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](#_Toc149509757)

[In scope and rewards 3](#_Toc149509758)

[Out of scope 3](#_Toc149509759)

[Reconnaissance 4](#_Toc149509760)

[Subdomain enumeration 4](#_Toc149509761)

[Gathering information about the target 5](#_Toc149509762)

[Virtual host discovery 8](#_Toc149509763)

[Subdomain takeover 9](#_Toc149509764)

[Scanning 10](#_Toc149509765)

[Using Nmap for scanning 10](#_Toc149509766)

[Using final recon for scanning 10](#_Toc149509767)

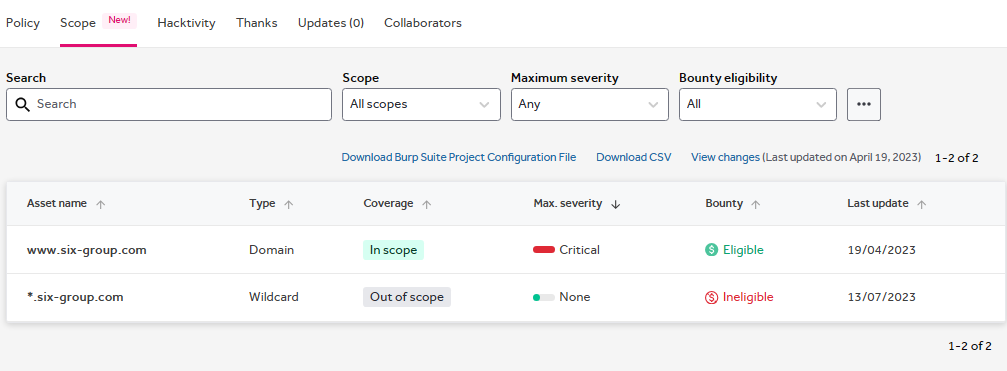
[Vulnerability checking 13](#_Toc149509768)

[Vulnerabilities found using NIKTO 13](#_Toc149509769)

[Vulnerabilities found using rapidscan 14](#_Toc149509770)

# Scope of the target

# In scope and rewards



## Out of scope

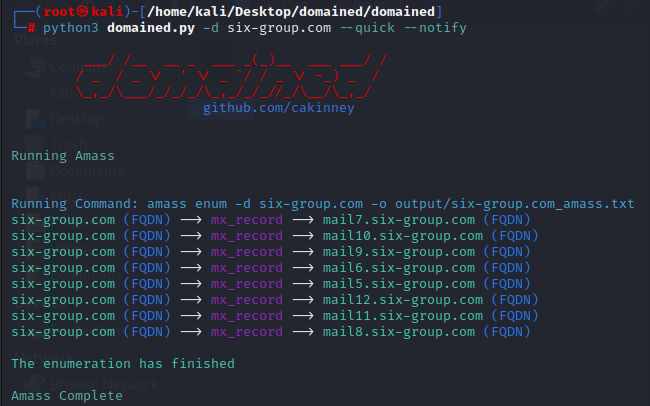
A screenshot of a computer screen

Description automatically generated

# Reconnaissance

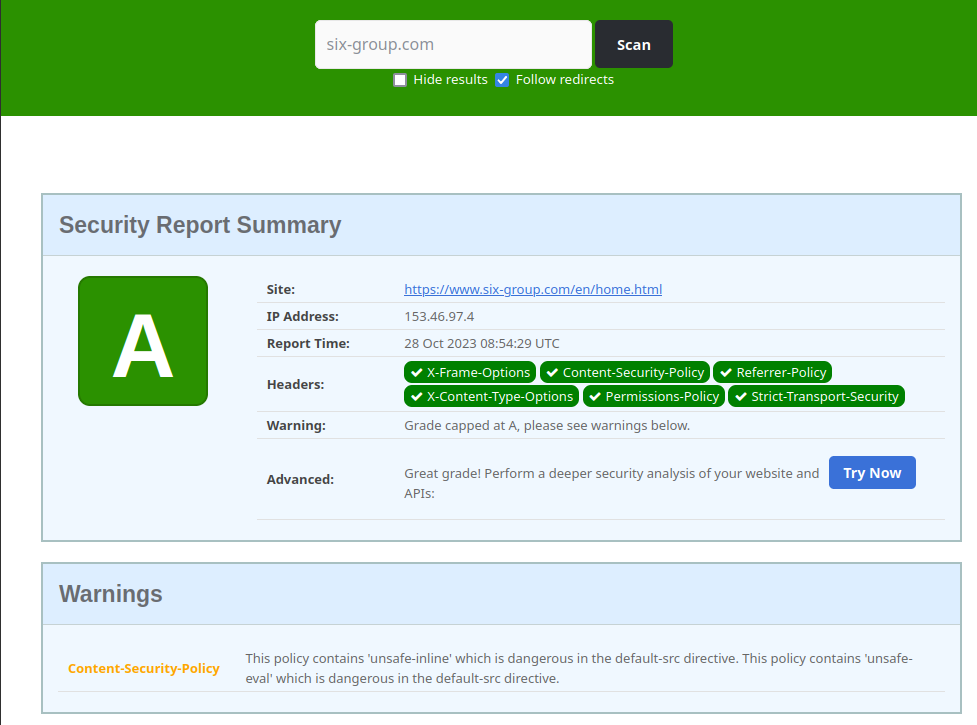
## Subdomain enumeration

* A screenshot of a computer screen

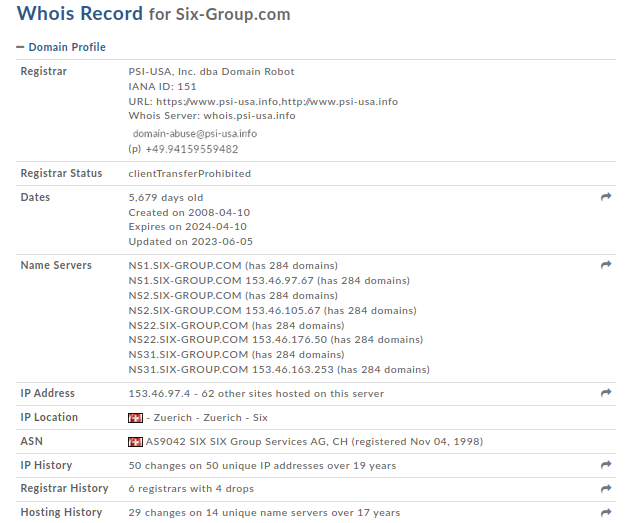
  Description automatically generated─# python3 domained.py -d six-group.com --quick --notify

## Gathering information about the target

* Security header checking



* No missing header found
* A screenshot of a computer screen

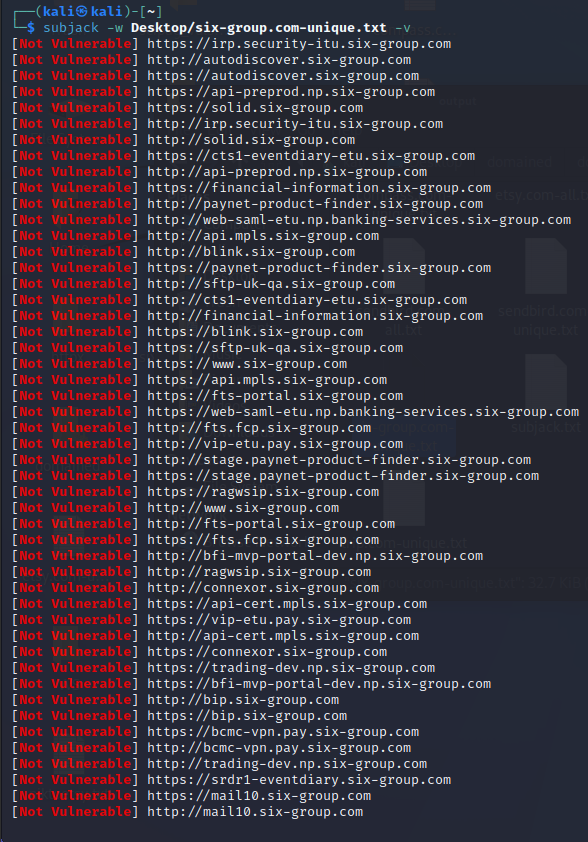
  Description automatically generatedDomain profile and whois records
* The whois records are redacted and there aren’t any information to be found
* A screenshot of a computer

  Description automatically generatedA screenshot of a computer

  Description automatically generatednetcraft scan to gather background, network, and certificate information

## A screenshot of a computer Description automatically generatedVirtual host discovery

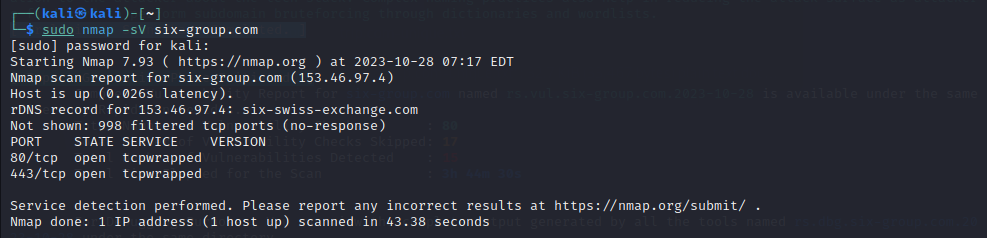
## Subdomain takeover

* └─$ subjack -w Desktop/six-group.com-unique.txt -v
* 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 six-group.com



## Using final recon for scanning

* └─$ finalrecon --full <https://www.six-group.com>

A computer screen shot of a computer

Description automatically generatedInformation gathered using the crawlers

A screen shot of a computer

Description automatically generatedsitemaps found using the crawler

* A screen shot of a computer program

  Description automatically generatedDNS records found

# Vulnerability checking

## Vulnerabilities found using NIKTO

└─$ nikto -h six-group.com

- Nikto v2.1.6

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

+ Target IP: 153.46.97.4

+ Target Hostname: six-group.com

+ Target Port: 80

+ Start Time: 2023-10-28 03:42:07 (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://six-group.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: 19 error(s) and 3 item(s) reported on remote host

+ End Time: 2023-10-28 04:26:26 (GMT-4) (2659 seconds)

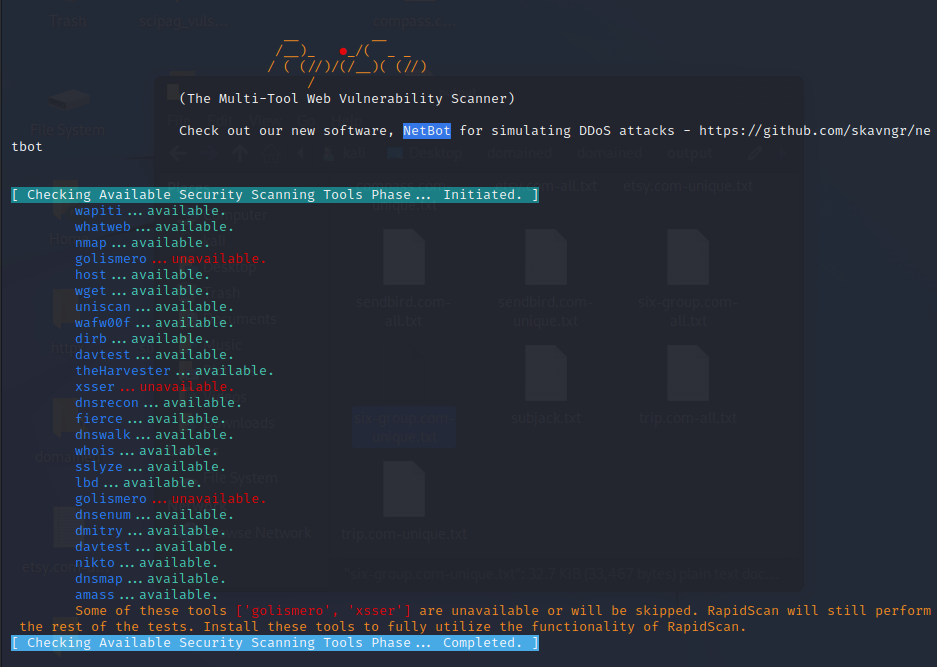
---------------------------------------------------------------------------

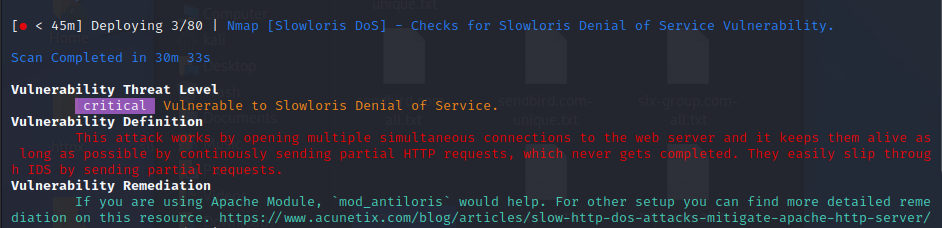
+ 1 host(s) tested

* Vulnerability
  + X-XSS Protection is not Present
* Vulnerability Definition
  + As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.
* Vulnerability Remediation
  + Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.

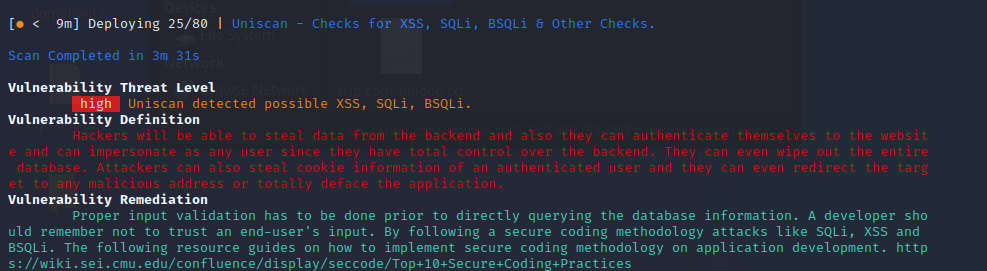
## Vulnerabilities found using rapidscan

* └─# ./rapidscan.py six-group.com

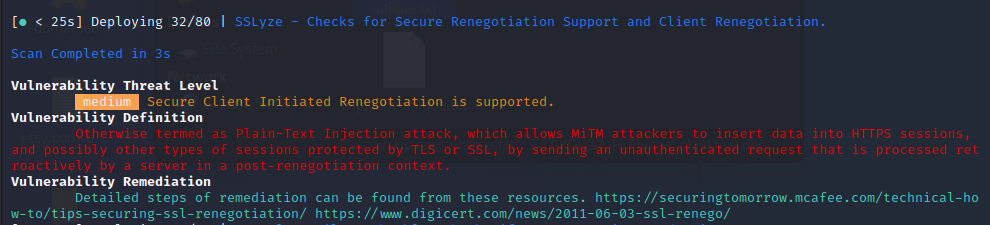


1. Vulnerability title – vulnerable to slowloris denial of service

* 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

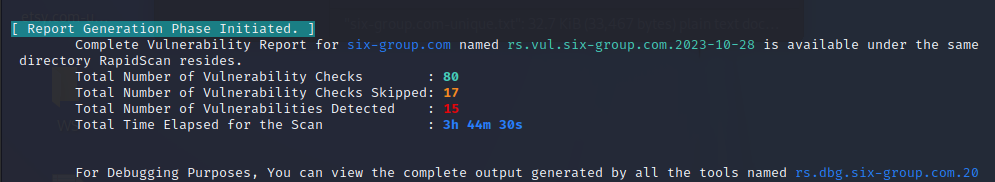
1. Vulnerability title - possible XSS, SQLi, BSQLi

* vulnerability threat level
  + high
* vulnerability description
  + Hackers will be able to steal data from the backend and, 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 - 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 titleA screenshot of a computer error

   Description automatically generated – no DNS/HTTP based load balancers found
   * vulnerability threat level
     + low
   * vulnerability definition
     + attackers may use the unavailability of load balancers as an advantage to leverage a denial of service attack on certain services or on the whole application itself
   * Affected components:
     + The vulnerability impacts the overall system's architecture, particularly in the context of network and traffic distribution.
   * proposed mitigation or fix
     + implementation of load balancers as that improve the performance times as well as data availability on during times of server outage