بسم الله الرحمن الرحیم

# آشنایی با حملات

Cross Site Scripting
Ver 1.0

**Cross Site Scripting چیست؟**

این نوع حملات به طور عمومی هنگامی رخ می دهند که یک صفحه ی وب داینامیک اطلاعات خطرناکی را از کاربر دریافت و بدون مقدار دهی وکنترل مقدار وارد شده ، آن ها را در آن صفحه نمایش دهد.این حملات که به XSS یا CSS هستند از نوع خطرناکی از حملات بر علیه کاربران وب سایت ها حساب می شوند که امنیت شخصی هر کاربر را به شدت به خطر می اندازند.این اطلاعات وارد شده بیشتر به صورت لینکی به سایت های حاوی برنامه ها و کدهای خطرناک می باشند.

توضیحی مختصر درباره ی بعضی از صفحات وب قبل از وارد شدن به مبحث پیشرفته لازم به نظر می رسد.یک صفحه ی وب شامل متن و یا Text و HTML markup می باشد که توسط وب سرور به وجود آمده و توسط مرورگر تفسیر و به کاربر نشان داده می شوند.وب سایت هایی که تنها به صورت استاتیک تولید شده باشند ، می توانند کنترل کاملی بر نحوه ی چگونگی تفسیر این صفحات توسط مرورگر داشته باشند.صفحاتی که به صورت داینامیک ایجاد شده اند کنترل کاملی بر این که چگونه صفحه ی مورد نظر توسط مرورگر تفسیر می شود ، ندارند.مهمترین مساله نیز ، وارد اطلاعات نادرست به صفحات داینامیک است که در این صورت ، اگر درون این صفحات کدهایی را برای تشخیص ورود این اطلاعات خطرناک نگذاریم وب سرور و یا مرورگر قادر به تشخیص این کدها نبوده و نمی توانند عمل پیشگری کننده ای را انجام دهند.

یک هکر می تواند به عنوان یک ابزار هک کردن ، با نوشتن و توزیع یک CSS URL و فرستادن آن به صفحه ی داینامیک تنها به وسیله ی یک مرورگر وب از آسیب پذیر بودن یا نبودن صفحه ی مورد نظر آگاه شود.یک هکر باید آشنایی کمی با HTML ، JavaScript ، یک زبان داینامیک داشته باشد تا بتواند URL را طراحی کند که غیر صحیح به نظر نرسد وبه این صورت بتواند یک حمله را انجام دهد.

هر صفحه ی وبی که پارامترهایی را به پایگاه داده ارسال می کند ، می تواند به این نوع از حملات آسیب پذیر باشد.این آسیب پذیری ها بیشتر در صفحات Login و Forgot Password رخ می دهند.

توجه : گاهی اوقات ممکن است نام این نوع حملات که به صورت CSS یا XSS بیان می شوند را با Cascading Style Sheets یا CSS را که به همراه صفحات وب هستند اشتباه بگیرید.

## اگر سایت شما آسیب پذیر باشد ، یک هکر چه کاری می تواند انجام دهد؟

این آسیب پذیری به هکر اجازه ی اجرای کدهای خطرناک JavaScript ، VBScript ، ActiveX ، HTML ، Flash را به یک صفحه ی وب داینامیک ارسال کند تا این کدها بر روی ماشین کاربر سایت اجرا شود و اطلاعاتی را از او بدزد.استفاده از حملات XSS موجب دزدیده شدن هویت کاربران ، دستکاری و یا دزدیدن cookie ها ، ایجاد درخواست های اشتباه برای کاربران کنترل شده ، اجرای کدهای خطرناک بر روی کاربران با دسترسی بالا در سیستم می شوند.

## نمونه ای از یک حمله ی Cross Site Scripting :

به عنوان یک مثال ساده ، یک موتور جستجو در سایت که از یک فیلد ساده و یک دکمه تشکیل شده است ، می تواند به این نوع حملات آسیب پذیر باشد.صفحه و یا متغیر کلمه ی مورد نظر برای جستجو که جستجو بر اساس آن انجام می شود ، در صفحه ی نتایج به همراه کلمات و یا موارد یافت شده مورد نظر نمایش داده می شوند.

## مثال:

Search Results for "XSS Vulnerability "

برای ذخیره کردن کلمه ی جستجو شده ، موتور جستجو به طور کلی متغیر را در URL می گذارد.در این حالت URL می تواند به این شکل به نظر رسد:

http://test.searchengine.com/search.php?q=XSS%20
Vulnerability

در این حالت می توانیم مقدار متغیر را به شکل زیر تغییر دهیم :

<script>alert('This is an XSS Vulnerability')</script>

با فرستادن این مقدار به صفحه ی search.php به صورت رمزنگاری شده در آمده و URL به شکل زیر خواهد بود:

http://test.searchengine.com/search.php?q=%3Cscript%3
Ealert%28%91This%20is%20an%20XSS%20Vulnerability%92%2
9%3C%2Fscript%3E

هنگامی که صفحه مجدد بارگذاری شد ، موتور جستجو ممکن است هیچ گونه نتیجه ای را برای شما نمایش دهد اما پیغام JavaScript را به شما نمایش می دهد که به وسیله ی آسیب پذیری XSS به صفحه تزریق شده بود.

## چگونه آسیب پذیری Cross site scripting را چک نماییم؟

برای چک کردن یک آسیب پذیری Cross site scripting بهترین راه استفاده از یک اسکنر آسیب پذیری برنامه های وب است.یک اسکنر آسیب پذیری برنامه های وب به صورت خودکار تمامی اطلاعات موجود در سایت شما را برای پیدا کردن آسیب پذیری Cross Site Scripting چک می نماید.پس از اتمام کار ، تمامی URL ها و scripts هایی که به این نوع حمله آسیب پذیر هستند نمایش داده می شوند و به این صورت می توانید آن ها را به راحتی اصلاح نمایید.علاوه بر آسیب پذیری گفته شده ، یک اسکنر می تواند آسیب پذیری های دیگری را نیز چک نماید.همچنین گزارش کاملی نیز در مورد آسیب پذیری های کشف شده و راه های اصلاح آن ها نیز به کاربر نمایش داده می شوند.

**چگونه از حملات** Cross Site Scripting **جلوگیری کنیم؟**

برای جلوگیری از این نوع حملات ، کاراکترهای خطرناک باید از ورودی های برنامه های وب خارج شوند و فیلتر گردند.این مقادیر باید در هر دومقدار ASCII و HEX فیلتر شوند.

acunetix

Scan group - saved on 14/7/2006, 13:32 , profile : default

Scan Thread 1 ( http://testphp.acunetix.com ) 214 alerts found

Scan Thread 1 ( http://testphp.acunetix.com )

Alerts summary

Threat level

acunetix threat level

Level 3: High

Acunetix threat level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts found

| | |
|---|---|
| Total alerts found | 214 |
| High | 131 |
| Medium | 8 |
| Low | 24 |
| Informational | 51 |

Executive summary

| Alert group | Number of alerts in this group |
|---|---|
| SQL injection | 84 |
| Script source code disclosure | 1 |
| Directory traversal (Windows) | 1 |
| Cross Site Scripting | 32 |
| PHP version vulnerable | 1 |
| Blind SQL/XPath injection for string inputs (double quotes) | 1 |
| Blind SQL/XPath injection for numeric inputs | 8 |
| Common files found | 6 |
| PHP code injection | 1 |
| Blind SQL/XPath injection for string inputs | 1 |

نمونه ای از یک Web Vulnerability Scanner

Copyright© by Siahacker
2005-2006 All Rights Reserved
Email:Siahacker@gmail.com