**TASK 5**

1. FIND 3 WEBSITES VULNERABLE TO CLICKJACKING/UI REDRESS VULNERABILITY.

NOTE: THIS VULNERABILITY SHOULD BE FOUND IN WEBSITES WHICH HAVE

RESPONSIBLE DISCLOSURE POLICY/REPORTING POLICY/SECURITY ISSUE DISCLOSURE POLICY

2. FIND 2 WEBSITES VULNERABLE TO NO RATE LIMITING VULNERABILITY IN LOGIN PAGES, USERNAME/EMAIL ENUMRATION-PAGES

NOTE: THIS VULNERABILITY SHOULD BE FOUND IN WEBSITES WHICH HAVE RESPONSIBLE DISCLOSURE POLICY/REPORTING POLICY/SECURITY ISSUE DISCLOSURE POLICY

3. FIND 1 WEBSITE WITH NO RATE LIMITING VULNERABILITY IN FOLLOWING CATEGORIES:

1. FORGOT PASSWORD/PASSWORD RESET PAGES

2. COMMENT PAGES

3. REVIEW PAGES

4. GET A QUOTE PAGE

CLICKJACKING/UI REDRESS VULNERABILITY:

Clickjacking, also known as UI redress vulnerability, is a type of cyber-attack where an attacker tricks a user into clicking on a seemingly innocuous element on a website or application, while the actual action being performed is hidden or disguised. This technique allows the attacker to hijack the user's clicks and perform unintended actions without their knowledge or consent.

Impact of clickjacking

Unauthorized data disclosure

Account hijacking

Malware installation

Remedial actions

Implement frame-busting code.

Implement x-frame-options header.

Content security policy (CSP)

User awareness and education

1.<https://www.debet.az>

A close-up of a pair of sunglasses

Description automatically generated with medium confidence

This website is vulnerable to Clickjacking because this can be added to another HTML page and can be embedded in that website.

Here we have an html file:

A screenshot of a computer program

Description automatically generated with medium confidence

This will add the following website to the HTML page

A screenshot of a web page

Description automatically generated with medium confidence

2. <https://www.hfsjg.ch>

A screenshot of a computer

Description automatically generated with low confidence

This website is vulnerable to Clickjacking because this can be added to another HTML page and can be embedded in that website.

Here we have an html file:

A screenshot of a computer program

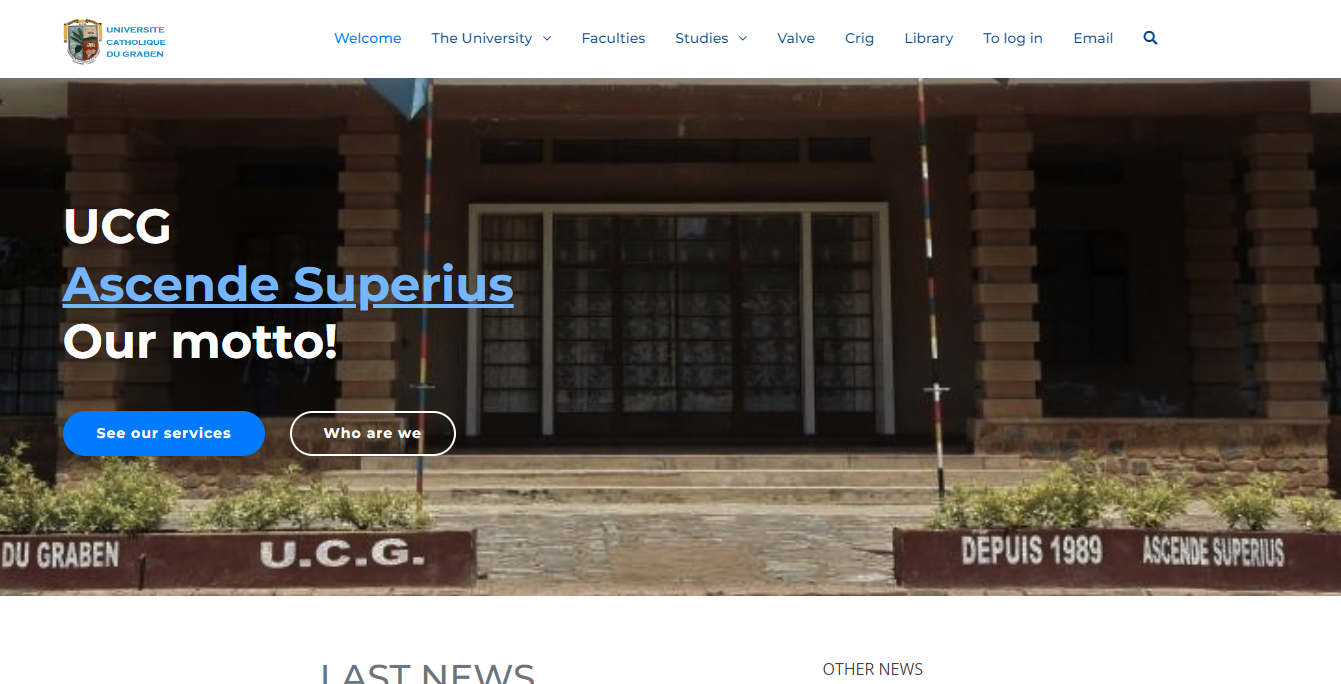
Description automatically generated with low confidence

This will add the following website to the HTML page

A screenshot of a web page

Description automatically generated with low confidence

3. <https://www.ucgraben.ac.cd>



This website is vulnerable to Clickjacking because this can be added to another HTML page and can be embedded in that website.

Here we have an html file:

A screenshot of a computer

Description automatically generated with medium confidence

This will add the following website to the HTML page

A screenshot of a website

Description automatically generated with low confidence

NO RATE LIMITING VULNERABILITY:

A no rate limiting vulnerability refers to a security flaw that allows an attacker to bypass rate limiting controls implemented by a system or application. Rate limiting is a technique used to control the rate of incoming requests or actions to prevent abuse or overload of resources. However, when a no rate limiting vulnerability is present, an attacker can bypass these limitations, potentially leading to a range of negative impacts.

Impacts of a no rate limiting vulnerability

Denial of service (dos) attacks

Account takeover

Data leakage

Remedial actions

Implement rate limiting controls

Monitoring and alerting

Input validation and sanitization

Regular security audits

Security patching and updates

1. <https://www.cruisecritic.com.au/>

The forgot password page of above website is vulnerable to no rate limiting vulnerability.

A screenshot of a computer screen

Description automatically generated with medium confidence

Steps to reproduce the vulnerability:

1. Turn the intercept to ON in burp suite.
2. Then capture the http request.
3. Send it to the intruder.
4. Clear all the payloads and add only payload to the email attribute.
5. Start the attack with null payloads.
6. We get status as 200 OK.

A screenshot of a computer

Description automatically generated with medium confidence

The http burp suite request.

A screen shot of a computer code

Description automatically generated with low confidence

Changing the payload values

A screenshot of a computer

Description automatically generated

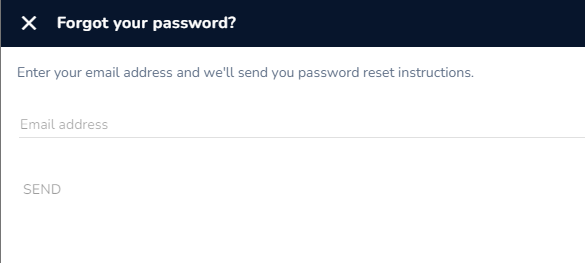
We get 200 OK after starting the attack with null payloads



As we can see,this shows the prescence of no rate limiting vulnerability using the email enumeration.

1. <https://app.salesflare.com/#/password/request>

The forgot password page of above website is vulnerable to no rate limiting vulnerability.



Steps to reproduce the vulnerability:

1.Turn the intercept to ON in burp suite.

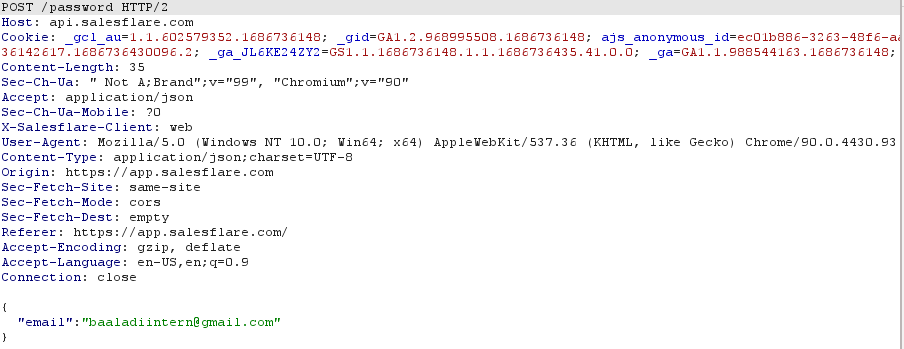
2.Then capture the http request.

3.Send it to the intruder.

4.Clear all the payloads and add only payload to the email attribute.

5.Start the attack with null payloads.

6.We get status as 200 OK.



The http burpsuite request



Setting the payload values

A screenshot of a computer

Description automatically generated with medium confidence

Giving the payload values

A picture containing text, screenshot, font

Description automatically generated

As we can see, we got 11 mails from the salesfare website which results in the prescence of no rate limiting vulnerability in the forgot password page.