



**The Assignment on Information Security**  
**(UE19CS347)**

Documented by Anurag.R.Simha


SRN	:	PES2UG19CS052
Name	:	Anurag.R.Simha
Date	:	06/05/2022
Section	:	A

Pentest report on:

1. <https://demopes.eoxvantage.com/>

✖ The following security headers are missing from the website:

**HIGH SEVERITY**


 **Strict Transport Security**

A HSTS Policy informing the HTTP client how long to cache the HTTPS only policy and whether this applies to subdomains.

---

[Strict Transport Security documentation](#)

**LOW SEVERITY**


 **X Content Type Options**

The only defined value, "nosniff", prevents Internet Explorer from MIME-sniffing a response away from the declared content-type. This also applies to Google Chrome, when downloading extensions

---

[X Content Type Options documentation](#)

**MEDIUM SEVERITY**


 **X Frame Options**

Clickjacking protection: deny - no rendering within a frame, sameorigin - no rendering if origin mismatch, allow-from - allow from specified location, allowall - non-standard, allow from any location

---

[X Frame Options documentation](#)

**HIGH SEVERITY**


 **Content Security Policy**

A computer security standard introduced to prevent cross-site scripting (XSS), clickjacking and other code injection attacks resulting from execution of malicious content in the trusted web page context

---

[Content Security Policy documentation](#)

**LOW SEVERITY**

 **X XSS Protection**


A Cross-site scripting filter

---


[X XSS Protection documentation](#)

It's noticed that the website is prone to attacks by cross site scripting. For, the header that thwarts this attack's missing from it. The absence of HSTS policy on the website leads any attacker to abate this website to HTTP. Hopefully, the site is safe from attacks by CSRF and SQL injection.


2. <https://frizzleweather.com/>

 The following security headers are missing from the website:


HIGH SEVERITY

 **Strict Transport Security**  
A HSTS Policy informing the HTTP client how long to cache the HTTPS only policy and whether this applies to subdomains.  
[Strict Transport Security documentation](#)


LOW SEVERITY

 **X Content Type Options**  
The only defined value, "nosniff", prevents Internet Explorer from MIME-sniffing a response away from the declared content-type. This also applies to Google Chrome, when downloading extensions  
[X Content Type Options documentation](#)


MEDIUM SEVERITY

 **X Frame Options**  
Clickjacking protection: deny - no rendering within a frame, sameorigin - no rendering if origin mismatch, allow-from - allow from specified location, allowall - non-standard, allow from any location  
[X Frame Options documentation](#)

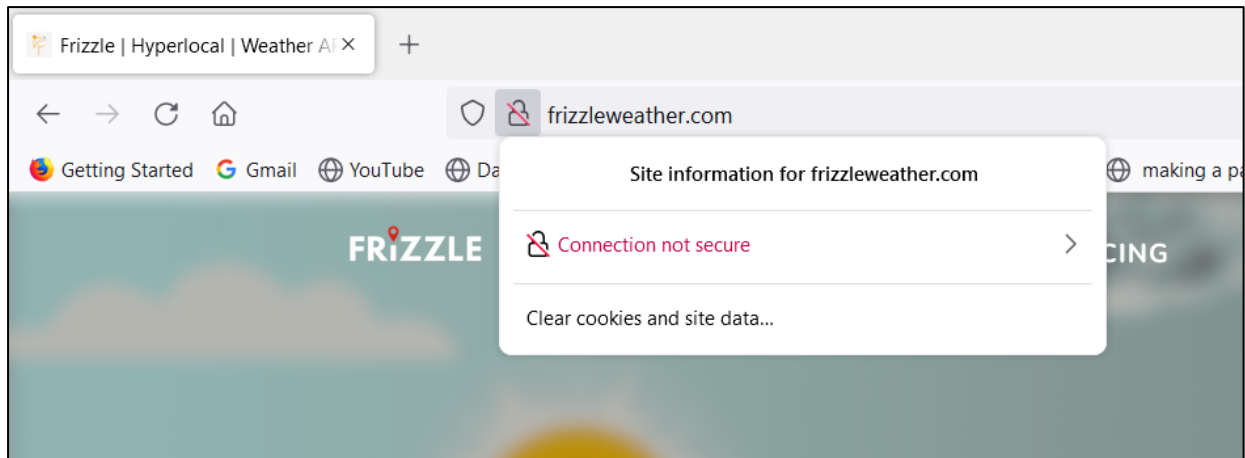
HIGH SEVERITY

 **Content Security Policy**  
A computer security standard introduced to prevent cross-site scripting (XSS), clickjacking and other code injection attacks resulting from execution of malicious content in the trusted web page context  
[Content Security Policy documentation](#)

LOW SEVERITY

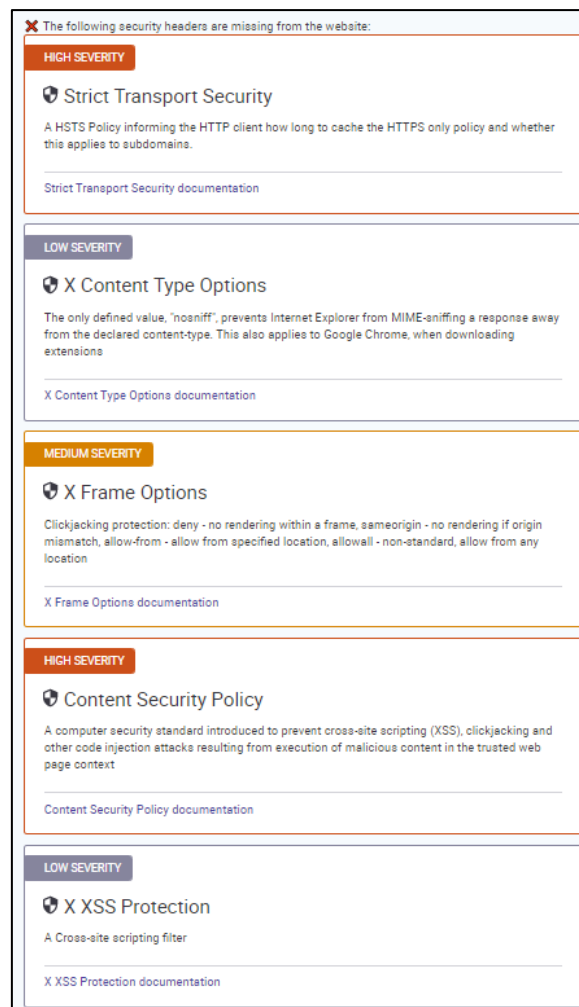
 **X XSS Protection**  
A Cross-site scripting filter  
[X XSS Protection documentation](#)

As observed in the previous website, the absence of a couple of headers poses hazardous harm to this website, with XSS taking the lion's share.



It's imperative to any website to load on HTTPS only, but is failed by this website. So, this poses another vulnerability and can make an apposite attack surface.

### 3. <https://assertify.me>



Once again, this website, too, is prone to XSS.

\*\*\*\*\*