

Group no :7
Name: Yasodhara Sai Kunta

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
```

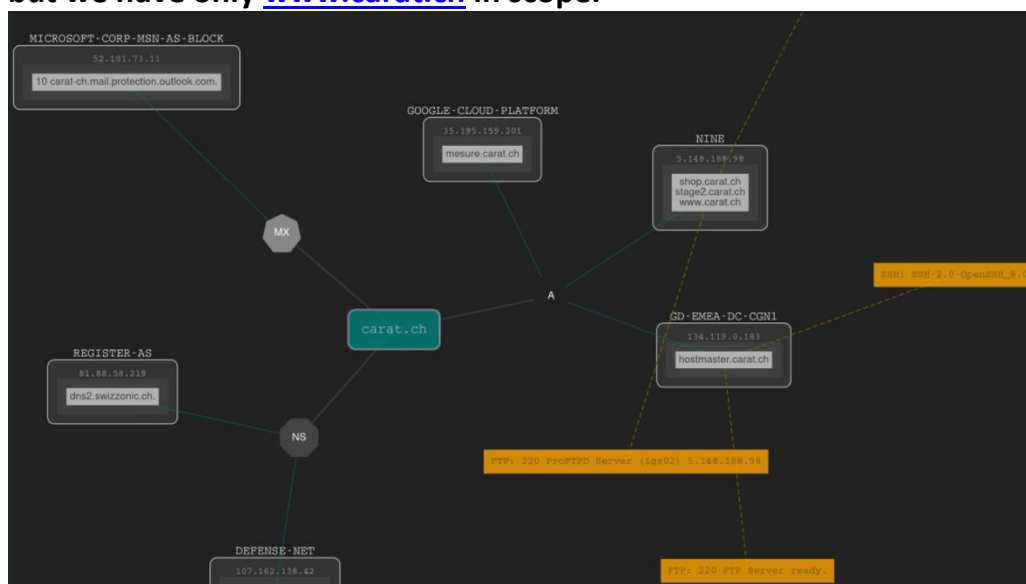
Step 3)

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

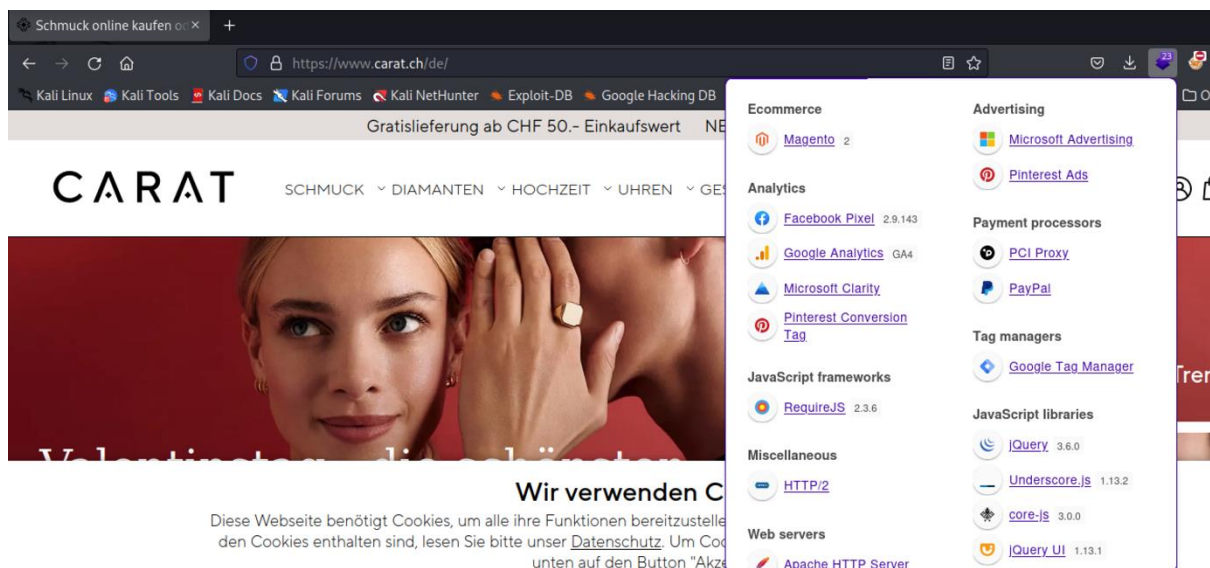
but we have only www.carat.ch in scope.



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 nmap.
Open Ports and services running on them listed below :

```
(kali@kali) ~$ sudo nmap -sV www.carat.ch
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-01 09:28 EST
Nmap scan report for www.carat.ch (5.148.188.98)
Host is up (0.20s latency).
rDNS record for 5.148.188.98: igs02.nine.ch
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD
22/tcp    open  ssh      OpenSSH 8.2p1 (protocol 2.0)
80/tcp    open  http     Apache httpd
443/tcp   open  ssl/http Apache httpd
1122/tcp  open  ssh      ProFTPD mod_sftp (protocol 2.0)
```

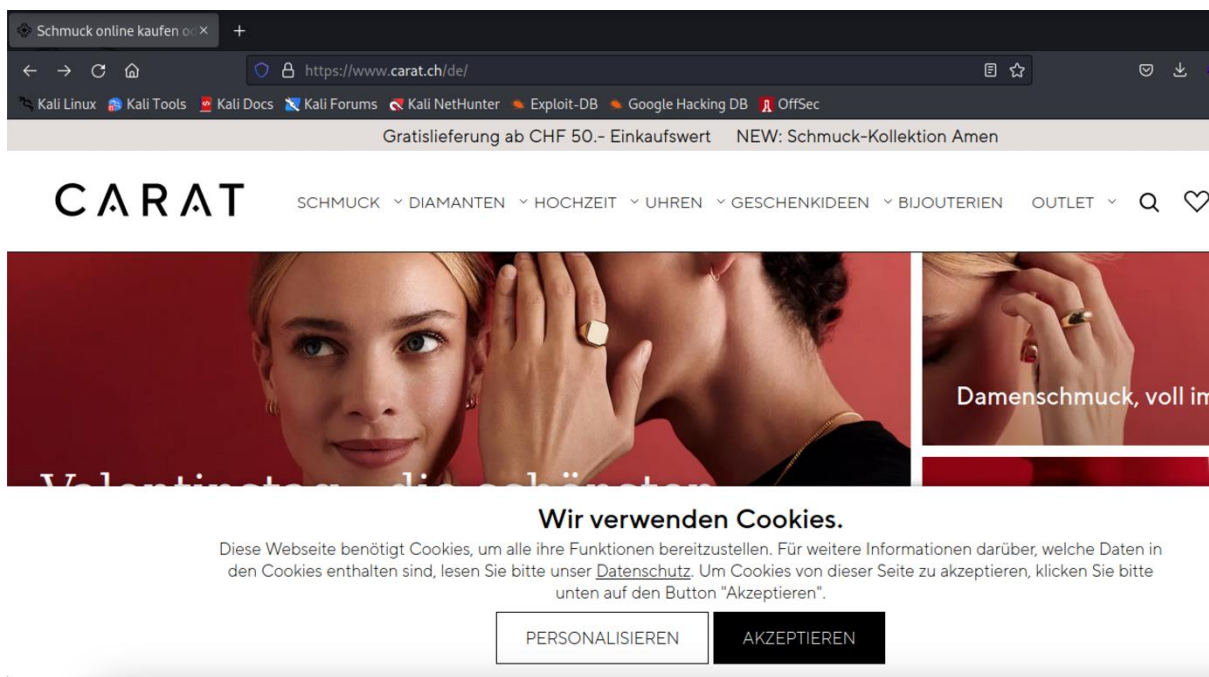
Nmap of carat.ch scan for open ports & services

- 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

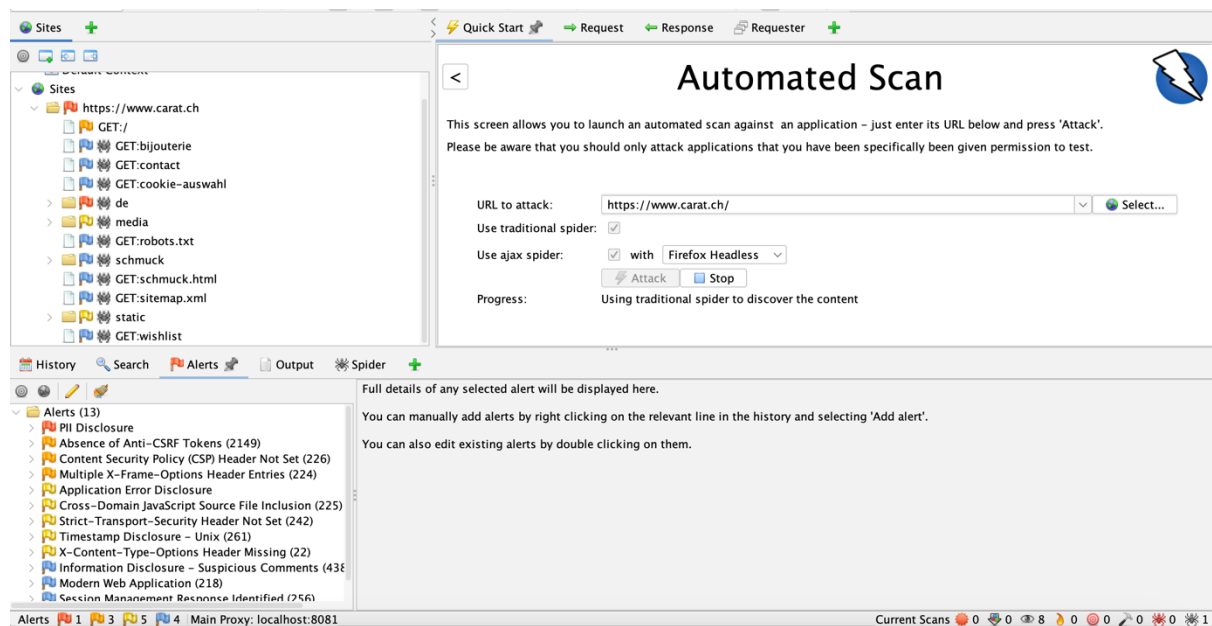
```
(kali@kali)-[~]
$ sudo nmap -sC -sV -O -p- 5.148.188.98
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-03 04:45 EST
Nmap scan report for igs02.nine.ch (5.148.188.98)
Host is up (0.075s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD
| ssl-cert: Subject: commonName=igs02.nine.ch
| Subject Alternative Name: DNS:igs02.nine.ch
| Not valid before: 2021-06-14T06:54:26
|_ Not valid after: 2031-06-12T06:54:26
22/tcp    open  ssh      OpenSSH 8.2p1 (protocol 2.0)
| ssh-hostkey:
|   3072 05ea6e0181ba275e169f4e9e12bc06ce (RSA)
|   256 5809df38c702c524aa90f9baf2bf82ce (ECDSA)
|_  256 18b0145db38e248cb2ad002549dc2234 (ED25519)
80/tcp    open  http
| fingerprint-strings:
|_  FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     Date: Sat, 03 Feb 2024 09:48:29 GMT
|     Content-Type: text/html; charset=iso-8859-1
|     Vary: Accept-Encoding
|     Pragma: no-cache
```

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.length; t++) if(r[t].indexOf('GTM=') === 0) { r[t] = r[t].replace('GTM=', ''); break; } } } }
<!-- 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

Input Vector:

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

Request

```

1 GET /de/catalogsearch/result/?q=%3Cimage+src%2Fonerror%3Dprompt%28%29%3E&product_list_order=news_from_date HTTP/2
2 Host: www.carat.ch
3 Cookie: _gcl_au=1.1.429790270.1706771802; _ga=GA1.1.552292085.1706771804; FPAU=1.1.429790270.1706771802; fbp=fb.1.1706771841332.1946723246; trkcg_fid=

```

Response

```

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 19:47:36 GMT
5 X-Content-Type-Options: nosniff
6 X-Xss-Protection: 1; mode=block

```

Suchergebnisse für: "test" | c: x +

https://www.carat.ch/de/catalogsearch/result/?q=test&product_list_order=news_from_date

Gratislieferung ab CHF 50.- Einkaufswert

NEW: Schmuck-Kollektion Amen

CARAT

SCHMUCK DIAMANTEN HOCHZEIT UHREN GESCHENKIDEEN BIJOUTERIEN OUTLET

Erweiterte Suche

<image src/onerror=prompt(8)>

RESSOURCEN

Insufficient server-side input sanitization

Request

```

1 GET /de/catalogsearch/result/?q=%3Cimage+src%2Fonerror%3Dprompt%28%29%3E&product_list_order=news_from_date HTTP/2
2 Host: www.carat.ch
3 Cookie: _gcl_au=1.1.429790270.1706771802; _ga=GA1.1.552292085.1706771804; FPAU=1.1.429790270.1706771802; fbp=fb.1.1706771841332.1946723246; trkcg_fid=9dd3b1013038077f1486f916583f23a8%3A%3A40o77566nw; form_key=uUnsaueEP3gA582u; _pin_unauth=dWlkPU9UQmhNV0k1TLRZdE9EQmxNaTAwWlRFMEExXSXdOVFl0WWpZeVlUSm1aV0prTwpWAA; _clck=1a13ija%7C2%7Cfiw%7C0%7C1492; _derived_epik=dj0yJnU9RE92Y24tbUJ1a1J3SGNaT1dnYzJiWEJkVHFNa0FaUWgmbj1IN1liWEo4cE81V25rWHlsN0FPLTNjM09MTAmdD1BQUFBQUdXN1JoNCZybT0xMCZydD1BQUFBQUdXN1JoNCZzcD0x; private_content_version=cdca4a29d5a0104d68b2be68f5763e48; trkcg_sid=53d73ea6880d7e1236b03497711d8f19e9021a7502ff32b79e079fac3f8d032d; PHPSESSID=6thc2ltneu7niq2o2fvbeegh5g; form_key=uUnsaueEP3gA582u; FPGSID=1.1706816548.1706816548.G-6CFZ0WG7YX.srymp1cF-6iCKK7IjRQtqQ; mage-cache-storage={}; mage-cache-storage-section-invalidation={}; mage-cache-sessid=true; mage-messages={}; recently_viewed_product={}; recently_viewed_product_previous={};

```

Response

```

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 19:44:18 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 20:44:18 GMT; Max-Age=3600; path=/; domain=www.carat.ch; secure; HttpOnly; SameSite=Lax
9 Set-Cookie: form_key=uUnsaueEP3gA582u; expires=Thu, 01-Feb-2024 20:44:18 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
11 Set-Cookie: wp_customerGroup=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; domain=www.carat.ch; SameSite=Lax
12 Vary: Accept-Encoding
13 X-Frame-Options: SAMEORIGIN
14 Content-Length: 105397

```

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	<input type="checkbox"/>	<input type="checkbox"/>	105670	
443	contents	200	<input type="checkbox"/>	<input type="checkbox"/>	105409	
444	contest	200	<input type="checkbox"/>	<input type="checkbox"/>	967	
445	contests	200	<input type="checkbox"/>	<input type="checkbox"/>	105409	
446	contract	200	<input type="checkbox"/>	<input type="checkbox"/>	105409	
447	Contract	200	<input type="checkbox"/>	<input type="checkbox"/>	105409	
448	contrib	200	<input type="checkbox"/>	<input type="checkbox"/>	105398	
449	contribute	200	<input type="checkbox"/>	<input type="checkbox"/>	105439	
450	control	200	<input type="checkbox"/>	<input type="checkbox"/>	105398	
451	controller	200	<input type="checkbox"/>	<input type="checkbox"/>	105439	
452	controlpanel	200	<input type="checkbox"/>	<input type="checkbox"/>	967	
453	controls	200	<input type="checkbox"/>	<input type="checkbox"/>	105409	
454	cookies	200	<input type="checkbox"/>	<input type="checkbox"/>	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=6thc2ltneu7nig2o2fvbeegh5g; 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=uUnsaueEP3gA582u; 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