Relatório de Correção de Vulnerabilidades

1. Cabeçalho da Política de Segurança de Conteúdo (CSP) Não Definido

Problema: A falta de um cabeçalho CSP permite a injeção de scripts maliciosos (XSS).

Correção: Adicione a seguinte diretiva no cabeçalho da resposta HTTP:

header("Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline'; object-src 'none';");

---

2. Cabeçalho Anti-Clickjacking Ausente

Problema: Sem esse cabeçalho, um atacante pode carregar seu site dentro de um iframe malicioso.

Correção: Adicione o seguinte cabeçalho HTTP:

header("X-Frame-Options: DENY");

Ou para permitir apenas sua própria origem:

header("X-Frame-Options: SAMEORIGIN");

---

3. Ausência de Tokens Anti-CSRF

Problema: Requisições maliciosas podem ser enviadas em nome do usuário autenticado.

Correção: Gerar e validar um token CSRF:

```
// Gerar token (no início da sessão)
session_start();
if (!isset($_SESSION['csrf_token'])) {
  $_SESSION['csrf_token'] = bin2hex(random_bytes(32));
}

// Incluir no formulário
echo '<input type="hidden" name="csrf_token" value="'.$_SESSION['csrf_token'].'">';
```

No processamento do POST:

```
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
  if (!isset($_POST['csrf_token']) || $_POST['csrf_token'] !== $_SESSION['csrf_token']) {
    die("CSRF token inválido.");
  }
```

}

---

4. Cookie sem atributo SameSite

Problema: Cookies sem SameSite podem ser enviados em contextos inseguros.

Correção: Definir SameSite e Secure nos cookies:

```
setcookie("sessao", session_id(), [
  'httponly' => true,
  'secure' => true,
  'samesite' => 'Strict'
]);
```

---

5. Vazamento de Informações do Servidor

Problema: O cabeçalho Server revela informações sobre o servidor web.

Correção: Para servidores Apache, edite apache2.conf ou .htaccess:

```
ServerTokens Prod
ServerSignature Off
```

Para Nginx, adicione no nginx.conf:

```
server_tokens off;
```

---

6. Cabeçalho X-Content-Type-Options Ausente

Problema: Sem esse cabeçalho, navegadores podem inferir o tipo de conteúdo, facilitando ataques XSS.

Correção: Adicionar no cabeçalho HTTP:

```
header("X-Content-Type-Options: nosniff");
```

---

7. Resposta de Gerenciamento de Sessão Identificada

Problema: A resposta pode conter informações sensíveis sobre a sessão.

Correção: Certifique-se de que nenhuma informação de sessão é exposta na resposta HTTP.

```
session_regenerate_id(true);
```

---

8. Fuzzer do Agente do Usuário

Problema: O sistema pode estar vulnerável a ataques de manipulação de User-Agent.

Correção: Filtrar e validar cabeçalhos HTTP suspeitos:

```
$allowed_agents = ['Mozilla', 'Chrome', 'Safari'];
if (!in_array($_SERVER['HTTP_USER_AGENT'], $allowed_agents)) {
   die("Acesso negado.");
}
```
