A screenshot of a computer

AI-generated content may be incorrect.

Ở bài này ta biết nội dung file index.php mục tiêu là bypass blacklist

Lướt qua trang chủ ta thấy như sau

A white screen with orange text

AI-generated content may be incorrect.

Oke tập trung vào src code

A black background with colorful lines

AI-generated content may be incorrect.

Website nhận 2 tham số user , pass qua method GET để thực hiện câu truy vấn

SELECT \* FROM users WHERE username='{$user}' AND password='{$pass}';

Blacklist cho phép sử dụng toán tử and , or , = , ta có thể tiêm lệnh

http://ip /?user=a&pass=a’or(1=1)=’1

=> query : SELECT \* FROM users WHERE username='a ' AND password= ‘a’or(1=1)=’1 ';

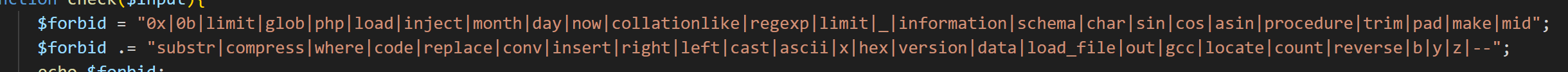
+ Mệnh đề where ở câu truy vấn trên nhận giá trị True ( còn tại sao anh em tự tìm hiểu )

KQ nhận được :

A screen shot of a computer

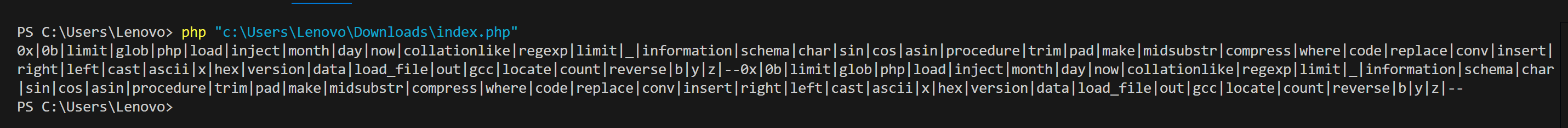
AI-generated content may be incorrect.

OKE đến đây sau 3 ngày ngồi mò các cách bypass backlist để có thể sử dụng 1 số hàm đặc biệt thì không cho ra kết quả khả quan . Ngồi đọc lại src code thì thấy blacklist bị lỏng lẻo 😊 thiết kế sai



Ở 2 câu lệnh sau trông thì perfect nma không =)) .

Tôi sẽ in ra biến $forbid để xem kết quả của nó sau 2 lệnh trên là gì



0x|0b|limit|glob|php|load|inject|month|day|now|collationlike|regexp|limit|\_|information|schema|char|sin|cos|asin|procedure|trim|pad|make|midsubstr|compress|where|code|replace|conv|insert|right|left|cast|ascii|x|hex|version|data|load\_file|out|gcc|locate|count|reverse|b|y|z|--0x|0b|limit|glob|php|load|inject|month|day|now|collationlike|regexp|limit|\_|information|schema|char|sin|cos|asin|procedure|trim|pad|make|midsubstr|compress|where|code|replace|conv|insert|right|left|cast|ascii|x|hex|version|data|load\_file|out|gcc|locate|count|reverse|b|y|z|--

Để ý có thể thấy hàm mid và hàm substr bị nối vào nhau => tạo ra chuỗi “midsubstr” và hàm này thì

k có nghĩa trong sqlite . Do đó blacklist này để lọt hàm mid , còn substr vẫn bị chặn do

*Cách Regex trong PHP hoạt động*

if (preg\_match("/$forbid/i", $input)) {

die("forbidden");

}

+ Hàm preg\_match của PHP sẽ coi nội dung biến $forbid là **pattern của regex**.

+ Dấu / ... /i là cú pháp bao regex trong PHP (i = không phân biệt hoa thường).

+ Nghĩa là: bất kỳ đoạn nào trong $input khớp với **biểu thức regex $forbid** → sẽ bị chặn.

*Biến $forbid*

+ Biến $forbid được xây dựng như sau

+ $forbid = "....|mid";

+ $forbid .= "substr|....";

+ Do thiếu dấu | khi nối, kết quả cuối cùng thành:

...|make|midsubstr|compress|...

+ Tức là trong regex, pattern bạn đang dùng là **midsubstr** (một cụm liền).

*Vì sao substr vẫn bị match*

+ Regex không yêu cầu phải match nguyên cả từ, nó chỉ cần thấy **chuỗi con**.

+ Khi bạn nhập substr, regex engine sẽ so sánh với pattern midsubstr.

+ Nó thấy **substr** đúng là phần đuôi của midsubstr.

→ Kết quả match thành công → bị chặn.

*Vì sao mid lại không bị match*

Ngược lại, khi bạn nhập mid:

+ Regex tìm mid trong pattern.

+ Nhưng pattern hiện tại **không có mid| riêng**, mà chỉ có midsubstr.

+ Regex engine so sánh:

midsubstr != mid (không chứa hẳn từ “mid” tách biệt).

→ Không khớp → thoát.

Như vậy đề bài để lọt hàm mid là hàm xử lí chuỗi trong sqlite có chức năng lấy ra 1 đoạn chuỗi con trong chuỗi đã cho ví dụ mid(“BuiGiap”, 1 , 2 ) tức là nó sẽ lấy ra chuỗi con có độ dài là 2 bắt đầu ở vị trí số 1 tức là mid(“BuiGiap”,1,2)=”Bu”

Nhắc đến xử lí chuỗi ta có 1 số hàm như hàm length trả về độ dài của chuỗi

OKE tìm hiểu sơ qua về hàm mid và đây cũng là chìa khóa của bài ta sẽ tấn công sqli Boolean base

+ Câu truy vấn gốc chỉ đúng khi mệnh đề dưới đây có có giá trị TRUE ( tại sao anh em tự tìm hiểu )

A computer code with text

AI-generated content may be incorrect.

Mở burp lên để check thôi

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Ta có thể test True , False dựa vào kq trả về từ http respone (“ welcome \o/” = True ) ( “Wrong !” = False )

Trước tiên chúng ta sẽ kiểm tra độ dài của username bằng hàm length

**Lưu ý : truy vấn Select length(username) from user;**

|  |  |
| --- | --- |
| username | password |
| buigiap | 123 |
| aaaa | 123 |
| vvv | 213 |
| rrr | 2312 |

**Kquar**

|  |
| --- |
| **username** |
| **7** |
| **4** |
| **3** |
| **3** |

**Như vậy length(username) = 7 và = 4 và =3 chứ không phải chỉ trả về 1 giá trị bất kì nào mà nó sẽ trả về đồng thời**

OKE sang tab intruder của burpsuite ta có thể check độ dài có thể có của username

A screenshot of a computer

AI-generated content may be incorrect.

Set payload

A screenshot of a computer

AI-generated content may be incorrect.

Oke bắt đầu attack và kq có đc như sau

A screenshot of a computer

AI-generated content may be incorrect.

Ở đây thì có thể dựa vào chuỗi trả vè ở body http respone còn tôi dựa vào length, oke kq cho ra có 2 giá trị thỏa mãn 3 và 5

Như vậy ta có thể đoán username có 2 loại giá trị độ dài ( 3 , 5 ) . LÀ 2 LOẠI GIÁ TRỊ ĐỘ DÀI K PHẢI chỉ có 2 bản ghi trong csdl tại vì độ dài có thể trùng nhau , nếu check thì chỉ cho ra 1 kq thôi

Bây giờ ta sẽ check độ dài password tương tự như check username thôi ta có kq trả về như sau

A screenshot of a computer

AI-generated content may be incorrect.

Ta có 4 loại độ dài mật khẩu thỏa mãn là 5 , 7 , 10 ,12 =)) .4 loại độ dài mật khẩu thì ít nhất là có 4 bản ghi rồi có thể có 2 or nhiều bản ghi cùng độ dài mật khẩu

Bây giờ ta sẽ kiểm tra với length(password) = 5 thì độ dài username tương ứng là bao nhiêu

Với câu truy vấn như sau

A screenshot of a computer

AI-generated content may be incorrect.

Kết quả nhận được

A screenshot of a computer

AI-generated content may be incorrect.

Length(password) = 5 => length(username) =5

Tương tự trên ta kiểm tra length(password) = 7 => length (username) = 3

Tương tự trên ta kiểm tra length(password) = 10 => length (username) = 5

Tương tự trên ta kiểm tra length(password) = 12 => length (username) = 5

Tới đây sử dụng hàm mid để kiểm tra kí tự với password = 12 thì username có thể là gì

Payload sau

A screenshot of a computer

AI-generated content may be incorrect.

KQ nhận được

A screenshot of a computer

AI-generated content may be incorrect.

Chữ ‘a’ là chữ cái đầu username , của bản ghi có length(username) = 12 và username = 5

Phân tích 1 chút blacklist nó không cho sử dụng kí tự b x y nên ta sẽ nhân được chuỗi “forbidden” khi trong input có 3 kí tự trên

Vậy nếu khi ta test 1 kí tự ở ví trí nào đó mà nó chỉ trả về gói tin dạng “ wrong ! “ và “forbidden” thfi kí tự ở ví trí đó là kí tự \_ ( và nó có theer là b x y ) (Tôi đặt là \_)

Oke tiếp tục bây giờ test kí tự thứ 2

A screenshot of a computer

AI-generated content may be incorrect.

Ta nhận được chữ “d” thỏa mãn cứ tiếp tục như vậy ta có chuỗi “admin” ứng với length (password) = 12

Vì cũng khá dài nên tôi tóm tắt kết quả

A number and arrows on a black background

AI-generated content may be incorrect.

Username có độ dài là 3 thì ta chỉ có thể đặt “\_”

Bây giờ ta sẽ check password tương ứng với từng username

Tôi sẽ chọn username = admin với câu truy vấn như sau

A screenshot of a computer

AI-generated content may be incorrect.

Oke kí tự đầu tiên là chữ n

A screenshot of a computer

AI-generated content may be incorrect.

Tiếp theo là chữ o

A screenshot of a computer

AI-generated content may be incorrect.

Tiếp theo là chữ t

A screenshot of a computer

AI-generated content may be incorrect.

Tiếp theo

A screenshot of a computer

AI-generated content may be incorrect.

KQ trả về k có gói tin nào “welcome \o/” chứng tỏ kí tự tiếp theo là 1 trong 3 kí tự cấm b x y nên ta sẽ đặt kí tự đó là “\_”

Oke cứ tiếp tục như vậy ta sẽ có password cho user admin là not\_the\_flag và format Flag của cuộc thi lần này là PTITCTF={string} => PTITCTF={not\_the\_flag}