بسم الله الرحمن الرحیم

آشنایی با حملات
CRLF injection

حملات CRLF injection چه هستند؟

اصطلاح CRLF از Carriage Return (CR, ASCII 13, \r) و Line Feed (LF, ASCII 10, \n) تشکیل شده است.این کارکترهای ASCII هیچ وقت نمایش داده نمی شوند اما توسط ویندوز برای مشخص کردن انتهای یک خط بسیار زیاد مورد استفاده قرار می گیرد.در سیستم های یونیکس و لینوکس تنها از Line Feed برای مشخص کردن انتهای خط استفاده می کند.
به عنوان مثال تلفیق CR و LF برای تعیین فشرده شدن کلید Enter بر روی صفحه ی کلید ، زمان شروع استفاده از یک برنامه ، فشرده شدن کلید Enter در یک برنامه برای ایجاد خط جدید در آن استفاده می شود.
یک حمله ی CRLF Injection attack هنگامی رخ می دهد که هکر مدیریت تزریق دستورات CRLF به سیستم را به دست بگیرد.این قسمت از حمله یک مشکل امنیتی در سیستم عامل یا نرم افزار سرور نیست ، اما در هنگام طراحی یک سایت باید به آن توجه داشت.بسیاری از طراحان سایت ها بدون توجه به این قسمت از حمله در را برای هکرها برای اجرای این دستورات باز می گذارند.

اگر سایت شما آسیب پذیر باشد یک هکر چه کارهایی می تواند انجام دهد؟

هنگامی که یک هکر سایتی را که به حملات CRLF Injection آسیب پذیر است را پیدا می کند ، تنها باید بداند که برنامه ی آسیب پذیر برا چه ساختاری ساخته شده است و رخنه ها و درزهای موجود در سیستم چگونه جدا می شوند.
در برخی از انواع سایت ها ، این رخنه ها و درزها برای امنیت برنامه های تحت وب بسیار خطرناک می باشند.در بعضی از حالات دیگر ، این درزها و رخنه ها تنها باگ کوچک همراه با حداقل ارزش نفوذ هستند.با این حال در مکان هایی که به کاربر اجازه ی دستکاری برنامه ی تحت وب را بدهند خطرناک می باشند.

مثال شماره ی یک از حمله CRLF Injection attack به سرور:

هر ورودی را که کاربر وارد می کند می تواند یک مشکل امنیتی برای سرور باشد.در این جا نمونه ای از یک logfile را می بینید:

Date	UserName	Message
25/07/2005-14:23:47	GoodSurfer	I perfectly agree!

این logfile طبیعی به نظر می آید اما هنگامی که یک کاربر ورودی شبیه زیر را وارد کند:

I also agree with you..\n25/07/2005-15:00:00 AnotherSurfer

در این زمان چه نظری می توان داشت.بنابراین با وجود این ورودی logfile می تواند شکلی شبیه زیر داشته باشد:

Date	UserName	Message
25/07/2005-14:23:47	GoodSurfer	I perfectly agree!
25/07/2005-14:42:19	BadSurfer	I also agree with you..
25/07/2005-15:00:00	AnotherSurfer	What are you talking about!?

با این کار همان طور که مشخص است ورودی کاربر بالا با کاربر پایین جا به جا شده است.در این حالت تا زمانی که ورودی کاربر از وجود کاراکترهای CR و LF فیلتر نشود ، ممکن است logfile ها دارای ورودی ها اشتباه ساخته شده توسط کاربر بشوند.

مثال شماره ی دو از حمله ی CRLF Injection Attack به سرور:

بیشتر پروتکل های موجود ، شامل پروتکل HTTP ، استفاده ی زیادی از تلفیق دستورات Carriage Return و Line Feed می کنند و در واقع هر خط از استفاده شده در این پروتکل شامل یک CRLF است.اگر که یک کاربر قادر باشد تا یک HTTP header فیلتر نشده را تعیین کند ، تا زمانی که به صورت مستقیم با سرور در ارباط است می تواند یک خطر بزرگ را برای آن ایجاد کند و ، لایه ی برنامه یا Application Layer را پس بزند.
برای مثال همه ی header های E-Mail، News ((NNTP)) ، HTTP بر مبنای Key: Value ساخته شده اند و هر خط آن ها شامل تلفیقی از CRLF در پایان آن ها است.کد Location: در HTTP header برای redirect کردن کاربر به URL دیگری می شود و Set-Cookie: برای کار با cookie ها استفاده می شود.اگر که این ورودی ها به طور صحیح مقدار دهی نشوند ، کاراکترهای CR و LF می توانند در ورودی کاربر وجود داشته باشند ، و اسکریپت های وب می توانند کارهای دیگری به جز کارهایی که برای آن طراحی شده اند را انجام دهند.
اگر ورودی از وجود کاراکترهای CR و LF چک نشوند و اسکریپت با استفاده از رشته ی زیر قصد redirect کردن را داشته باشد:

```
Location: $url%0d%0a
```

تا زمانی که تنظیمات یک cookie با رشته ی $url ((تنها به عنوان یک رشته)) تنظیم شده باشد می توانیم به یک سایت کاربر را redirect کنیم:

```
http://www.i-was-redirected.com/%0d%0aSet-Cookie: Authenticated=yes%0d%0aReferer:
www.somesite.com
```

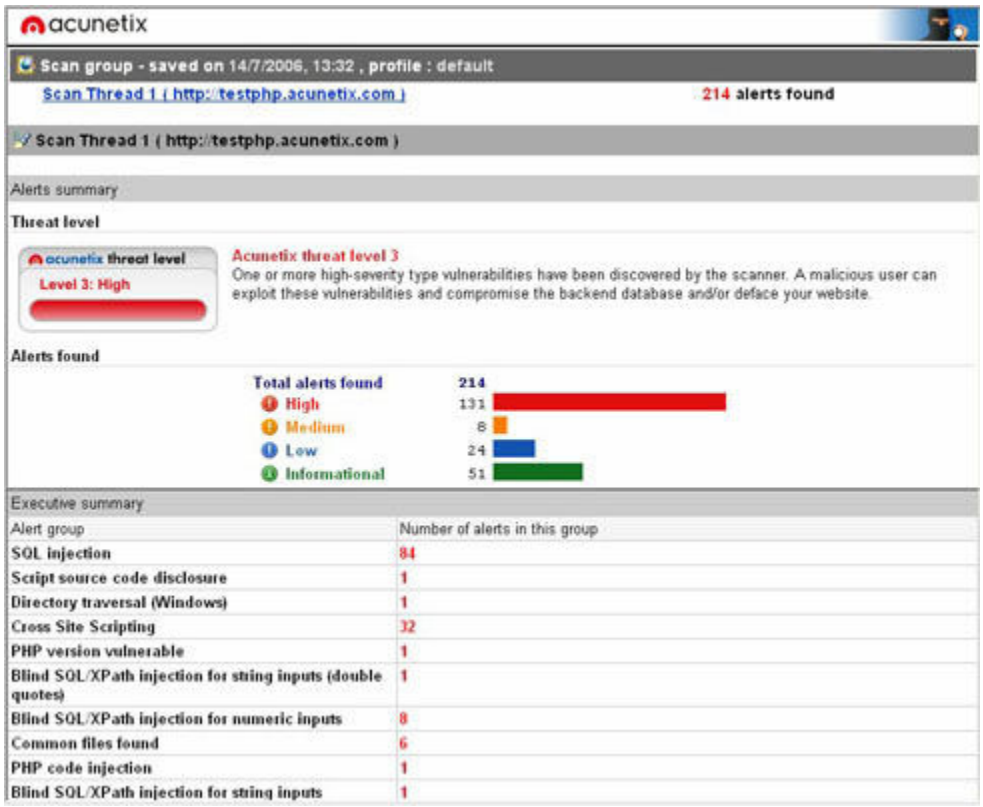
اگر یک هکر URL هایی را که سایر کاربران به آن redirect می شوند را ، که شامل cookie هایی با اطلاعات مهم هستند ، ذخیره کند می تواند خطر زیادی را ایجاد کند.

چگونه آسیب پذیری CRLF را چک نماییم؟

بهترین راه برای چک نمودن این آسیب پذیری ها بر روی سایت ها و یا سرور ها ، استفاده از یک اسکنر آسیب پذیری برنامه های وب است.این اسکنرها سایت یا سرور را به دنبال این آسیب پذیری ها جستجو می کنند و گزارشی را بعد از انجام این کار تهیه می کنند.در این گزارش آسیب پذیری های یافت شده همراه با راه رفع آن ها آمده است.

جلوگیری از آسیب پذیری CRLF در سایت:

راه مناسب و آسان برای جلوگیری از انجام این حملات ، چک کردن ورودی های کاربر از وجود این کاراکترها و حذف کردن کارکترهای خطرناک و نگه داشتن کاراکترهای صحیح است.این کار می تواند از ورود اطلاعات و مقادیر خطرناک به سرور جلوگیری کند.



نمونه ای از یک Web Vulnerability Scanner

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