# **CTF Topic: Vulnerability Scanning with IMMUNIWEB**

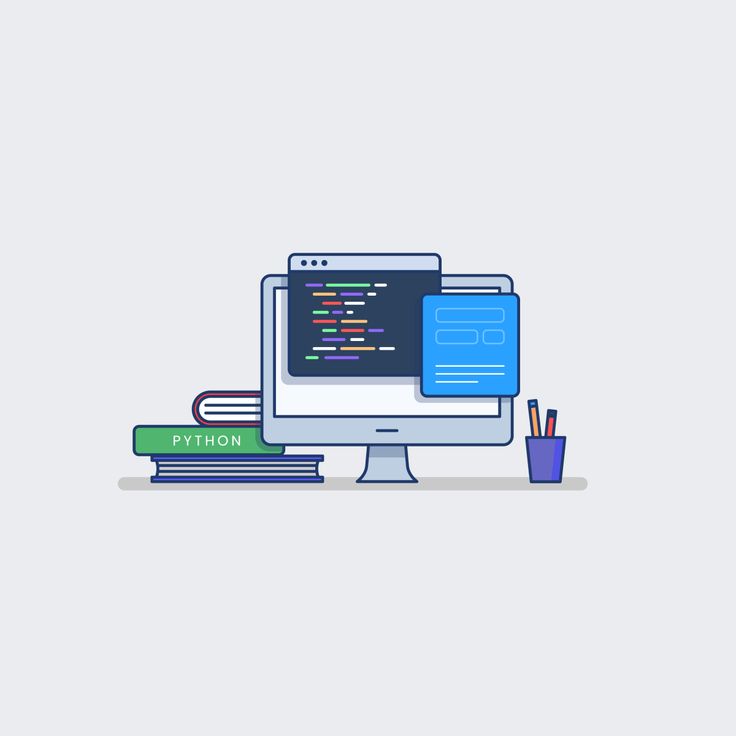


# **Introduction**



ImmuniWeb is a cybersecurity platform offering various tools for web security testing, including web vulnerability scanning, dark web monitoring, and more. In this guide, we'll focus on using ImmuniWeb's tools to gather information on a target IP address, specifically its associated website: [www.hackthissite.org](http://www.hackthissite.org).

# **Scenario**



Assuming you are participating in a CTF challenge, you will use the information gathered from ImmuniWeb to identify and exploit potential vulnerabilities on the target website. Here are some possible steps:

# **Process to Follow while Performing CTF**

Step 1: Go through the ImmuniWeb tool: <http://www.immuniweb.com>

Step 2: then enter the URL [www.hackthissite.org](http://www.hackthissite.org).on the search box

Step 3: Now identify the flag and solve it

# 

# 

# 

# **Let's Begin The Challenge**

# **Question**

Flag1: How many Vulnerabilities are there in the target system?

Answer: **6**

Flag2: which vulnerability on the target system?

Answer: **Cross-site Scripting/XSS**

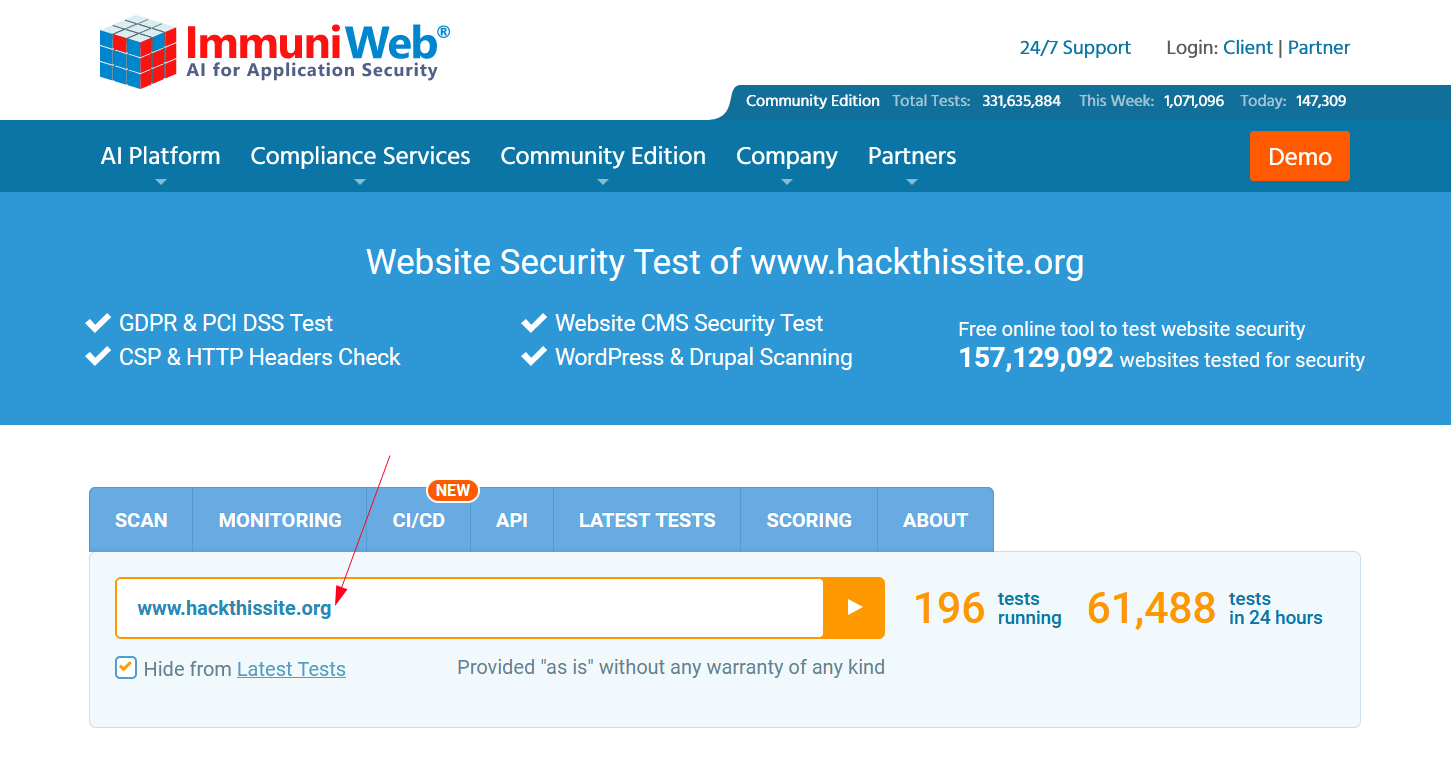
Flag3: what is the CVSS status of XSS?

Answer: **Medium**

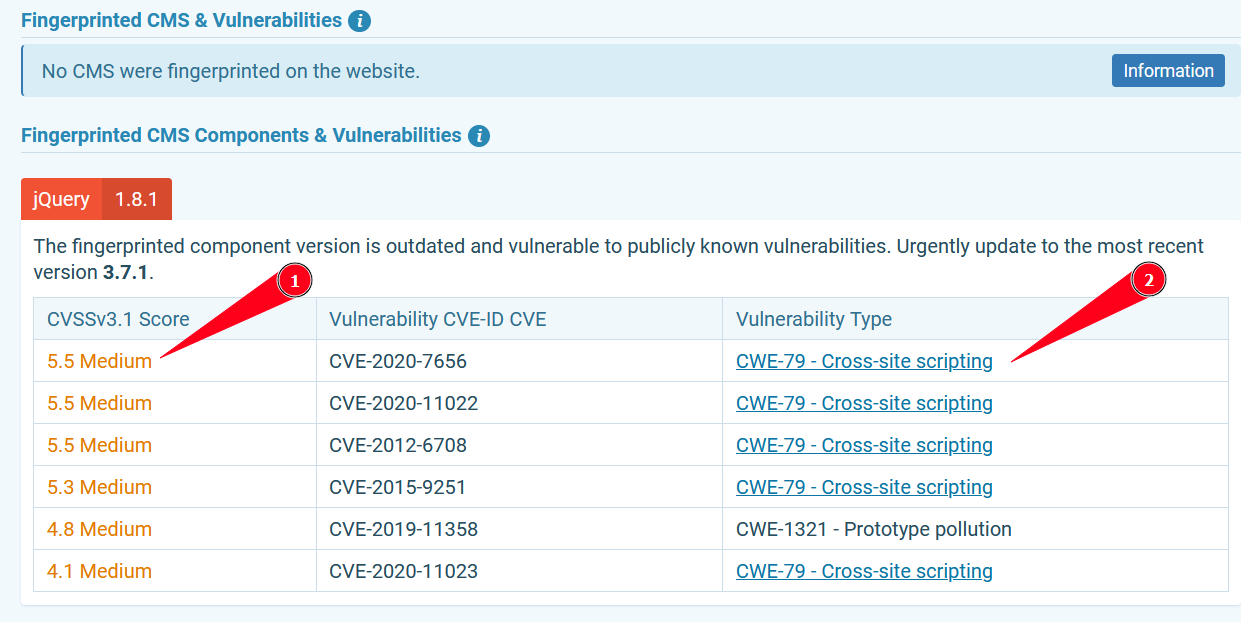
Flag 3:IS TLS Encrypted(yes/No)

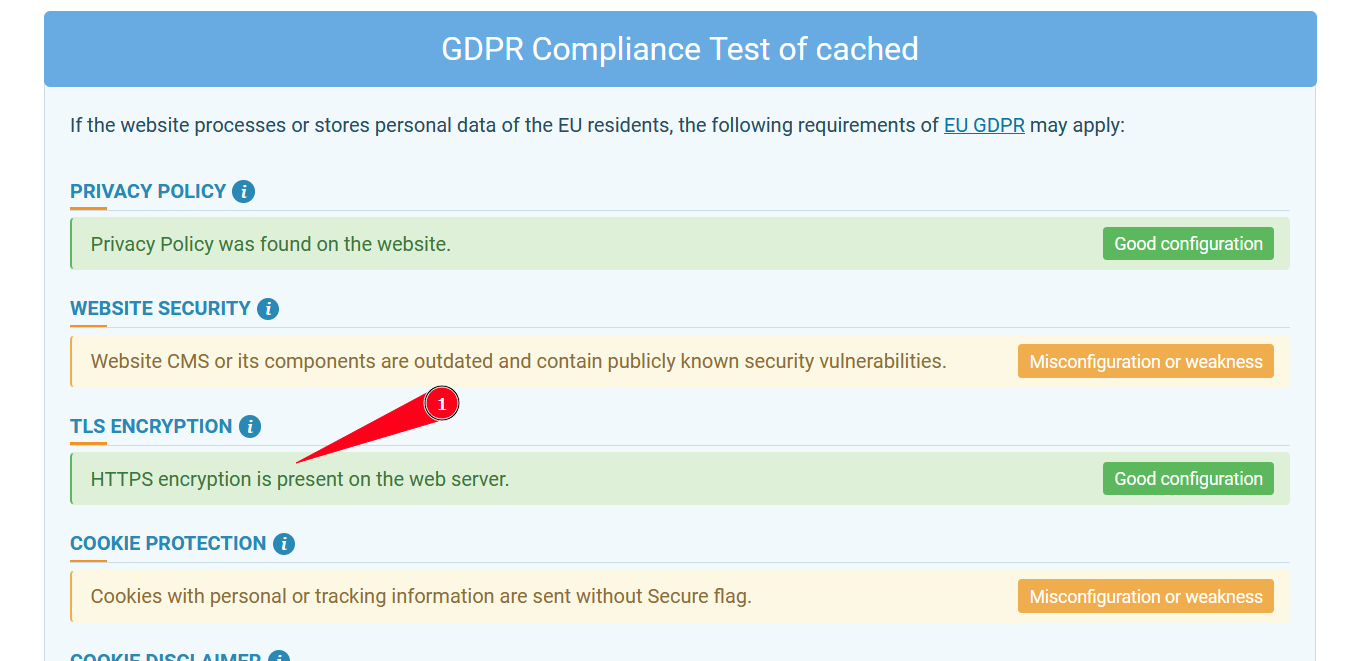
Answer: **Yes**

# **Hint**



****

****

****