به نام خدا

تزریق LDAP

OWASP Attack Category: LDAP Injection

مقدمه:

تزریق LDAP حمله ای است که جهت اکسپلوییت برنامه های تحت وب که بر اساس ورودی های کاربر دستورات و عبارات LDAP را می سازند، انجام می شود. زمانی که برنامه نمی تواند به درستی ورودی های کاربر را بسنجد و آن را اعتبارسنجی کند هکر می تواند با استفاده از پروکسی محلی (local proxy) عبارات LDAP را تغییر دهد. نتیجه ی این حمله شامل افزایش مجوز دسترسی جهت اجرای یک کوئری به صورت بدون اعتبارسنجی و تغییر محتوای درون درخت LDAP و اجرای سایر دستورات از این قبیل است.

سایر روش های پیشرفته ای که در SQL Injection مطرح است، در تزریق LDAP نیز شبیه سازی می شود.

عوامل ریسک:

/*مطلب این بخش ناقص است*/

نمونه ها:

مثال ۱

کد زیر مربوط به صفحه شامل فرم جستجوی نام کاربری است که قرار است مقداری را وارد آن کنیم و برنامه به وسیله ی آن یک کوئری LDAP ایجاد کرده و از آن در دیتابیس LDAP استفاده نماید.

```
<input type="text" size=20 name="userName">Insert the
username</input>
```

کد و کوئری به شکل زیر خواهد بود:

```
String ldapSearchQuery = "(cn=" + $userName + ")";
System.out.println(ldapSearchQuery);
```

اگر مقدار متغیر $userName به درستی وارد نشود، ممکن است باعث تزریق LDAP شود. برای مثال:

- اگر کاربر در کادر جستجو مقدار * را وارد نماید، ممکن است باعث چاپ و نمایش تمام usernameهای LDAP شود.
- اگر کاربر رشته ی زیر را وارد کند:

```
“jonys) (| (password = * ) )”
```

کد زیر باعث نمایش رمز عبور joyns خواهد بود.

```
( cn = jonys ) ( | (password = * ) )
```

مثال ۲

کدی که در ادامه آمده یک کد آسیب پذیر است که در یک برنامه تحت وب به زبان ASP جهت loginکردن با دیتابیس LDAP استفاده می شود. در خط ۱۱، userName مقداردهی می شود و بعد از آن چک می شود که تا در صورتی که مقدار آن خالی و NULL بود، پیغام خطا تولید کند.

سپس از مقدار این متغیر جهت ساختن کوئری LDAP و به وسیله ی SearchFilter در خط ۲۸ استفاده می شود. هکر می تواند تغییرات مورد نظر خود را وارد کوئری و نتایج آن را در خطوط ۳۳ و ۴۱ مشاهده کند؛ (تمام نتایج و رفتارها و خطاها به نمایش در می آیند.)

قطعه کد آسیب پذیر به زبان ASP:

```
1.      <html>
2.      <body>
3.      <%@ Language=VBScript %>
4.      <%
5.      Dim userName
6.      Dim filter
7.      Dim ldapObj
8.
9.      Const LDAP_SERVER = "ldap.example"
10.
11.     userName = Request.QueryString("user")
12.
13.     if( userName = "" ) then
14.     Response.Write("Invalid request. Please specify a valid
15.     user name")
16.     Response.End()
17.     end if
18.
19.     filter = "(uid=" + CStr(userName) + ")" ' searching for the
user entry
20.
21.     'Creating the LDAP object and setting the base dn
22.     Set ldapObj = Server.CreateObject("IPWorksASP.LDAP")
23.     ldapObj.ServerName = LDAP_SERVER
24.     ldapObj.DN = "ou=people,dc=spilab,dc=com"
25.
26.     'Setting the search filter
27.     ldapObj.SearchFilter = filter
28.
29.     ldapObj.Search
30.
31.     'Showing the user information
32.     While ldapObj.NextResult = 1
```

```
33.     Response.Write("<p>")
34.
35.     Response.Write("<b><u>User information for: " +
36.     ldapObj.AttrValue(0) + "</u></b><br>")
37.     For i = 0 To ldapObj.AttrCount -1
38.     Response.Write("<b>" + ldapObj.AttrType(i) +"</b>: " +
39.     ldapObj.AttrValue(i) + "<br>" )
40.     Next
41.     Response.Write("</p>")
42.     Wend
43.     %>
44.     </body>
45.     </html>
```

در مثال بالا، کارکتر * را در پارامتر user قرار می دهیم. با این کار uid=* می شود. با این کار عبارت LDAP تمام اشیایی که uid دارند را به صورت کامل برمی گرداند. مثل usernameها

http://www.some-site.org/index.asp?user=*

سایر حمله های مرتبط:

- Interpreter Injection
- SQL Injection
- Command Injection
- Relative Path Traversal
- Resource Injection
- Path Manipulation

منابع:

- http://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf
- http://www.ietf.org/rfc/rfc1960.txt A String Representation of LDAP Search Filters (RFC1960)
- http://www.redbooks.ibm.com/redbooks/SG244986.html IBM RedBooks - Understanding LDAP
- http://www.webappsec.org/projects/threat/classes/ldap_injection.shtml

لینک مطلب:https://www.owasp.org/index.php/LDAP_injection

تاریخ ساخت: July 7, 2009 یا ۱۶ تیر ۱۳۸۸

تاریخ تحقیق: Aug 6, 2014 یا ۱۵ مرداد ۱۳۹۳

/* تصحیح این مقاله، چه در ترجمه و چه در مباحث علمی ، توسط شما دوستان باعث خوشحالی خواهد بود. لطفا آن را با tamadonEH@gmail.com مطرح نمایید.*/

برای مشاهده لیست مقالات کار شده توسط گروه ما به لینک زیر مراجعه فرمایید

https://github.com/tamadonEH/list/blob/master/list.md