A6 - Security Misconfiguration

globo.com

GTS 33 | PA 05/2019

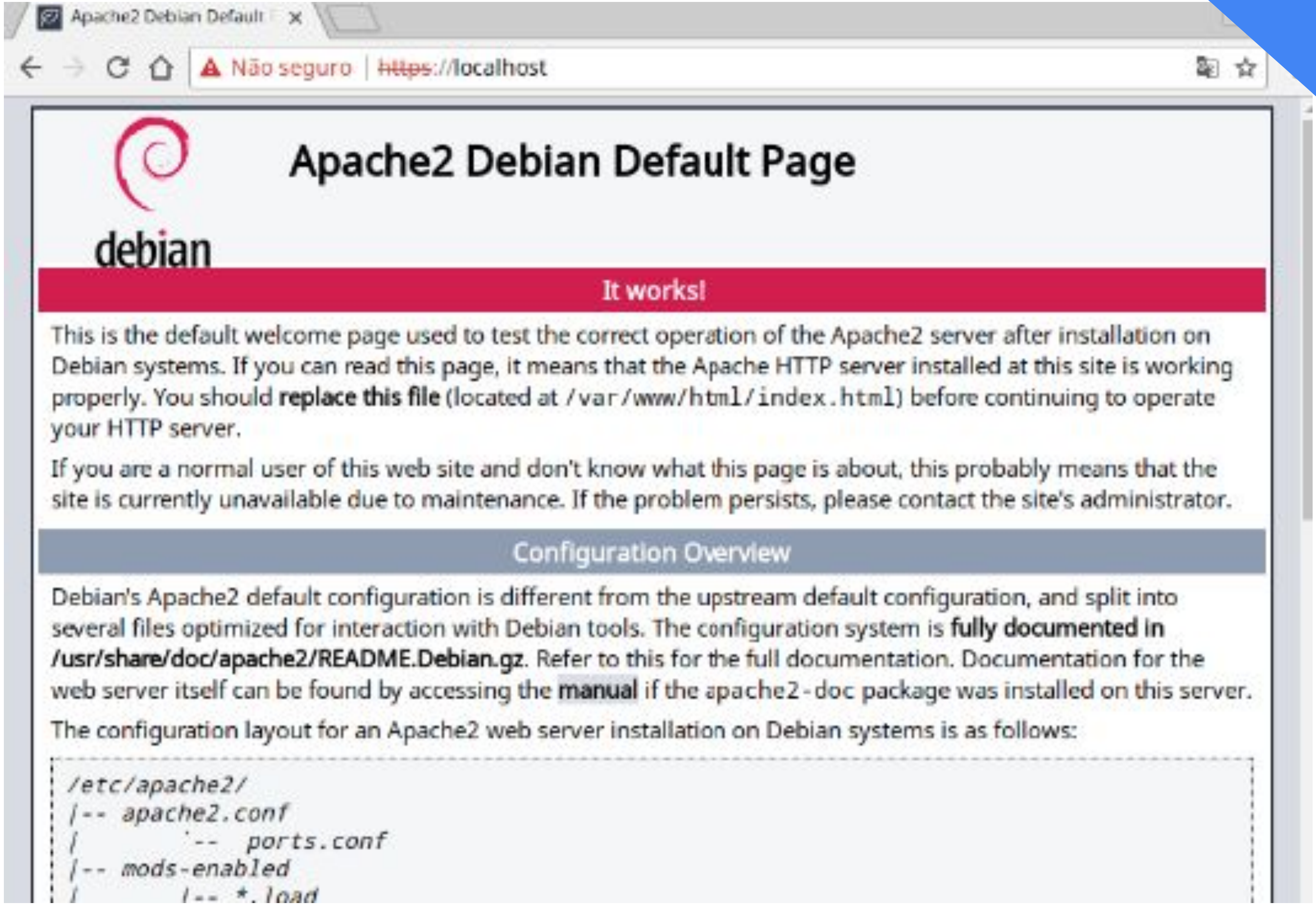
Agenda - A6 - Security Misconfiguration

1. Do que se trata?
2. Exemplos
3. Como se proteger?
4. Stegonography

Do que se trata?

Vulnerabilidade mais comum de todo OWASP Top 10!

É o resultado de configurações inseguras "default", cabeçalhos/métodos HTTP, mensagens de erro "verbose", modo debug habilitado, entre muitas outras!



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

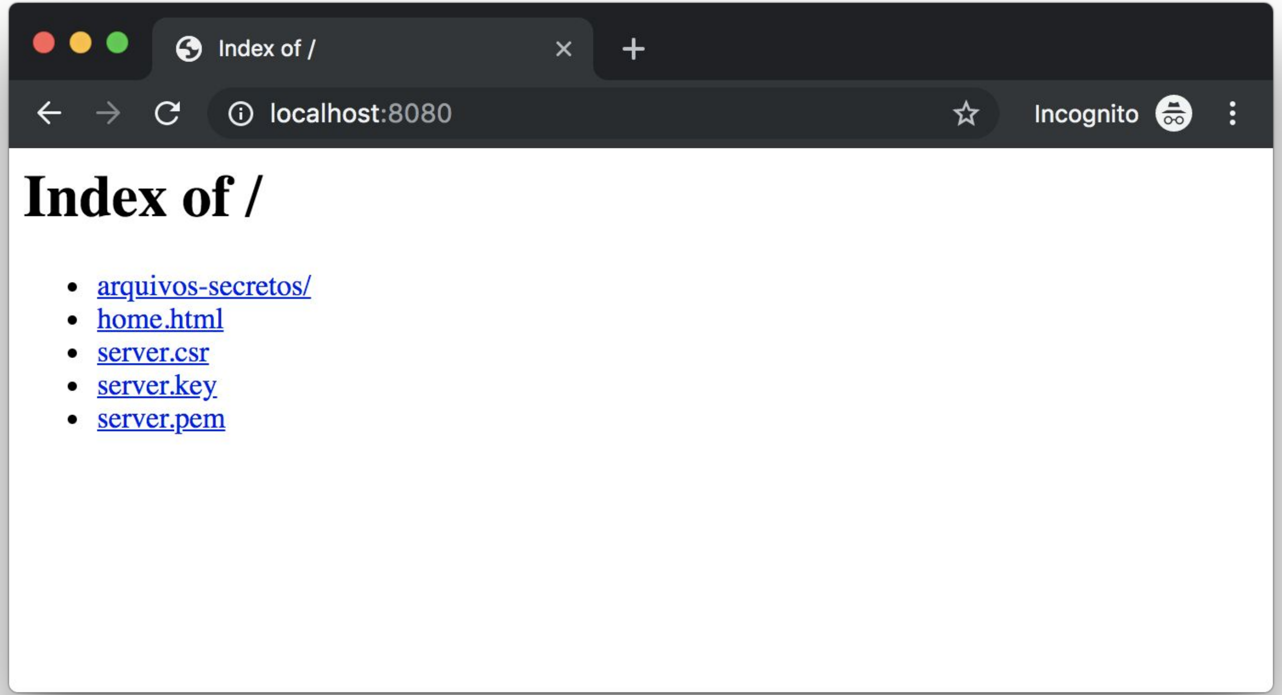
Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
```

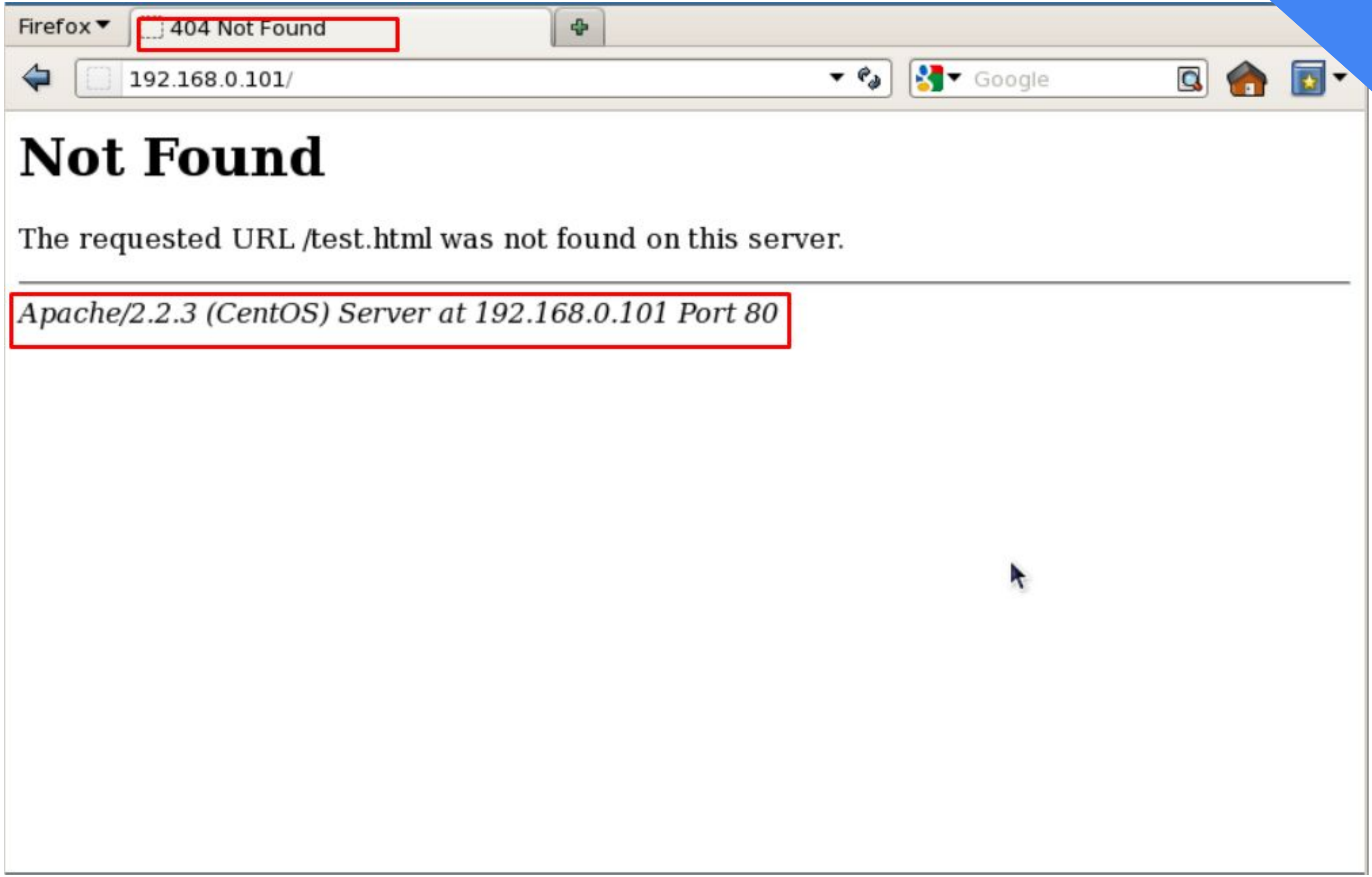
Configuração padrão



Index of /

- arquivos-secretos/
- home.html
- server.csr
- server.key
- server.pem

Arquivos não protegidos

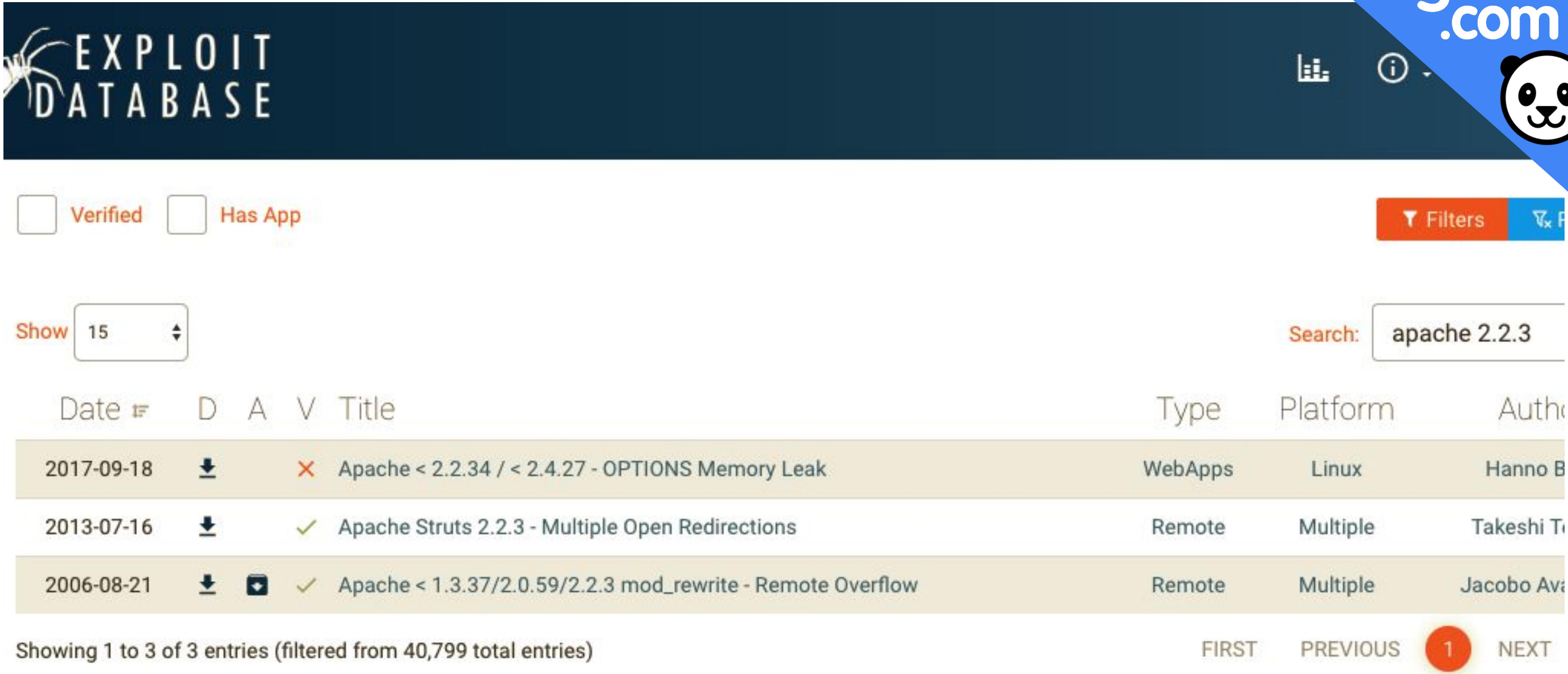


Not Found

The requested URL /test.html was not found on this server.

Apache/2.2.3 (CentOS) Server at 192.168.0.101 Port 80

Mensagens de erro



□ Verified □ Has App

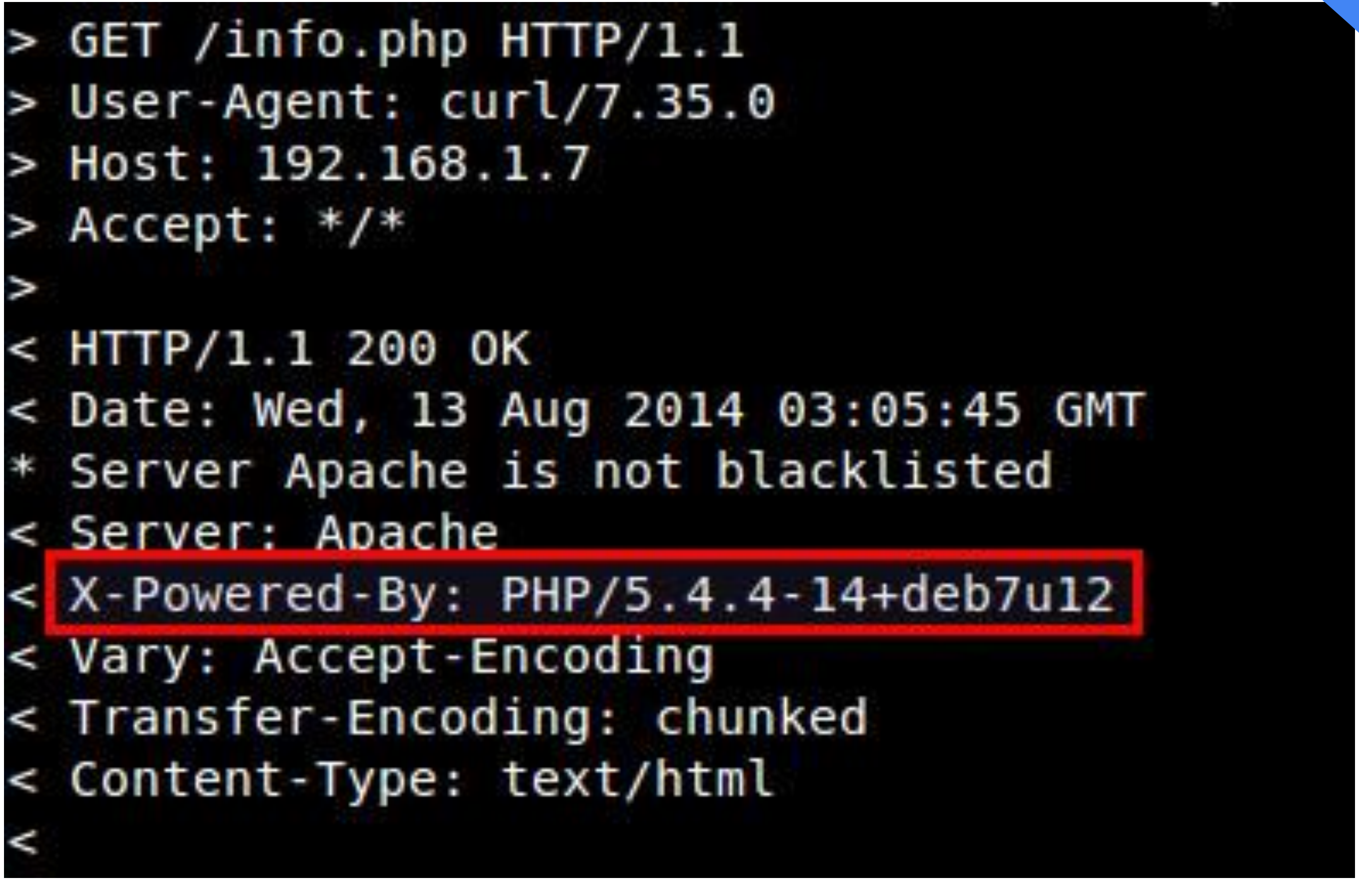
Show 15

Search: apache 2.2.3

Date	D	A	V	Title	Type	Platform	Auth
2017-09-18	⬇		✗	Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak	WebApps	Linux	Hanno B
2013-07-16	⬇		✓	Apache Struts 2.2.3 - Multiple Open Redirections	Remote	Multiple	Takeshi T
2006-08-21	⬇	▣	✓	Apache < 1.3.37/2.0.59/2.2.3 mod_rewrite - Remote Overflow	Remote	Multiple	Jacobo Av

Showing 1 to 3 of 3 entries (filtered from 40,799 total entries)

Mensagens de erro



```
> GET /info.php HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 192.168.1.7
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Wed, 13 Aug 2014 03:05:45 GMT
* Server Apache is not blacklisted
< Server: Apache
< X-Powered-By: PHP/5.4.4-14+deb7u12
< Vary: Accept-Encoding
< Transfer-Encoding: chunked
< Content-Type: text/html
<
```

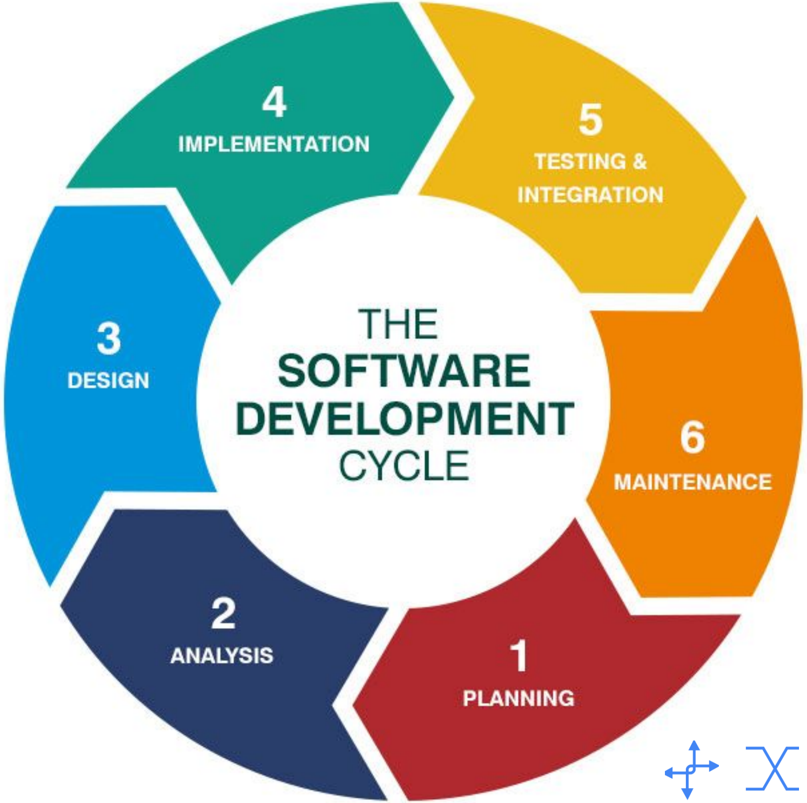
Exposição de informações

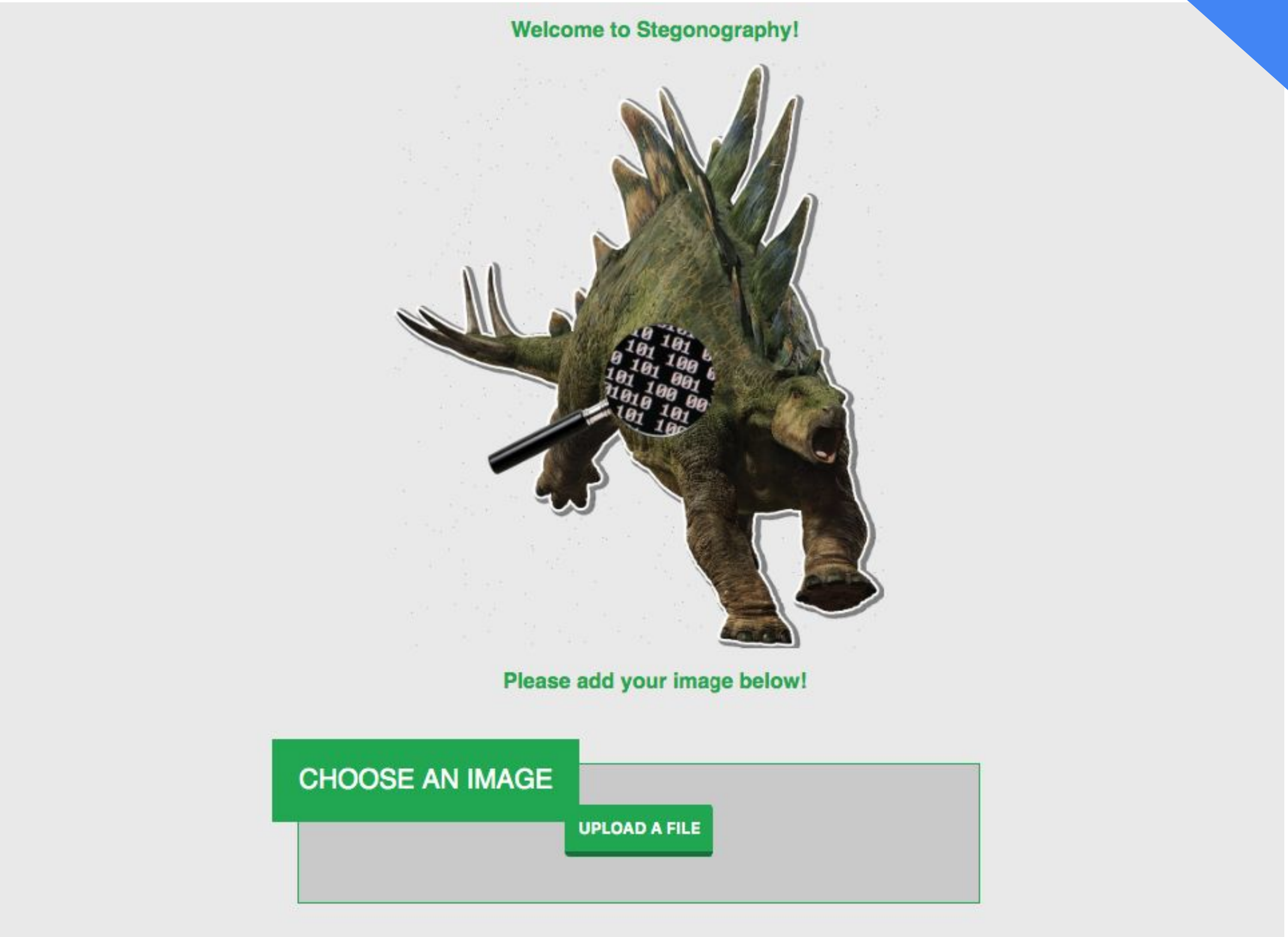
- HSTS
- X-XSS-Protection
- X-Content-Type-Options
- Content-Security-Policy
- Access-Control-Allow-Origin

Cabeçalhos de segurança

Como se proteger?

1. Garantir que cabeçalhos de segurança estejam sempre **habilitados**.
2. Ciclo contínuo de ***hardening*** implementado dentro da equipe para verificar os requisitos e configurações de segurança **regularmente**.





Welcome to Stegonography!

Please add your image below!

Narrativa do ataque

Hands on!

1. Entrar na pasta da app

```
$ cd owasp-top10-2017-apps/a6/stegonography/
```

2. Inicializar o container

```
$ make install
```

3. Acessar a página

```
localhost:10006
```

secDevLabs

A6 - Security Misconfiguration