NOTE : The SIEM environment was set up by connecting the local CLA website to an XAMPP Apache server. The DUMPIO module was installed and configured within Apache to capture and log the body of HTTP requests into the error_log file. The HTTP response status codes were recorded in the access_log file. By matching the timestamps between the error_log and access_log files, we were able to correlate request payloads with their corresponding response status codes.

Real-World Incident Report
Executive Summary
Incident ID: INC2019-0422-022
Incident Severity: High (P2)
Incident Status: Resolved

Incident Overview:
On September 15, 2024, at 02:19:00, the website CLA was found to have vulnerabilities exploited through unauthorized activity. The attack was identified as a combination of brute force, SQL injection, XSS, and path traversal attacks. The lack of sufficient security measures on the website allowed the attackers to bypass normal security controls and gain unauthorized access to the website's backend.

Key Findings:

- The website was targeted through a brute force attack to guess user credentials.
- SQL injection was used to manipulate the website's database and access sensitive information.
- Path traversal vulnerability allowed attackers to access files and directories outside the web root folder.
- While no significant data exfiltration was detected, the website's integrity and security were compromised.

Immediate Actions:

- Vulnerabilities were identified to avoid similar attacks in the future.
- All activity logs were collected using the Splunk monitoring tool for further analysis.

Technical Analysis

Affected Systems & Data

Due to **insufficient network access controls**, the unauthorized entity was able to exploit vulnerabilities on the main domain of the CLA website and gain access to internal systems.

The unauthorized entity successfully gained control over the following areas within CLA's infrastructure:

CLA.com (Main Domain):
This is the primary domain of CLA's platform, which houses user data and sensitive operational information. The attacker exploited multiple vulnerabilities, including brute force attacks, SQL injection, and path traversal. Logs indicate that the attacker navigated various directories, raising concerns about the potential compromise of the website's structure and user data.

Sensitive User Data:
The database containing user data was compromised during the attack. Although no API keys or third-party service credentials were exposed, the database stores personally identifiable information (PII) such as usernames, passwords, and other account details. Unfortunately, this database was **unencrypted**, significantly increasing the risk of data theft and future exploitation.

Attack Details

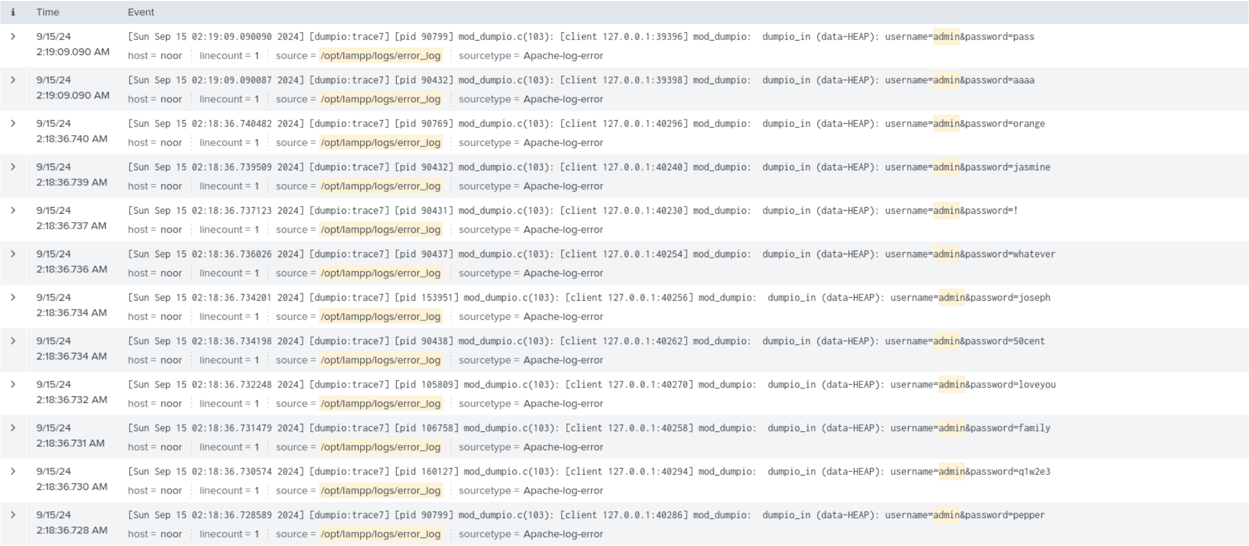
The unauthorized entity’s IP address was logged, as were the **SQL injection and path traversal attempts** used to navigate and extract information from the database. The attacker managed to interact with sensitive user data, though there is no evidence to suggest data was exfiltrated at this point. However, the risk of identity theft, credential stuffing, or other fraudulent activities remains high due to the exposure of user credentials.

Evidence Sources & Analysis

Incident #1: brute force attack

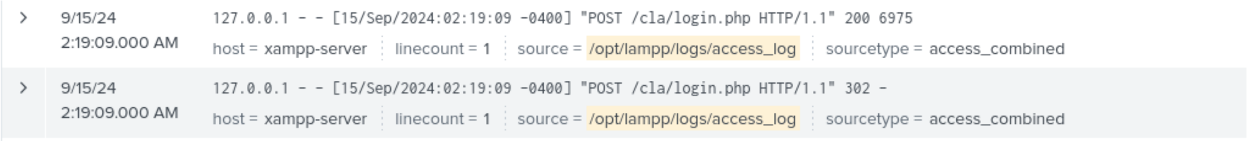
URL: http://localhost/cla
Incident Date: September 15, 2024
Time of Detection: 02:19:00

On the night of September 15, 2024, at 02:19:00, the Security Operations Center (SOC) detected unauthorized activity on the CLA website. This activity was identified through the Splunk SIEM solution, which flagged abnormal payloads being sent to the server. The following screenshot highlights the suspicious activity detected.



```
i  Time         Event
>  9/15/24      [Sun Sep 15 02:19:09.090090 2024] [dumpio:trace7] [pid 90799] mod_dumpio.c(103): [client 127.0.0.1:39396] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=pass
   2:19:09.090 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24      [Sun Sep 15 02:19:09.090087 2024] [dumpio:trace7] [pid 90432] mod_dumpio.c(103): [client 127.0.0.1:39398] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=aaaa
   2:19:09.090 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24      [Sun Sep 15 02:18:36.740482 2024] [dumpio:trace7] [pid 90769] mod_dumpio.c(103): [client 127.0.0.1:40296] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=orange
   2:18:36.740 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24      [Sun Sep 15 02:18:36.739509 2024] [dumpio:trace7] [pid 90432] mod_dumpio.c(103): [client 127.0.0.1:40240] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=jasmine
   2:18:36.739 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24      [Sun Sep 15 02:18:36.737123 2024] [dumpio:trace7] [pid 90431] mod_dumpio.c(103): [client 127.0.0.1:40230] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=!
   2:18:36.737 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24      [Sun Sep 15 02:18:36.736026 2024] [dumpio:trace7] [pid 90437] mod_dumpio.c(103): [client 127.0.0.1:40254] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=whatever
   2:18:36.736 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24      [Sun Sep 15 02:18:36.734201 2024] [dumpio:trace7] [pid 153951] mod_dumpio.c(103): [client 127.0.0.1:40256] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=joseph
   2:18:36.734 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24      [Sun Sep 15 02:18:36.734198 2024] [dumpio:trace7] [pid 90438] mod_dumpio.c(103): [client 127.0.0.1:40262] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=50cent
   2:18:36.734 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24      [Sun Sep 15 02:18:36.732248 2024] [dumpio:trace7] [pid 105809] mod_dumpio.c(103): [client 127.0.0.1:40270] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=loveyou
   2:18:36.732 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24      [Sun Sep 15 02:18:36.731479 2024] [dumpio:trace7] [pid 106758] mod_dumpio.c(103): [client 127.0.0.1:40258] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=family
   2:18:36.731 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24      [Sun Sep 15 02:18:36.730574 2024] [dumpio:trace7] [pid 160127] mod_dumpio.c(103): [client 127.0.0.1:40294] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=q1w2e3
   2:18:36.730 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24      [Sun Sep 15 02:18:36.728589 2024] [dumpio:trace7] [pid 90799] mod_dumpio.c(103): [client 127.0.0.1:40286] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=pepper
   2:18:36.728 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
```

The logs show a **brute force attack** targeting the website's admin user account. One of the attack attempts returned an **HTTP status code 200**, indicating that the attacker successfully obtained the admin credentials. This unauthorized access was facilitated by an IP address, **127.0.0.1**, which was subsequently blocked by security systems.



```
>  9/15/24         127.0.0.1 - - [15/Sep/2024:02:19:09 -0400] "POST /cla/login.php HTTP/1.1" 200 6975
   2:19:09.000 AM  host = xampp-server | linecount = 1 | source = /opt/lampp/logs/access_log | sourcetype = access_combined
>  9/15/24         127.0.0.1 - - [15/Sep/2024:02:19:09 -0400] "POST /cla/login.php HTTP/1.1" 302 -
   2:19:09.000 AM  host = xampp-server | linecount = 1 | source = /opt/lampp/logs/access_log | sourcetype = access_combined
```

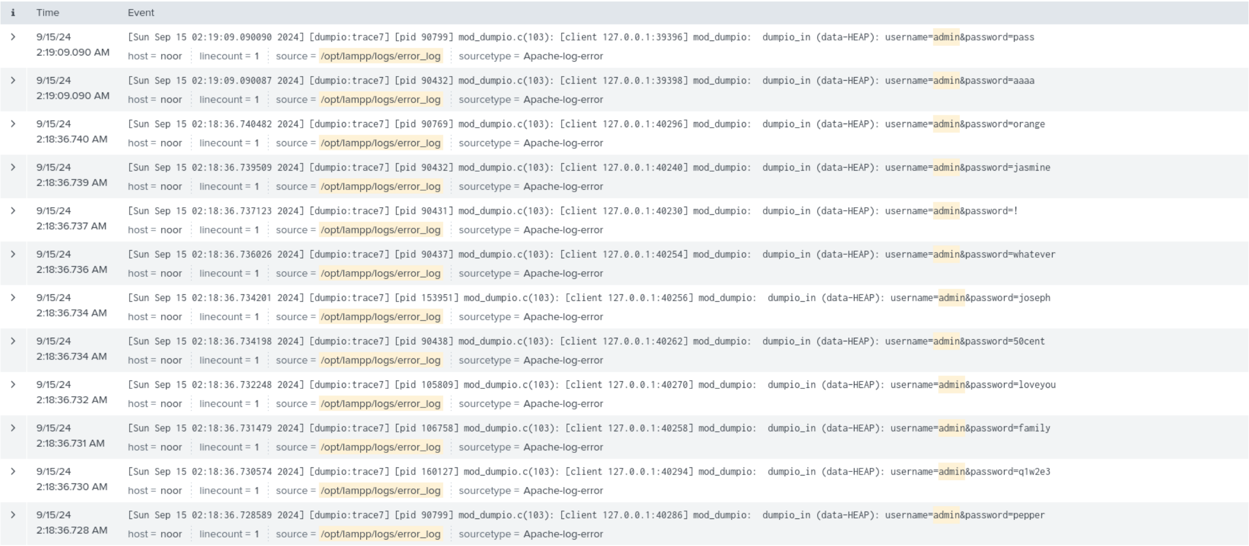
The use of Splunk provided critical real-time monitoring, allowing for rapid detection of the attack. However, due to the successful response from the server, it’s clear the attack compromised admin-level access, putting sensitive user data and system controls at risk.

Evidence Sources & Analysis

Incident #2: Path Traversal Attack

URL: http://localhost/cla
Incident Date: September 15, 2024
Time of Detection: 02:19:00

On the night of September 15, 2024, at 02:19:00, the Security Operations Center (SOC) detected unauthorized activity on the CLA website. This activity was identified through the Splunk SIEM solution, which flagged abnormal payloads being sent to the server. The following screenshot highlights the suspicious activity detected.



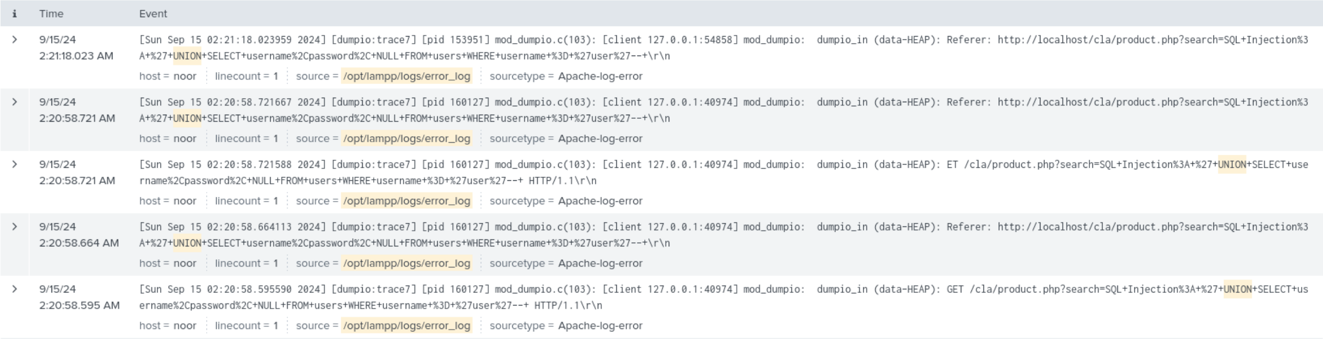
```
i  Time            Event
>  9/15/24         [Sun Sep 15 02:19:09.090090 2024] [dumpio:trace7] [pid 90799] mod_dumpio.c(103): [client 127.0.0.1:39396] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=pass
   2:19:09.090 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24         [Sun Sep 15 02:19:09.090087 2024] [dumpio:trace7] [pid 90432] mod_dumpio.c(103): [client 127.0.0.1:39398] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=aaaa
   2:19:09.090 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24         [Sun Sep 15 02:18:36.740482 2024] [dumpio:trace7] [pid 90769] mod_dumpio.c(103): [client 127.0.0.1:40296] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=orange
   2:18:36.740 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24         [Sun Sep 15 02:18:36.739509 2024] [dumpio:trace7] [pid 90432] mod_dumpio.c(103): [client 127.0.0.1:40240] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=jasmine
   2:18:36.739 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24         [Sun Sep 15 02:18:36.737123 2024] [dumpio:trace7] [pid 90431] mod_dumpio.c(103): [client 127.0.0.1:40230] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=!
   2:18:36.737 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24         [Sun Sep 15 02:18:36.736026 2024] [dumpio:trace7] [pid 90437] mod_dumpio.c(103): [client 127.0.0.1:40254] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=whatever
   2:18:36.736 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24         [Sun Sep 15 02:18:36.734201 2024] [dumpio:trace7] [pid 153951] mod_dumpio.c(103): [client 127.0.0.1:40256] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=joseph
   2:18:36.734 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24         [Sun Sep 15 02:18:36.734198 2024] [dumpio:trace7] [pid 90438] mod_dumpio.c(103): [client 127.0.0.1:40262] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=50cent
   2:18:36.734 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24         [Sun Sep 15 02:18:36.732248 2024] [dumpio:trace7] [pid 105809] mod_dumpio.c(103): [client 127.0.0.1:40270] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=loveyou
   2:18:36.732 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24         [Sun Sep 15 02:18:36.731479 2024] [dumpio:trace7] [pid 106758] mod_dumpio.c(103): [client 127.0.0.1:40258] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=family
   2:18:36.731 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24         [Sun Sep 15 02:18:36.730574 2024] [dumpio:trace7] [pid 160127] mod_dumpio.c(103): [client 127.0.0.1:40294] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=q1w2e3
   2:18:36.730 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
>  9/15/24         [Sun Sep 15 02:18:36.728589 2024] [dumpio:trace7] [pid 90799] mod_dumpio.c(103): [client 127.0.0.1:40286] mod_dumpio:  dumpio_in (data-HEAP): username=admin&password=pepper
   2:18:36.728 AM  host = noor | linecount = 1 | source = /opt/lampp/logs/error_log | sourcetype = Apache-log-error
```

The logs show a **brute force attack** targeting the website's admin user account. One of the attack attempts returned an **HTTP status code 200**, indicating that the attacker successfully obtained the admin credentials. This unauthorized access was facilitated by an IP address, **127.0.0.1**, which was subsequently blocked by security systems.

The use of Splunk provided critical real-time monitoring, allowing for rapid detection of the attack. However, due to the successful response from the server, it’s clear the attack compromised admin-level access, putting sensitive user data and system controls at risk.

Incident #2: Union SQL Injection

Shortly after the initial brute force attack, the Security Operations Center (SOC) identified a second, more sophisticated attack involving an SQL injection vulnerability. This was detected at 02:19:00 on September 15, 2024, just 2 minutes after the brute force attack.

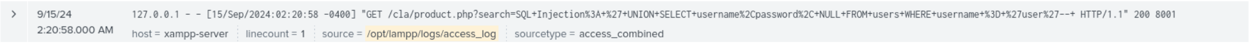


```
i  Time              Event
>  9/15/24           [Sun Sep 15 02:21:18.023959 2024] [dumpio:trace7] [pid 153951] mod_dumpio.c(103): [client 127.0.0.1:54858] mod_dumpio:  dumpio_in (data-HEAP): Referer: http://localhost/cla/product.php?search=SQL+Injection%3
   2:21:18.023 AM    A+%27+UNION+SELECT+username%2Cpassword%2C+NULL+FROM+users+WHERE+username+%3D+%27user%27--+\r\n
                     host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>  9/15/24           [Sun Sep 15 02:20:58.721667 2024] [dumpio:trace7] [pid 160127] mod_dumpio.c(103): [client 127.0.0.1:40974] mod_dumpio:  dumpio_in (data-HEAP): Referer: http://localhost/cla/product.php?search=SQL+Injection%3
   2:20:58.721 AM    A+%27+UNION+SELECT+username%2Cpassword%2C+NULL+FROM+users+WHERE+username+%3D+%27user%27--+\r\n
                     host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>  9/15/24           [Sun Sep 15 02:20:58.721588 2024] [dumpio:trace7] [pid 160127] mod_dumpio.c(103): [client 127.0.0.1:40974] mod_dumpio:  dumpio_in (data-HEAP): ET /cla/product.php?search=SQL+Injection%3A+%27+UNION+SELECT+use
   2:20:58.721 AM    rname%2Cpassword%2C+NULL+FROM+users+WHERE+username+%3D+%27user%27--+ HTTP/1.1\r\n
                     host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>  9/15/24           [Sun Sep 15 02:20:58.664113 2024] [dumpio:trace7] [pid 160127] mod_dumpio.c(103): [client 127.0.0.1:40974] mod_dumpio:  dumpio_in (data-HEAP): Referer: http://localhost/cla/product.php?search=SQL+Injection%3
   2:20:58.664 AM    A+%27+UNION+SELECT+username%2Cpassword%2C+NULL+FROM+users+WHERE+username+%3D+%27user%27--+\r\n
                     host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>  9/15/24           [Sun Sep 15 02:20:58.595590 2024] [dumpio:trace7] [pid 160127] mod_dumpio.c(103): [client 127.0.0.1:40974] mod_dumpio:  dumpio_in (data-HEAP): GET /cla/product.php?search=SQL+Injection%3A+%27+UNION+SELECT+us
   2:20:58.595 AM    ername%2Cpassword%2C+NULL+FROM+users+WHERE+username+%3D+%27user%27--+ HTTP/1.1\r\n
                     host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
```

Using Splunk, the SOC detected an SQL injection attempt sent through the product page search box input fields on the CLA website. The malicious query was designed to exploit an input validation vulnerability, allowing the attacker to access sensitive user credentials. The SQL query used was:

' UNION SELECT username, password, NULL FROM users WHERE username = 'user'--

This payload bypassed security checks and allowed the attacker to retrieve **usernames and passwords** from the database. Logs confirm that the attacker successfully executed these queries, exposing sensitive user information. The compromised data included usernames and passwords, which posed a significant risk to user accounts.



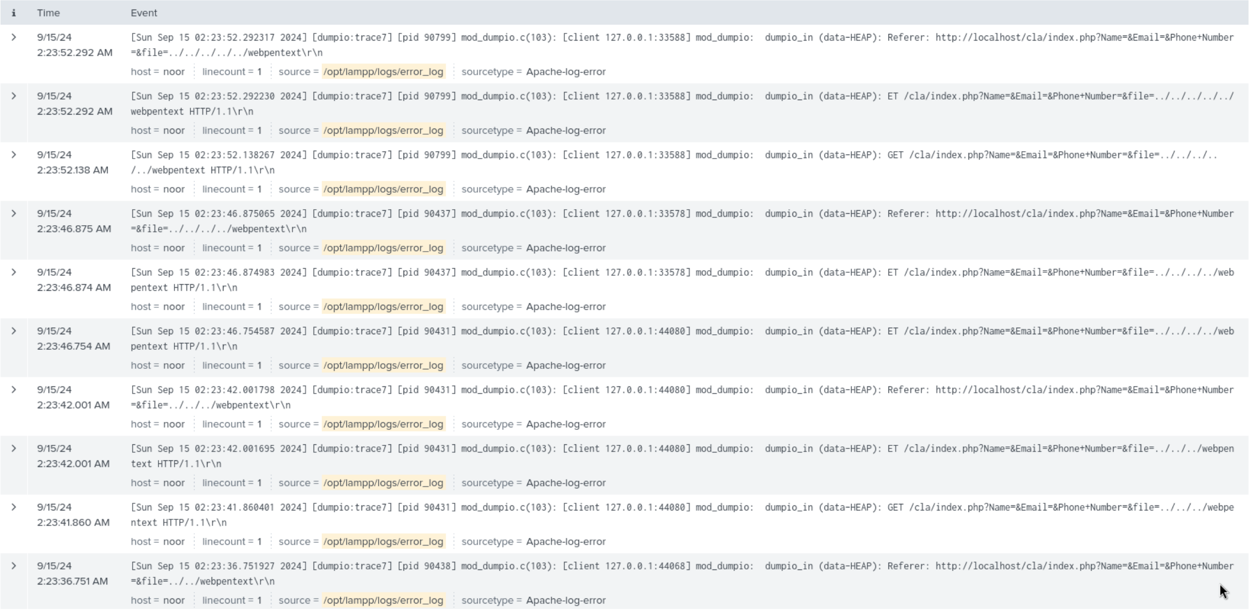
```
>  9/15/24           127.0.0.1 - - [15/Sep/2024:02:20:58 -0400] "GET /cla/product.php?search=SQL+Injection%3A+%27+UNION+SELECT+username%2Cpassword%2C+NULL+FROM+users+WHERE+username+%3D+%27user%27--+ HTTP/1.1" 200 8001
   2:20:58.000 AM    host = xampp-server   linecount = 1   source = /opt/lampp/logs/access_log   sourcetype = access_combined
```

Incident #3: Path Traversal Attack

Following the SQL injection attack, the **Security Operations Center (SOC)** identified a third incident involving a **path traversal attack**. This occurred shortly after the SQL injection, with the attacker leveraging vulnerabilities in the CLA website's input validation to access unauthorized system files.

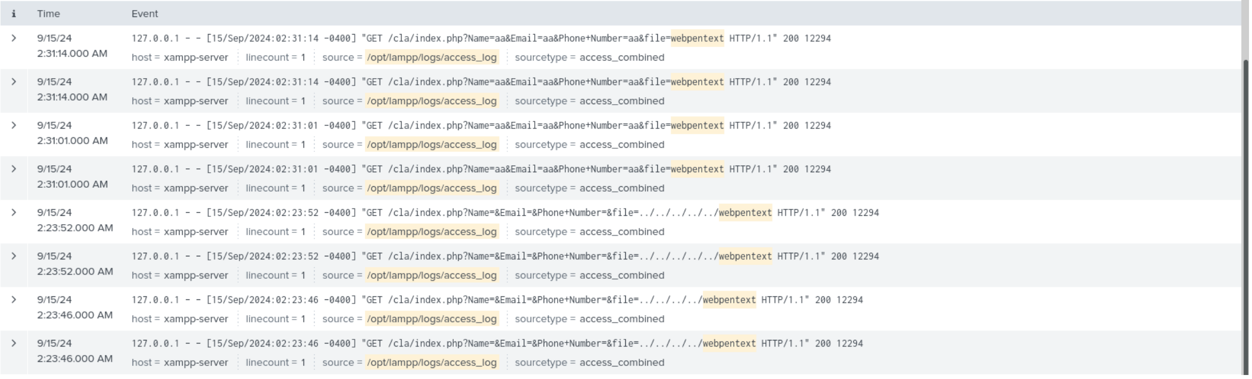
At **02:21:00 on September 15, 2024**, the attacker crafted a malicious URL targeting a vulnerable script located at http://localhost/cla/index.php. The attacker used the following payload to exploit the path traversal vulnerability:

```
http://localhost/cla/index.php?Name=&Email=&Phone+Number=&file=..\..\..\..\webpentext
```



```
i  Time                Event
>  9/15/24             [Sun Sep 15 02:23:52.292317 2024] [dumpio:trace7] [pid 90799] mod_dumpio.c(103): [client 127.0.0.1:33588] mod_dumpio:  dumpio_in (data-HEAP): Referer: http://localhost/cla/index.php?Name=&Email=&Phone+Number
   2:23:52.292 AM      =&file=../../../../../webpentext\r\n
                       host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>  9/15/24             [Sun Sep 15 02:23:52.292230 2024] [dumpio:trace7] [pid 90799] mod_dumpio.c(103): [client 127.0.0.1:33588] mod_dumpio:  dumpio_in (data-HEAP): ET /cla/index.php?Name=&Email=&Phone+Number=&file=../../../../../
   2:23:52.292 AM      webpentext HTTP/1.1\r\n
                       host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>  9/15/24             [Sun Sep 15 02:23:52.138267 2024] [dumpio:trace7] [pid 90799] mod_dumpio.c(103): [client 127.0.0.1:33588] mod_dumpio:  dumpio_in (data-HEAP): GET /cla/index.php?Name=&Email=&Phone+Number=&file=../../../..
   2:23:52.138 AM      /../webpentext HTTP/1.1\r\n
                       host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>  9/15/24             [Sun Sep 15 02:23:46.875065 2024] [dumpio:trace7] [pid 90437] mod_dumpio.c(103): [client 127.0.0.1:33578] mod_dumpio:  dumpio_in (data-HEAP): Referer: http://localhost/cla/index.php?Name=&Email=&Phone+Number
   2:23:46.875 AM      =&file=../../../../webpentext\r\n
                       host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>  9/15/24             [Sun Sep 15 02:23:46.874983 2024] [dumpio:trace7] [pid 90437] mod_dumpio.c(103): [client 127.0.0.1:33578] mod_dumpio:  dumpio_in (data-HEAP): ET /cla/index.php?Name=&Email=&Phone+Number=&file=../../../../web
   2:23:46.874 AM      pentext HTTP/1.1\r\n
                       host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>  9/15/24             [Sun Sep 15 02:23:46.754587 2024] [dumpio:trace7] [pid 90431] mod_dumpio.c(103): [client 127.0.0.1:44080] mod_dumpio:  dumpio_in (data-HEAP): ET /cla/index.php?Name=&Email=&Phone+Number=&file=../../../../web
   2:23:46.754 AM      pentext HTTP/1.1\r\n
                       host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>  9/15/24             [Sun Sep 15 02:23:42.001798 2024] [dumpio:trace7] [pid 90431] mod_dumpio.c(103): [client 127.0.0.1:44080] mod_dumpio:  dumpio_in (data-HEAP): Referer: http://localhost/cla/index.php?Name=&Email=&Phone+Number
   2:23:42.001 AM      =&file=../../../webpentext\r\n
                       host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>  9/15/24             [Sun Sep 15 02:23:42.001695 2024] [dumpio:trace7] [pid 90431] mod_dumpio.c(103): [client 127.0.0.1:44080] mod_dumpio:  dumpio_in (data-HEAP): ET /cla/index.php?Name=&Email=&Phone+Number=&file=../../../webpen
   2:23:42.001 AM      text HTTP/1.1\r\n
                       host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>  9/15/24             [Sun Sep 15 02:23:41.860401 2024] [dumpio:trace7] [pid 90431] mod_dumpio.c(103): [client 127.0.0.1:44080] mod_dumpio:  dumpio_in (data-HEAP): GET /cla/index.php?Name=&Email=&Phone+Number=&file=../../../webpe
   2:23:41.860 AM      ntext HTTP/1.1\r\n
                       host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>  9/15/24             [Sun Sep 15 02:23:36.751927 2024] [dumpio:trace7] [pid 90438] mod_dumpio.c(103): [client 127.0.0.1:44068] mod_dumpio:  dumpio_in (data-HEAP): Referer: http://localhost/cla/index.php?Name=&Email=&Phone+Number
   2:23:36.751 AM      =&file=../../webpentext\r\n
                       host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
```

Logs confirm that This attack allowed the attacker to traverse directories on the server and access system files, specifically the **webpentext** file,. By manipulating the file parameter, the attacker bypassed directory restrictions, enabling them to explore sensitive files on the server.

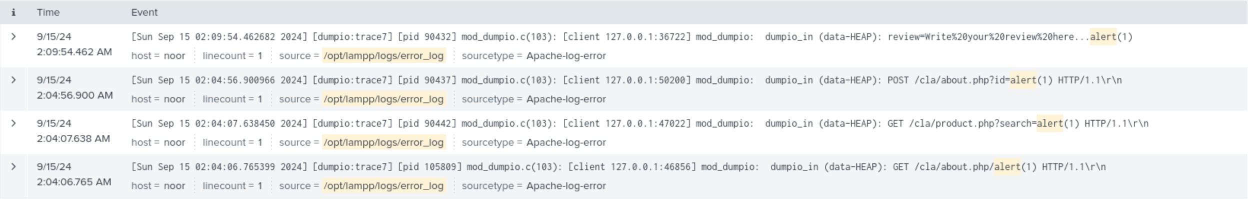


```
i  Time                Event
>  9/15/24             127.0.0.1 - - [15/Sep/2024:02:31:14 -0400] "GET /cla/index.php?Name=aa&Email=aa&Phone+Number=aa&file=webpentext HTTP/1.1" 200 12294
   2:31:14.000 AM      host = xampp-server   linecount = 1   source = /opt/lampp/logs/access_log   sourcetype = access_combined
>  9/15/24             127.0.0.1 - - [15/Sep/2024:02:31:14 -0400] "GET /cla/index.php?Name=aa&Email=aa&Phone+Number=aa&file=webpentext HTTP/1.1" 200 12294
   2:31:14.000 AM      host = xampp-server   linecount = 1   source = /opt/lampp/logs/access_log   sourcetype = access_combined
>  9/15/24             127.0.0.1 - - [15/Sep/2024:02:31:01 -0400] "GET /cla/index.php?Name=aa&Email=aa&Phone+Number=aa&file=webpentext HTTP/1.1" 200 12294
   2:31:01.000 AM      host = xampp-server   linecount = 1   source = /opt/lampp/logs/access_log   sourcetype = access_combined
>  9/15/24             127.0.0.1 - - [15/Sep/2024:02:31:01 -0400] "GET /cla/index.php?Name=aa&Email=aa&Phone+Number=aa&file=webpentext HTTP/1.1" 200 12294
   2:31:01.000 AM      host = xampp-server   linecount = 1   source = /opt/lampp/logs/access_log   sourcetype = access_combined
>  9/15/24             127.0.0.1 - - [15/Sep/2024:02:23:52 -0400] "GET /cla/index.php?Name=&Email=&Phone+Number=&file=../../../../../webpentext HTTP/1.1" 200 12294
   2:23:52.000 AM      host = xampp-server   linecount = 1   source = /opt/lampp/logs/access_log   sourcetype = access_combined
>  9/15/24             127.0.0.1 - - [15/Sep/2024:02:23:52 -0400] "GET /cla/index.php?Name=&Email=&Phone+Number=&file=../../../../../webpentext HTTP/1.1" 200 12294
   2:23:52.000 AM      host = xampp-server   linecount = 1   source = /opt/lampp/logs/access_log   sourcetype = access_combined
>  9/15/24             127.0.0.1 - - [15/Sep/2024:02:23:46 -0400] "GET /cla/index.php?Name=&Email=&Phone+Number=&file=../../../../webpentext HTTP/1.1" 200 12294
   2:23:46.000 AM      host = xampp-server   linecount = 1   source = /opt/lampp/logs/access_log   sourcetype = access_combined
>  9/15/24             127.0.0.1 - - [15/Sep/2024:02:23:46 -0400] "GET /cla/index.php?Name=&Email=&Phone+Number=&file=../../../../webpentext HTTP/1.1" 200 12294
   2:23:46.000 AM      host = xampp-server   linecount = 1   source = /opt/lampp/logs/access_log   sourcetype = access_combined
```

While there is no immediate evidence that critical system files were altered, the ability to access internal files like the webpentext file raises significant concerns about potential further exploitation or system tampering.

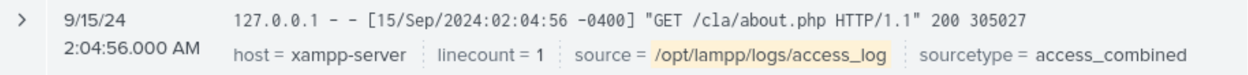
Incident #4: Cross-Site Scripting (XSS) Attack

In addition to the previous incidents, the Security Operations Center (SOC) detected a fourth vulnerability involving a Cross-Site Scripting (XSS) attack. The attack was first noticed due to suspicious payloads observed in the logs, indicating the injection of malicious scripts into the site’s input fields or URL parameters.



```
i   Time          Event
>   9/15/24       [Sun Sep 15 02:09:54.462682 2024] [dumpio:trace7] [pid 90432] mod_dumpio.c(103): [client 127.0.0.1:36722] mod_dumpio:  dumpio_in (data-HEAP): review=Write%20your%20review%20here...alert(1)
    2:09:54.462 AM  host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>   9/15/24       [Sun Sep 15 02:04:56.900966 2024] [dumpio:trace7] [pid 90437] mod_dumpio.c(103): [client 127.0.0.1:50200] mod_dumpio:  dumpio_in (data-HEAP): POST /cla/about.php?id=alert(1) HTTP/1.1\r\n
    2:04:56.900 AM  host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>   9/15/24       [Sun Sep 15 02:04:07.638450 2024] [dumpio:trace7] [pid 90442] mod_dumpio.c(103): [client 127.0.0.1:47022] mod_dumpio:  dumpio_in (data-HEAP): GET /cla/product.php?search=alert(1) HTTP/1.1\r\n
    2:04:07.638 AM  host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
>   9/15/24       [Sun Sep 15 02:04:06.765399 2024] [dumpio:trace7] [pid 105809] mod_dumpio.c(103): [client 127.0.0.1:46856] mod_dumpio:  dumpio_in (data-HEAP): GET /cla/about.php/alert(1) HTTP/1.1\r\n
    2:04:06.765 AM  host = noor   linecount = 1   source = /opt/lampp/logs/error_log   sourcetype = Apache-log-error
```

The injected payloads triggered HTTP status code 200 responses, confirming that the malicious scripts were successfully executed on the CLA website. This allowed the attacker to manipulate the website’s behavior and execute arbitrary JavaScript code within users’ browsers.



```
>   9/15/24           127.0.0.1 - - [15/Sep/2024:02:04:56 -0400] "GET /cla/about.php HTTP/1.1" 200 305027
    2:04:56.000 AM    host = xampp-server   linecount = 1   source = /opt/lampp/logs/access_log   sourcetype = access_combined
```

The successful execution of these payloads highlights a critical XSS vulnerability, allowing the attacker to inject and execute arbitrary code, which could lead to session hijacking, data theft, or further exploitation of user interactions.

Response and Recovery Analysis

1. Brute Force Attack on Admin Credentials

Response:

- **Immediate Actions:**
  - Block the attacker’s IP address (already done).
  - Change and strengthen the admin credentials, using multi-factor authentication (MFA) for added security.
  - Review and enhance password policies, enforcing strong, unique passwords and regular changes.

Recovery:

- **Long-Term Measures:**
  - Implement and monitor rate-limiting to prevent brute force attacks.
  - Conduct regular security training for staff on recognizing and responding to such attacks.
  - Perform a thorough audit of login mechanisms to identify and fix any weaknesses.

2. SQL Injection and Path Traversal Attack

Response:

- **Immediate Actions:**
    - Patch the SQL injection and path traversal vulnerabilities by updating input validation and sanitization mechanisms.
    - Perform a comprehensive scan to detect and remove any unauthorized modifications or data accessed during the attack.
    - Review and secure the database and web application configuration to prevent further SQL injection and traversal attacks.

Recovery:

- **Long-Term Measures:**
    - Implement prepared statements and parameterized queries to safeguard against SQL injection.
    - Ensure proper encoding and validation of user inputs to prevent path traversal and other injection attacks.
    - Regularly review and update the security measures, including conducting penetration testing and code reviews.

3. Path Traversal Attack

Response:

- **Immediate Actions:**
    - Fix the path traversal vulnerability by enforcing strict input validation and file path restrictions.
    - Remove or secure any sensitive files that could be accessed through this vulnerability.
    - Check the system for any signs of unauthorized access or changes made during the attack.

Recovery:

- **Long-Term Measures:**
    - Implement robust access controls and directory restrictions to prevent unauthorized access to server files.

    - Regularly audit server configurations and permissions to ensure they align with security best practices.
    - Educate developers on secure coding practices to avoid similar vulnerabilities in the future.

4. Cross-Site Scripting (XSS) Attack

Response:

- **Immediate Actions:**
    - Remove or sanitize any malicious scripts injected into the website.
    - Update input fields and URL parameters to prevent script injection, applying proper escaping and sanitization.
    - Notify affected users and provide guidance on how to secure their accounts if necessary.

Recovery:

- **Long-Term Measures:**
    - Implement Content Security Policy (CSP) headers to restrict the sources of executable scripts.
    - Regularly conduct security assessments to identify and fix potential XSS vulnerabilities.
    - Provide training for developers on preventing XSS by using safe coding practices and libraries.

General Recommendations:

- **Incident Response Plan:** Develop and maintain a comprehensive incident response plan to quickly address and mitigate future security incidents.
- **Security Monitoring:** Enhance monitoring capabilities to detect and respond to anomalies in real-time.
- **Regular Audits:** Schedule regular security audits and vulnerability assessments to proactively identify and address weaknesses.