A blue and orange logo

Description automatically generated

**IE2062 – Web Security**

**Year 2, Semester 2**

**Scanning report – sorare.com**

**IT21831904 – K.M. Weerasinghe**

Table of Contents

[Scope of the target 3](#_Toc149509664)

[In scope and rewards 3](#_Toc149509665)

[Out of scope 4](#_Toc149509666)

[Reconnaissance 5](#_Toc149509667)

[Subdomain enumeration 5](#_Toc149509668)

[Gathering information about the target 6](#_Toc149509669)

[Virtual host discovery 8](#_Toc149509670)

[Subdomain takeover 9](#_Toc149509671)

[Scanning 10](#_Toc149509672)

[Using Nmap for scanning 10](#_Toc149509673)

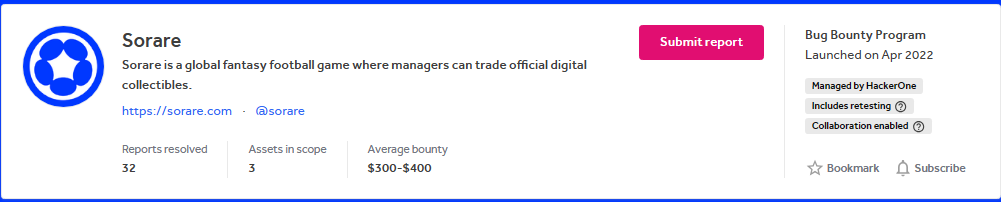
[Using final recon for scanning 10](#_Toc149509674)

[Vulnerability checking 12](#_Toc149509675)

[Vulnerabilities found using NIKTO 12](#_Toc149509676)

[Vulnerabilities found using rapidscan 13](#_Toc149509677)

# Scope of the target



## In scope and rewards

A screenshot of a computer

Description automatically generated

## Out of scope

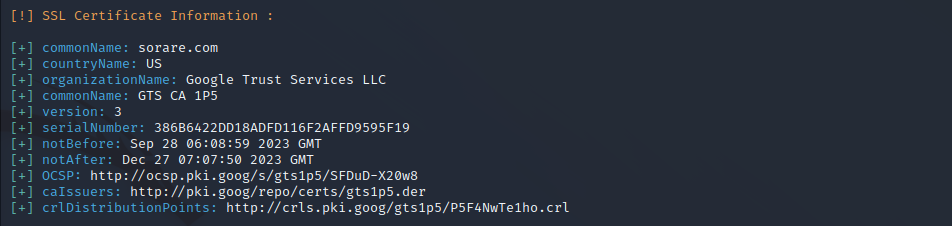
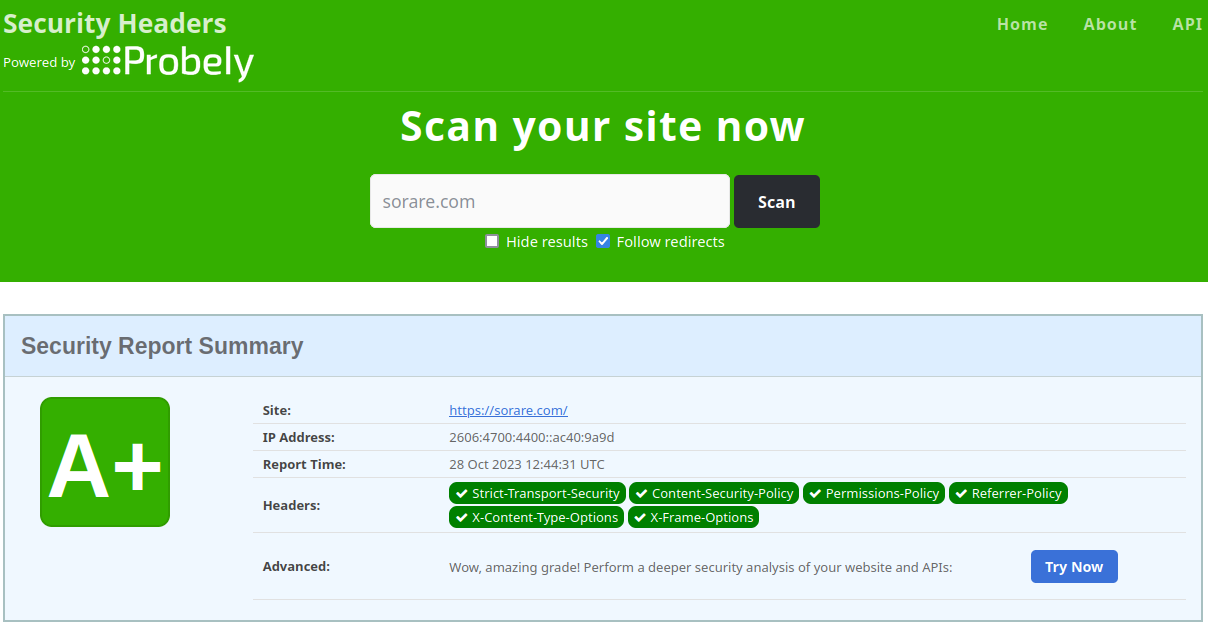
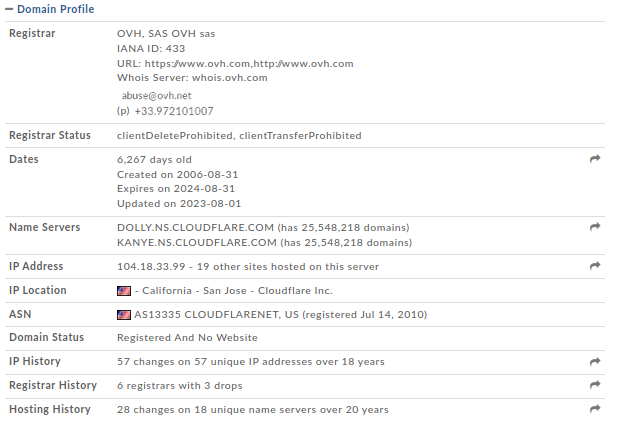
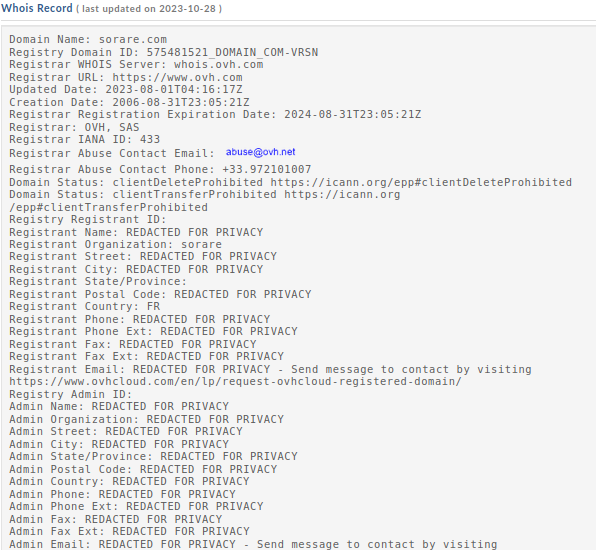
A screenshot of a computer program rules

Description automatically generated

# Reconnaissance

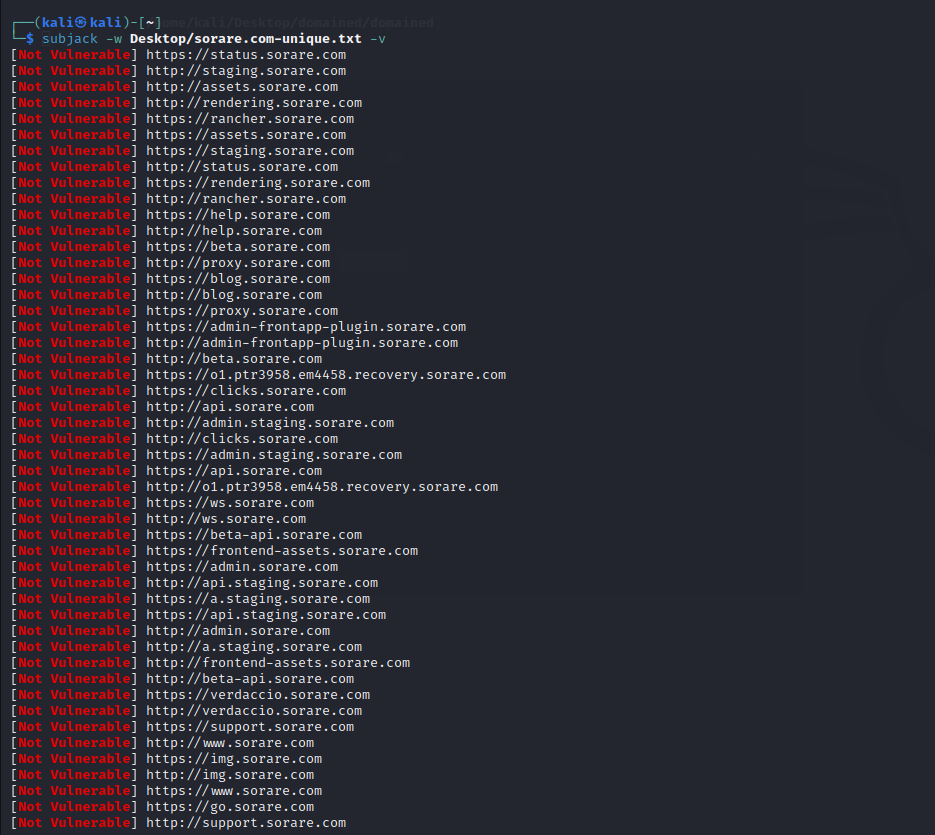
## A screenshot of a computer Description automatically generatedSubdomain enumeration

## Gathering information about the target

*  SSL certificate information found
* Security header checking
  + There are no missing headers found in this site
  + The site has better security header ratings
* Domain profile and whois records
  + Domain profile
  + Whois records
* The information related to whois records are redacted and there aren’t any usable information gathered

## Virtual host discovery

## Subdomain takeover

* └─$ subjack -w Desktop/sorare.com-unique.txt -v
* Identifying if any of the found subdomains from the previous scans are vulnerable to takeover
* No vulnerable subdomains were found
* All subdomains appear to be secure
* No issues were identified in the subdomain analysis

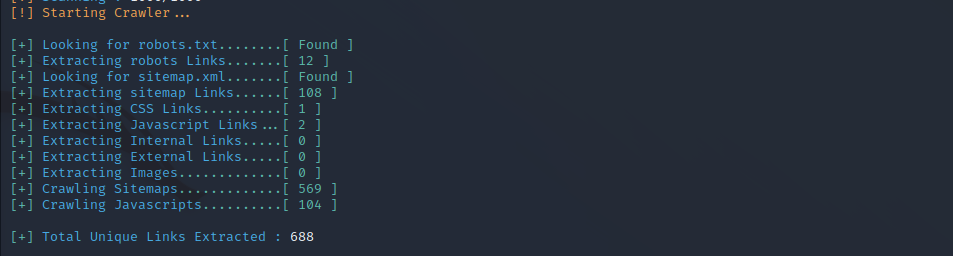
# Scanning

## Using Nmap for scanning

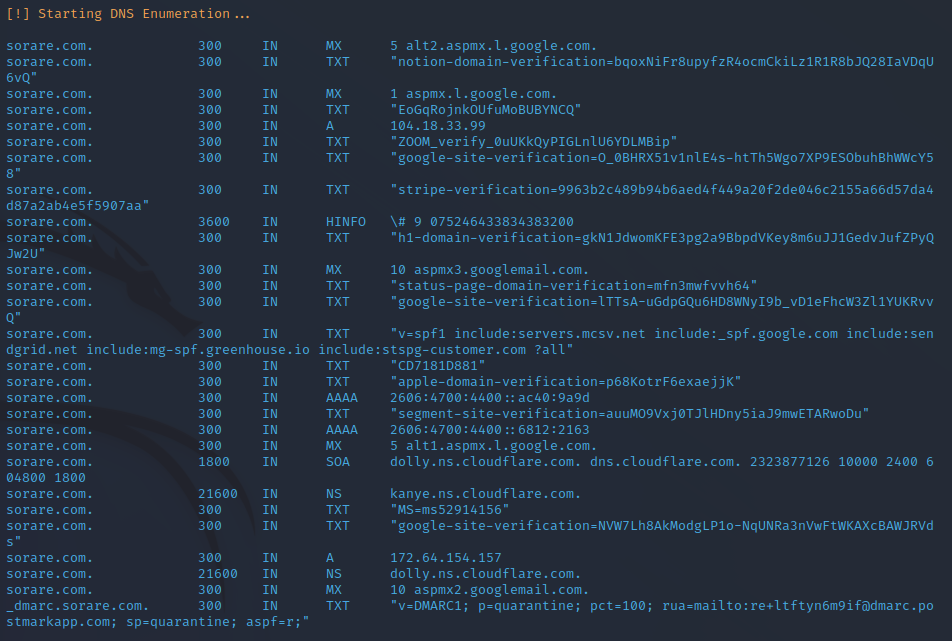
* The ports 80, 8080, 443 and 8443 are open

## Using final recon for scanning

* └─$ finalrecon --full https://www.sorare.com

information gathered using crawlers

DNS records gathered



# Vulnerability checking

## Vulnerabilities found using NIKTO

* └─$ nikto -h sorare.com

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 104.18.33.99

+ Target Hostname: sorare.com

+ Target Port: 80

+ Message: Multiple IP addresses found: 104.18.33.99, 172.64.154.157

+ Start Time: 2023-10-28 08:00:41 (GMT-4)

---------------------------------------------------------------------------

+ Server: cloudflare

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms o

+ Uncommon header 'alt-svc' found, with contents: h3=":443"; ma=86400

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site infferent fashion to the MIME type

+ All CGI directories 'found', use '-C none' to test none

+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Transport endpoint is not connected

+ Scan terminated: 19 error(s) and 3 item(s) reported on remote host

+ End Time: 2023-10-20 08:39:29 (GMT-4) (2328 seconds)

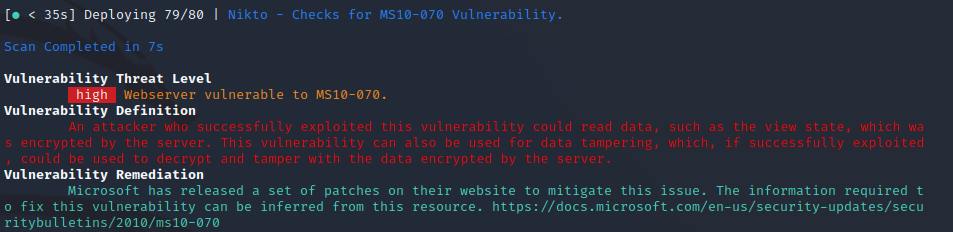
---------------------------------------------------------------------------

+ 1 host(s) tested

## Vulnerabilities found using rapidscan

* └─# ./rapidscan
* A screenshot of a computer program

  Description automatically generated└─# ./rapidscan.py sorare.com

1. Vulnerability title – webserver vulnerable to MS010-070

* Vulnerability threat level
  + High
* Vulnerability description
  + An attacker who successfully exploited this vulnerability could read data, such as the view state, which was encrypted by the server. This vulnerability can also be used for data tampering, which, if successfully exploited, could be used to decrypt and tamper with the data encrypted by the server
* Impact assessment
  + The impact of this vulnerability is assessed as high, as it allows unauthorized access to encrypted data and potential data tampering.
* Affected components
  + The webserver is the affected component in this vulnerability
* Proposed mitigation or fix
  + Microsoft has released a set of patches on their website to mitigate this issue. The information required to fix this vulnerability can be inferred from this resource.

1. A screen shot of a computer

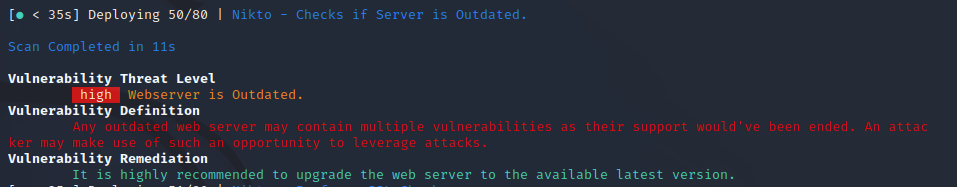
   Description automatically generatedVulnerability title - vulnerable to slowloris denial of service

* Vulnerability threat level
  + Critical
* Vulnerability description
  + This attack works by opening multiple simultaneous connections to the web server and it keeps them alive as long as possible by continuously sending partial HTTP requests, which never get completed. They easily slip through IDS by sending partial requests.
* Affected components
  + affects web servers, could include a wide range if web server software’s
* Impact assessment
  + it can effectively deny legitimate users access to the targeted web server, disrupt services, and potentially lead to significant downtime.
* How an attack could be carried out
  + Establish multiple simultaneous connections to the target web server.
  + Keep these connections open by sending partial HTTP requests that are never completed.
  + Continuously maintain these connections to exhaust server resources.
* Proposed mitigation or fix –
  + Implementation of rate limiting to limit the number of concurrent connections from a single Ip address.
  + Implementing intrusion detection and prevention systems
  + Distribute traffic across multiple servers to reduce the impact of these type of attacks

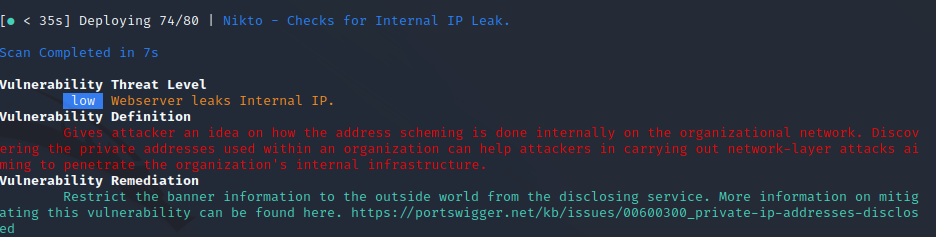
1. Vulnerability title – vulnerabilities reported in SSL scans

* A screen shot of a computer

  Description automatically generatedVulnerability threat level
  + Medium
* Vulnerability description
  + SSL related vulnerabilities break the confidentiality factor. An attacker may perform a MiTM attack, interpreting and eavesdrop the communication.
* Affected components
  + SSL and TLS libraries and the communication channels using them
* Proposed mitigation or fix
  + Proper implementation and upgraded version of SSL and TLS libraries to address and eliminate the reported vulnerabilities.

1. Vulnerability title – webserver is outdated

* Vulnerability threat level
  + High
* Vulnerability description
  + Any outdated web server may contain multiple vulnerabilities as their support would have been ended. An attacker may make use of such an opportunity to leverage attacks
* Impact assessment
  + High, as the outdated web servers are more susceptible to attacks and compromise, potentially leading to data breaches, service disruptions, or unauthorized access.
* Proposed mitigation or fix
  + Upgrade the web servers to latest version

1. vulnerability title - webserver leaks internal Ip

* vulnerability threat level
  + low
* vulnerability description
  + Gives attacker an idea on how the address scheming is done internally on the organizational network. Discovering the private addresses used within an organization can help attackers in carrying out network-layer attacks aiming to penetrate the organization's internal infrastructure.
* Affected components
  + The vulnerability affects the network infrastructure and services that expose internal address information to the public.
* impact assessment
  + The threat level for this vulnerability is low, as it primarily provides information that could be used in subsequent attacks rather than being an immediate security breach.
* Proposed mitigation or fix
  + Restrict the banner information to the outside world from the disclosing service. More information on mitigating this vulnerability can be found here.

