Group no :5
Name: BEJAWADA GOPINADH

Process of Bug bounty

Step 1) The target for bug hunting is chosen from websites and web applications listed on OpenBugBounty.
The Target system selected from openbugbounty Programs is:

- https://www.carat.ch

Reconnaissance (Information Gathering)

Step 2)
Firstly, we verify the connection by sending a ping to the target machine.
And we Found Ip for target machine is 5.148.188.98

```
┌──(kali㉿kali)-[~]
└─$ ping carat.ch
PING carat.ch (5.148.188.98) 56(84) bytes of data.
64 bytes from igs02.nine.ch (5.148.188.98): icmp_seq=1 ttl=128 time=94.5 ms
64 bytes from igs02.nine.ch (5.148.188.98): icmp_seq=2 ttl=128 time=97.3 ms
64 bytes from igs02.nine.ch (5.148.188.98): icmp_seq=3 ttl=128 time=97.6 ms
^C
```
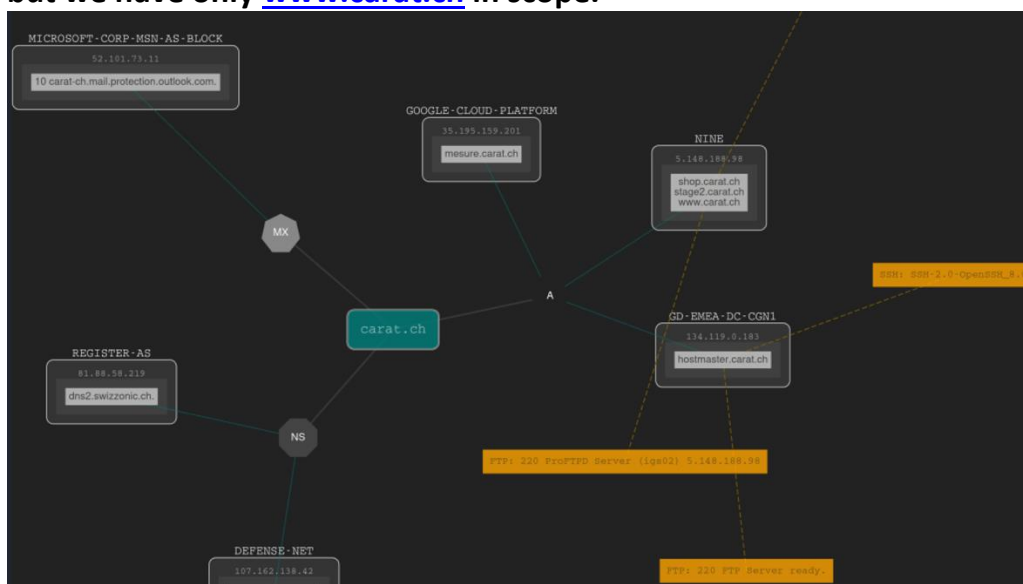
Step 3)
DNSDumpster provides a visual representation of the DNS (Domain Name System) information related to a domain. This includes subdomains, associated IP addresses, and other DNS records.
We found these subdomains:
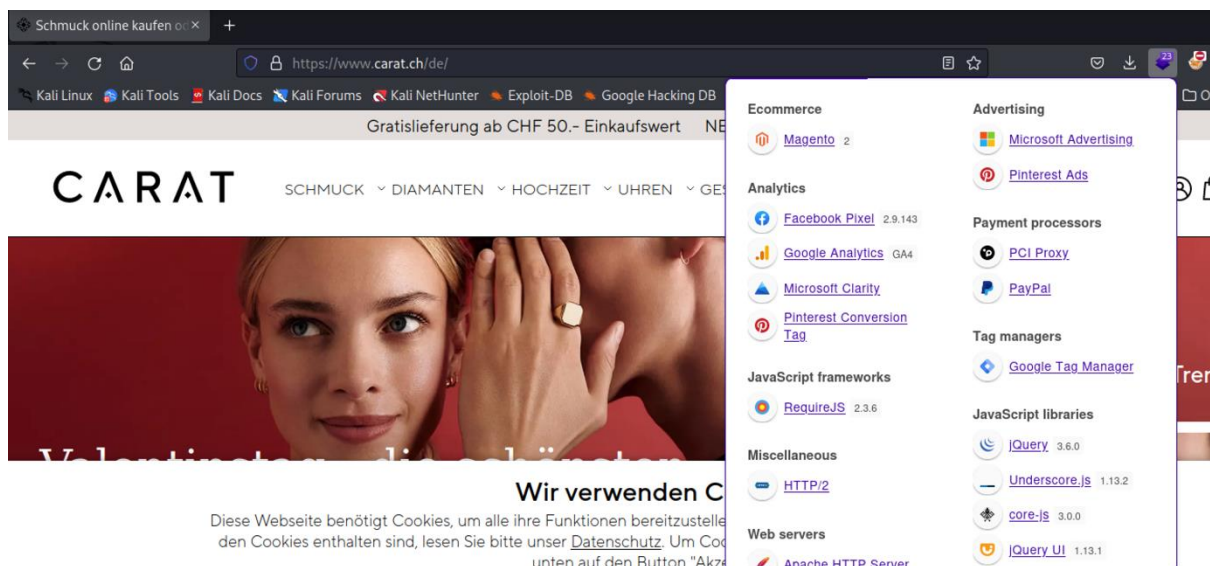
- Shop.carat.ch
- Stage2.carat.ch
- www.carat.ch

but we have only www.carat.ch in scope.

Step 4)

Identify the target application and gather relevant details. we've extracted this Information by using tools whois, wappalyzer, Host, builtwith, and curl.

- Address: 5.148.188.98
- Identify web server: Apache HTTP Server
- E-commerce: Megento
- Database MySQL

Scanning

Step 5)

Performing port scan on the target machine using namp.
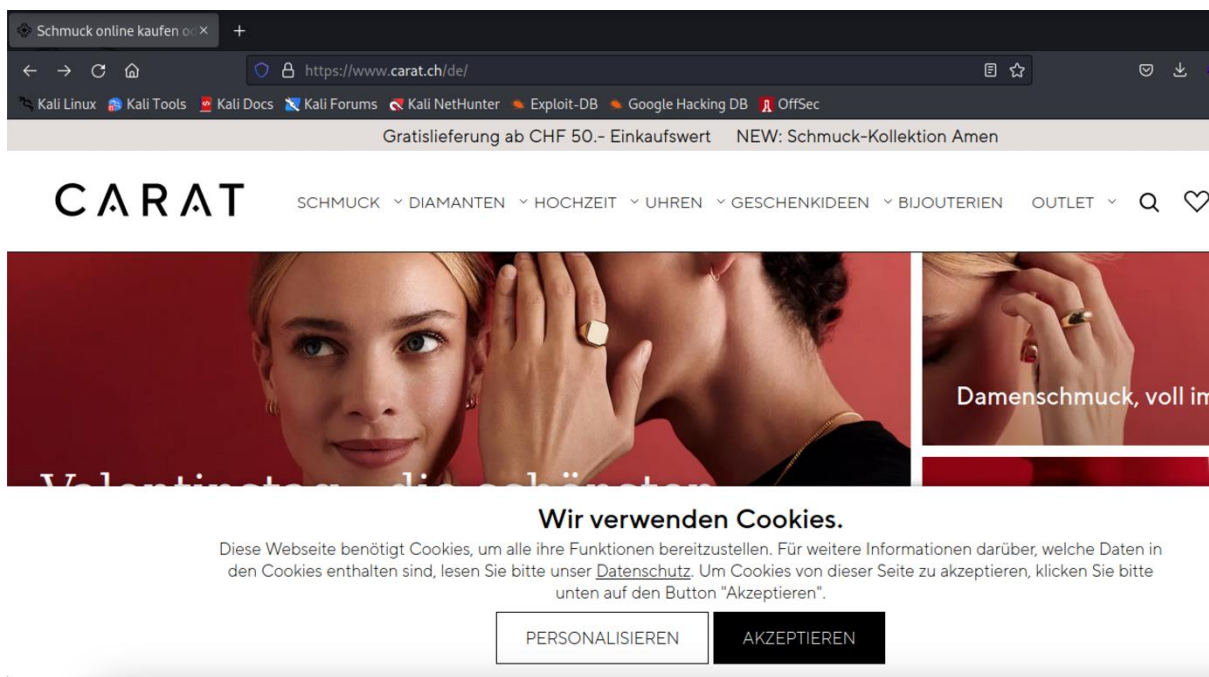Open Ports and services running on them listed below :

Nmap of carat.ch scan for open ports & services

- Port 80(HTTP) is running and an apache server is running on port 443.
- Also, port 1122 is also open for SSH.

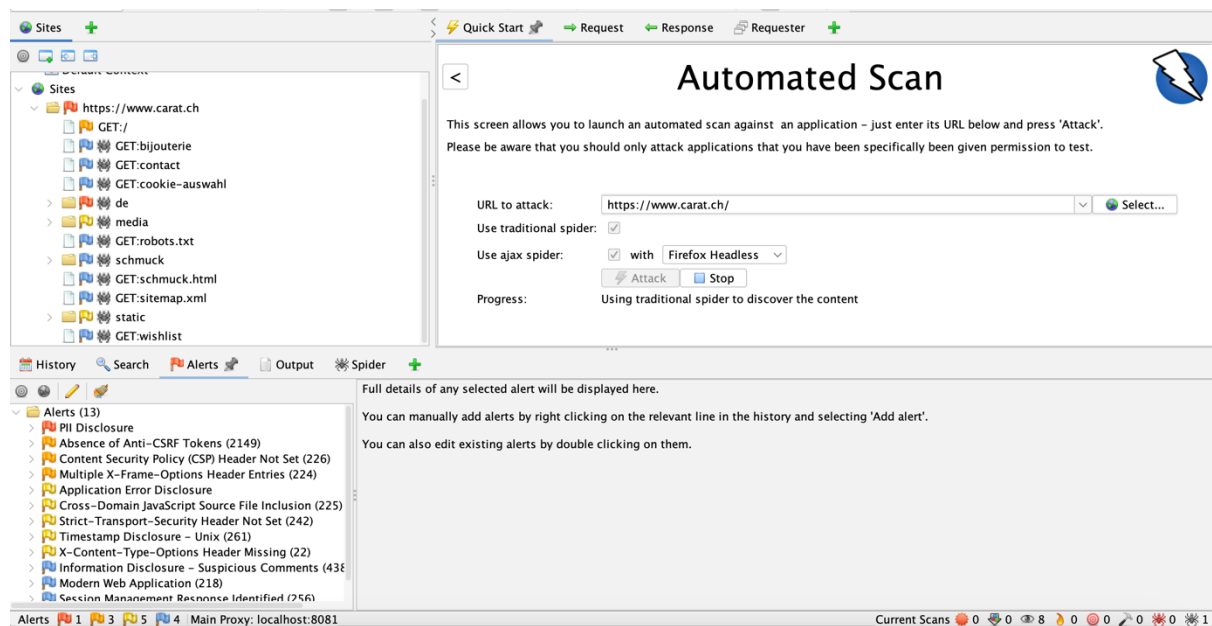- Port 21 is open for ftp
- Port 22 open for ssh

Step 6) Checking the web service running on target machine

Upon inspecting the page, we can find "Search" input fields on the website.

Step 7) We will scan the website using OWASP ZAP to look for potential vulnerabilities.

Upon scanning, we can discover these vulnerabilities.

- PII Disclosure   HIGH
- Absence of Anti-CSRF Tokens   MEDIUM
- Information Disclosure - Suspicious Comment   MEDIUM
- Content Security Policy (CSP) Header Not Set   MEDIUM

PII Disclosure: HIGH

Description:

PII (Personally Identifiable Information) disclosure occurs when sensitive personal information about individuals is exposed or improperly handled, posing a risk to their privacy and security. This can include details such as names, addresses, social security numbers, financial data, and other information that can be used to identify or target individuals.

POC:

```
HTTP/1.1 200 OK
Date: Thu, 01 Feb 2024 08:50:44 GMT
Server: Apache
Pragma: no-cache
Cache-Control: max-age=0, must-revalidate, no-cache, no-store
Expires: Wed, 01 Feb 2023 08:50:54 GMT
X-Magento-Tags: FPC
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Set-Cookie: PHPSESSID=d34mv0ghlphnfcffatbd46ma69; expires=Thu, 01-Feb-2024 09:50:54 GMT; Max-Age=3600; path=/;
domain=www.carat.ch; secure; HttpOnly; SameSite=Lax
Set-Cookie: wp_customerId=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; domain=www.carat.ch;
```

```
        <div class="product-item-info" data-container="product-grid">

        <a href="https://www.carat.ch/de/pandora-zirkonia-ring-silber-925-pandora-timeless-190050c01-52-57003029
```

PII Disclosure
URL: https://www.carat.ch/de/schmuck/ringe.html?brand=5458
Risk: 🚩 High
Confidence: High
Parameter:
Attack:
Evidence: 5700302953534
CWE ID: 359
WASC ID: 13
Source: Passive (10062 – PII Disclosure)
Input Vector:
Description:
The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.

Remediation:

Minimize data collected, employ robust encryption, and enforce strict access controls to mitigate PII disclosure risks.

Absence of Anti-CSRF Tokens   MEDIUM

The form on the website doesn't have a security feature called Anti-CSRF tokens. These tokens act like safety checks to make sure that actions on the website are done by you and not by someone else trying to trick you.

Without these tokens, there's a risk that someone could make you do things on the website without you knowing.

This is a common problem, especially if you're logged in, authenticated, or on the same network as the website.

Remediation:

To stay safe, websites should use Anti-CSRF tokens to protect users from these sneaky tricks.

POC:

Absence of Anti-CSRF Tokens
URL: https://www.carat.ch/
Risk: 🚩 Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form class="form minisearch" id="search_mini_form" action="https://www.carat.ch/de/catalogsearch/result/" method="get">
CWE ID: 352
WASC ID: 9
Source: Passive (10202 – Absence of Anti-CSRF Tokens)

```
HTTP/1.1 200 OK
Date: Thu, 01 Feb 2024 08:44:22 GMT
Server: Apache
Pragma: no-cache
Cache-Control: max-age=0, must-revalidate, no-cache, no-store
Expires: Wed, 01 Feb 2023 08:44:22 GMT
X-Magento-Tags: FPC
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Set-Cookie: PHPSESSID=53opa4t2inudqbpsqe4jb37d15; expires=Thu, 01-Feb-2024 09:44:22 GMT; Max-Age=3600; path=/;
domain=www.carat.ch; secure; HttpOnly; SameSite=Lax
Set-Cookie: wp_customerId=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; domain=www.carat.ch;
        <div class="search">
            <div class="search-label" id="openAjaxSearch">
                <svg class="search-icon" version="1.1"
                    xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" xmlns:a="htt
```

Information Disclosure - Suspicious Comment

The response appears to contain suspicious comments which may help an attacker.

Description:

Information Disclosure occurs when a system unintentionally reveals sensitive data to unauthorized individuals. This can involve exposing details about the system's configuration, user accounts, or other confidential information.

Remediation:

Mitigating Information Disclosure involves managing error messages, configuring access controls, and regularly auditing systems to prevent the exposure of sensitive information.

```
HTTP/1.1 404 Not Found
Date: Thu, 01 Feb 2024 08:44:27 GMT
Server: Apache
Pragma: no-cache
Expires: Wed, 01 Feb 2023 08:44:27 GMT
Cache-Control: max-age=0, must-revalidate, no-cache, no-store
X-Magento-Tags: FPC
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Set-Cookie: PHPSESSID=d34mv0ghlphnfcffatbd46ma69; expires=Thu, 01-Feb-2024 09:44:27 GMT; Max-Age=3600; path=/;
domain=www.carat.ch; secure; HttpOnly; SameSite=Lax
Set-Cookie: wp_customerId=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; domain=www.carat.ch;
```

```
</script>
<!-- Google Tag Manager -->
<script>!function(){"use strict";function e(e){return function(e){for(var t=0,r=document.cookie.split(";");t<r.leng
<!-- End Google Tag Manager --><!-- NO Pixel ID is configured, please goto Admin -->
```

Information Disclosure - Suspicious Comments

URL:	https://www.carat.ch/de/sitemap.xml
Risk:	🏳 Informational
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	Admin
CWE ID:	200
WASC ID:	13
Source:	Passive (10027 - Information Disclosure - Suspicious Comments)

Content Security Policy (CSP) Header Not Set

Content Security Policy (CSP) is like a protecting shield for websites. CSP acts like a rulebook for the browser, telling it where it's okay to get stuff like pictures, videos, or special web powers (JavaScript). This ensures the browser only listens to trusted sources, keeping your website safe from troublemakers.

Content Security Policy (CSP) Header Not Set

URL:	https://www.carat.ch/
Risk:	🚩 Medium
Confidence:	High
Parameter:	
Attack:	
Evidence:	
CWE ID:	693
WASC ID:	15
Source:	Passive (10038 – Content Security Policy (CSP) Header Not Set)
Alert Reference:	10038–1

Manual Testing

- Directories Enumeration
- Insufficient server-side Input sanitization
- No rate of limit implemented on search(fuzzing Applied)

Step 8) Checking for /hidden/ directory
Here we can discover three user based on this message

- https://www.carat.ch/de/robots.txt
- https://www.carat.ch/de/agb
- https://www.carat.ch/de/cms
- https://www.carat.ch/de/contact
- https://www.carat.ch/de/datenschutz
- https://www.carat.ch/de/enable-cookies
- https://www.carat.ch/de/home
- https://www.carat.ch/de/jobs

```
  ┌──(kali㉿kali)-[~]
  └─$ dirb https://www.carat.ch/de/


  ─────────────────────
  DIRB v2.22
  By The Dark Raver
  ─────────────────────


  START_TIME: Sat Feb  3 05:13:17 2024
  URL_BASE: https://www.carat.ch/de/
  WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt


  ─────────────────────


  GENERATED WORDS: 4612

  ──── Scanning URL: https://www.carat.ch/de/ ────
  + https://www.carat.ch/de/agb (CODE:200|SIZE:113173)
  + https://www.carat.ch/de/catalog (CODE:302|SIZE:0)
  + https://www.carat.ch/de/checkout (CODE:302|SIZE:0)
  + https://www.carat.ch/de/cms (CODE:200|SIZE:453676)
  + https://www.carat.ch/de/contact (CODE:200|SIZE:104756)
  + https://www.carat.ch/de/datenschutz (CODE:200|SIZE:126486)
  + https://www.carat.ch/de/enable-cookies (CODE:200|SIZE:102646)
  + https://www.carat.ch/de/home (CODE:200|SIZE:109350)
  + https://www.carat.ch/de/Home (CODE:301|SIZE:0)
  + https://www.carat.ch/de/jobs (CODE:200|SIZE:103052)
```

Step 9) Looking for vulnerabilities by Manual testing:-

Insufficient server-side Input sanitization

Improper validation and sanitization of input on the server side pose a security
vulnerability in web applications. When a web application fails to thoroughly validate
and cleanse user-provided data, it opens the door to potential cyber threats such as
injection attacks, cross-site scripting (XSS), and unauthorized data access.
POC

Insufficient server-side input sanitization

Recommendations:

- Implement thorough input validation and sanitization.
- Use parameterized queries or prepared statements for database interactions.
- Apply output encoding to prevent XSS attacks.

Step 10)

No Rate Limiting (fuzzing Applied on search bar)

The "Unlimited Search Requests" vulnerability in a web application indicates a lack of restrictions on the number of search requests a user can make within a set timeframe.

This gap in security can result in misuse, including brute force attacks and resource exhaustion, potentially causing performance issues and impacting the application's availability.

Recommendation:

Establish strong rate-limiting mechanisms to manage the number of search requests a user can initiate, preventing misuse and bolstering overall security. Regularly monitor and analyze traffic patterns, and perform security audits to verify the efficacy of rate-limiting controls.

Request	Payload	Status code ^	Error	Timeout	Length	Comment
442	content	200			105670	
443	contents	200			105409	
444	contest	200			967	
445	contests	200			105409	
446	contract	200			105409	
447	Contract	200			105409	
448	contrib	200			105398	
449	contribute	200			105439	
450	control	200			105398	
451	controller	200			105439	
452	controlpanel	200			967	
453	controls	200			105409	
454	cookies	200			105398	

Request   Response

Pretty   Raw   Hex   Render

```
1 HTTP/2 200 OK
2 Pragma: no-cache
3 Cache-Control: max-age=0, must-revalidate, no-cache, no-store
4 Expires: Wed, 01 Feb 2023 20:25:57 GMT
5 X-Content-Type-Options: nosniff
6 X-Xss-Protection: 1; mode=block
7 X-Frame-Options: SAMEORIGIN
8 Set-Cookie: PHPSESSID=6thc2ltneu7niq2o2fvbeegh5g; expires=Thu, 01-Feb-2024 21:25:56 GMT; Max-Age=3600; path=/;
  domain=www.carat.ch; secure; HttpOnly; SameSite=Lax
9 Set-Cookie: form_key=uUnsauoEP3gA582u; expires=Thu, 01-Feb-2024 21:25:56 GMT; Max-Age=3600; path=/;
  domain=www.carat.ch; secure; SameSite=Lax
10 Set-Cookie: wp_customerId=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; domain=www.carat.ch;
   SameSite=Lax
```