exigir que as senhas sejam definidas com base na política de complexidade de senha.

❑ Gerenciamento de Sessões



❑ Gerenciamento de Sessões

- Sessões e conexões devem ser totalmente encerradas após o logout;
- Vários logins não devem ser permitidos no mesmo ID de usuário;
- Com base nos riscos e objetivos de negócios, o intervalo de tempo limite de inatividade da sessão deve ser o mais baixo possível;