A blue and orange logo

Description automatically generated

**IE2062 – Web Security**

**Year 2, Semester 2**

**Scanning report – Bitstamp**

**IT21831904 – K.M. Weerasinghe**

Table of Contents

[Scope of the target 3](#_Toc149509713)

[In scope and rewards 3](#_Toc149509714)

[Out of scope 3](#_Toc149509715)

[Reconnaissance 4](#_Toc149509716)

[Subdomain enumeration 4](#_Toc149509717)

[Gathering information about the target 5](#_Toc149509718)

[Virtual host discovery 8](#_Toc149509719)

[Subdomain takeover 9](#_Toc149509720)

[Scanning 10](#_Toc149509721)

[Using FinalRecon for scanning 10](#_Toc149509722)

[DNS records 11](#_Toc149509723)

[Vulnerability checking 12](#_Toc149509724)

[Vulnerabilities found using nikto 12](#_Toc149509725)

[Vulnerabilities found using rapidscan 13](#_Toc149509726)

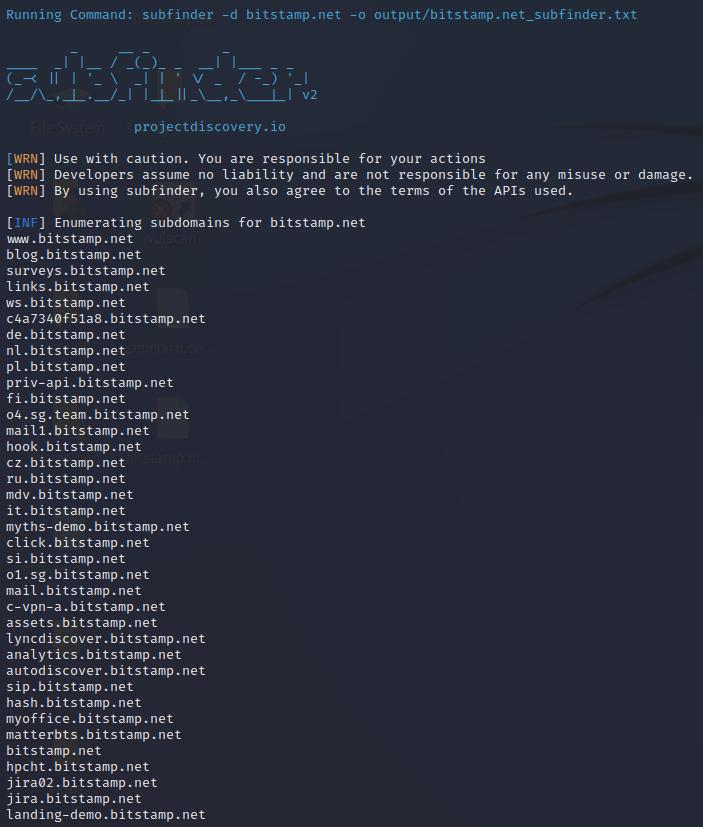
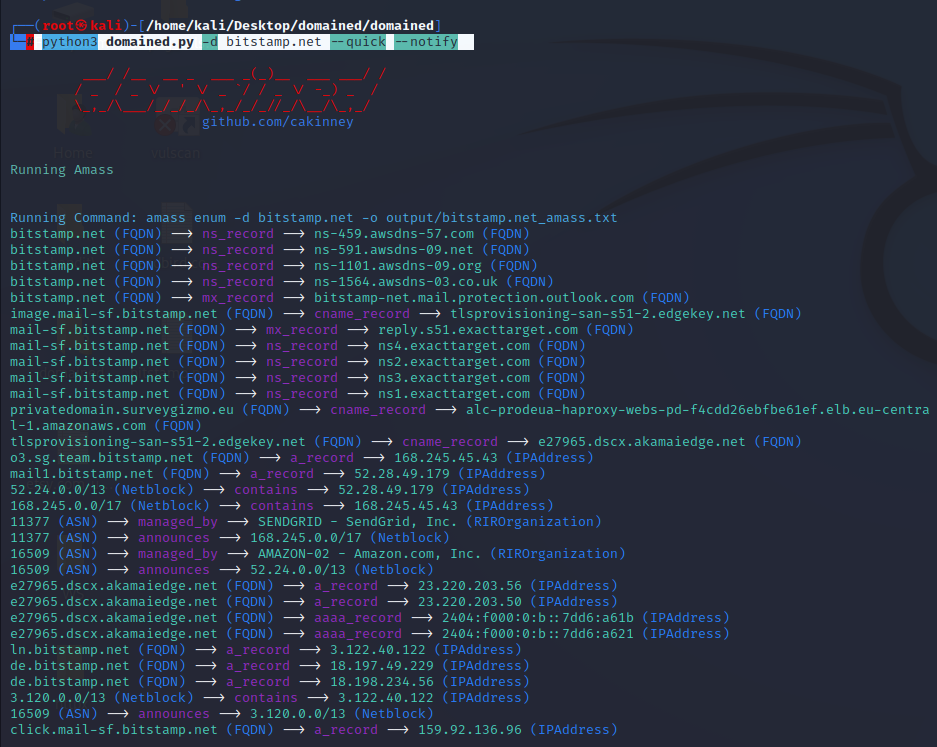
# Scope of the target

## In scope and rewards

## A screenshot of a computer program Description automatically generatedOut of scope

# Reconnaissance

## Subdomain enumeration

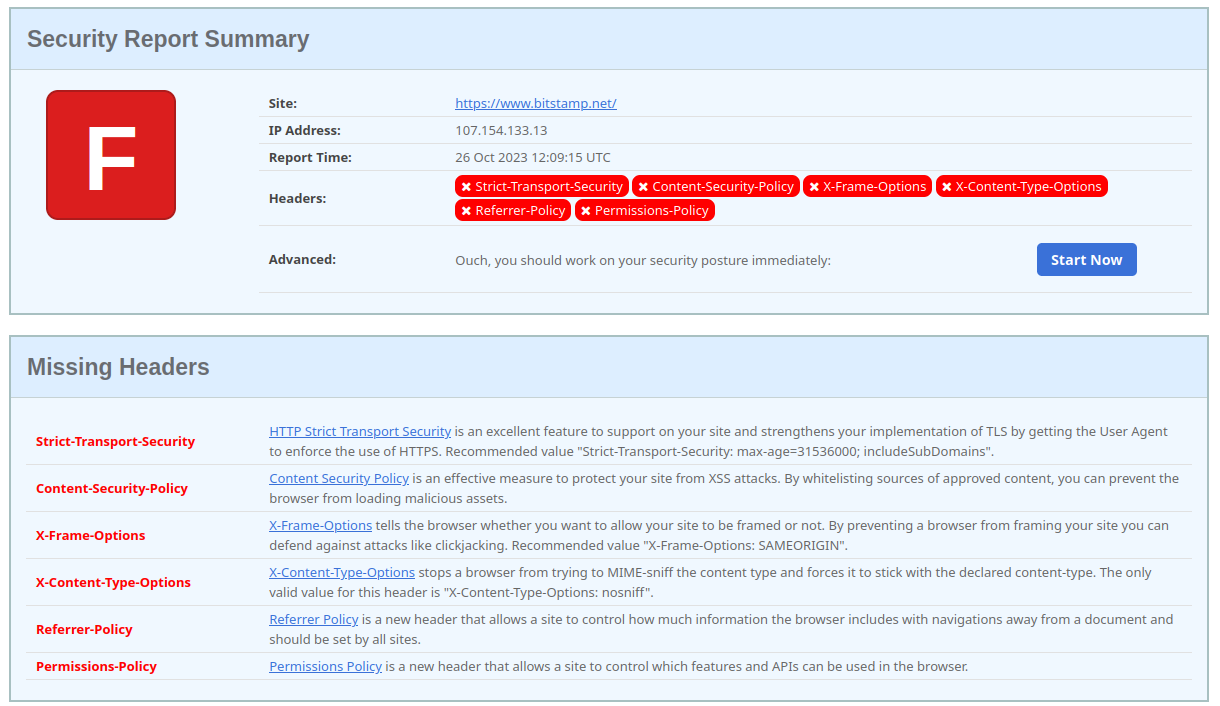
* Using domained.py tools amass and subfinder to do the subdomain enumeration of the bitstamp.net
* └─# python3 domained.py -d bitstamp.net --quick –notify
* The output of the scanned domains are save in a text file

# Gathering information about the target

* Domain profile and the whois records of the target
  + Domain profile
  + A screenshot of a computer

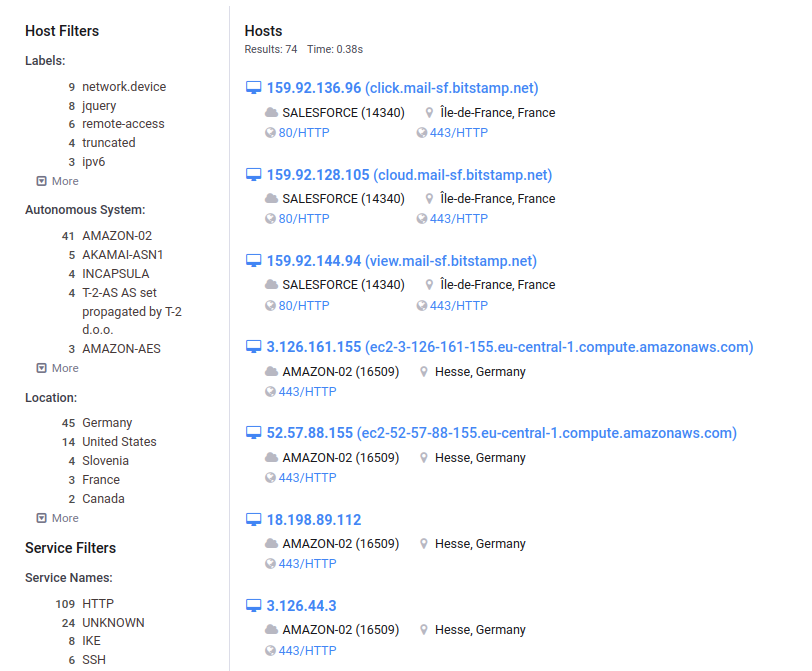
    Description automatically generatedwhois record
* A screenshot of a computer

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

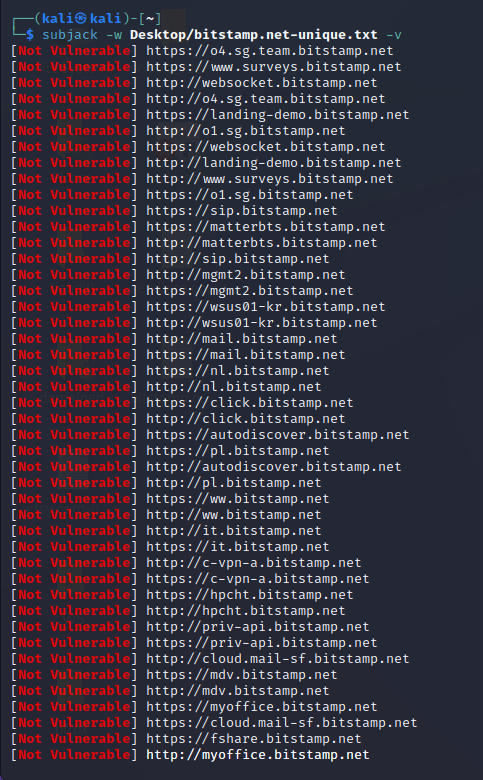


• SSL/TLS certificates were found to be appropriately configured without any evident weaknesses or misconfigurations.

• 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.

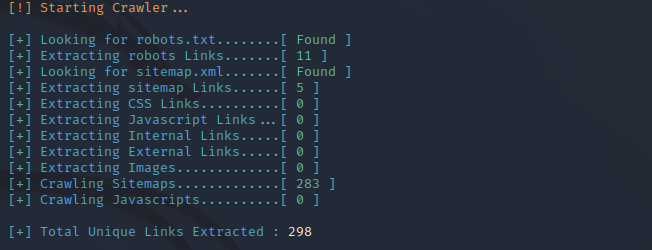
## Subdomain takeover

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

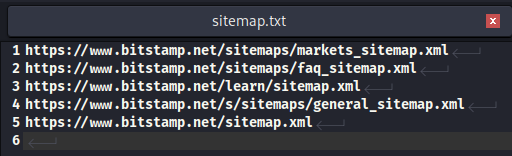
# Scanning

## Using FinalRecon for scanning

**Information gathered using crawlers**

****

**Sitemap**

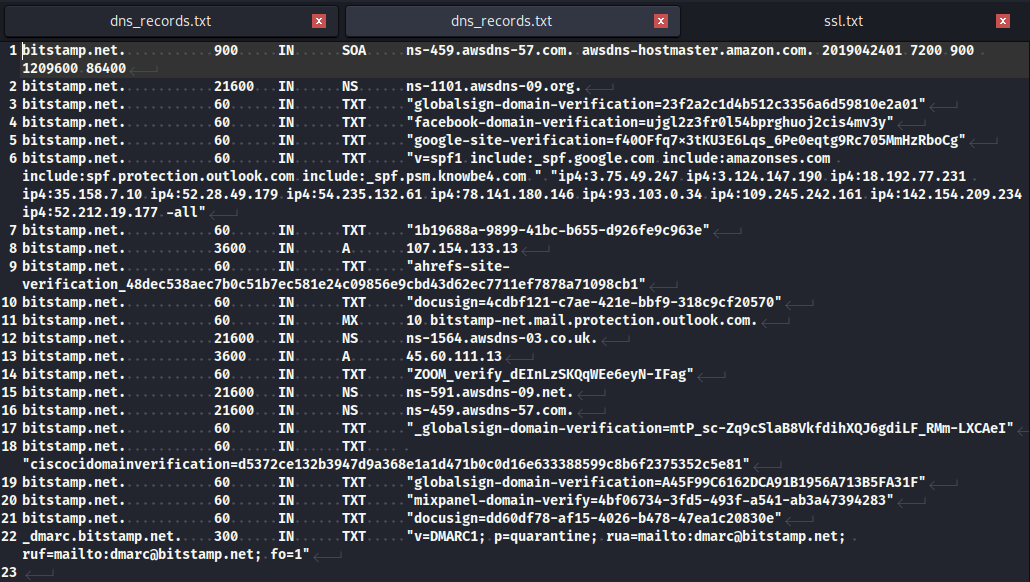
****

**A screenshot of a computer

Description automatically generated**

* 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.
* Mitigation or fix
  + It is a good practice not to include sensitive links in the robots or sitemap files.

## DNS records



* How DNS records could be used
  + DNS hijacking, which is a type of DNS attack in which DNS queries are incorrectly resolved to unexpectedly redirect users to malicious sites
  + DNS tunneling: Attackers can use DNS records to tunnel traffic to and from their own servers. This can be used to bypass network security controls, such as firewalls and web application firewalls.
  + DNS amplification attacks: Attackers can use DNS records to launch DNS amplification attacks against the bug bounty program's website or other infrastructure. This can be done by sending large DNS requests to the bug bounty program's DNS servers. If the attack is successful, it can overwhelm the servers and cause the website to become unavailable.

# Vulnerability checking

## Vulnerabilities found using nikto

* Basic nikto scan for searching vulnerabilities
  + └─$ nikto -h bitstamp.net

- Nikto v2.1.6

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

+ Target IP: 107.154.133.13

+ Target Hostname: bitstamp.net

+ Target Port: 80

+ Message: Multiple IP addresses found: 107.154.133.13, 45.60.111.13

+ Start Time: 2023-10-26 07:15:56 (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://www.bitstamp.net/

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

+ Uncommon header 'x-iinfo' found, with contents: 14-56290933-0 0NNN RT(1698319353222 0) q(0 -1 -1 -1) r(0 -1)

+ ERROR: Error limit (20) reached for host, giving up. Last error:

+ Scan terminated: 3 error(s) and 4 item(s) reported on remote host

+ End Time: 2023-10-26 07:28:01 (GMT-4) (725 seconds)

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

+ 1 host(s) tested

* Vulnerability title – X-XSS header not found
* Vulnerability description - This vulnerability pertains to the absence of the X-XSS-Protection header in the target web server's response. This absence makes older web browsers vulnerable to Reflected Cross-Site Scripting (XSS) attacks, which can allow malicious code to be executed within a user's browser context
* Proposed mitigation or fix - To mitigate this vulnerability, the web server should be configured to include the X-XSS-Protection header in its responses. This header can be set to enable the browser's built-in XSS protection mechanisms. Additionally, it's essential to keep web browsers updated to the latest versions with improved security features.

## Vulnerabilities found using rapidscan

* Commands for the full rapidscan
* └─# ./rapidscan.py
* ─# ./rapidscan.py bitstamp.net

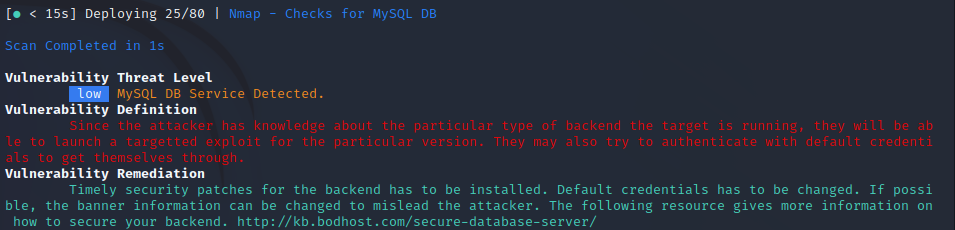
1. Vulnerability title – FTP service detected

A screen shot of a computer

Description automatically generated

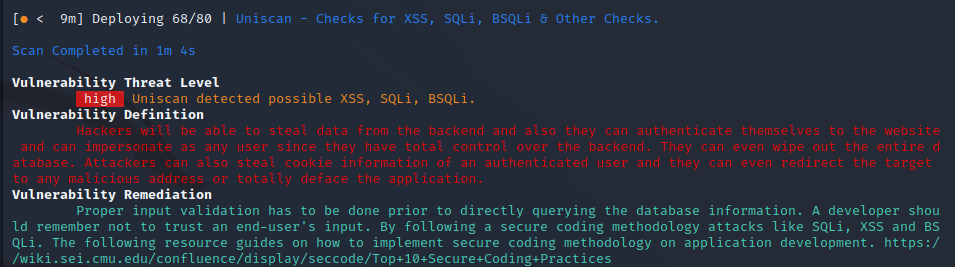
* Vulnerability description
  + This protocol does not support secure communication and there are likely high chances for the attacker to eavesdrop the communication. Also, many FTP programs have exploits available on the web such that an attacker can directly crash the application or get a SHELL access to that target.
* Affected components
  + FTP service running on the target system
* Impact assessment
  + The impact of this vulnerability is significant, as it exposes communication to potential eavesdropping and the risk of the FTP service being exploited to compromise the target system's security.
* Proposed mitigation or fix
  + To mitigate this vulnerability, it is recommended to replace the FTP protocol with SSH (Secure Shell) for secure communication. SSH provides a more secure alternative to FTP, ensuring confidentiality and data integrity during file transfers and remote access.

1. Vulnerability title – MySQL DB services detected



* Vulnerability threat level
  + low
* Vulnerability description
  + Since the attacker has knowledge about the particular type of backend the target is running, they will be able to launch a targeted exploit for the particular version. They may also try to authenticate with default credentials to get themselves through.
* Affected components
  + MySQL database services.
* Proposed mitigation or fix
  + Timely security patches for the backend should be installed to address known vulnerabilities.
  + Change default credentials to more secure and unique ones to prevent unauthorized access

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