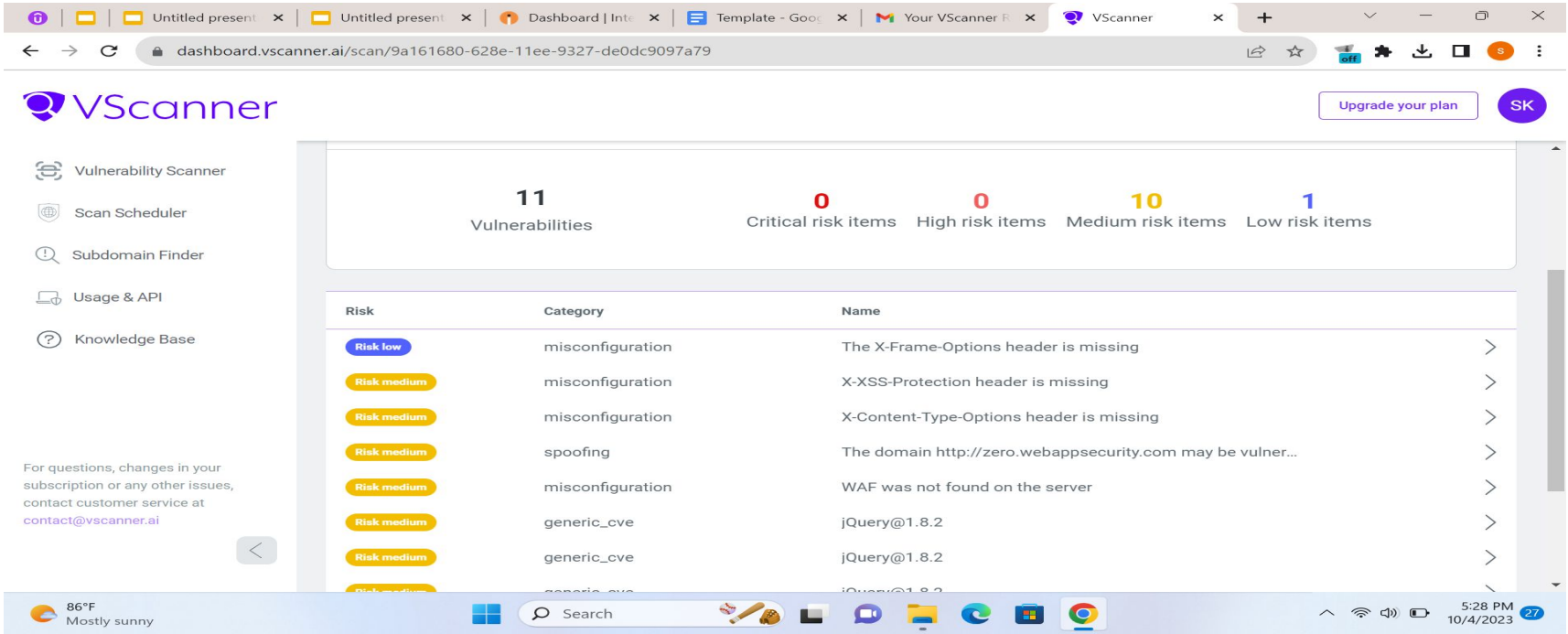
Ethical Hacking Internship Project 2

Vulnerability finding :http://zero.webappsecurity.com/

By Santosh kumar

Vuln report by VS Scanner:-

Sir there is some technical error in drive link you have provided for netsparker ton download so i have usd here vs scanner.



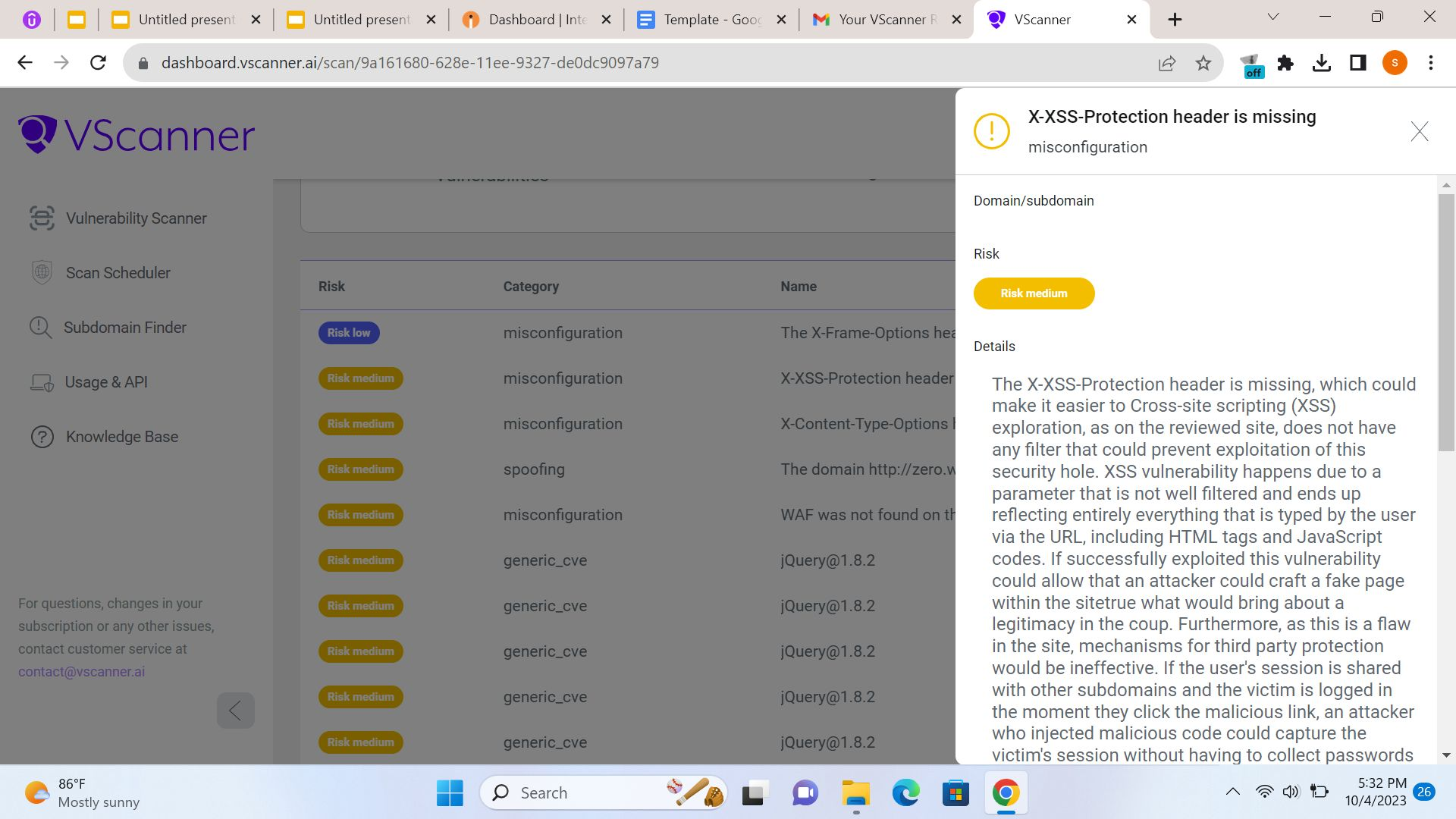
vulnerabilities

X-XSS-Protection header is missing (misconfiguration)

The X-XSS-Protection header is missing, which could make it easier to Cross-site scripting (XSS) exploration, as on the reviewed site, does not have any filter that could prevent exploitation of this security hole. XSS vulnerability happens due to a parameter that is not well filtered and ends up reflecting entirely everything that is typed by the user via the URL, including HTML tags and JavaScript codes. If successfully exploited this vulnerability could allow that an attacker could craft a fake page within the site true what would bring about a legitimacy in the coup. Furthermore, as this is a flaw in the site, mechanisms for third party protection would be ineffective. If the user's session is shared with other subdomains and the victim is logged in the moment they click the malicious link, an attacker who injected malicious code could capture the victim's session without having to collect passwords and would have the same access privileges as that user. This situation becomes even more serious if a certain session captured for some administrative access, which could cause the elevation of an attacker's privileges or the exploitation of others security flaws.

Solution

The X-XSS-Protection header in the web server response and a Web Application Firewall are recommended to prevent security vulnerabilities like XSS attacks. Adding the X-XSS-Protection header to all web pages can be done through server configuration or direct HTML code insertion. A typical setting, "X-XSS-Protection: 1; mode=block", activates browser's XSS protection and blocks any identified XSS attack.


Untitled present
Untitled present
Dashboard | Inte
Template - Goo
Your VScanner R
VScanner
dashboard.vscanner.ai/scan/9a161680-628e-11ee-9327-de0dc9097a79
VScanner
Vulnerability Scanner
Scan Scheduler
Subdomain Finder
Usage & API
Knowledge Base
For questions, changes in your subscription or any other issues, contact customer service at contact@vscanner.ai
Risk
Category
Name
Risk low
misconfiguration
The X-Frame-Options hea
Risk medium
misconfiguration
X-XSS-Protection header
Risk medium
misconfiguration
X-Content-Type-Options
Risk medium
spoofing
The domain http://zero.w
Risk medium
misconfiguration
WAF was not found on th
Risk medium
generic_cve
jQuery@1.8.2
Risk medium
generic_cve
jQuery@1.8.2
Risk medium
generic_cve
jQuery@1.8.2
Risk medium
generic_cve
jQuery@1.8.2
Risk medium
generic_cve
jQuery@1.8.2
X-XSS-Protection header is missing
misconfiguration
Domain/subdomain
Risk
Risk medium
Details
The X-XSS-Protection header is missing, which could make it easier to Cross-site scripting (XSS) exploration, as on the reviewed site, does not have any filter that could prevent exploitation of this security hole. XSS vulnerability happens due to a parameter that is not well filtered and ends up reflecting entirely everything that is typed by the user via the URL, including HTML tags and JavaScript codes. If successfully exploited this vulnerability could allow that an attacker could craft a fake page within the sitetrue what would bring about a legitimacy in the coup. Furthermore, as this is a flaw in the site, mechanisms for third party protection would be ineffective. If the user's session is shared with other subdomains and the victim is logged in the moment they click the malicious link, an attacker who injected malicious code could capture the victim's session without having to collect passwords
86°F
Mostly sunny
Search
5:32 PM
10/4/2023
26