# **CTF Topic: Web Vulnerability Scanning with sucuriNet**



# **Introduction**

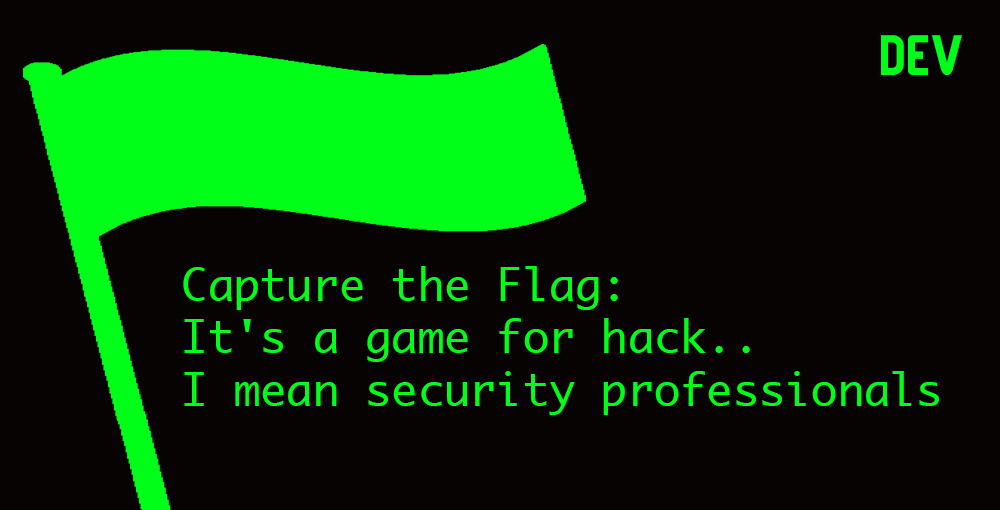


Sucuri is a comprehensive website security platform offering various services, including website firewalls, malware removal, performance optimization, and web vulnerability scanning. This guide will focus on using Sucuri’s web vulnerability scanning capabilities to analyze the target website http://altoro.testfire.net/.

# **Tools and requirements**

[sucuri](https://sitecheck.sucuri.net/)

**Scenario**



Assuming you are participating in a CTF challenge, you will use the information gathered from Sucuri to identify and exploit potential vulnerabilities on the target website.

# **Process to Follow while Performing CTF**

Step 1: Go through the [sucuri](https://sitecheck.sucuri.net/) tool which is linked above in the tool and requirement section

Step 2: then enter the target URL <http://altoro.testfire.net/> on the search box

Step 3: Now identify the flag and solve it

# 

# **Let's Begin The Challenge**

# **Question**

Flag 1: What is the IP Address of The target system?

Answer:**65.61.137.117**

Flag 2: What is the Running Server and version of the system?

Answer: **Apache-Coyote 1.1**

Flag 3: What is the Risk Status?

Answer: **Medium**

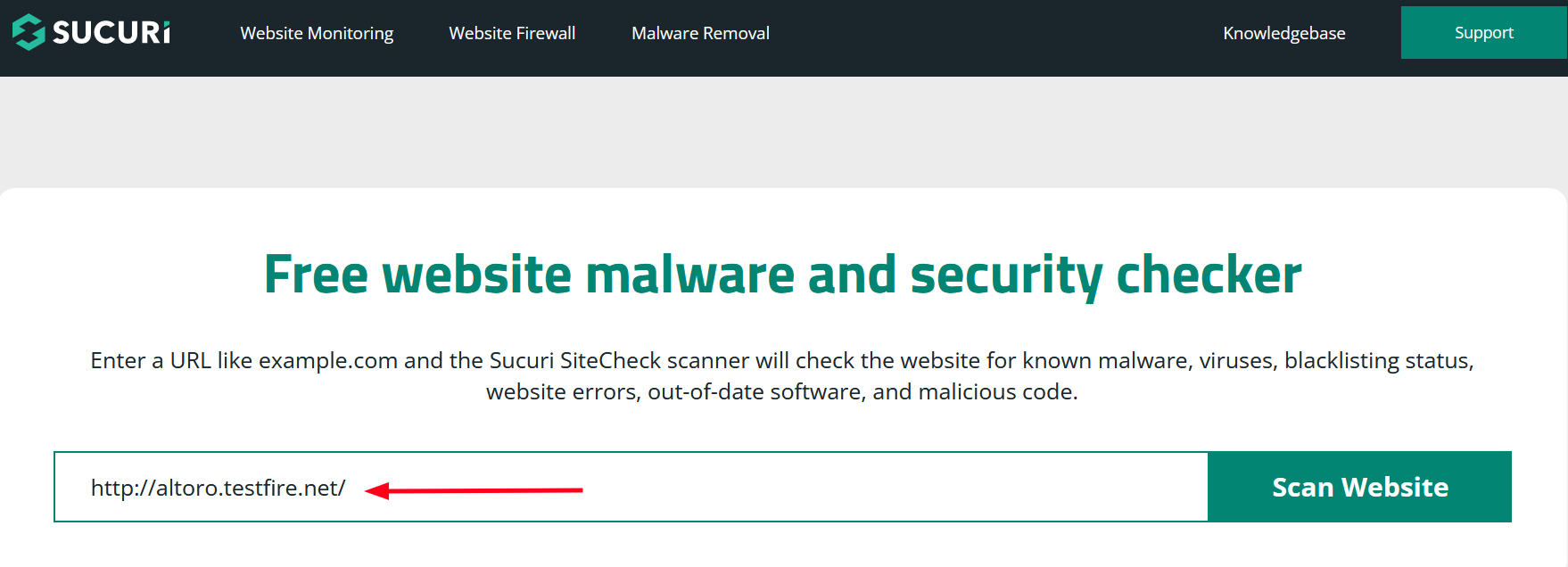
Flag 4: What Password input field is detected?

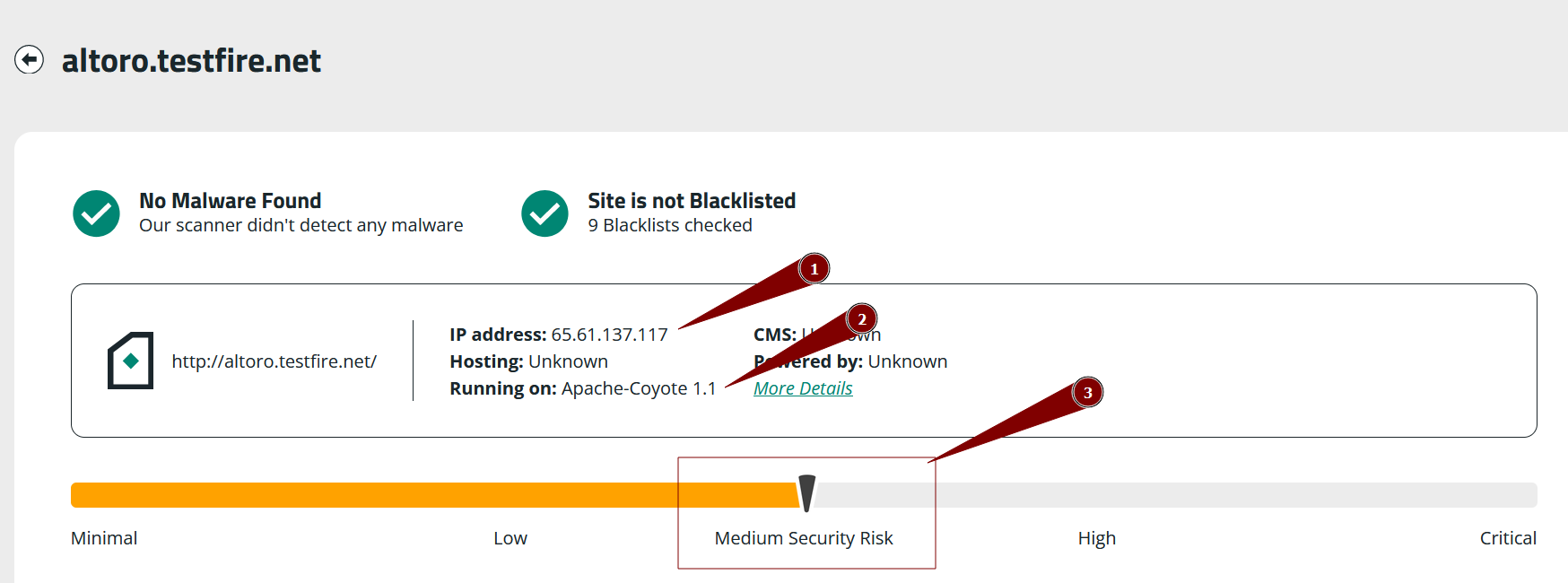
Answer: **Unencrypted**

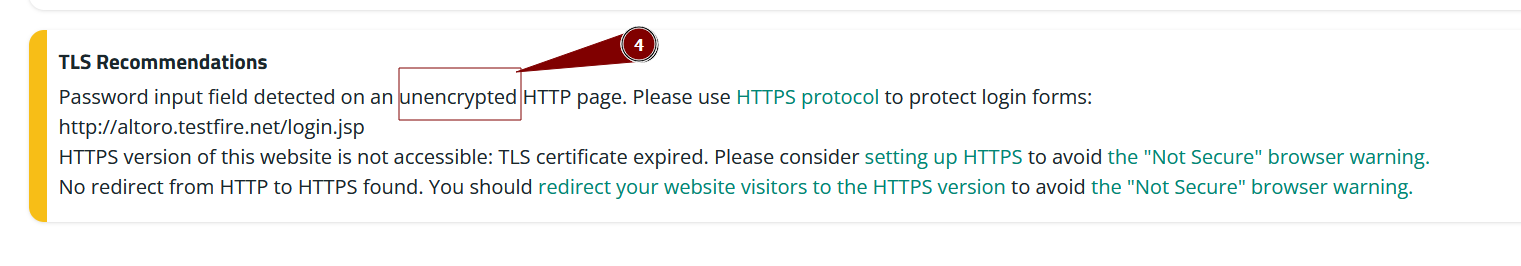
Flag 5: What major Security header protection is missing on the target site?

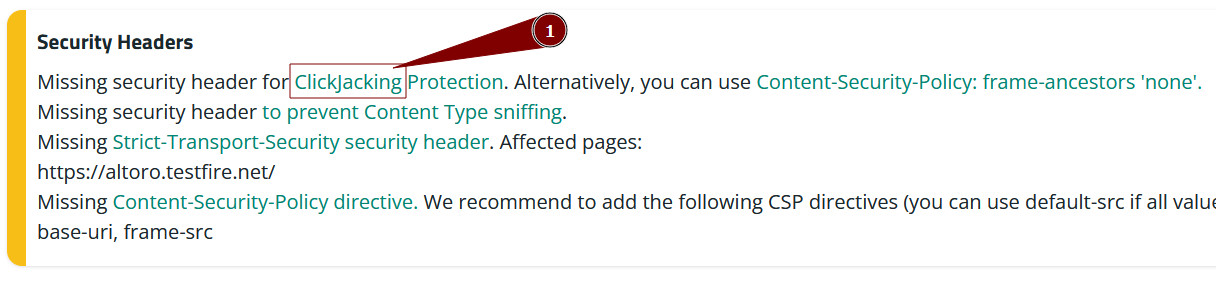
Answer: **Clickjacking**

# **Hint**

****

****

****

****