A blue and orange logo

Description automatically generated

**IE2062 – Web Security**

**Year 2, Semester 2**

**Scanning report – sendbird.com**

**IT21831904 – K.M. Weerasinghe**

Table of Contents

[Scope of the target 3](#_Toc149226929)

[In scope and rewards 3](#_Toc149226930)

[Out of scope 3](#_Toc149226931)

[Reconnaissance 4](#_Toc149226932)

[Subdomain enumeration 4](#_Toc149226933)

[Gathering information about the target 5](#_Toc149226934)

[Virtual host discovery 8](#_Toc149226935)

[Subdomain takeover 9](#_Toc149226936)

[Scanning 10](#_Toc149226937)

[Using Nmap to scan for open ports. 10](#_Toc149226938)

[Using final recon for scanning 10](#_Toc149226939)

[Vulnerability checking 12](#_Toc149226940)

[Vulnerabilities found using NIKTO. 12](#_Toc149226941)

[Vulnerabilities found using rapidscan] 13](#_Toc149226942)

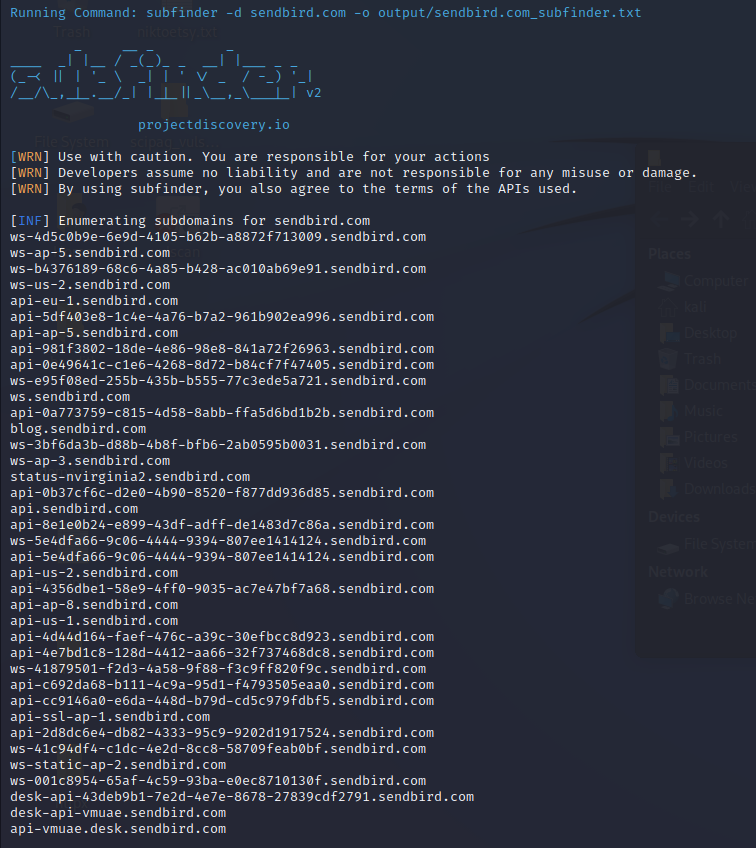
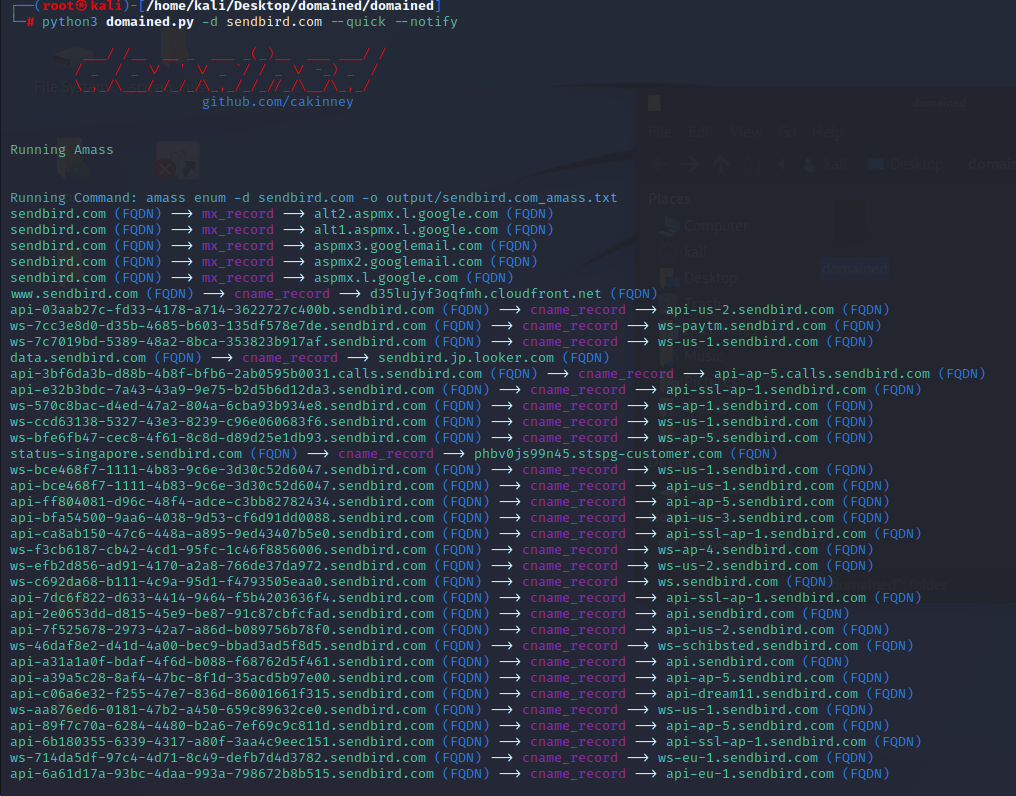
# Scope of the target

## In scope and rewards

## Out of scope

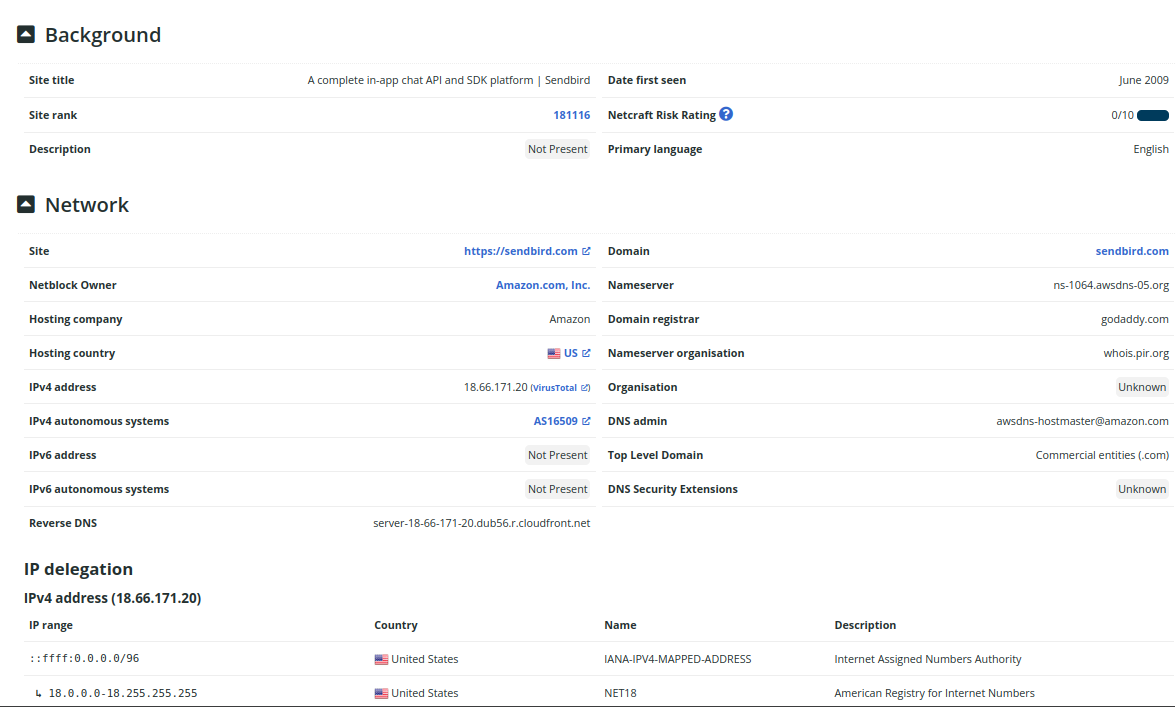
# Reconnaissance

## Subdomain enumeration

* Using domained.py tools amass and subfinder to do the subdomain enumeration of the sendbird.com
* └─# python3 domained.py -d sendbird.com --quick –notify
* The subdomains are outputted to a text file.

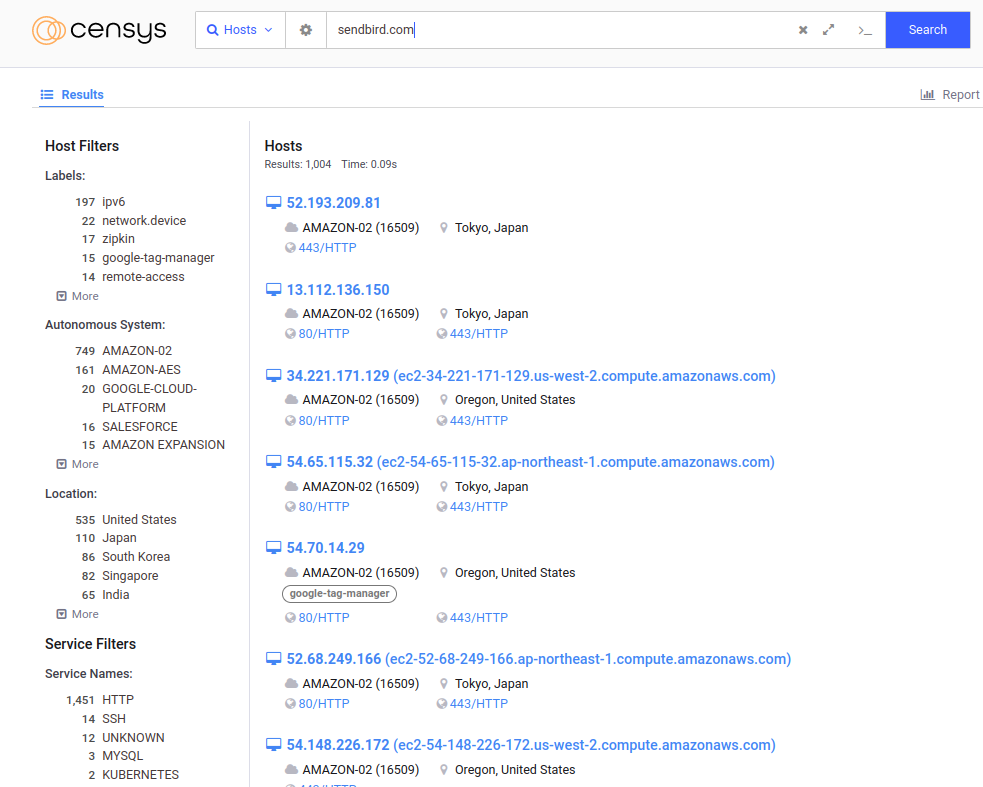
## Gathering information about the target

* A screenshot of a computer

  Description automatically generatedWhois records, domain profile and whois records
* Netcraft scan to gather additional information
* A screenshot of a computer

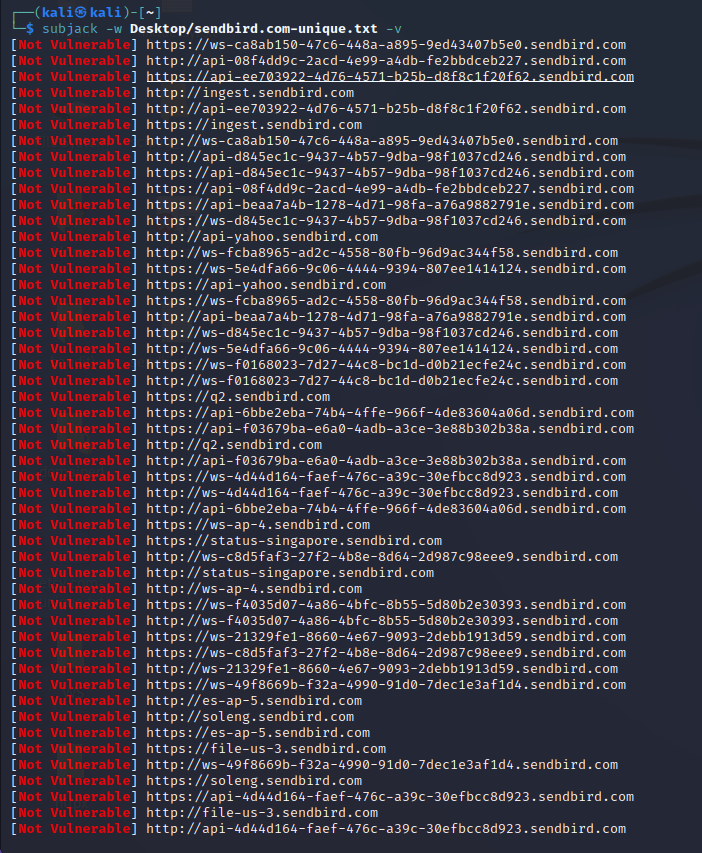
  Description automatically generatedSecurity header checking
* Missing headers found
  + content-Security - Policy Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
  + X-Frame-Options - X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
  + X-Content-Type-Options - X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
  + 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.

## Virtual host discovery



* SSL/TLS certificates were found to be appropriately configured without any evident weaknesses or misconfigurations.
* DNS records did not reveal any additional attack vectors or improperly configured subdomains.
* Sensitive data, such as databases, was not identified as publicly accessible through the Censys scan.

## Subdomain takeover

* checking if any of the subdomains found using the domained.py are vulnerable to takeover
* └─$ subjack -w Desktop/sendbird.com-unique.txt -v
* No vulnerable subdomains were found by the subjack scan
* All subdomains look secure
* No issued were found in the subdomain analysis for the sendbird.com

# Scanning

## A computer screen shot of a program Description automatically generatedUsing Nmap to scan for open ports.

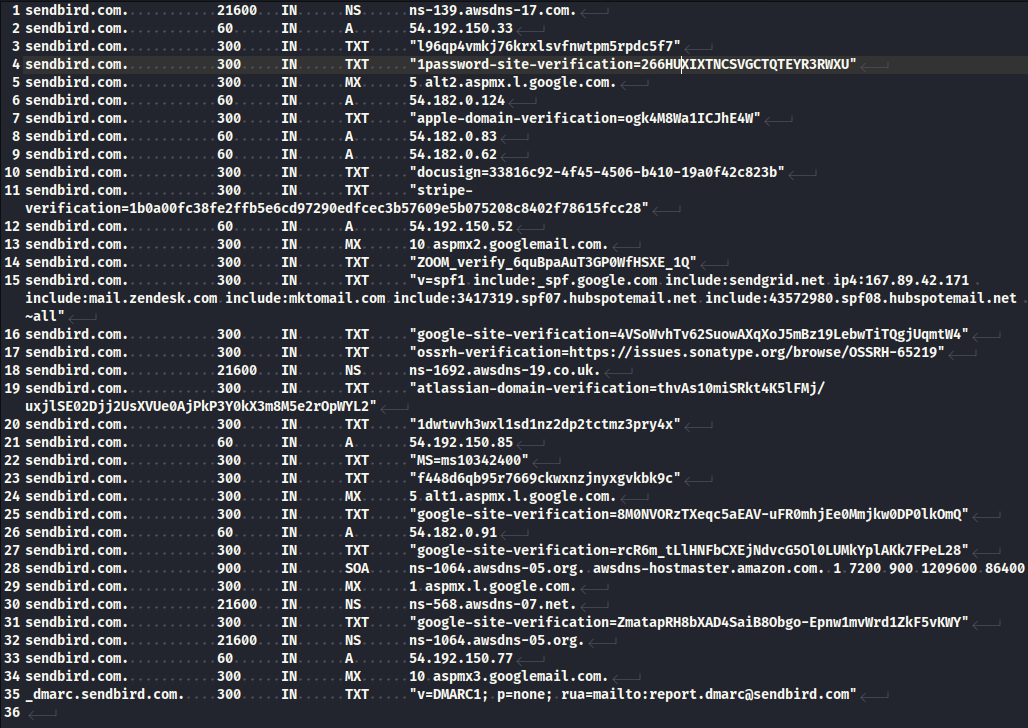
* No open ports were found while doing the Nmap scan

## Using final recon for scanning

**A blue and white object

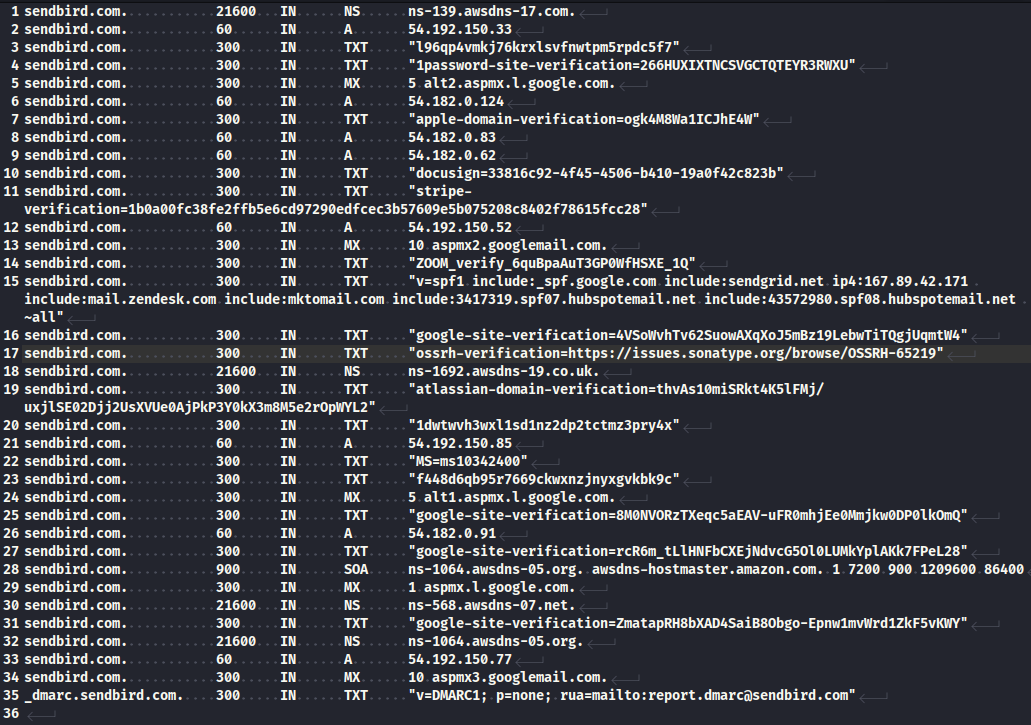
Description automatically generated with medium confidenceInformation gathered using crawler**

**DNS records gathered**



**A screen shot of a computer

Description automatically generatedSitemap for the senbird**

**DNS record of the website**

* Sometimes robots.txt or sitemap.xml may contain rules such that certain links that are not supposed to be accessed/indexed by crawlers and search engines. Search engines may skip those links but attackers will be able to access it directly.

# Vulnerability checking

## Vulnerabilities found using NIKTO.

* ┌──(kali㉿kali)-[~]

└─$ nikto -h sendbird.com

- Nikto v2.1.6

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

+ Target IP: 54.192.150.33

+ Target Hostname: sendbird.com

+ Target Port: 80

+ Message: Multiple IP addresses found: 54.192.150.33, 54.192.150.77, 54.192.150.52, 54.192.150.85

+ Start Time: 2023-10-12 02:48:16 (GMT-4)

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

+ Server: CloudFront

+ Retrieved via header: 1.1 f5171077d7910626ec3cf65e0c222f3c.cloudfront.net (CloudFront)

+ 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

+ Uncommon header 'x-cache' found, with contents: Redirect from cloudfront

+ Uncommon header 'x-amz-cf-pop' found, with contents: SIN2-C1

+ Uncommon header 'x-amz-cf-id' found, with contents: eygNkeIfIHlK6lVWUsQtsSrKhGVdU7JytdsLrRpbSO3WnNkozlnNYQ==

+ 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://sendbird.com/

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

+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Operation now in progress

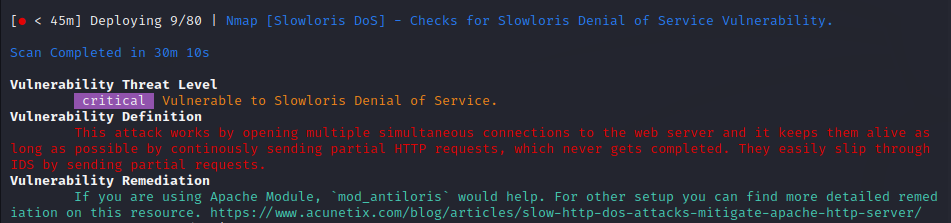
+ Scan terminated: 17 error(s) and 7 item(s) reported on remote host

+ End Time: 2023-10-26 03:04:25 (GMT-4) (969 seconds)

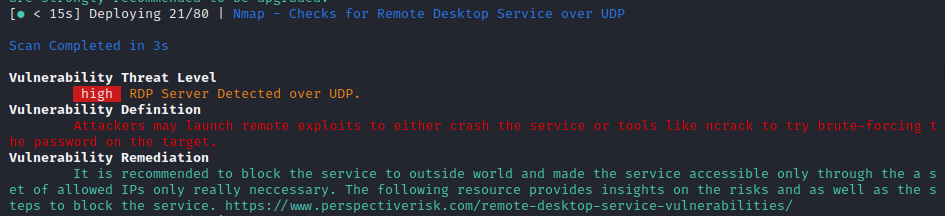
---------------------------------------------------------------------------

+ 1 host(s) tested

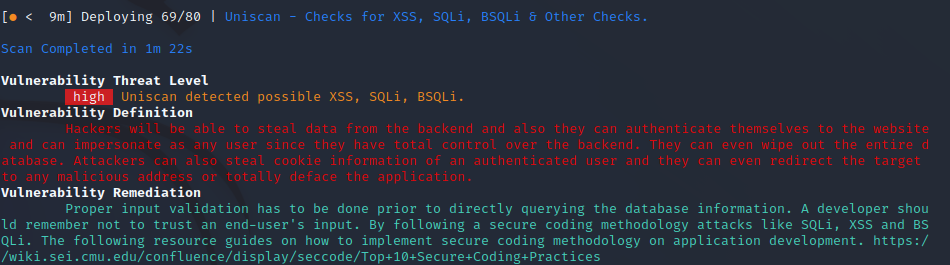
## Vulnerabilities found using rapidscan

1. Vulnerability title – vulnerability check for slowloris DoS attacks using Nmap

* 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

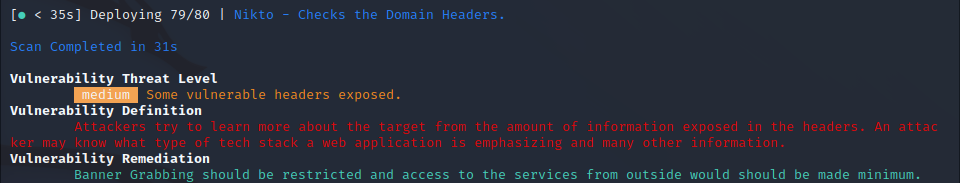
1. vulnerability title – RDP server detected over UDP.

* Vulnerability threat level
  + High
* Vulnerability description
  + Attacker may launch remote exploits to either crash the service or tools like ncrack to try brute-forcing the password of the target.
* Impact assessment
  + The vulnerability has a high threat level, as it can lead to service disruptions or unauthorized access
* Proposed mitigation or fix
  + It is recommended that to block the service outside world and make the service accessible only through the set of allowed IPs only necessary to prevent potential exploits.

1. Vulnerability title – possible XSS, SQLi, BSQLi

* vulnerability threat level
  + high
* vulnerability description
  + hackers will be able to steal data from the backend and also they can authenticate themselves to the website and can impersonate as any user since they have total control over the backend. They can even wipe out the entire database. Attackers can also steal cookie information of an authenticated user and they can even redirect the target to any malicious address or totally deface the application.
* Affected components
  + This vulnerability impacts the application's backend and data storage components
* Impact assessment
  + The impact of this vulnerability is high, as it allows for data theft, unauthorized access, potential data loss, and various forms of user manipulation.
* Steps to reproduce
  + Identify input fields or areas in the application that lack proper validation.
  + Inject malicious scripts or SQL queries into these input fields.
  + Observe how the application responds to these inputs, and whether it executes the injected code.
* Proposed mitigation or fix
  + Proper input validation needs to be implemented before querying the database information
  + A developer should remember not to trust an end users input
  + Follow secure coding methodology

1. Vulnerability title - Vulnerable headers exposed



* Vulnerability description
  + 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.
* Affected components
  + affects the web server's response headers, potentially exposing sensitive information about the web application and its underlying technologies.
* Impact assessment
  + vary depending on the information exposed, but it could aid attackers in crafting more targeted attacks or identifying potential weaknesses in the web application.
* Proposed mitigation or fix
  + Banner Grabbing should be restricted and access to the services from outside would should be made minimum.
  + configuring the web server to provide minimal information in its headers and implementing network security measures to limit external access to sensitive information.