A blue and orange logo

Description automatically generated

**IE2062 – Web Security**

**Year 2, Semester 2**

**Scanning report –**

**IT21831904 – K.M. Weerasinghe**

Table of Contents

[Scope of the target 3](#_Toc149466710)

[In scope and rewards 3](#_Toc149466711)

[Out of scope 4](#_Toc149466712)

[Reconnaissance 5](#_Toc149466713)

[Subdomain enumeration 5](#_Toc149466714)

[Gathering information about the target 6](#_Toc149466715)

[Subdomain takeover 9](#_Toc149466716)

[Scanning 10](#_Toc149466717)

[Using Nmap for scanning 10](#_Toc149466718)

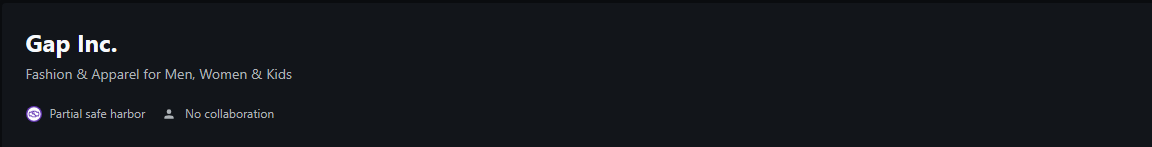
[Using final recon for scanning 10](#_Toc149466719)

[Vulnerability checking 11](#_Toc149466720)

[Vulnerabilities found using NIKTO 11](#_Toc149466721)

[Vulnerabilities found using rapidscan 12](#_Toc149466722)

# Scope of the target



## In scope and rewards

A screenshot of a computer

Description automatically generated

## Out of scope

A screenshot of a computer

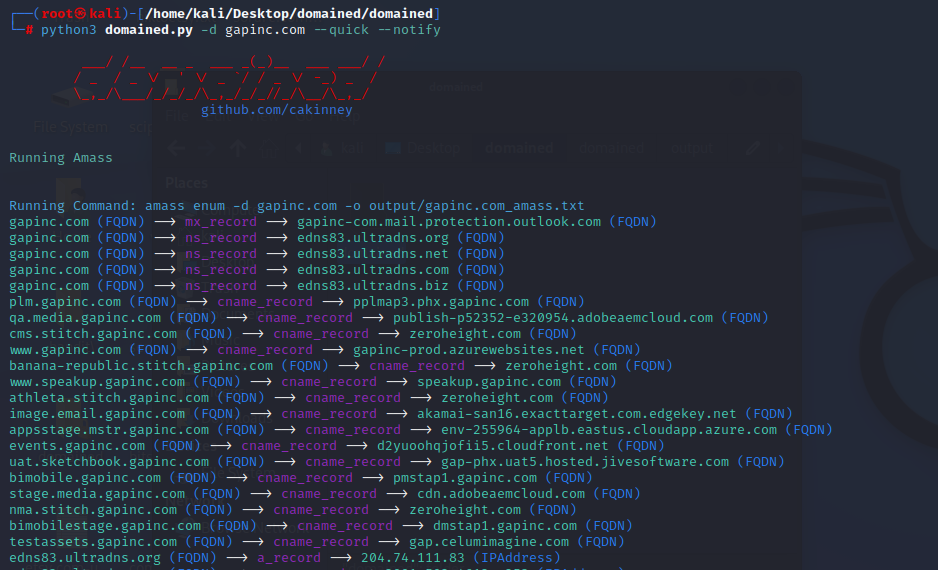
Description automatically generated

# Reconnaissance

## Subdomain enumeration

* └─# python3 domained.py -d gapinc.com --quick –notify

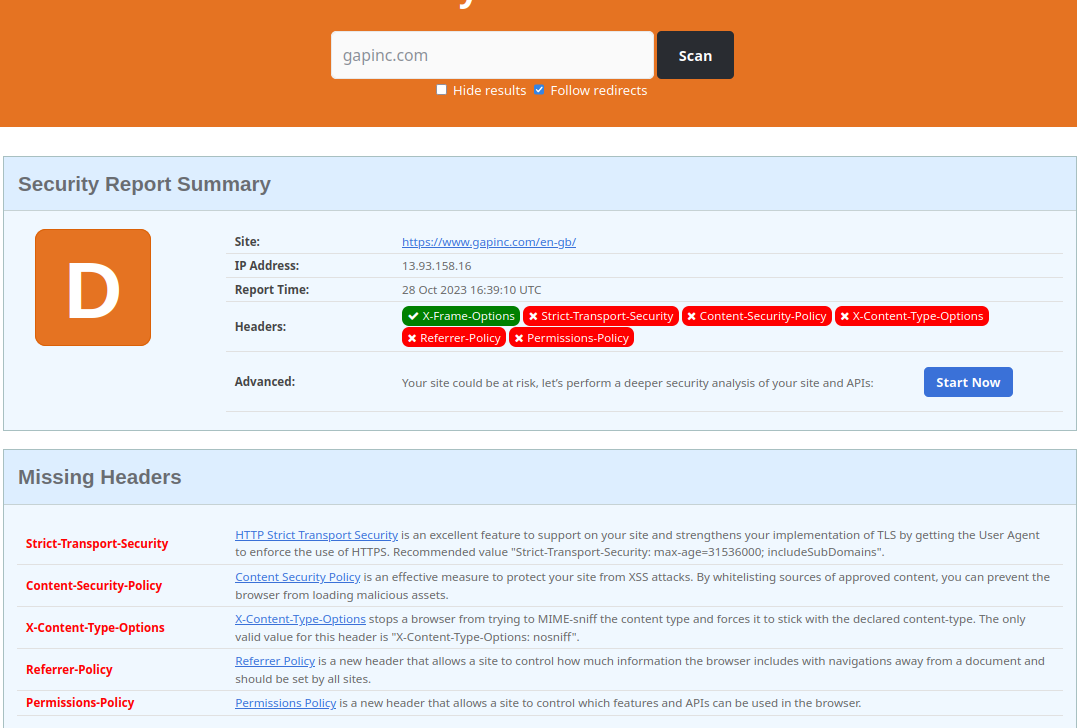
A screen shot of a computer

Description automatically generated

* 843 subdomains found using subfinder

## Gathering information about the target

* Security header checking



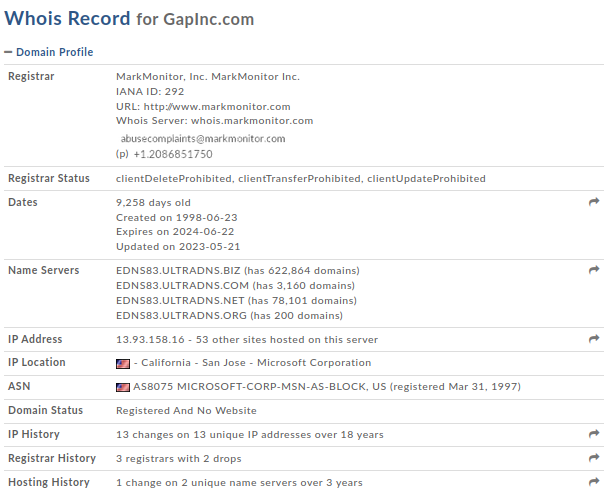
missing headers - Attackers try to learn more about the target from the amount of information exposed in the headers. An attacker may know what type of tech stack a web application is emphasizing and many other information.

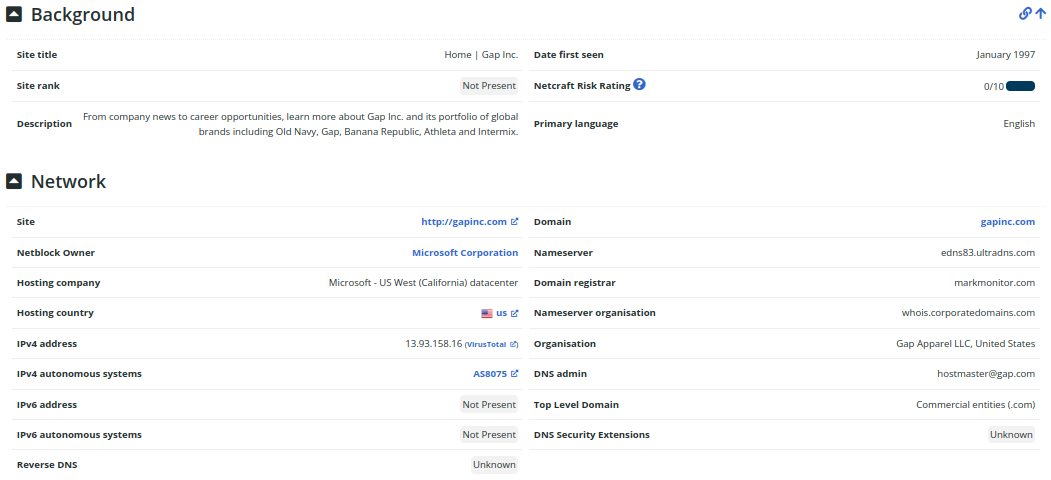
* + Strict-Transport-Security
    - HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".
  + Content-Security-Policy
    - Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
  + Referrer-Policy
    - Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
  + Permissions-Policy

Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

* Domain profile and whois records
  + No sensitive data are shown in the whois records

A screenshot of a computer

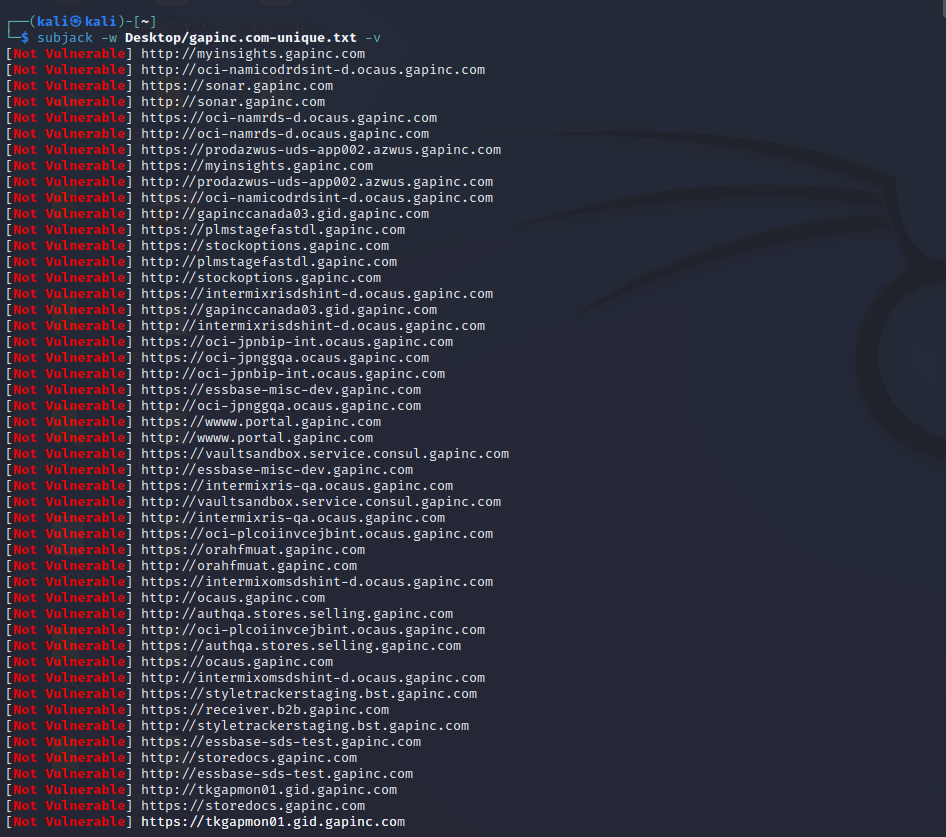
Description automatically generated

* + netcraft scan to gather background, network, and certificate information

A screenshot of a computer

Description automatically generated

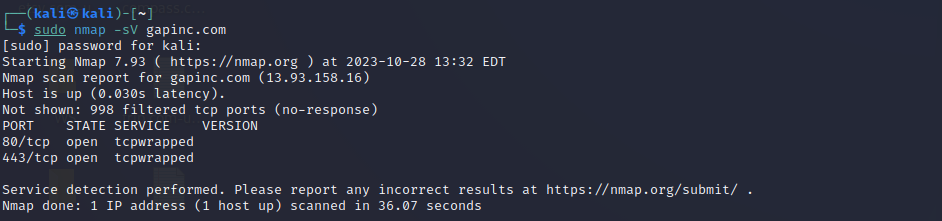
## Subdomain takeover

* ─$ subjack -w Desktop/gapinc.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

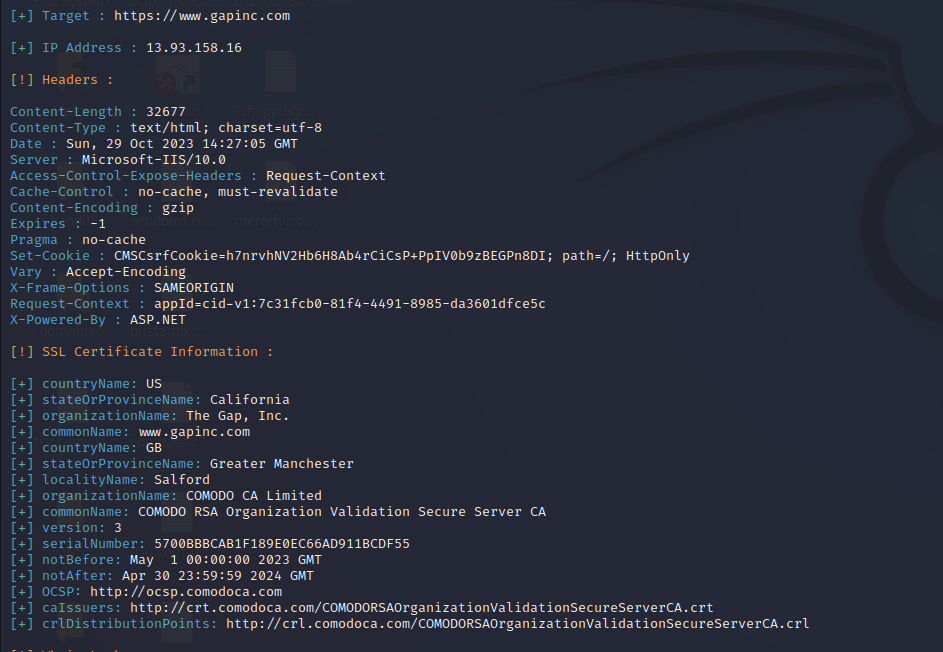
## Using Nmap for scanning

* └─$ sudo nmap -sV gapinc.com



## Using final recon for scanning

Headers and SSL certificate information gathered



# Vulnerability checking

## Vulnerabilities found using NIKTO

* └─$ nikto -h gapinc.com

- Nikto v2.1.6

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

+ Target IP: 13.93.158.16

+ Target Hostname: gapinc.com

+ Target Port: 80

+ Start Time: 2023-10-28 12:53:24 (GMT-4)

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

+ Server: No banner retrieved

+ The anti-clickjacking X-Frame-Options header is not present.

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

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

+ Root page / redirects to: https://gapinc.com/

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ 7785 requests: 0 error(s) and 3 item(s) reported on remote host

+ End Time: 2023-10-28 13:36:43 (GMT-4) (2599 seconds)

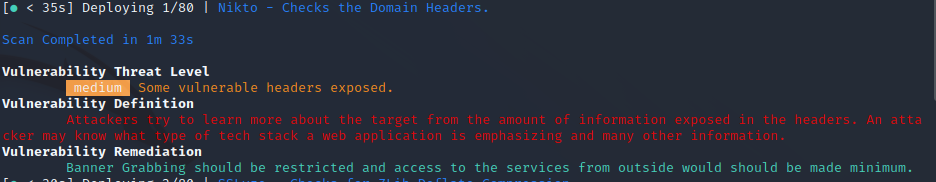
---------------------------------------------------------------------------

+ 1 host(s) tested

## Vulnerabilities found using rapidscan

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

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

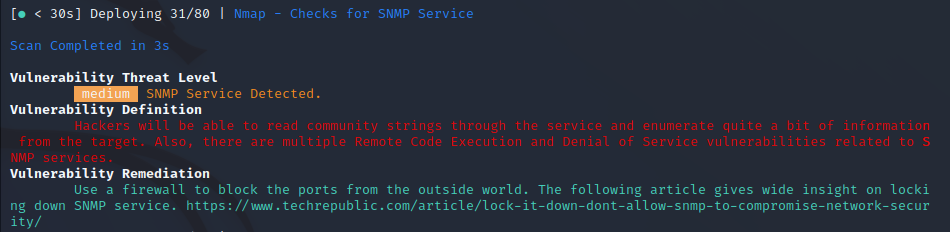
1. Vulnerability title – some vulnerable headers exposed

* Vulnerability threat level
  + Medium
* Vulnerability description
  + Attackers might learn more about the target from the amount of information exposed in the headers. An attacker may know what type of tech stack or a web application is emphasizing and many other information
* Affected components
  + This vulnerability affects the HTTP headers of the target system or web application
* Steps to reproduce
  + To reproduce this vulnerability, an attacker would inspect the HTTP response headers of the target system or web application and identify the exposed information.
* Proposed mitigation or fix
  + It is recommended to restrict banner grabbing and minimize access to services from outside the network. This can be achieved through configuration changes and firewall rules to limit the information disclosed in headers and restrict access to the system or application from external sources. Additionally, ensuring that sensitive information is not included in HTTP response headers can help reduce the risk associated with this vulnerability.

1. A screen shot of a computer

   Description automatically generatedVulnerability title - Secure client-initiated renegotiation vulnerability

* Vulnerability threat level
  + Medium
* Vulnerability description
  + This vulnerability, otherwise known as a Plain-Text Injection attack, allows Man-in-the-Middle (MiTM) attackers to insert data into HTTPS sessions, and potentially other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context.
* Affected components.
  + Secure client renegotiation that supports TLS or SSL protocols
* Proposed mitigation or fix
  + Disable Secure Client Initiated Renegotiation
  + Use strict certificate validation.

1. Vulnerability title – SNMP service detected

* Vulnerability threat level
  + Medium
* Vulnerability description
  + Attackers will be able to read the community strings through the service and enumerate quite a bit of information from the target
  + Also, there are multiple remote code execution and denial of service vulnerabilities related to SNMP services.
* Affected components
  + SNMP service
* Proposed mitigation or fix
  + Use a firewall to block the ports from the outside world