

Web App Hardening

HTTP Headers

Gildásio Júnior

Conceitos

Conceitos

Hardening

- Hardening vem de deixar algo mais forte, resistente
- **Em computação:** é o processo de deixar um sistema **mais seguro**

Conceitos

Hardening

- Hardening vem de deixar algo mais forte, resistente
- **Em computação:** é o processo de deixar um sistema **mais seguro**

HTTP

- *Hypertext Transfer Protocol* [RFC2616]
- Protocolo para transferência de hipertexto
- Arquitetura cliente-servidor

Conceitos

Hardening

- Hardening vem de deixar algo mais forte, resistente
- **Em computação:** é o processo de deixar um sistema **mais seguro**

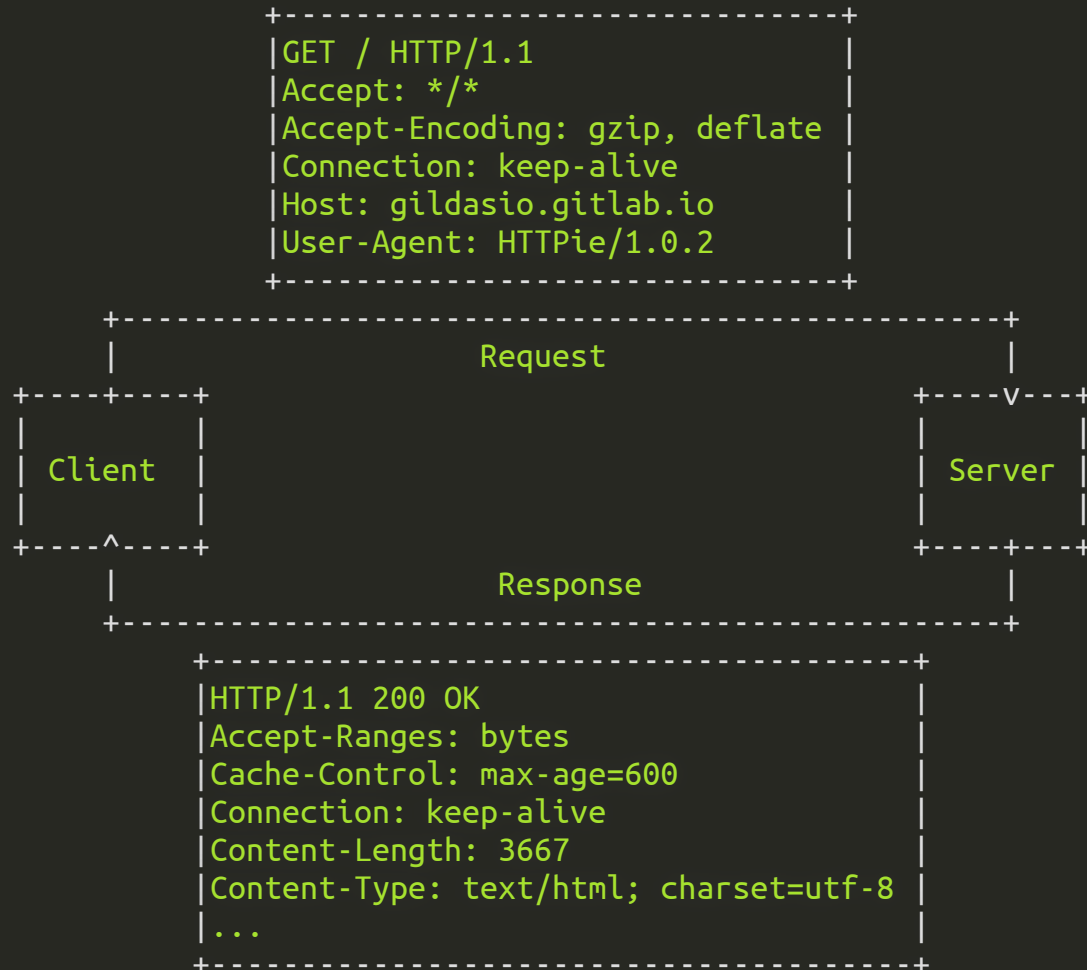
HTTP

- *Hypertext Transfer Protocol* [RFC2616]
- Protocolo para transferência de hipertexto
- Arquitetura cliente-servidor

Defesa em Profundidade

- Não depender apenas de um mecanismo de defesa aplicado, por mais seguro que seja

HTTP



Arquitetura web

Atores envolvidos



Arquitetura web

Atores envolvidos



Problemas de Segurança

Problemas de segurança

Information Disclosure

Session Hijacking

MITM

XSS

CSRF

ClickJacking

Information Disclosure

Serviço deixa exposto algumas informações

Informações que podem facilitar a vida de atacantes

Exemplos:

- Servidor
- Linguagem de programação
- Framework
- CMS
- Dados da aplicação
- ...

Mais info: https://en.wikipedia.org/wiki/Information_disclosure_statement

Session Hijacking

Roubo de Sessão

Atacante consegue pegar o identificador da sessão do usuário

Utiliza esse identificador para ter acesso à aplicação com o mesmo privilégio do usuário

Mais info: https://pt.wikipedia.org/wiki/Session_hijacking

MITM

Man in The Middle

Atacante se coloca no meio da troca de dados

Sendo assim, consegue editar o tráfego para os envolvidos

Mais info: https://pt.wikipedia.org/wiki/Ataque_man-in-the-middle

MITM

Man in The Middle



MITM

Man in The Middle



XSS

Cross Site Script

Aplicação recebe dados do usuário mas não sanitiza

Atacante percebe isso e insere strings especiais nos inputs

Pela forma como foi colocado na página, essas strings serão interpretadas como script

Mais info: https://pt.wikipedia.org/wiki/Cross-site_scripting

CSRF

Cross Site Request Forgery

Aplicação não valida de onde veio a requisição

Assim permite que, de qualquer lugar, possa ser feita uma requisição à aplicação

Atacante cria um site que, quando acessado pela vítima, faz a requisição para o sistema alvo como se fosse o usuário

Mais info: https://pt.wikipedia.org/wiki/Cross-site_request_forgery

ClickJacking

Aplicação maliciosa rouba clicks do usuário

Atacante cria uma aplicação diferente que parece inofensiva

Mas, *por debaixo* dos panos, a interação do usuário é feita na verdade com o sistema alvo

Mais info: <https://pt.wikipedia.org/wiki/Clickjacking>

Problemas de segurança

Information Disclosure ✓

Problemas de segurança

Information Disclosure ✓

Session Hijacking ✓

Problemas de segurança

Information Disclosure ✓

Session Hijacking ✓

MITM ✓

Problemas de segurança

Information Disclosure ✓

Session Hijacking ✓

MITM ✓

XSS ✓

Problemas de segurança

Information Disclosure ✓

Session Hijacking ✓

MITM ✓

XSS ✓

CSRF ✓

Problemas de segurança

Information Disclosure ✓

Session Hijacking ✓

MITM ✓

XSS ✓

CSRF ✓

ClickJacking ✓

Mecanismos de Defesa

Cabeçalhos

Informações do Servidor

Podem dar detalhes como versão específica da ferramenta ao atacante

- Server
- X-Powered-By
- X-AspNet-Version
- X-Powered-CMS
- Powered-By
- X-Drupal-Version
- Set-Cookie
- ...

Remova eles (ou diminua o detalhamento)

Cabeçalhos

Cookies

Flag **HttpOnly**

Uso do cookie é permitido apenas para enviar via HTTP

Ajuda a prevenir roubo de sessão

Cabeçalhos

Cookies

Flag **HttpOnly**

Uso do cookie é permitido apenas para enviar via HTTP

Ajuda a prevenir roubo de sessão

Flag **Secure**

Transferência do cookie é feita apenas via canal criptografado (HTTPS)

Ajuda a prevenir information disclosure e diminuir impactos de MITM

Cabeçalhos

Cookies

Flag **HttpOnly**

Uso do cookie é permitido apenas para enviar via HTTP

Ajuda a prevenir roubo de sessão

Flag **Secure**

Transferência do cookie é feita apenas via canal criptografado (HTTPS)

Ajuda a prevenir information disclosure e diminuir impactos de MITM

Flag **SameSite**

Informa que o cookie só deve ser enviado caso a requisição seja feita a partir do próprio site

Ajuda a prevenir ataques CSRF

Cabeçalhos

Referrer-Policy

Informa ao browser qual informação deve ser enviada no cabeçalho `Referer` das requisições

Podem ser definidas algumas condições, como o protocolo, destino...

Ajuda a diminuir informações divulgadas

Cabeçalhos

Referrer-Policy

Informa ao browser qual informação deve ser enviada no cabeçalho `Referer` das requisições

Podem ser definidas algumas condições, como o protocolo, destino...

Ajuda a diminuir informações divulgadas

X-XSS-Protection

Instrui o browser sobre o uso da funcionalidade de filtro de XSS refletido

Qual ação tomar: bloquear, sanitizar, aceitar, reportar...

Ajuda a diminuir ataques de XSS e melhora monitoramento do comportamento da aplicação

Cabeçalhos

X-Frame-Options

Informa ao browser se o site pode ser utilizado em um frame ou não

Ajuda a proteger contra ataques de clickjacking

Cabeçalhos

X-Frame-Options

Informa ao browser se o site pode ser utilizado em um frame ou não

Ajuda a proteger contra ataques de clickjacking

Content-Security-Policy

Informa ao browser de onde podem ser carregados conteúdos, exemplo: JavaScript

Pode desabilitar recursos carregados de outros sites, **JavaScript inline**, etc

Ajuda a proteger contra ataques de XSS

Cabeçalhos

Strict-Transport-Security (HSTS)

Informa ao browser que o site deve ser acessado apenas via HTTPS

Guarda essa informação para uso futuro: todas as próximas requisições serão feitas dessa forma

Pode deixar essa opção "hardcoded" no navegador com a opção `preload`

Ajuda a diminuir eficácia de MITM

Cabeçalhos

Public-Key-Pins

Informa ao browser que o site deve ser acessado apenas com determinada chave

Também guarda essa informação para uso futuro: uma conexão que vier com outra chave não será aceita

Ajuda a diminuir eficácia de MITM

Atenção: Se for habilitar, informe ao menos duas chaves, para ter backup em caso de extravio ou renovação

Teste sua Aplicação

h2t

HTTP Hardening Tool

github.com/gildasio/h2t

Ferramenta para hardening de aplicações web

Estágio atual:

Analisa cabeçalhos HTTP da aplicações e sugere melhorias:

- Cabeçalhos a **remover/modificar**
- Cabeçalhos a adicionar

```
venv h2t master $ ./h2t.py scan securityheaders.com
```

```
      eeee  
e    e      8 eeeee  
8    8      8  8  
8eee8 eee8    8e  
88   8 8      88  
88   8 8eee   88
```

<https://github.com/gildasio/h2t>

Output explanation:

- [+] Good headers. Already used in your website. Good job!
- [+] Good headers. We recommend applying it
- [-] Bad headers. We recommend remove it

<http://securityheaders.com>

- [-] Content-Security-Policy too permissive
- [-] Server
- [+] Except-CT
- [+] Clear-Site-Data
- [+] X-Permitted-Cross-Domain-Policies
- [+] Public-Key-Pins
- [+] X-Download-Options

```
venv h2t master $
```

```
venv h2t master $ ./h2t.py scan securityheaders.com -s
```

```
|      /\      |  
| /\      . /\  |  
|      | /__  |
```

<https://github.com/gildasio/h2t>

Output explanation:

- [+] Good headers. Already used in your website. Good job!
- [+] Good headers. We recommend applying it
- [-] Bad headers. We recommend remove it

<http://securityheaders.com>

- [-] Content-Security-Policy too permissive
- [-] Server
- [+] Content-Security-Policy
- [+] Feature-Policy
- [+] X-Content-Type-Options
- [+] HTTP Strict Transport Security [HSTS]
- [+] X-Frame-Options
- [+] Referrer-Policy
- [+] X-XSS-Protection

```
venv h2t master $
```

```
venv h2t master $ ./h2t.py list
```



```
https://github.com/gildasio/h2t
```

```
[ - ] Access-Control-Allow-Origin too open
[ - ] X-Permitted-Cross-Domain-Policies too open
[ - ] HSTS without includeSubDomains
[ - ] HSTS without preload
[ - ] Cookie not HTTP Only
[ - ] Cookie not over SSL/TLS
[ - ] Cookie not only from SameSite
[ - ] Content-Security-Policy too permissive
[ - ] Server
[ - ] Public-Key-Pins without a backup key
[ - ] Referrer-Policy with bad practices
[ + ] X-Permitted-Cross-Domain-Policies
[ + ] HTTP Strict Transport Security [HSTS]
[ + ] X-Content-Type-Options
[ + ] Clear-Site-Data
[ + ] X-Download-Options
[ + ] Feature-Policy
[ + ] X-Frame-Options
[ + ] Except-CT
[ + ] Content-Security-Policy
[ + ] Public-Key-Pins
[ + ] Referrer-Policy
[ + ] X-XSS-Protection
```

```
venv h2t master $ ./h2t.py list -H set-cookie Public-Key-Pins X-Frame-Options --print description
```

<https://github.com/gildasio/h2t>

[-] Public-Key-Pins without a backup key

Description: Using Public-Key-Pins with only one key is dangerous because if you lost your key (CA hacked, renew...) the user can't access the site with the new key once the browser will not accept the new key.

```
[-] Cookie not HTTP Only
```

Description: Using the flag 'HttpOnly' the cookie won't be read from JavaScript only sent by HTTP

```
[-] Cookie not over SSL/TLS
```

Description: Using the flag 'Secure' the cookie will be sent only in HTTPS traffic avoiding MITM read its content

```
[-] Cookie not only from SameSite
```

```

Description: Samesite cookies tells to browser send the cookie only in requests initiated from the
same domain. It avoid CSRF attacks

```

[+] Public-Key-Pins

Description: Treat website as valid only if that HTTPS certificate match a hash in this list

[+] X-Frame-Options

Description: X-Frame-Options indicates to browser if the website can be framed or not. It protects against clickjacking attacks

```
venv h2t master $
```

```
venv h2t master $ ./h2t.py scan gildasio.gitlab.io -v
```

```
  _/
 _/_/_/  _/_/_/  _/_/_/_/
 _/_/_/  _/_/_/  _/_/_/_/
 _/_/_/  _/_/_/  _/_/_/_/
 _/_/_/  _/_/_/  _/_/_/_/
```

```
https://github.com/gildasio/h2t
```

Output explanation:

- [+] Good headers. Already used in your website. Good job!
- [+] Good headers. We recommend applying it
- [-] Bad headers. We recommend remove it

```
http://gildasio.gitlab.io
```

```
HTTP/1.1 200 OK
```

```
Accept-Ranges: bytes
```

```
Cache-Control: max-age=600
```

```
Content-Length: 3667
```

```
Content-Type: text/html; charset=utf-8
```

```
Expires: Tue, 19 Mar 2019 20:43:50 UTC
```

```
Last-Modified: Fri, 23 Nov 2018 21:17:19 GMT
```

```
Vary: Origin
```

```
Date: Tue, 19 Mar 2019 20:33:50 GMT
```

- [+] Feature-Policy
- [+] Referrer-Policy
- [+] X-XSS-Protection
- [+] Content-Security-Policy
- [+] X-Download-Options
- [+] X-Content-Type-Options
- [+] X-Frame-Options
- [+] Public-Key-Pins
- [+] X-Permitted-Cross-Domain-Policies
- [+] HTTP Strict Transport Security [HSTS]
- [+] Clear-Site-Data
- [+] Except-CT

```
venv h2t master $
```

Referências

```
venv h2t master $ ./h2t.py list --print description refs
```

[illegible]

<https://github.com/gildasio/h2t>

```
[-] Cookie not HTTP Only
```

Description: Using the flag 'HttpOnly' the cookie

Refs :

<https://tools.ietf.org/html/rfc6265#section-5>.

Obrigado!

Perguntas?

Gildásio Júnior

gildasio@protonmail.com

gildasio.gitlab.io/talks/h2t-semcomp/

github.com/gildasio/h2t