@karnil

کارنیل
karnil.com

✓کارنیل، بزرگترین شبکه موفقیت ایرانیان می باشد، که افرادی زیادی توانسته اند با آن به موفقیت برسند، فاطمه رتبه ۱۱ کنکور کارشناسی، محمد حسین رتبه۶۸ کنکور کارشناسی، سپیده رتبه ۳ کنکور ارشد، مریم و همسرش راه اندازی تولیدی مانتو، امیر راه اندازی فروشگاه اینترنتی،کیوان پیوستن به تیم تراکتور سازی تبریز، میلاد پیوستن به تیم صبا، مهسا تحصیل در ایتالیا، و..... این موارد گوشه از افرادی بودند که با کارنیل به موفقیت رسیده اند، شما هم می توانید موفقیت خود را با کارنیل شروع کنید.

برای پیوستن به تیم کارنیلی های موفق روی لینک زیر کلیک کنید.

www.karnil.com

همچنین برای ورود به کانال تلگرام کارنیل روی لینک زیر کلیک کنید.

https://telegram.me/karnil

@karnil

وب میدان جنگ امروز

نویسنده: امیر حسین شریفی
info@WebSecurityMgz.com
تاریخ : ٦ دی ماه ١٣٨٢

امروزه تعداد سایتهای وب و برنامه های کاربردی آنها به سرعت در حال افزایش می باشد و شاید تا چند سال قبل هیچکس پیش بینی این وضعیت را نمی کرد. امروزه تقریبا بسیاری از صنایع و حرفه ها از اینترنت و وب استفاده می کنند. و خیلی از حرفه ها و صنایع به وسیله وب ایجاد شده اند. در یکی از مقالاتی که راجع به شغلهایی که توسط اینترنت ایجاد شده است، مطالعه می کردم و این مساله در ذهنم آمد که کلاهبرداری های امروزی نیز عوض شده و شاید بتوان گفت که دیگر دزدان امروزی آدمهای لات و اوباش کنار خیابان نمی باشند ، بلکه آدمهای بسیار باهوش و تیزبین ، با معلوماتی که شاید یک مهندس کامپیوتر و یا مدیر یک شبکه به ندرت با آنها آشنا باشد!!! و این مساله خیلی جالب می باشد که همراه با پیشرفت علم کامپیوتر و حرفه ای تر شدن برنامه های کاربردی ، نفوذگران وب هم پیشرفت می کنند. البته این را هم باید بگویم که این نفوذگران هرچند باعث خرابکاری هایی می شوند ولی نمی توان از تلاش بعضی از آنها در گسترش و پیشرفت اینترنت و وب چشم پوشی کرد.

تا دیروز برنامه های مخربی همچون ویروسها ، در عین خطرناک بودن خیلی به کندی پیشرفت می کردند و کامپیوترهای کمی را آلوده می کردند ، اما امروزه یک کرم اینترنتی ، همچون subig ، به سرعت خود را روی اینترنت انتشار می دهند و باعث آلودگی هزاران کامپیوتر می شوند و میلیونها دلار خسارت وارد می کنند.

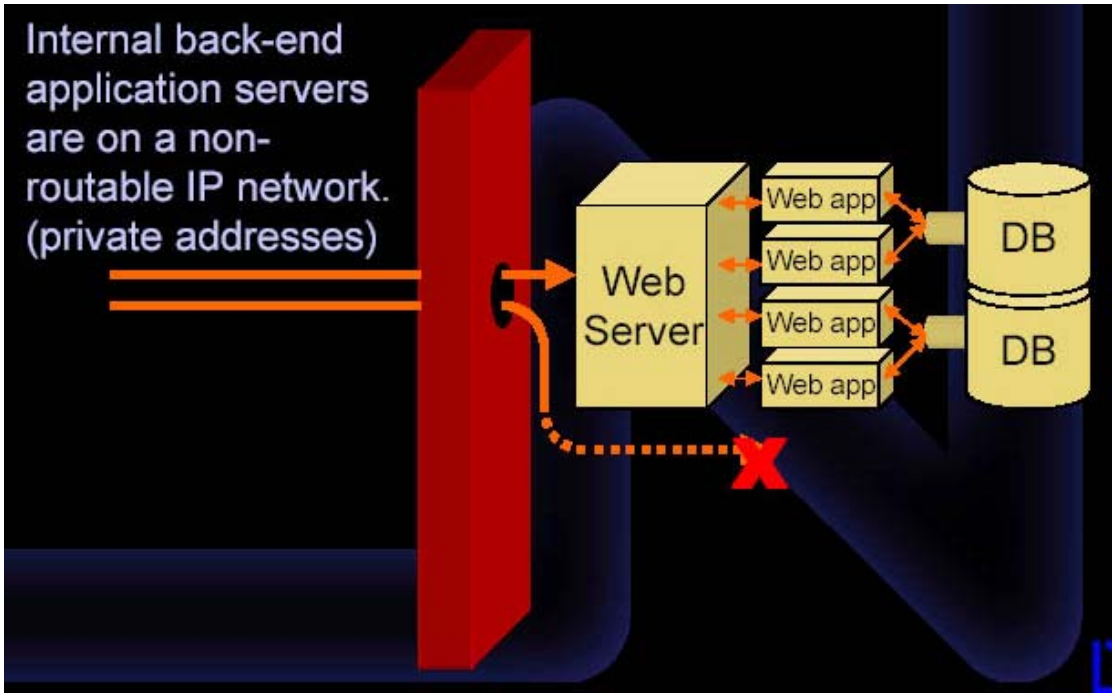
اما در کنار اینگونه خرابکاری ها ، متخصصین وب نیز بیکار ننشتند و ، شبکه های مجهز تر و با استحکام تری را بنا کردند و با تجهیزاتی همچون دیواره آتش[1] و IDS ها تا حدود زیادی موفق به مهار اینگونه حملات شده اند.

1 - Firewall

@karnil

امروزه مدیران شبکه با توجه به تجربه های گذشته ، شبکه های مدرن و بسیار مستحکمی ساخته اند و دیواره های آتش تقریبا در تمامی شبکه ها استفاده می شود و همین امر باعث شده است که بسیاری از نفوذگران نتوانند به راحتی حریم شبکه ها را بشکنند و به آنها نفوذ کنند. سیستمهای عامل و سرورهای شبکه نیز چنین می باشند . و بسیاری از اشکالاتی که در گذشته برای آنها ایجاد مشکل می کرده است را رفع کرده اند و برای مشکلات آینده نیز به سرعت قطعه تعمیری (Patch) آن را می سازند و بین کاربران خود منتشر می کنند. و از همه مهمتر دیواره های آتش می باشند که هم از شبکه و هم از سیستمهای عامل محافظت می کنند. دیگر مانند گذشته یک شبکه در تیرراس نفوذگران قرار نمی گیرد و برای وارد شدن به آن واقعا باید دیواره ای از آتش را پیمود!

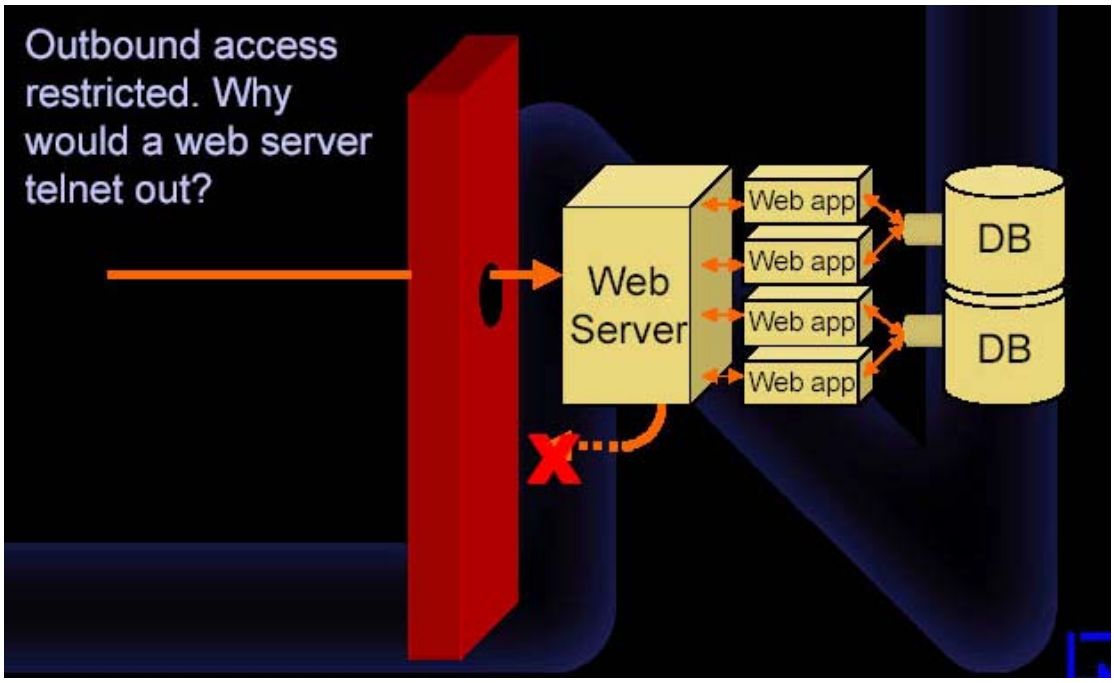
بسیاری از سرورهای انتهایی برنامه های کاربردی دیگر از طریق اینترنت قابل دسترس نمی باشند و با آدرسهای غیر قابل میسر دهی[2] ، آدرس دهی شده اند.



دیگر مدیران شبکه به راحتی به هر کسی اجازه نمی دهند که با هر پورتی با بیرون از شبکه ارتباط برقرار کنند و به وسیله دیوارهای آتش جلو بسیاری از اینگونه دسترسی ها گرفته شده است. یک مدیر شبکه باید دیگر خیلی نادان باشد که بخواهد به سرور شبکه خود از طریق اینترنت ارتباط تل نت برقرا کند. و همچنین است ارتباطات از داخل شبکه به بیرون از آن !

2 - non-Routable

آیا واقعا لازم است که کارکنان یک سازمان از طریق شبکه سازمان خود به وسیله YM! با دوستان خود چت کنند ؟! مسلما پاسخ منفی است.



البته همه این مشکلات به وسیله قرار دادن یک دیواره آتش قابل حل است.

حال این سوال مطرح است که آیا حالا با وجود یک دیواره ، شبکه ما امن است ؟

خب ! هنوز نگرانی شنود اطلاعات وجود دارد که آن هم به وسیله پروتکل SSL حل شده است. دیگر با ۱۲۸ بیت رمزگزاری به وسیله پروتکل SSL هیچ بنی بشری(حداقل تا امروز !) قادر نخواهد بود اطلاعات شنود شده شما را رمزگشایی کند. حال چطور ؟ خیالتان راحت شد ؟

باید به شما بگویم که سخت در اشتباه هستید. درست است که اینگونه روشهای هک محدود شده است ولی روشهای جدید دیگر ابداع شده که به نوبه خود ساده اما دقیق و بسی خطرناک تر از زمان گذشته خود می باشد.

همراه با برنامه های کاربردی وب ، نفوذ به این برنامه ها نیز پیشرفت می کند و همراه با تکنولوژیهای جدیدی که توسط سازمانها ارائه می شود ، تکنولوژیهای جدید نفوذگری نیز ابداع می شود و در دنیای نفوذگران ارائه می شود. اگر شما یک نگاه کوچکی به تمام برنامه های کاربردی تحت وب بیاندازید می بینید که همه آنها حداقل ! از طریق پروتکل HTTP با کاربران خود ارتباط برقرار می کنند. یعنی یک پورت همیشه در دیواره های آتش باز است و آن هم پورت 80 می باشد. همین درِ باز برای نفوذگران کافی است که دیگر به فکر بالا رفتن از دیوار نیفتند!!

@karnil

برای تمامی دیواره های آتش ترافیک وب به عنوان ترافیک عمومی و تقریبا قابل اعتماد می باشد. برای همین بدون هیچ نظارتی بر آن ، اجازه ورود برای آن صادر می کنند. برای همین برای یک نفوذگر با ذهن خلاق چه چیز بی دردسر تر از این دروازه!

باید گفت که تنها ابزار کار برای نفوذگران وب :

۱- یک مرورگر وب

۲- یک ارتباط اینترنت

۳- یک ذهن خلاق ...

می باشد که من در اینجا یک دسته بندی کوچک از حملاتی که از این طریق انجام می شود را برای شما بیان می کنم ولی توضیحات آن به صورت جزیی در مقالات بعدی به شما ارائه خواهد شد.

حملات نفوذگران وب در دسته بندی زیر می گنجد:

۱- حملات تفسیر URL [۳]

۲-حملات صحت ورودی ها [۴]

۳-حملات تزریق SQL [۵]

۴-حملات جعل هویت [۶]

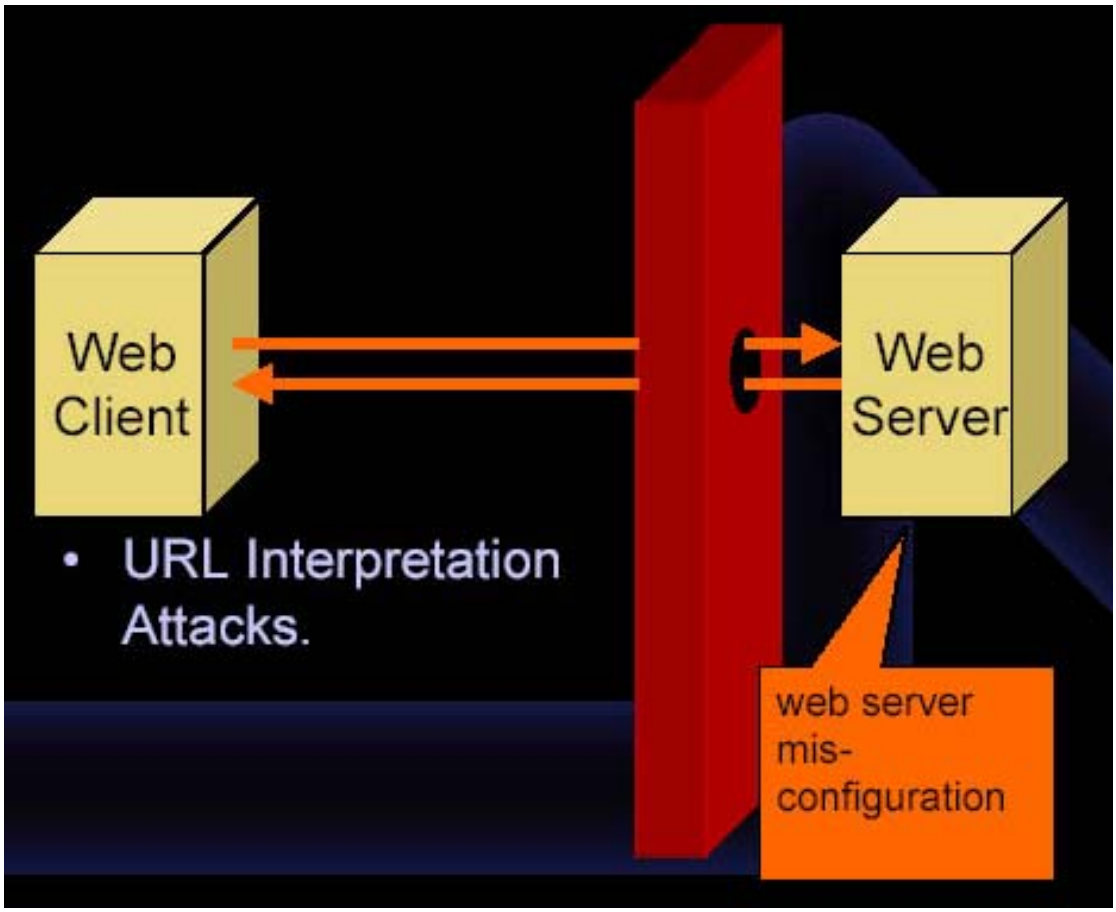
۵-حملات سرریزی بافر [۷]

3 -URL Interpretation Attacks
4 - Input Validation Attacks
5 - SQL Injection Attacks
6 - Impersonation Attacks
7 - Buffer Overflow Attacks

@karnil

۱–حملات تفسیر URL

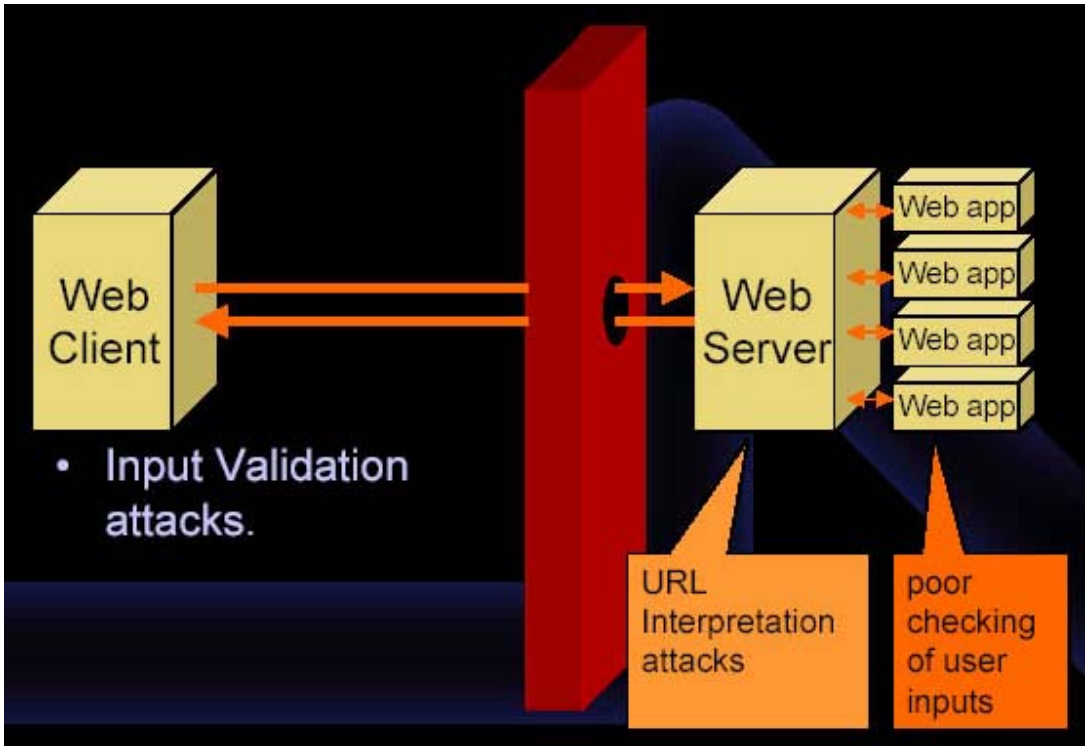
این نوع حمله به علت پیکربندی ضعیف سرورهای وب اتفاق می افتد و باعث حملات بسیار خطرناکی می شود. و دیواره های آتش نمی تواند در این نوع حمله ، از سرور ما دفاع کند ، زیرا که این نوع حمله از طریق پروتکل HTTP و از طریق پورت 80 (یا پورت 443) انجام می شود.



@karnil

۲-حملات صحت ورودی ها

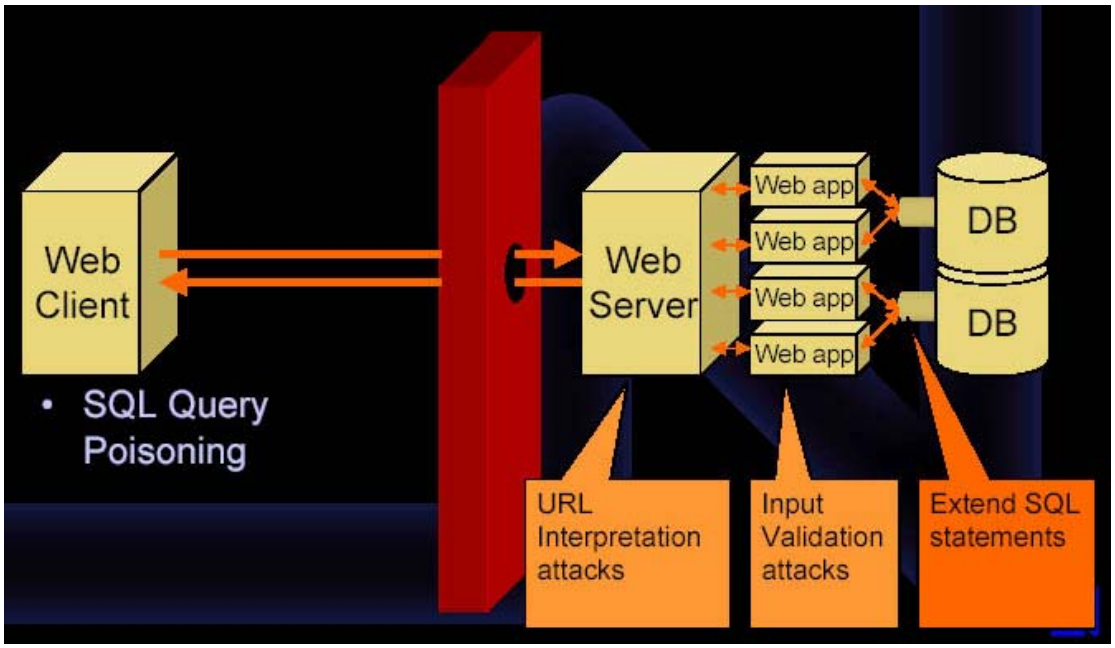
این حمله نیز از اینجا ناشی می شود که لایه منطقی برنامه کاربردی به درستی صحت داده های ورودی کاربر را آزمایش نمی کند. که این نوع حمله نیز از طریق دیواره آتش نمی تواند محافظت شود زیرا از طریق پورت 80 و به وسیله پروتکل HTTP انجام می شود.



@karnil

۳-حملات تزریق SQL

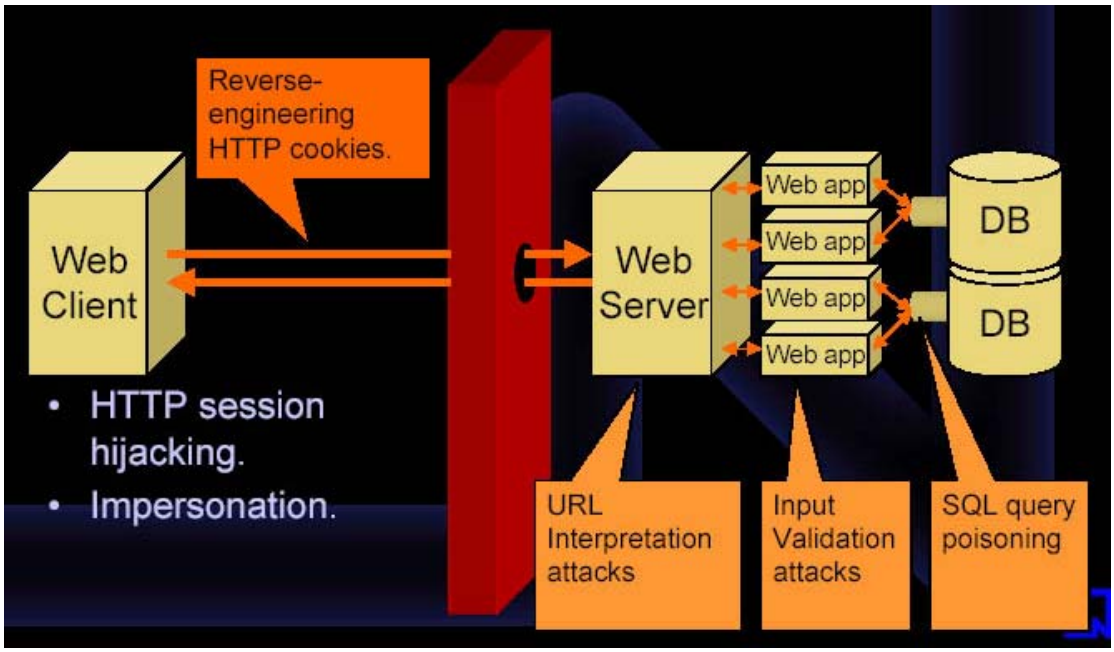
این نوع حمله نیز که بسیار جالب و خطرناک می باشد از طریق تزریق دستورات SQL ، لابه لای داده های ورودی توسط کاربر انجام می شود. این حمله نیز نمی تواند توسط دیواره های آتش محافظت شود زیرا که از طریق پورت 80 و به وسیله پروتکل HTTP انجام می گردد.



@karnil

۴-حملات جعل هویت

این نوع حمله که بسیار زیرکانه طراحی می شود شامل دزدین کوکیها و بعد از آن جعل کردن یک نشست توسط نفوذگر انجام می شود. از این نوع حملات می توان Session Hijacking و Cross Site Scripting را نام برد که هر کدام در قسمتهای جداگانه بحث خواهد شد.



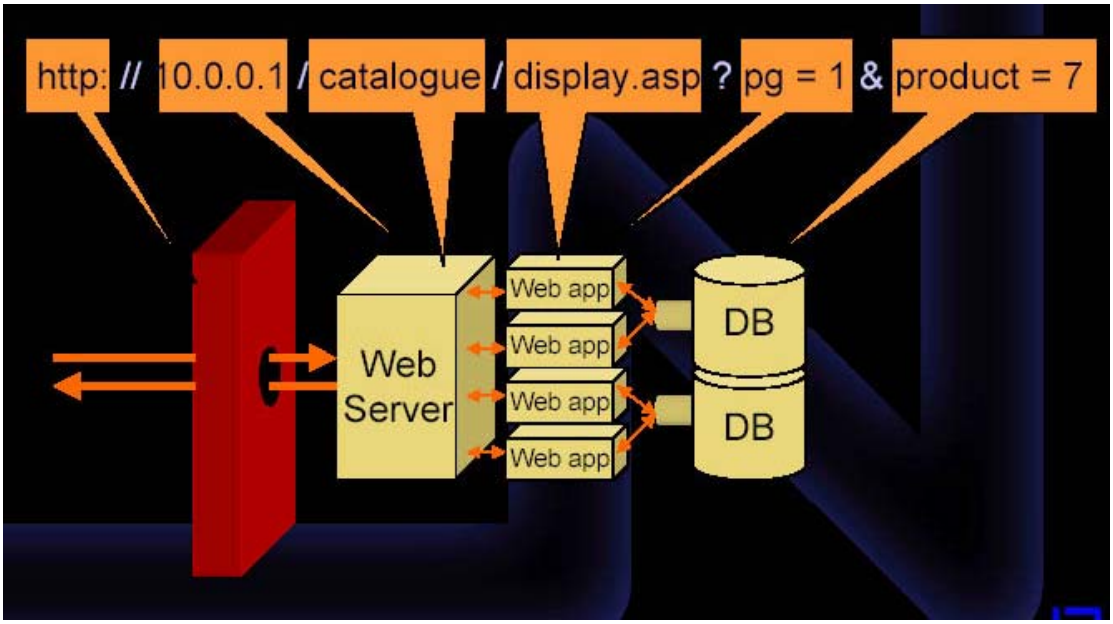
@karnil

۵-حملات سرریزی بافر

این نوع از حملات که بسیار ماهرانه طرح ریزی می شود و بعضی از انواع آن ، جزء حملاتی می باشد که توسط دیواره های آتش هم نمی تواند محافظت شود. زیرا که این نوع حملات نیز از طریق پورت ۸۰ انجام می شود. کرمهای مشهور CodeRed و Nimda جزء حملاتی می باشد که از طریق سرریز بافر طرح ریزی شده بودند.البته این نوع حمله را در آینده به صورت جزئی تر توضیح می دهیم.

به طور کلی باید بگویم که امروزه وب محل کارزار نفوذگران گشته است و آنها بدون دردسر و از طریق حداقل امکاناتی که دارند می توانند خطرناک ترین حملات را انجام دهند.

همانطور که مشاهده کردید پورتهای 80 و یا 443 همیشه در دیواره های آتش باز می باشند. و همیشه یک URL روی تک تک مولفه های یک برنامه کاربردی دسترسی دارد پس تنها راه مقابله با اینگونه حملات کدنویسی های امن تر برای برنامه های کاربردی می باشد.





آیا می دونستید لذت مطالعه و درصد یادگیری با کتاب های چاپی بیشتره؟

کارنیل (محبوب ترین شبکه موفقیت ایران) بهترین کتاب های موفقیت فردی رو برای همه ایرانیان تهیه کرده

از طریق لینک زیر به کتاب ها دسترسی خواهید داشت

www.karnil.com

با کارنیل موفقیت سادست، منتظر شما هستیم

Karnil Karnil.com