Relatório de Correção

1. **Configuração de HttpOnly** e **Uso de Secure**:

   Correção do arquivo php.int localizado em: **/var/www/html**

`session.cookie_httponly = 1`

`session.cookie_secure = 1`

2. **Ação Corretiva**:

Restringir o Acesso aos Diretórios Sensíveis:

1. Criou-se regras no Apache para restringir o acesso a esses diretórios, utilizando o arquivo de configuração: **/etc/apache2/apache2.conf**
- Assegurou-se que os diretórios `/config/`, `/docs/`, e `/external/` foram protegidos adequadamente para evitar o acesso público.

3. **Configuração do robots.txt**:

Editou-se o arquivo robots.txt localizado em: **/var/www/html**/robots.txt

```
User-agent: *
Disallow: /config/
Disallow: /docs/
Disallow: /external/
```

4. Acesso à Página de Login

4.1 Procedimentos realizados:

- Instalação do fail2ban
- configuração do fail2ban para proteger os serviços do servidor como ssh, dvwa dentre outros
  - `sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local`
  - sudo fail2ban-client status
- criação de um filtro personalizado com fail2ban e configuração personalizada para o dvwa
  - /etc/fail2ban/filter.d
  - sudo nano /etc/fail2ban/jail.d/dvwa-login.conf
  - `sudo fail2ban-client set dvwa-login unbanip 10.0.0.100`
- edição no arquivo `/etc/fail2ban/jail.conf`

5. Correção de serviços no servidor

1. Corrigiu-se o erro onde aparece a versão do Apache e porta do serviço nas pagina de forbbiden:
   a. editou-se o arquivo em: `/etc/apache2/conf-available/security.conf`:
      i.
      ```
      ServerTokens Prod
      ServerSignature Off
      ```

Explicando:

- `ServerTokens Prod` : limita o header `Server:` para apenas “Apache” (sem versão, SO, etc.)
- `ServerSignature Off` :remove a assinatura do Apache das páginas de erro (como `403`, `404`, etc.)

2. Aprimoramento da configuração SSH

a. Desabilitou-se a autenticação via senha no servidor

   i. nano /etc/sshd/sshd_config

b. Gerou-se uma chave rsa no client:

   i.
```
ssh-keygen -t rsa -b 4096 -C "silasmaques@outlook.com"
```

c. copiou-se a chave RSA no arquivo de autorização do servidor

   i.
```
ssh-copy-id -i id_rsa.pub silas@exemple.org
```

```
To                         Action      From
--                         ------      ----
Anywhere                   REJECT      10.0.0.100                # by Fail2B
an after 3 attempts against DVWA
80                         ALLOW       Anywhere
443                        ALLOW       Anywhere
22                         ALLOW       Anywhere
8080                       ALLOW       Anywhere
80 (v6)                    ALLOW       Anywhere (v6)
443 (v6)                   ALLOW       Anywhere (v6)
22 (v6)                    ALLOW       Anywhere (v6)
8080 (v6)                  ALLOW       Anywhere (v6)
```

3.