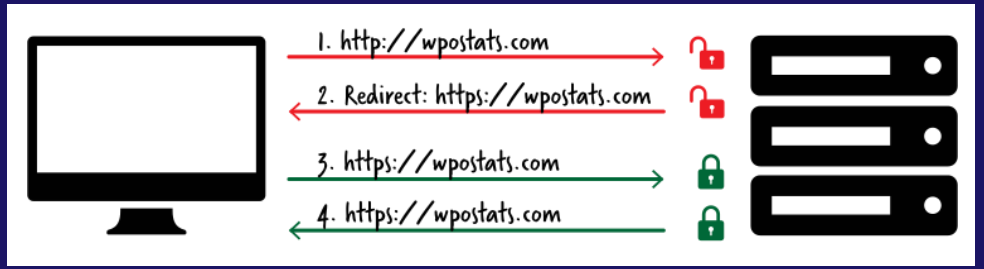
HTTP Security Headers

Why Security Headers?

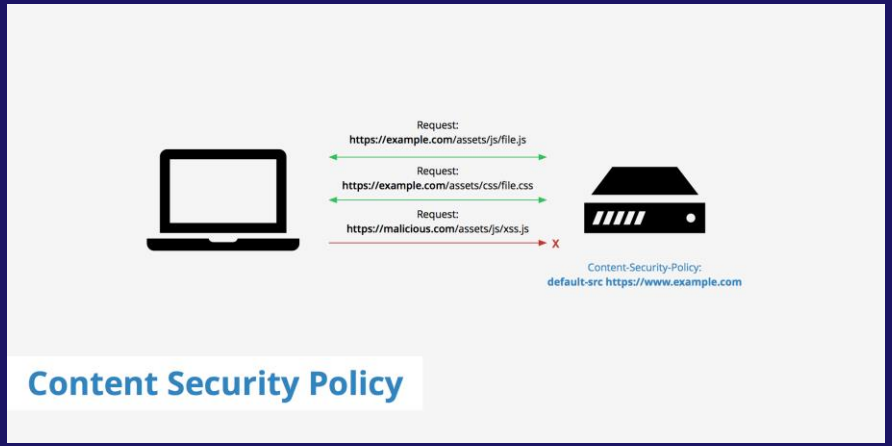
Strict Transport Security (HSTS)

- Enforces the use of encrypted HTTPS connections instead of plain-text HTTP communication
- Helps to protect websites against protocol downgrade attacks and cookie hijacking
- IETF standard and is specified in RFC 6797




```
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
```

Content Security Policy (CSP)



- It allows you to precisely control permitted content sources and many other parameters.
- Requires careful tuning and precise definition of the policy.
- Prevents the exploitation of Cross-Site Scripting (XSS), ClickJacking, and HTML injection attacks.
- base-uri, default-src, script-src, style-src, img-src, frame-ancestors, form-action

X-Content-Type-Options

- Prevents the browser from interpreting files as a different MIME type to what is specified in the Content-Type header.
- With MIME sniffing, the browser will ignore the declared content type, and instead of rendering an image will execute the script.
- Using this, the browser will no longer analyze the file.

```
X-Content-Type-Options: nosniff
```

X-Frame-Options

Value	Description
`deny`	No rendering within a frame.
`sameorigin`	No rendering if origin mismatch.
`allow-from: DOMAIN`	Allows rendering if framed by frame loaded from DOMAIN.

- Instructs the browser whether the content can be displayed within frames.
- Improves the protection of web applications against clickjacking
- Ignored if CSP frame-ancestors is used

```
X-Frame-Options: deny
```

Referrer-Policy

- Controls if and how much referrer information should be revealed to the web server.
- A website publisher can choose to send no information as to the referrer, they can choose to send just the domain name or they can send the entire URL string.

```
Referrer-Policy: origin-when-cross-origin
```

- Referrer-Policy: no-referrer.
- Referrer-Policy: no-referrer-when-downgrade.
- Referrer-Policy: origin.
- Referrer-Policy: origin-when-cross-origin.
- Referrer-Policy: same-origin.
- Referrer-Policy: strict-origin.
- Referrer-Policy: strict-origin-when-cross-origin.
- Referrer-Policy: unsafe-url.

Many more..

1. Clear-Site-Data
2. Cross-Origin-Embedder-Policy
3. Cross-Origin-Opener-Policy
4. Cross-Origin-Resource-Policy
5. Cache-Control
6. Feature-Policy
7. X-XSS-Protection
8. X-Permitted-Cross-Domain-Policies

THANKS !

Do you have any questions?
bittentech98@gmail.com
Twitter: techhacker98

CREDITS: This presentation template was created by Slidesgo, incluiding icons by Flaticon, and infographics & images by Freepik.

Please, keep this slide for attribution.