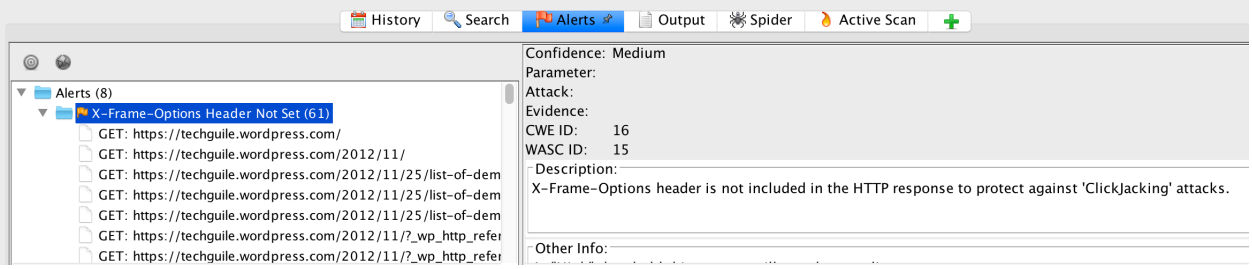
IS 2545 Software Quality Assurance
Deliverable 5

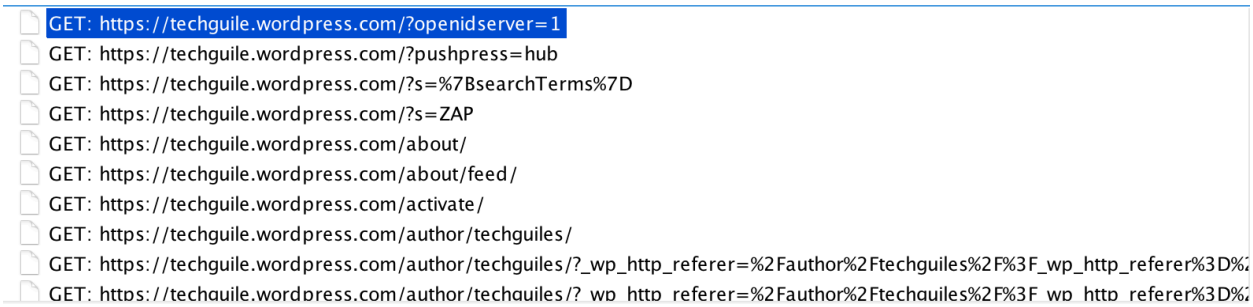
Nanxun Xie(nax4)
Yifan Zhao(yiz105)

4 vulnerabilities in
https://techguile.wordpress.com/2012/11/25/list-of-demo-websites-of-security-testing-purpose/

1. X-Frame-Options Header Not Set



URLs with this vulnerability:
https://techguile.wordpress.com/
https://techguile.wordpress.com/2012/11/
https://techguile.wordpress.com/2012/11/25/list-of-demo-websites-of-security-testing-purpose/
https://techguile.wordpress.com/2012/11/?_wp_http_referer=%2F2012%2F11%2F%3F_wp_http_referer%3D%252F2012%252F11%252F%253F_wp_http_referer%253D%25252F2012%25252F11%25252F%25253F_wp_http_referer%25253D%2525252F2012%2525252F11%2525252F%2526_wpnonce%25253Deba3fdaa1f%252526carousel-reblog-content%252526carousel-reblog-submit%25253DReblog%25252BPost%2526_wpnonce%253Deba3fdaa1f%2526carousel-reblog-content%2526carousel-reblog-submit%253DReblog%252BPost%26_wpnonce%3Deba3fdaa1f%26carousel-reblog-content%26carousel-reblog-submit%3DReblog%2BPost&_wpnonce=eba3fdaa1f&carousel-reblog-content&carousel-reblog-submit=Reblog+Post
and etc.



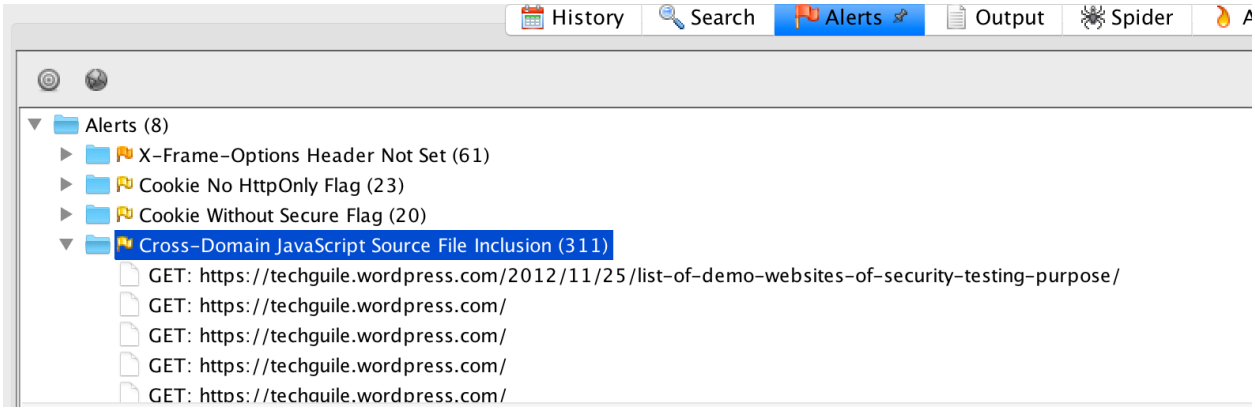
Without setting X-Frame-Options Header, the site can be easily attacked by 'Clickjacking', an attack using multiple transparent layers or frames to trick site browser into clicking the buttons or links which are not belong to the original website. Malicious coding is hidden beneath these buttons or links on a website.

This vulnerability attacks integrity and belongs to modification security attacks. Attacks that exploit this vulnerability are active because it can modify the system in some way.

Exploiting this vulnerability might damage the reputation of the website, users' private information disclosure and even financial loss.

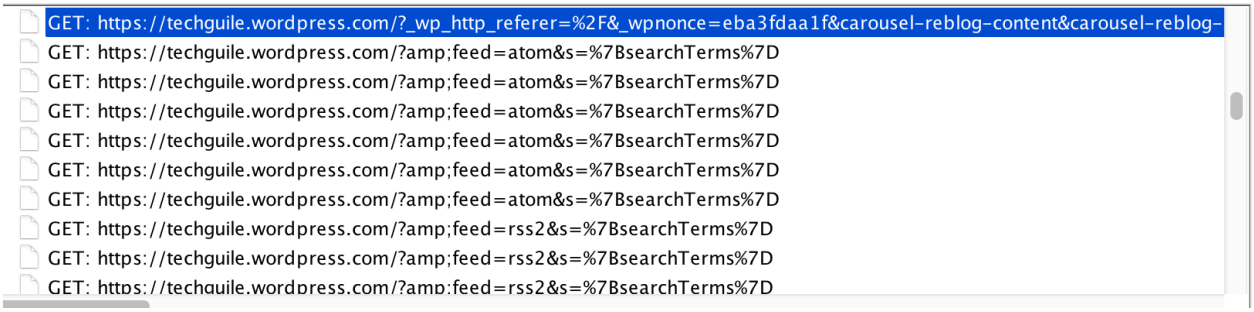
Steps to fix this vulnerability:
a. Set X-Frame-Options HTTP header on all web pages returned by this site.
b. Employ defensive code in the UI to ensure that the current frame is the most top level window.

2. Cross-Domain JavaScript Source File Inclusion



URLs with this vulnerability:
https://techguile.wordpress.com/2012/11/25/list-of-demo-websites-of-security-testing-purpose/
https://techguile.wordpress.com/
https://techguile.wordpress.com/2012/11/

https://techguile.wordpress.com/2012/11/25/list-of-demo-websites-of-security-testing-purpose/
https://techguile.wordpress.com/2012/11/?_wp_http_referer=%2F2012%2F11%2F&_wpnonce=eba3fdaa1f&carousel-reblog-content&carousel-reblog-submit=Reblog+Post
and etc.



Cross-Domain JavaScript Source File Inclusion vulnerability means that the site includes one or more script files from a third-party domain. If these third party scripts are compromised or changed to be invasive, the site might turn out to be vulnerable.

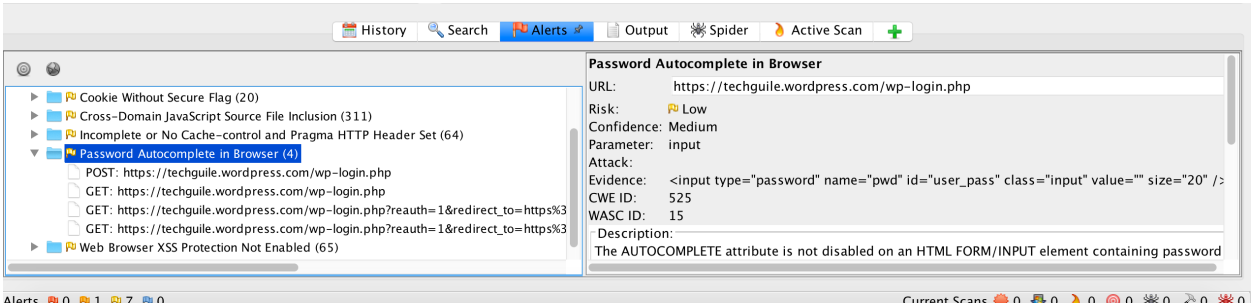
This vulnerability attacks confidentiality and belongs to interception security attacks. Attacks that exploit this vulnerability are passive.

Exploiting this vulnerability might steal information from the site and affect the relationship between users and the site.

Steps to fix this vulnerability:

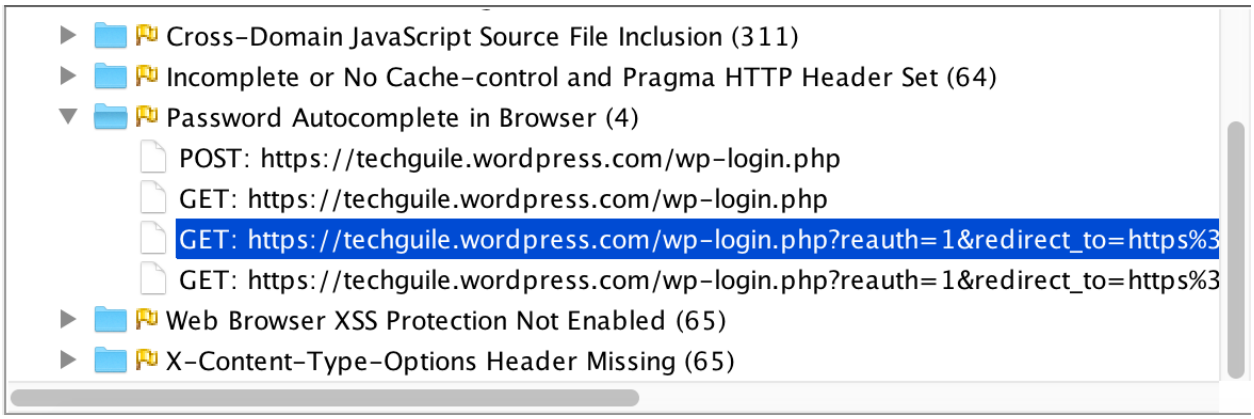
a. Ensure JavaScript source files are only loaded from trusted sources.
b. The JavaScript sources can't be controlled by end users of the application.

3. Password Autocomplete in Browser



URLs with this vulnerability:
https://techguile.wordpress.com/wp-login.php

https://techguile.wordpress.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Ftechguile.wordpress.com%2Fwp-admin%2F
https://techguile.wordpress.com/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Ftechguile.wordpress.com%2Fwp-admin%2Fpost-new.php%3Fpost_type%3Dpage



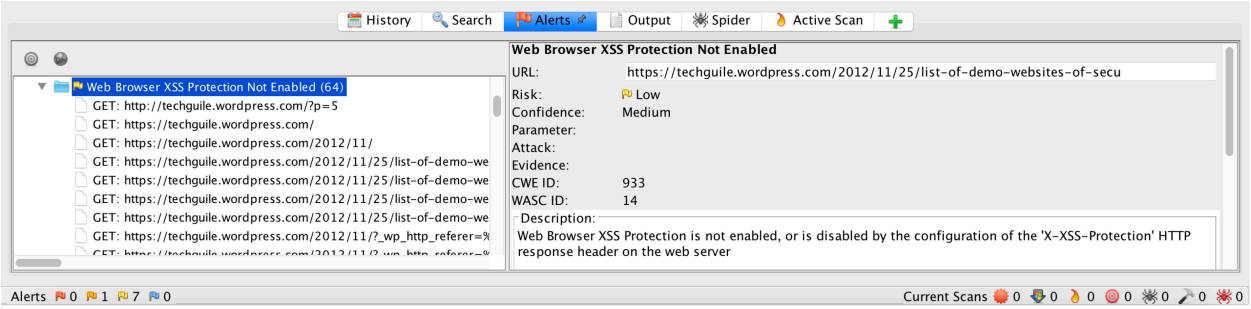
Password Autocomplete in Browser means the passwords may be stored in the browsers and can be retrieved next time. The AUTOCOMPLETE attribute is abled on an HTML FORM/INPUT element containing password type input.

This vulnerability attacks confidentiality and belongs to interception security attack. Attacks that exploit this vulnerability are passive because it does not modify system in any way.

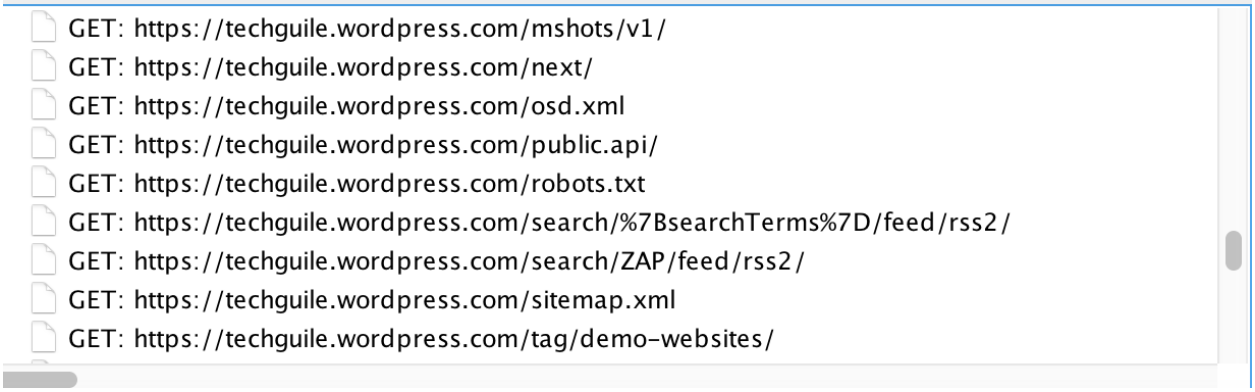
This vulnerability can highly increase the possibility to allow the unauthorized access, leak users' privacy, and cause financial loss, further damage the reputation of the website.

Steps to fix this vulnerability:
Setting AUTOCOMPLETE='OFF' to turn off the AUTOCOMPLETE attribute in forms or individual input elements containing password inputs.

4. Web Browser XSS Protection Not Enabled



URLs with this vulnerability:
http://techguile.wordpress.com/?p=5
https://techguile.wordpress.com/2012/11/
https://techguile.wordpress.com/2012/11/25/list-of-demo-websites-of-security-testing-purpose/amp/
https://techguile.wordpress.com/?amp;feed=rss2&s=%7BsearchTerms%7D
https://techguile.wordpress.com/?_wp_http_referer=%2F&_wpnonce=4db6ea6af4&carousel-reblog-content&carousel-reblog-submit=Reblog+Post
and etc.



When Web Browser XSS Protection Not Enabled, it allows a third party to execute code on the system. It is similar to an injection attack, but with an intermediary. Usually Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server. When an attacker gets a user's browser to execute their own code, it will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser.

This vulnerability attacks integrity and also belongs to modification security attack. Attacks that exploit this vulnerability are active because it allows attackers to execute their own code to modify the system.

This vulnerability could increase the possibility to damage the reputation of the website, leak users' privacy and stored datasets, and cause financial loss.

Steps to fix this vulnerability:

a. Setting the X-XSS-Protection HTTP response header to '1' to Ensure that the web browser's XSS filter is enabled