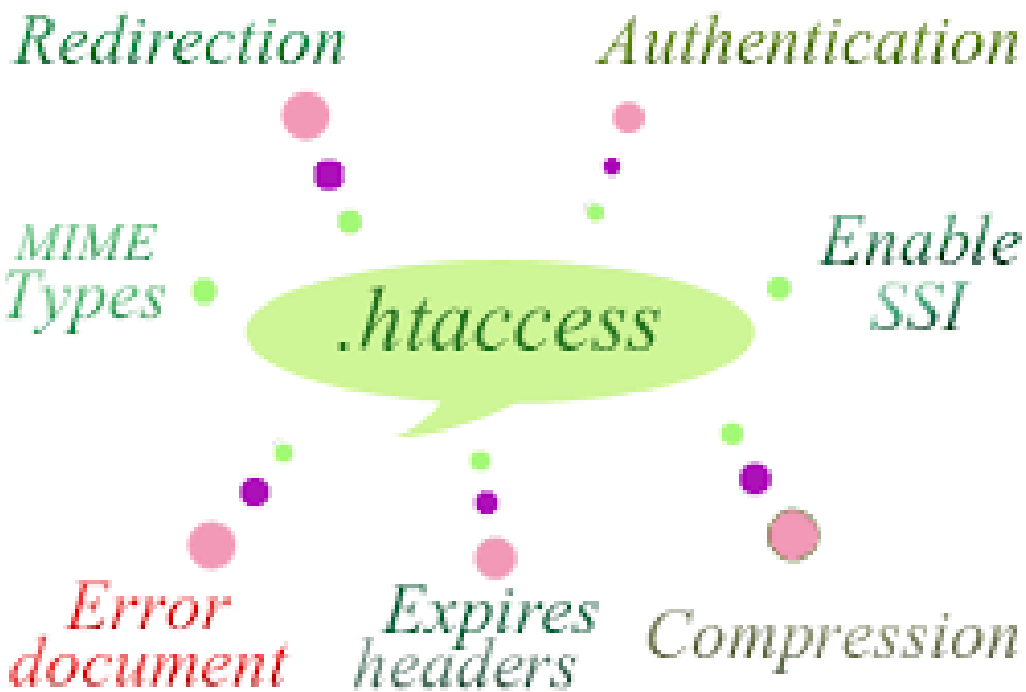
✓کارنیل، بزرگترین شبکه موفقیت ایرانیان می باشد، که افرادی زیادی توانسته اند با آن به موفقیت برسند، فاطمه رتبه ۱۱ کنکور کارشناسی، محمد حسین رتبه۶۸ کنکور کارشناسی، سپیده رتبه ۳ کنکور ارشد، مریم و همسرش راه اندازی تولیدی مانتو، امیر راه اندازی فروشگاه اینترنتی،کیوان پیوستن به تیم تراکتور سازی تبریز، میلاد 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



امنیت وب سایت با

Htaccess

مقدماتی-متوسط

سید سعید حسینی

www.esecurity.ir

telegram.me/Esecurity

مقدمه نویسنده

امروز هیچ تجارتی را نمی توان بدون داشتن یک وب سایت جهت معرفی خود و یا معرفی محصولات و کالاها و یاحتی فروش و در یک عرصه کاملا الکترونیکی تجارت الکترونیکی را در نظر گرفت وجود بی شمار وب سایت های مختلف که به عر ضه خود در تمامی بخش ها مـشغول هـستندو هر روز با تعدادی از این ها در ارتباط هســـتیم .با تمامی این پیشـــرفت ها تعداد زیادی از افرادی که دارای وب سایت هـستند دانش کمی ابتدا در خـصوص طراحی و ایجاد یک وب دارند و ثانیا در حوزه امنیت این فضا باید گفت بدون دانش هـستند . لذا داشتن یک سایت ما را مجبور خاهد کرد که به دنیای امنیت پا بگذاریم . ولی به لحاظ تخصصی بودن این حوزه علمی و گستردگی آن ما را بر آن داشت که با دانش حداقلی بتوانیم تا حدودی وب سایت خود را امن نماییم. کتاب حا ضر به این مو ضوع می پردازد و با یادگیری فایل Htaccessکه یکی از مهمترین فایلهای موجود در یک وب اســـت بتوانید به امنیت دارایی الکترونیکی خود کمک نمایید.

مولف

سید سعید حسینی

تقدیم به

یااباصالح ازپرده برون آی که دلم غرق تمناست
تقصیردلم نیست تماشای توزیباست. . .

اللهم عجل لولیک الفرج...

فهرست

مقدمه 7
تعریف سرور 7
انواع وب سرور 9
سرورهای اینترنتی 9
انواع حملات بر روی وب سرورها : 10
ابزارهای رایج حمله به وب سرور : 11
آشنایی با وب سرور آپاچی 12
وب سرور 12
دلیل استفاده از وب سرور APACHE 15
APACHE رایگان است 16
کد منبع APACHE به رایگان در دسترس است. 16
قابلیت‌هاي وب سرور APACHE 18
دستیابي به منابع مورد نیاز 19
اطمینان از صحت نصب برنامه APACHE 21
فصل دوم 22
پیکربندی HTACESS 22
معرفی زبان پیشفرض (DEFAULTCHARSET) : 32
تنظیم TIMEZONE 33

84 HTTP://HTACCESSBUILDER.COM
85 HTTP://WWW.HTACCESSREDIRECT.NET
86 HTTP://WWW.HTACCESSEDITOR.COM/EN.SHTML
86 HTTP://WWW.GENERATEIT.NET/MOD-REWRITE/INDEX.PHP

مقدمه

استفاده از شبکه‌های کامپیوتری در سالیان اخیر روندی تصاعدی پیدا کرده است. شبکه‌های کامپیوتری، زیر ساخت مناسب برای سازمان‌ها و موسسات را در رابطه با تکنولوژی اطلاعات فراهم می‌نمایند. مقوله تکنولوژی اطلاعات به همان اندازه که جذاب و موثر است، در صورت عدم رعایت اصول امنیت به همان میزان و یا شاید بیشتر، نگران کننده و مسئله آفرین خواهد بود. اغلب سازمان‌های دولتی و خصوصی در کشور، دارای وب سایت اختصاصی خود در اینترنت می‌باشند. سازمان‌ها برای ارائه وب سایت، یا خود امکانات مربوطه را فراهم نموده و با نصب تجهیزات سخت افزاری و تهیه پهنای باند لازم، اقدام به عر ضه سایت خود در اینترنت نموده‌اند یا از امکانات مربوط به شرکت‌های ارائه دهنده خدمات میزبانی استفاده می‌نمایند. بدون تردید سرویس دهنده وب یکی از مهمترین نرم افزارهای موجود در دنیای اینترنت محسوب می‌گردد. کاربرانی که به سایت یک سازمان یا مو سسه مت صل و درخوا ست اطلاعاتی را می‌نمایند، خوا سته آنان در نهایت در اختیار سرویس دهنده وب گذا شته می شود. سرویس دهنده وب، اولین نقطه ورود اطلاعات و آخرین نقطه خروج اطلاعات از یک سایت است. نصب و پیکربندی مناسب چنین نرم افزار مهمی، بسیار حائز اهمیت بوده و تدابیر امنیتی خاصی را طلب می‌نماید.

تعریف سرور

به سرویس‌گیرنده‌ها و استفاده کنندگان از سرویس‌ها، میزبان و به سرویس دهنده‌ها و ارائه کنندگان سرویس، سرور گفته می‌شود. سرورها بسته به نوع خدماتی که ارائه می‌دهند دسته‌بندی‌های متفاوتی دارند. به عنوان مثال، به سرورهای زیر نگاهی بیاندازید:

- Mail Server: سروری که به کاربران شبکه خدمات ایمیل را ارائه می‌دهد.
- DHCP Server: سروری که به کاربران شبکه به طور خودکار آدرس IP می‌دهد.
- DNS Server: سروری که امکان تبدیل درخواست کاربران شبکه، را برای دسترسی به سایت‌های اینترنت، با ارائه آدرس واقعی سایت مزبور می‌دهد، بدین ترتیب دیگر نیازی به حفظ بودن آدرس‌های IP سایت‌ها نخواهد بود.

- Web Server: سروری که خدمات تحت وب را از قبیل میزبانی وب و ... را ارائه می‌دهد.

وب سرور در واقع به دو معنی است:

- برنامه کامپیوتری که مسئول قبول کردن درخواستهای Http از مشتریان است که همان مرورگرهای وب هستند و پاسخ‌ها را به همراه یک سری اطلاعات به آنها پست می‌کنند. این پاسخ ها صفحات Html هستند. بطور مثال اگر در صفحه مرورگر آدرس http://piau.ac.ir/index.phpرا وارد کنید، یک درخواست به دامنه‌ای که نامش piau.ac.irاست، فرستاده می‌شود. آنگاه سرور صفحه index.php را می‌فرستد.
- کامپیوتری است که یک برنامه‌ی کامپیوتری را اجرا می‌کند و کارایی اش همانند مطالبی است که در بالا گفته شد. هر کامپیوتری می‌تواند با نصب نرم افزار سرور به وب سرور تبدیل شود.

در عمل بسیاری از وب سرورها، ویژگیهای زیر را نیز پیاده‌سازی می‌کنند:

- شناسایی: درخواست شناسایی اختیاری قبل از اجازه دسترسی به انواع منابع

نه تنها مفاهیم استاتیک (مفاهیم فایلی که بر روی سیستم فایلی وجود دارد) بلکه مفاهیم دینامیک را با یک یا چند ساختار مانند CGI, SSI, ASP.NET,ASP,PHP,JSP,FastCGI,SCGI اداره می‌کند.

- پشتیبانی از HTTPS تا به کاربران اجازه دهد اتصالات مطمئنی به سرور را بر روی پورت ٤٤٣ به جای ٨٠ برقرار کنند.
- فشرده‌سازی مطالب تا بتوان از حجم پاسخها کم کرد) توسط کدسازی.(GZIP
- پشتیبانی از فایلهای بزرگ تا بتواند فایلهای بزرگ‌تر از ۲ گیگا بایت را سرویس‌دهی کند.
- کنترل کردن پهنای باند: تا سرعت پاسخها را محدود کند و شبکه را پر ازدحام نکند و قادر باشد تعداد بیشتری مشتری را سرویس دهی کند.

- ترجمه مسیر : وب سرورها قادرند تا کامپوننت مسیر URL را به منابع فایل سیستم محلی (برای درخواستهای استاتیک) و نام برنامه داخلی یا خارجی (برای درخواستهای دینامیک) نگاشت کنند

برای مثال کاربر آدرس زیر را درخواست می‌کند:http://www.example.com/path/file.html مرورگر وب کاربر آنرا به یک اتصال به http://www.example.com با درخواست http 1.1 ترجمه می‌کند: GET/path/file.html.php HTTP/1.1 HOST:http://www.example.com وب سرور بر روی http://www.example.com، مسیر درخواستی را به آدرس مسیر اصلی اضافه می‌کند. آنگاه اگر وب سرور فایلی داشته باشد، آن را خوانده و پاسخ را که مجموعه‌ای از مطالب فایل است به عنوان پاسخ می‌فرستد.

انواع وب سرور

- وب سرور داخلی روی شبکهIntranet
- وب سرور خارجی روی شبکهInternet
- روی شبکه خصوصی قرار می‌گیرند.
- از اطلاعات مختص به شرکت نگهداری می‌کند.
- دسترسی به این سرور فقط از طریق کاربران داخلی است.
- روی شبکه عمومی قرار می‌گیرد.
- از اطلاعات کالاها، خدمات و تجارت شرکت نگهداری می‌کند.
- دسترسی به این سرور از طریق تمام کاربران امکان پذیر که ریسک بالایی دارد.

سرورهای اینترنتی

سهم استفاده بازار، از نرم افزارهای وب سرور، در زیر نشان داده شده است که در برآورد Netcraft در ژانویه ۲۰۰۹ منتشر شده است.

جدول ۰-۱: سهم استفاده بازار، از نرم افزارهای وب سرور

فروشنده محصول	نام محصول	وب سایتهای میزبانی شده	درصد
بنیاد نرم افزار آپاچی	سرور آپاچی	۹۶،۵۳۱،۰۳۳	٪۵۲/۰۵
مایکروسافت	IIS	۴۷۴،۰۲۳،۶۱	٪۳۲/۹۰
گوگل	GWS	۹،۸۶۴،۳۰۳	٪۵/۳۲
Nginx	nginx	۳،۴۶۲،۵۵۱	٪۱/۸۷
Lighttpd	lighttpd	۲،۹۸۹،۴۱۶	٪۱/۶۱
Oversee	Oversee	۱،۸۴۷،۰۳۹	٪۱/۰۰
دیگر	–	۹،۷۵۶،۶۵۰	٪۵/۲۶
مجموع	–	۱۸۵،۴۷۴،۴۶۶	٪۱۰۰/۰۰

انواع حملات بر روی وب سرورها :

حملات پیمایش پوشـــه (traversal attacks Directory) : این نوع از حملات باگ های موجود در وب سرور را به کار گرفته تا د ستر سی غیرمجاز به فایل‌ها و پو شه هایی که در مـسیر عمومی قرار ندارند را بکاربگیرند . زمانی که هکر دسـترسـی را بدسـت آورد می‌تواند اطلاعات حیاتی را دریافت کرده و دستورات دلخواه خود را بر روی وب سرور اجرا کند یا بدافزار نصب کند .

حملات رد سرویس (Service Attacks Denial of) : با ا ستفاده از این نوع حمله و سرور ممکن است از سرویس دهی خارج شود و سرویس دهی صورت نپذیرد .

سرقت سیستم نام دامنه (Name System Hijacking Domain) : با استفاده از این نوع حمله اطلاعات دی آن اس به نقطه‌ای که هکر می‌خواهد تغییر یافته . در نتیجه همه ترافیکی که بایستی به سرور اصلی هدایت شود به سرور هکر هدایت می‌شود .

شنود (Sniffing) : داده‌های رمزنگاری نشده بر روی شبکه ممکن است به منظور دسترسی بدون مجوز بکار گرفته شوند و شنود شوند .

فیشینگ (Phishing) : این نوع حمله با ایجاد یک صفحه جعلی و هدایت کاربران به صفحه جعلی به منظور سرقت اطلاعات انجام می‌شود .

دیفیس (Defacement) : این نوع حمله معمولاً توسط هکرهای خرده پا صورت می‌گیرد . حملات دیفیس با استفاده از یکی از متدهای تزریق اسکیو ال یا دیگر متدهای حمله به منظور قرار دادن امضای هکر بر روی یکی از صفحات سایت به دلایل شخصی ، مذهبی و اعتقادی و یا حتی ضربه زدن به وجهه اجتماعی سایت هدف صورت می‌پذیرد .

خوب اکنون که انواع حملات را شناختید این حملات توسط چه ابزارهایی صورت می پذیرند ؟

ابزارهای رایج حمله به وب سرور :

متااسپلوییت (Metasploit) : این یک ابزار متن باز می‌باشد که دارای نسخه تجاری هم می‌باشد . به منظور بکارگیری اکسپلوییت های موجود در سمت سرور بکارگرفته می شود . این ابزار به صورت پیش‌فرض دارای اکسپلوییت های زیادی هست ولی شما در صورت تسلط به زبان روبی قادر به نوشتن اکسپلوییت های سفارشی نیز هستید . متااسپلوییت در اصل ابزاری به منظور تست آسیب‌پذیری به شمار می‌رود .

Mpack : یک ابزار بکارگیری وب است . به زبان PHP نوشته شده است و توسط پایگاه داده MySQL پشتیبانی می‌شود . زمانی که وب سرور توسط Mpack مورد حمله قرار گرفت همه ترافیک آن به سکن سایت‌های دانلود مخرب هدایت می‌شود .

زئوس (Zeus) : این ابزار قادر است سیستم بکارگرفته شده را به یک بوت ، زامبی تبدیل کند . بوت کامپیوتر هک شده است که به منظور دیگر حملات اینترنتی از آن استفاده می شود . بوتنت مجموعه از کامپیوترهای بکارگرفته شده است . بوتنت ها را می‌توان در ارسال ایمیل‌های اسپم و حملات DOS مورد استفاده قرار داد .

Neosplit : این ابزار را می‌توان به منظور نصب حذف یا کپی برنامه‌ها مورد استفاده قرار داد .

آشنایی با وب سرور آپاچی

امروزه اطلاعات، در دنیای ما نقش بسیار مهمی دارند و بسیاری از این اطلاعات توسط اینترنت انتقال پیدا می‌کنند. متداولترین پروتکلی که برای انتقال اطلاعات از آن اســتفاده می شــود، پروتکل HTTP اســت. پروتکل HTTP به عنوان پروتکلی ســریع، قوی و با بار کم بر روی CPU و حافظه ســرور طراحی شده است و البته برای جلوگیری از کاهش پیدا کردن کارایی وب بر اثر استفاده بسیار زیاد از این پروتکل، باید کارایی اش را بهینه سازی کرد.

دو استراتژی اصلی برای بهینه سازی کارایی وجود دارد:

۱- بهینه سازی کارایی وب سرور

۲- بهینه سازی کارایی پروتکل HTTP

وب سرور

البته یکی از چیزهایی که باعث می شود افراد سردرگم شوند حالت طراحی وب و مفهوم وب سرور است. بیشتر مردم فکر می‌کنند سرور یک ماشین فیزیکی بزرگ مثل سیستم کامپیوتری است که در یک اتاق ســرد نگهداری می‌شــود و یا حتی مثل ســیســتم هکرهاســت! که همه فکر می‌کنند زیرِ زمین هستند.

وب سرور ها کامپیوتر هایی هستند که صفحات وب را اماده نمایش می کنند هر وب سرور یک ای پی اختصاصی و دامنه دارد. برای مثال زمانی که ادرسی را در مرورگر تایپ می کنید برای مثال http://www.esecurity.ir/index.htmlدرخواستی برای وب سرور فرستاده میشود وب سروری که دامنه اش esecurity.irاست سپس سرور صفحه ای به نام index.html را بازخوانی و به مرورگر ار سال می کند.هر کامپیوتری با نصب برنامه سرور و اتصال به اینترنت می تواند یک وب سرور باشد.برنامه های متعددی برای این کار وجود دارد که از معروف ترین ان ها می توان به Apache، NCSAو Netscape ا شاره نمود.وب سرور ها امکان دارد به دلایل متفاوتی کند شوند مثلا در خواست های متعددی که در مدت زمان کوتاهی ارسال میشوند میتوانند وب سرور را کند کنند اما با توجه به پردازش بسیار سریع این وب سرور ها این کند شدن هم معمولا به چشم کاربر نیامده و متوجه ان نمیشود.دیتایی که توسط پردازنده فرستاده میشود باید در پروتکلی که HTTP نام دارد مطابقت داده شود تا از ارتباط سرور ها با یکدیگر اطمینان حاصل گشته و خطایی به وجود نیاید.وب سرور ها علاوه بر انتشار صفحات وب کارهای دیگری از قبیل دانلود فایل ها از طریقFTP، خدمات مربوط به ار سال ایمیل و... را انجام میدهد.برای انتخاب یک وب سرور منا سب باید به گزینه هایی از قبیل چگونگی کارکرده ان با بقیه سیستم عامل ها و سرور ها، قدرت مدیریت برنامه نویسی ان در سمت سرور، ویژگی های امنیتی،موتورهای جست و جوگر، تجهیزات ساختمان سایت و... که ممکن است نیاز باشد توجه نمود.

البته وب سرور نرم‌افزار هایی مثل آپاچی روی یک سیستم کامپیوتری اختصاص داده شده است که می‌توانید از ویژگی‌های میزبانی وب اکثر سیستم عامل‌های ساخته شده مثل IIS ویندوز ا ستفاده کنید و ضمناً خوب است بدانید اوبونتو هم یک وب سرور محسوب می شود.

در حقیقت راه اندازی یک وب سرور باعث می‌شود صفحات وبی که از کامپیوتر های دیگر ارایه شده، آسانتر و سریعتر باز شوند. البته وب سرور جنبه های پیچیده‌تری هم دارد، مثل ارائه محتوای پویا (داینامیک) با اشکال یا محتوای صفحاتی که اطلاعات ورودی کاربر را می پذیرد، پردازش آن‌ها، و حتی ایجاد صفحات سفارشی جدید.

وب سایت های سطح بالاتر شما را قادر می سازند با ا ستفاده از نرم افزار هایی مانند آپاچی، که توانایی پردازش ورودی اطلاعات کاربران را دارد، به طور خودکار صـــفحات وب را ایجاد کنید و با استفاده از زبان های برنامه نویسی وب مانند PHP، جاوا و ... آن ها را کامل تر سازید.

لینوکس (Linux) به هسته ی سیستم‌عامل‌های شبه یونیکس می‌گویند که که در سال ۱۹۹۱ توسط لینوس تروالدز توسعه یافت. برخی به سیستم عامل‌هایی که از هسته ی لینوکس استفاده می‌کنند نیز لینوکس می‌گویند (در این دانشـنامه هم منظور از لینوکس، سـیسـتم عامل‌هایی اسـت که از هسـته ی لینوکس استفاده می‌کنند.)

امروزه لینوکس بر روی اکثر ابزار های هوشـــمند اطراف ما نظیر ســـاعت های هوشـــمند، تلفن های همراه، تبلت ها، مسیریاب ها، کامپیوتر های خانگی، سرور ها، ابر کامپیوتر ها و... استفاده می شود. اکثر توزیع های لینوکس، بسته کامل نصبی LAMP را برای نصب به صورت آماده در خود دارند. با توجه به بررسی های انجام گرفته توسط W3Techs در اکتبر سال 2013، 58.5%سهم بازار وب سرور ها بین دو توزیع محبوب Debian و Ubuntu تقسیم شده بود، در حالیکه سه توزیع RHEL، Fedoraو CentOS با همدیگر تنها 37.3٪ از سهم بازار را در اختیار داشته اند.

نقش وب سرور LAMP را رسماً وب سرور Apache آپاچی ایفا می کند. ســـرویس دهنده ی اچ تی تی پی آپاچی که بیشـــتر آن را آپاچی می‌نامند، یک برنامه‌ی وب سرور است که نقش کلیدی در توسعه دنیای وب ایفا می‌کند و اکثر شرکت های هاستینگ از این وب سـرور برای ارائه خدمات میزبانی خود اسـتفاده می کنند. در سـال ۲۰۰۹ آپاچی اولین برنامه ی وب سرور بود که حدود ۱۰۰ میلیون وب سایت به کمک آن سرویس‌دهی می‌کردند. آپاچی به‌طور معمول در محیط های بر پایه یونیکس و لینوکس استفاده می‌شود.

این برنامه تحت مجوز آپاچی بوده و به صورت متن‌باز (Open Source) ا ست. و از سال ۱۹۹۶ تاکنون پرکاربردترین برنامه در حوزه ی خود است. تخمین زده شده است که این وب سرور محبوب تا ژوئن سال 2014 میلادی بیش از 52.27٪ وب سایت های فعال را پشتیبانی کرده است .

ویژگی‌های این برنامه بسیار گسترده است؛ از پشتیبانی زبان‌های برنامه‌نویسی سمت سرور مانند PHP، Perl، Python و TCL گرفته تا احراز هویت TLS و SSL.

یکی از کاربردی ترین موارد مربوط به آپاچی وب سرور برای برنامه‌نویسان استفاده از پرونده فایل htaccess است. برنامه‌نویس می‌تواند با اعمال تغییراتی در این پرونده که بر هر شاخه‌ای قابل اضافه شدن است دستورات ویژه ی آن شاخه را به سرور ارائه دهد. برای نمونه اگر بخواهد که در صورت وارد کردن نشانی aa.html نام آن باقی بماند ولی در واقع پرونده main.php?page=bb اجرا شود به‌وسیله ی این پرونده قادر به اعمال دستورش خواهد بود.

دلیل استفاده از وب سرور Apache

حقیقت این است که وب سرور Apache به یکی از عوامل موفقیت وب تبدیل شده است. با وجودی که این ادعا ممکن است برای عده‌ای ناخوشایند باشد، اما دلیل زیادی برای اثبات این واقعیت وجود دارد. برر سی‌های اخیر حاکی از آن ا ست که بی شترین وب سایت‌های موجود در حال حاظر از وب سرور Apache به عنوان سرویس دهنده وب استفاده می‌کنند. این دلیل را می‌توان علت این موفقیت برشمرد:

- Apache رایگان است.
- کد منبع Apache به رایگان در دسترس است. (به این گونه نرم‌افزارها اصطلاحاً "کدباز" یا open source گفته می‌شود.)
- Apache بر روی مجموعه‌ای بسیار متنوعی از سیستم‌های عامل قابل استفاده است.
- Apache دائماً در حال توسعه و افزایش قابلیت‌های جدید است.

- Apache بسیار توانمند بوده و به واسطه طراحی ماجولار به راحتی قابل توسعه است.

Apache رایگان است.

وب سرور Apache ضمن برخورداری از ویژگی‌ها و توانایی‌های قابل توجه کاملاً رایگان است. با این وجود از آنجا که به واسطه انتشار این وب سرور هیچ‌گونه منفعتی نصیب سازمان توسعه دهنده آن یعنیApache software foundation نمی‌شود طبیعی است که نرم‌افزار مزبور از هیچ‌گونه پشتیبانی فنی از طریق تلفن یا به صورت online که در مورد نرم‌افزارهای تجاری شاهد آن هستیم در رابطه با وب سرور Apache مرسوم نیست.

با این همه مستندات بسیار جامعی از نرم‌افزار مرود بحث از طریق وب سایت مربوطهدر دسترس علاقه‌مندان قرار دارد.

کد منبع Apache به رایگان در دسترس است.

چنانچه در برنامه‌نویسی تبحر دارید می‌توانید کد منبع Apache را آن گونه که مورد نیاز شما ست دستخوش تغییر کنید. با این حال بیشتر کاربران با هدف تغییر نحوه عملکرد Apache دست به این اقدام نمی‌زنند، بلکه صرفاً نحوه پیکربندی آن را تغییر می‌دهند، و با کمپایل مجدد که منبع Apache انتظاراتی که وب سرور دارند، تأمین می‌کنند. از این رودکی در صورتی که به یک وب سرور مختصر و سبک نیاز دارید می‌توانید Apache را به گونه‌ای کمپایل کنید که تنها نیازهای خواسته شده را تأمین کند. به این ترتیب چنانچه با مشکل حادی برخورد کردید یا مایلید تغییراتی را در کد منبع Apache اعمال کنید می‌توانید با برخورداری از دانش برنامه‌نویسی این کار را انجام دهید.
Apache بر روی مجموعه بسیار متنوعی از سیستم‌های عامل قابل استفاده است.

نسخه‌های مختلف وب سرور Apache به منظور بهره‌گیری تحت سیستم‌های عامل متداولی از جمله این موارد توسعه یافته است.

- unix

- liunx

- ویندوز (شامل نسخه‌هایی x9 تا XP هر چند که نسخ‌های تحت NT و 2000 از قابلیت‌های بیشتری برخوردارند.)

- Novell Netware

- Mac OSX

منهای برخی اختلافات جزیی مانند استقرار فایل‌های وب سرور Apache در سیستم فایلعملکرد این وب سرور در تمامی محیط‌های عامل فوق یکسان است.
Apacheدایماً در حال توسعه و افزایش قابلیت‌های جدید است.

مسئولیت توسعه و بهبود کارایی وب سرور Apache به عهده سازمان software foundation یعنی پدید آورنده آن است. شگفت‌انگیز است، به طوری که تنها پس از گذشت تنها چند روز اشکالات و شکاف‌های امنیتی یافت شده اصلاح می‌شود. نکته مذکور Apache را به پایدارترین و در عین حال ایمن‌ترین وب سرور حال حاضر تبدیل کرده است. البته این ویژگی یکی از مهم‌ترین دلایل مقبولیت آن است.

مزیت دیگری که به واسطه سرعت بالای توسعه و انتشار نسخه‌های جدید نرم‌افزار به دست می‌آید، مجموعه‌ای ارزشمند از قابلیت‌هاست، که البته وب سرور Apache نیز از این قاعده مستثنی نیست.

به این ترتیب تکنولوژی جدیدی که همه روزه در درارتباط با شـــبکه جهانی اینترنت با آنها مواجه می شویم، پیش از هر وب سرور دیگری تو سط Apache پیاده سازی شده و مورد پشتیبانی قرار می‌گیرند.

قابلیت‌های وب سرور Apache

وب ســرور Apache نام خود را از شــیوه‌ای که نخشــتین بار برای توســعه آن به کار رفت، گرفته است. اساساً این وب سرور از مجموعه‌ای مؤلفه نرم‌افزاری یا اصطلاحاً patch (با تلفظ پچ)تشکیل شــده اســت به گونه‌ای که بســیاری از توســعه دهندگان برای تاکید این موضــوع از اصــطلاح " a patchy server " با تلفظ "اپچی سرور" به معنی سروری که از مجموعه‌ای مؤلفه‌های نرم‌افزاری ایجاد شده است، استفاده می‌کردند.

مدت‌هاست که توسعه وب سرور Apache در قالب قطعات یا ماجول‌های نرم‌افزاری مستقل صورت می‌گیرد. تو سعه وب سرور Apache بر ا ساس این ماجولا (ا صطلاحاً تو سعه "ماجولار") موجب شده که بهره‌گیری از Apache به عنوان وب سرور سربار کمتری را به سخت‌افزار و سیستم عامل میزبانی که بر روی آن مستقر شده است تحمیل کند.

به بیان بهتر در ا ستفاده از این وب سرور تنها ماجول‌های مورد نیاز بر روی سخت‌افزار و سیستم عامل میزبان مســتقر می‌شــوند. این ویژگی هم‌چنین روند توســعه و پشــتیبانی از ماجول‌هایی راکه شرکت و برنامه‌نویسان مستقل (ا صطلاحاً third parties)به منظورهای مختلف تو سعه می‌دهند، تسهیل می‌کند.

وب ســرور Apache تقریباً تمامی تکنولوژی اینترنت را که در ارتباط با وب تویعه پیدا کرده‌اند به خوبی مورد پشتیبانی قرار می‌دهد. این قابلیت حتی شامل برخی تکنولوژی‌های اختصا صی از جمله Microsoft Frontpage Extensions نیز می‌شــود. وب ســرور Apache تمام مشــخصــات

پروتکل HTTP اسکریپت‌نویسی، احراز هویت و قابلیت استفاده از سایر تکنولوژی‌ها را به خوبی مورد پشتیبانی قرار داده است.

دسته‌ای از قابلیت‌ای وب سرور Apache عبارتنداز:

- پشتیبانی جامع و کامل از پروتکل HTTP
- قاژبلیت پیکربندی بالا وامنیت قابل ملاحظه
- پشتیبانی از PHP
- پشتیبانی از CGI و سایر زبان‌های اسکریپت‌نویسی

دستیابی به منابع مورد نیاز

هر آنچه که در ارتباط با نصب وب سرور Apache بدان نیاز دارید از طریق وب سایت Apache به آدرس http// www. Apache. Otg قابل دستیابی است. از طریق این آدرس اینترنتی می‌توانید کد منبع نسخه اجرایی (اصطلاحاً binaryversion) وب سرور Apacheرا برای محیط عامل UNIX و linux و همچنین شکل صفحه اصلی وب سایت Apache را نشان می‌دهد.

نسخه‌های مختلفی از وب سرور Apache برای بهره برداری تحت نسخه‌های مختلف سیستم عامل Linux توسعه یافته است. برای مثال کاربارن سیستم عامل Redhat Linux می‌توانند از طریق مکانیزم Redhat package Manager یا اصطلاحاً RPM وب سرور Apache را بر روی سیستم خود نصب کنند.

نصب برنامه Apacheتحت سیستم عامل Linux از طریق کمپایل کد منبع

چنانچه مایل به کمپایل Apache با شید، لازم ا ست ابتدا کد منبع منا سبی رادر اختیار دا شته با شید. برای شـــروع فایل مورد نظر را از آدرس مذکور در یک فهرســـت موقت یادر موقعیت /usr/src از سیستم فایب که معمولاً برای این منظور ازآن استفاده می‌شود بارگذاری کنید. برای .باز کردن آشیو کد منبع (و عموماً هر آر شیو دیگر) رو شهای مختلفی وجود دارد. روش مورد ا ستفادهبرای این کار به برنامه‌های نصب شده بر روی کامپیوتر و نوع آرشیوی که بارگذاری کرده‌اید بستگی دارد.

چنانچه نسخه‌ای از آرشیو را که با استفاده از برنامه فشرده‌ساز gzip فشرده شده است، بارگذاری کرده‌اید. (در این صـورت فایلی با پسـوند tar.gz در اختیار دارید.) پیش از این هر گونه اقدامی برای باز کردن آر شیو، لازم ا ست با ا ستفاده از همین برمنامه ف شرده ساز آن را از حالت ف شرده خارج سازید. فرمان زیر که از فهر ست نژمیزبان فایل httpd-2.0. tar. gzرا به طور توأم انجام می‌دهد. (علامت $ اعلان سیستم عامل unix است.)

```
$ tra-zxvf httpd-2.0.8.tra.z
```

اما اگر ن سخه ای از آر شیو را با ا ستفاده از برنامه ف شرده سازی bzip یا bzip2 (یا ن سخه های دیگری از این برنامه ف شرده ساز) ف شرده شده ا ست بارگذاری کرده اید (در این صورت فایلی با پسوند tar.z در اختیار دارید) با صدور فرمان زیر علاوه بر اینکه فایل مورد نظر را از حالت فشرده خارج می کنید بلکه آرشیون مزبور را نیز باز می کنید:

```
$ tar -zxvf httpd-2.0.8.tra.z
```

نتیجه اجرای هر دو فرمان مذکور یکســـان اســـت، به طوری که در نهایت فایل های حاوی کد منبع Apache در فهرسـت تحت عنوان httpd-2.0 مسـتقر می شـوند. که علامت سـتاره بیانگر شـماره نسخه minor است.

اطمینان از صحت نصب برنامه Apache

پس از نصب و راه اندازی برنامه Apache به منظور اطمینان از صحت عملیات به سادگی می توانید مرورگر اینترنت خود را باز کرده و نام ماشین میزبان وب سرور Apache را در فیلد آدرس آن بنویسید. بر روی ماشین میزبان وب سرور Apache کافی است آدرس زیر را در فیلد آدرس مرور گر اینترنت وارد کنید:

http:// localhost

با این اقدام باید نتیجه ای شبیه به شکل را مشاهده کنید. در صورتی که با استفاده از کامپیوتر دیگری به ماشین میزبان وب سرور Apache متصل شده اید. کافی است عبارت local host را در آدرس فوق با نام کامل آن اصطلاحا fully qualified name یا آدرس IP مربوطه جایگزین کنید.

وب سروری که به درستی پیکربندی نشده است می تواند به سرعت به عاملی برای نفوذ به ماشین میزبان یا حتی شبکه ای که ماشین مزبور ر روی آن مستق شده تبدیل شود پس از نصب وب سرور بی درنگ آن را متوقف کرد. برای متوقف کردن وب سرور کافی است فرمان زیر را صادر کنید

$ usr/sbin/ Apachectl stop

فصل دوم

پیکربندی Htacess

.htaccess یک فایل پیکر بندی برای وب سایت هایی است که از سرور آپاچی استفاده می کنند. وقتی این فایل در یکی از پو شه های وب سایت قرار می گیرد، وب سرور آپاچی برر سی می کند که چه د ستوراتی در این فایل وجود دارد و بعد طبق این د ستورات، آن قسمت از سایت که htaccess در آن قرار دارد را پیکر بندی می کند. این فایل می تواند برای فعال و یا غیر فعال کردن یک سری از توابع و ویژگی های وب سرور آپاچی مورد استفاده قرار بگیرد.

فایل .htaccess یک فایل ساده اسکی (ASCII) می‌باشد که می‌توانید آن را به وسیله نرم‌افزارهای متنی ساده نظیر Notepad و یا SimpleText به وجود آورید. دقت داشته باشید که این فایل دارای هیچ نامی نمی باشد و فقط دارای پسوند است که پسوند آن، htaccess می‌باشد. برای درست کردن این فایل می‌توانید فایل متنی خود را که مثلا به صورت test.txt می باشد، تغییر نام داده و آن را به صورت .htaccess درآورید.

تذکر: اگر از ویندوز استفاده می کنید و هنگام تغییر نام دادن فایل به .htaccess، پیغام خطایی مبنی بر اینکه «می بایست برای فایل خود نامی را اختیار کنید» دریافت می کنید، فایل را بر روی سرور آپلود کرده و سپس در سرور آن را تغییر نام دهید. این کار به وسیله نرم‌افزارهای FTP نظیر CuteFTP یا AbsoluteFTP بسیار ساده می باشد.

در هنگام استفاده از فایل .htaccess دانستن چهار نکته از اهمیت به سزایی برخوردار است:

نکته اول: فایل .htaccess را می بایست به صورت ASCII آپلود کرده و مجوز دسترسی به آن را بر روی 644 (یا rw-r–r–) تنظیم نمایید.

نکته دوم: فایل .htaccess را می‌توانید به پو شه های مختلفی اعمال نمایید. به عنوان مثال اگر آن را بر روی root آپلود نمایید، تنظیمات آن به کل وب سایت اعمال خواهد شد و اگر آن را درون پوشه‌ای نظیر images/ آپلود نمایید، تنظیمات آن به پوشه images و زیرپوشه های آن اعمال خواهد شد.

نکته سوم: هر htaccess را می بایست درون یک خط تایپ نمایید. یعنی در انتهای هر د ستور، می بایست یک‌بار کلید Enter را فشار دهید.

نکته چهارم: به دلیل آنکه نحوه پیکربندی این فایل مانند پیکربندی فایل اصلی سرور (httpd.conf)است تصمیمات بر اساس شرایط اخذ می شود. البته تمامی امکانات httpd.conf را شامل نمی شود!

استفاده از این فایل در همه موارد پیشنهاد نمی شود زیرا امنیت وب سرور را تحت شعاع قرار می دهد. اما در مواقعی که سرور به صورت اشتراکی و اصطلاحا share شده خدمت رسانی می کند و تعداد زیادی سایت برروی آن قرار دارد پیشنهاد آن است که از فایل htaccess استفاده شود. زیرا هر سایت باید توانایی پیکر بندی قسمت مربوط به خود را دارا باشد.

دستوراتی که در یک فایل htaccess مورد استفاده قرار می گیرند، شامل فرامینی جهت کنترل موارد زیر هستند:

چند نکته :

اگر از وب سرور آپاچی برای وب سایت خود استفاده می‌کنید، دیگر نیازی نیست برای هر مشکل جزئی و کوچک، با هاست تان تماس بگیرید. با یادگیری قابلیت‌های مهم فایل .htaccess، می‌توانید کنترل کامل وب‌سایت خود را برعهده بگیرید.

در هنگام استفاده از فایل .htaccess، دانستن سه نکته از اهمیت به سزایی برخوردار است:

نکته اول: فایل .htaccess را می‌بایست به صورت ASCII آپلود کرده و مجوز دسترسی به آن را بر روی 644 (یا rw-r--r--) تنظیم نمایید.

نکته دوم: فایل .htaccess را می‌توانید به پوشه های مختلفی اعمال نمایید. به عنوان مثال اگر آن را بر روی root آپلود نمایید، تنظیمات آن به کل وب‌سایت اعمال خواهد شد و اگر آن را درون پوشه‌ای نظیر images/ آپلود نمایید، تنظیمات آن به پوشه images و زیرپوشه های آن اعمال خواهد شد.

نکته سوم: هر htaccess را می بایست درون یک خط تایپ نمایید. یعنی در انتهای هر دستور، می‌بایست یک‌بار کلید Enter را فشار دهید.

در میان تعداد زیاد ابزارهای مدیریت وب سایت، .Htaccess یکی از مهم ترین آن ها به شما می رود که با یک سری تغییرات ساده و د ستورنوی سی ها سریع می توانید د ستر سی به بسیاری از بخش های وب سایت خود را تغییر داده، نحوه ی آدرس دهی به آن ها را عوض کنید و بسیاری از کاراهای مفید و جذاب دیگر را روی وب سایت خود پیاده سازی کنید.

مهمترین بخش های این فایل و نحوه ی دستورنویسی

هر فردی که وب سایت خود را بر روی Apache قرار داده است، مطمئنا روزی به یک آموزش کامل و جامع در مورد کار با .Htaccess پیدا کرده است.

این فایل توانایی کار با هر گونه زبان تحت وب از PHP گرفته تا Ruby را نیز دارد.

چرا از .Htaccess استفاده کنیم؟

این یک سوال مهم ا ست که قبل از شروع کار باید به آن پا سخ داد که ممکن ا ست شما بعد از دیدن این سوال سریعا بپرسید اصلا یک فایل .Htaccess چیست و چه می کند؟

و من باید پاسخ بدهم که این یک فایل تنظیماتی مهم است که توسط سرور Apache مورد استفاده قرار می گیرد و می تواند به وب سرور بگوید که چگونه دستورات موجود در header های HTTP را هندل کند.

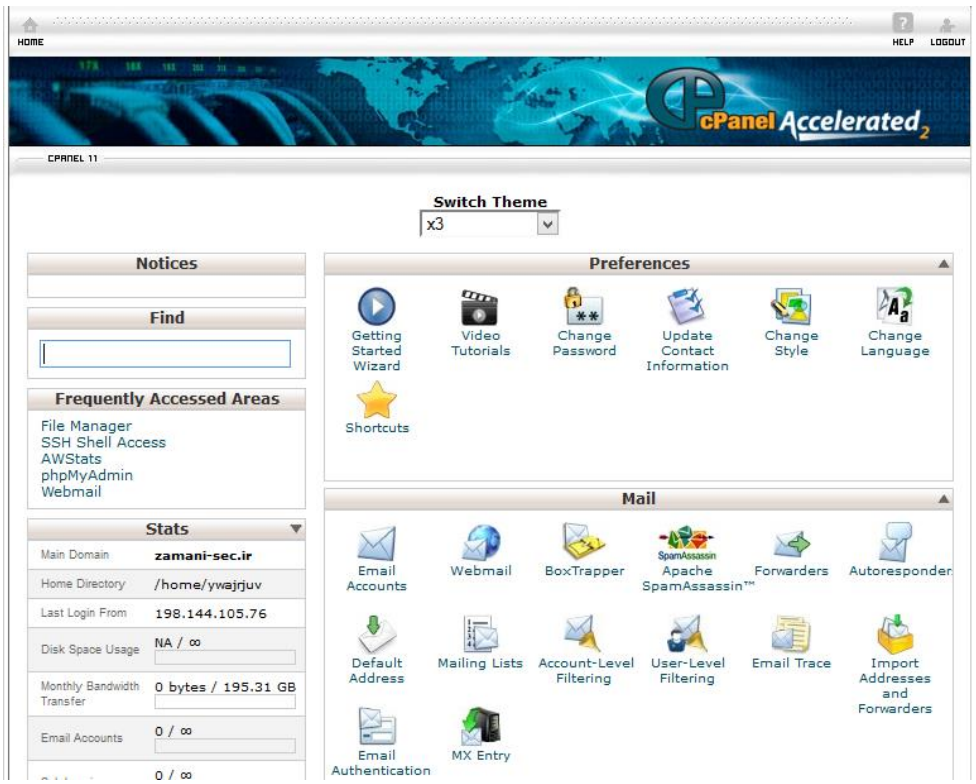
بزرگترین دلیل استفاده از این فایل بحث امنیت می باشد؛ شما می توانید با استفاده از فایل .Htaccess روی فایل های خود پسورد بگذارید، دسترسی به آن ها را محدود کنید، کاربر را به صفحات 404 بفرستید و...

در شروع باید نحوه دسترسی به فایل Htaccess را به شما آموزش دهم لذا مراحل زیر را انجام دهید

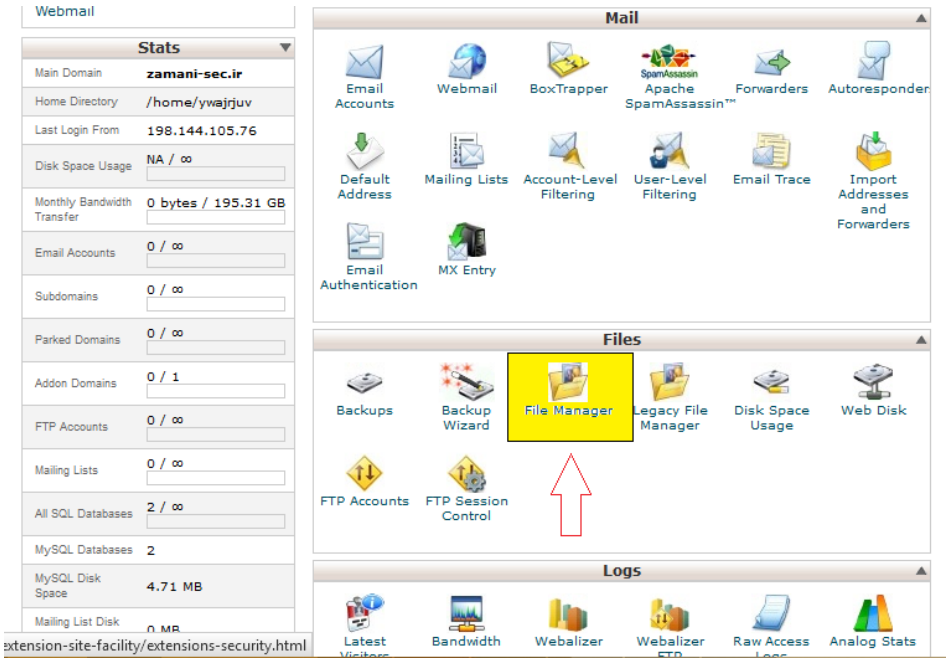
وارد سی پنل سایت خود شوید

http:// example.com/cpanel

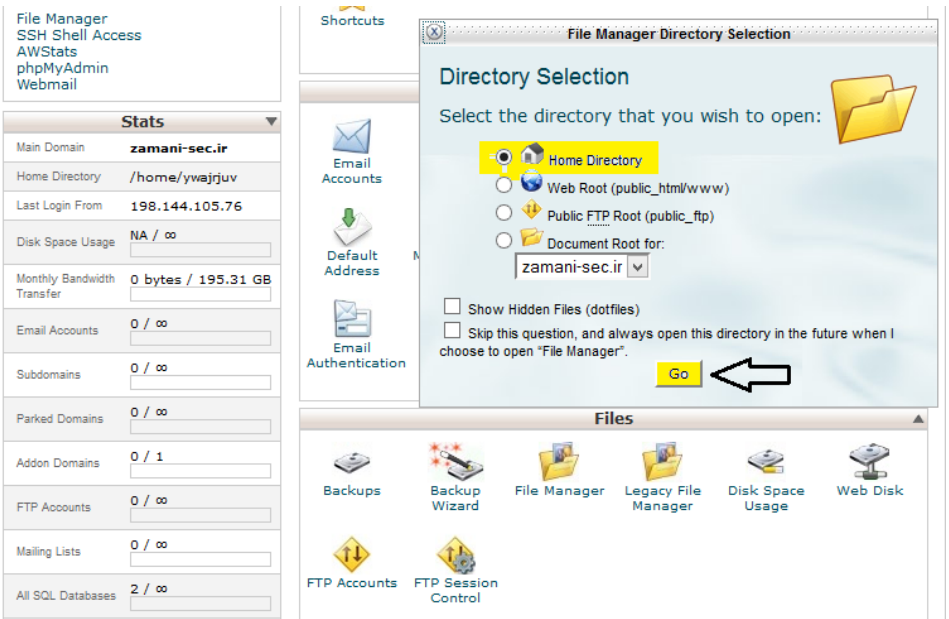
http:// example.com:2082



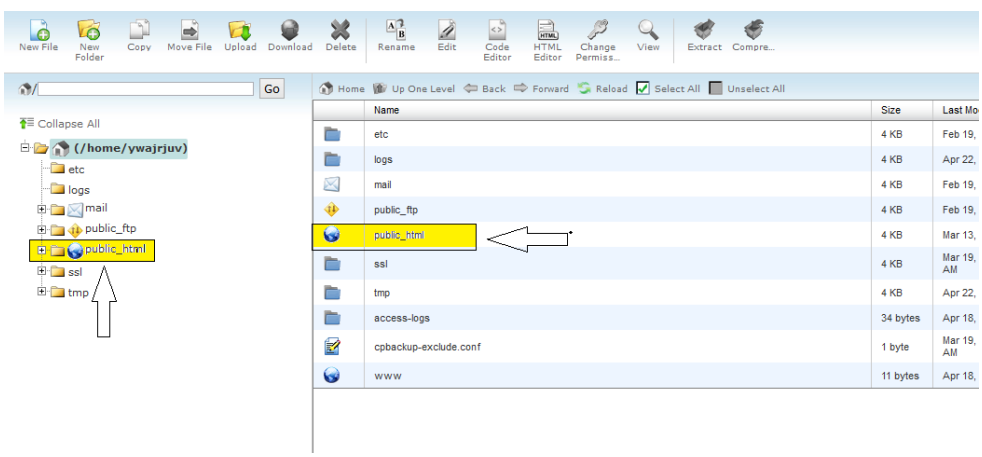
بر روی **File Manager** کلیک نمایید



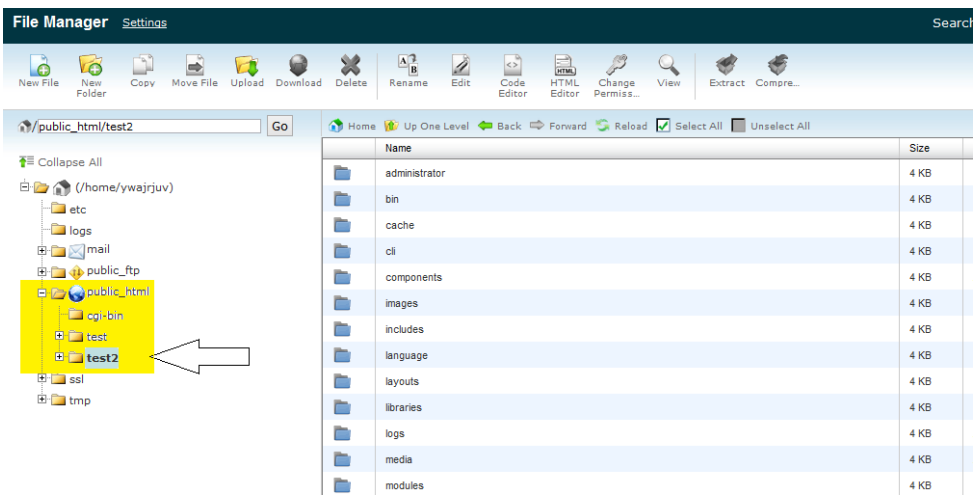
Home Directoryرا انتخاب نموده و بر روی GOکلیک نمایید



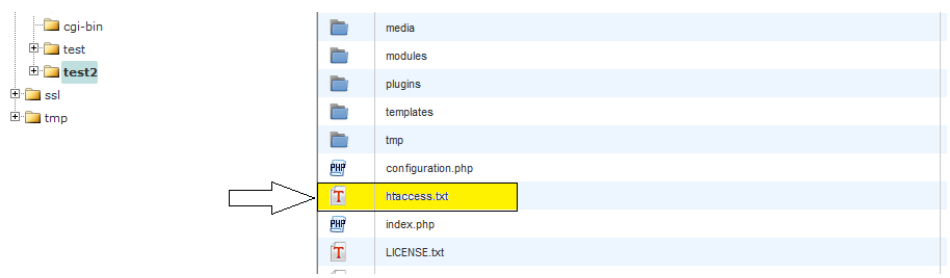
Public Html را انتخاب نمایید زیرا محل قرارگیری وب سایتها در این دایرکتوری می باشد



انتخاب وب سایتمان و ورود به دایرکتوری



و ایجاد فایل Htaccess.txt



و بعد از کانفیگ و اضـــافه نمودن دســـتورات نام فایل را به Htaccess. تغییر داده چون در سیستمهای لینوکسی نقطه قبل از اسم باعث مخفی شدن فایل خواهد شد.

و حالا وارد بحث آموزش نحوه ی دستورنویسی در این فایل می شویم، با ما همراه باشید:

جلوگیری از دسترسی به فایل htaccess

این کد دسترسی سایر کاربران را به فایل htaccess شما محدود خواهد کرد :

کد:

```
# secure htaccess file
<Files .htaccess>
  order allow,deny
   deny from all
   </Files>

prevent viewing of a specific file
   <Files secretfile.jpg>
   order allow,deny
   10deny from all
   </Files>
multiple file types
<FilesMatch ".(htaccess|htpasswd|ini|phps|fla|psd|log|sh"$>
```

```
Order Allow,Deny
Deny from all
</FilesMatch>
```

معرفی زبان پیشفرض (DefaultCharset) :

برای اینکه زبان پیشفرض استفاده شده رو به مرورگر ها بگین بیشتر وقتها اون رو در قسمت هدر کدهای سایت قرار میدین. با دستور کوتاه زیر به آپاچی میگیم که همیشه صفحات را با زبان خاصی ارسال کن. این عمل برای سئو سایت تاثیری خوبی داره.

```
#pass the default character set
AddDefaultCharset utf-8
```

روشن و آماده استفاده کردن mod_rewrite :

mod_rewrite را می توانید از درون فایل htaccess خود اجرا کنید برای اینکه ماژول mod_rewrite را آماده استفاده کنید

از کد زیر در فایل htaccess استفاده کنید. بهترین مکان برای قرار دادن این کد در همان سطر اول htaccess می باشد.

```
RewriteEngine on
```

فراموش نکنید که htaccess به بزرگی و کوچکی حروف حساس است

و اینکه این کد را در خط اول همه فایل های htaccess ای که در آن ها از mod_rewrite استفاده می کنید قرار دهید.

- حالت نمونه کد های mod_rewrite

حالت ساده و نمونه mod_rewrite بصورت زیر است

[p]
RewriteRule Pattern Substitution [Flag(s)]
[/p]

تنظیم Timezone

بعضـی اوقات، شـما از توابع date یا mktime در PHP اسـتفاده می کنید، پیغام خنده داری ممکن است به شما بدهد. این کد راه حل آن است. timezone را برای سرور خود ست می کنید. لیستی از timezone ها را می توانید در دیدن لینک ها برای شما امکان پذیر نیست. لطفا ثبت نام کنید یا وارد حساب خود شوید تا بتوانید لینک ها را ببینید.

مشاهده کنید.

کد:

SetEnv TZ Asia/Tehran

SEO Friendly

چرا SEO Friendly ؟ این روزها، همه موتورهای جستجوی مدرن قابلیت شناسایی 301 Permanent Redirect ها را دارند.

کد:

```
Redirect 301 <a>
href="http://www.datisdesign.com">http://www.datisdesign.com/</a>
/http://www.datisdesign.com
```

گذشتن از پیغام دانلود

کد:

```
AddType application/octet-stream .pdf
AddType application/octet-stream .zip
AddType application/octet-stream .mov
```

Skip WWW

یکی از نکات بهینه سازی برای موتورهای جستجو اطمینان از این نکته است که تنها یک آدرس است که به وب سایت شما اشاره می کند. بنابراین، شما نیاز دارید که همه ترافیک www را به سمت non-www ارجاع دهید و یا بالعکس :

کد:

```
RewriteEngine On RewriteBase /  RewriteCond %{HTTP_HOST}
^www.datisdesign.com [NC] RewriteRule ^(.*)$  http://datisdesign.com/$1
[L,R=301]
```

Cache Files

کش یعنی اینکه یه سری از فایلهای سایت شما که تغییراتی ندارن و یا در فوا صل زمانی زیاد دچار تغییرات قرار میگرن مشن رو در یک محفظه به نسبت امن در مرورگر کاربر ذخیره کنیم تا در دفعات

بعدی مراجعه به سایت این فایلها از خود سیستم اون بارگزاری بشن و در نهایت سرعت بارگزاری سایت خودمون رو چندین چند برابر کنیم.

کدی که در پاین قرار دادم کدی هست که من خودم دارم ازش استفاده میکنم و به مرور کامل شده و شما می تونید از هر بخش اون بنا به نیاز خودتون استفاده کنین :

```
 #BEGIN Expire headers
<ifModule mod_expires.c>
  ExpiresActive On
  ExpiresDefault "access plus 1 month"
  ExpiresByType image/x-icon "access plus 1 year"
  ExpiresByType image/jpeg "access plus 1 month"
  ExpiresByType image/png "access plus 1 month"
  ExpiresByType image/gif "access plus 1 month"
  ExpiresByType image/jpg "access plus 1 month"
  ExpiresByType application/x-shockwave-flash "access plus 1 month"
  ExpiresByType text/css "access plus 1 month"
  ExpiresByType text/javascript "access plus 1 year"
  ExpiresByType application/javascript "access plus 1 year"
  ExpiresByType application/x-javascript "access plus 1 year"
  ExpiresByType text/html "access plus 600 seconds"
  ExpiresByType application/xhtml+xml "access plus 600 seconds"
  ExpiresByType font/ttf "access plus 1 year"
  ExpiresByType font/woff "access plus 1 year"
</ifModule>

 #END Expire headers
 #BEGIN Cache-Control Headers
<ifModule mod_headers.c>
<"$<filesMatch "\.(ico|jpe?g|png|gif|swf|woff|ttf)
"Header set Cache-Control "max-age=2592000, public
<filesMatch/>
<"$filesMatch "\.(css)>
"Header set Cache-Control "max-age=2592000, public
<filesMatch/>
<"$filesMatch "\.(js)>
```

```
"Header set Cache-Control "max-age=2592000, private
<filesMatch/>
<"$filesMatch "\.(x?html?|php)>
"Header set Cache-Control "max-age=600, private, must-revalidate
<filesMatch/>
</ifModule>
 #END Cache-Control Headers

 #BEGIN Turn ETags Off
<ifModule mod_headers.c>
  Header unset ETag
</ifModule>
FileETag None
 #END Turn ETags Off

 #BEGIN Remove Last-Modified Header
<ifModule mod_headers.c>
  Header unset Last-Modified
</ifModule>
 #END Remove Last-Modified Header
```

غیرفعال کردن کش برای یکسری از فایلها

برای بعضی از فایلها هم میتوانید کش را غیرفعال کنید :

کد:

```
 #explicitly disable caching for  scripts and other dynamic files
<filesmatch>Header unset  Cache-Control </filesmatch>
```

یک انتقال ساده

اگر خوا ستید یه انتقال ساده از یک url به یک url دیگر دا شته با شید می توانید از کد زیر ا ستفاده کنید

[p]
RewriteRule ^fileone.html$ filetwo.html
[/p]

این کد باعث میشـــه که اگر ســـرور درخواســـتی در مورد بازکردن فایل fileone.html دریافت کرد فایل filetwo.html باز شود.

ممنوع ورود کردن یک آی پی خاص

اگر خواستید از ورود شخصی با آی پی خاص به وبسایتتان جلوگیری کنید می توانید از کد زیر استفاده کنید

$RewriteCond %{REMOTE_ADDR} ^(A.B.C.D)
RewriteRule ^/* http://www.domain.com/sorry.html [L]

بـه جـای A B C D اجـزای چـهـارگـانـه IP مـورد نـظـر رو وارد کـنـیـد و بـه جایhttp://www.domain.com/sorry.html آدرس مورد نظر که مثلا می تونه یک صـــفحه حاوی پیغام هشدار باشه رو وارد کنید

خلاص شدن از دست Query Strings

اگر بیشتر url ها در وبسایت شما چیزی مانند

http://www.domain.com/home.html?example=12345abcd

هست پس باید یه فکری برای نجات دادن خودتون بکنید چون در این صورت وبسایت شما بدرستی در سایت هایی نظیر گوگل ذخیره نمیشه و حتی کاربرانتون اگر بخوان آدرس یک صفحه رو توی ذهنشون داشته باشند تا جای دیگر از اون استفاده کنند این عمل براشون دشوار میشه . برای اینکه از دست اینجور آدرس ها خلاص شید از کد زیر استفاده کنید

```
RewriteCond %{QUERY_STRING} ^id=456&lid=789.* [NC]
RewriteRule (.*) http://www.domain.com/$1? [R=301]
```

با این کد نه تنها از دست query ه راحت میشید بلکه از دست اون علامت سوال هم را حت میشید .

این کار یه جنبه امنیتی هم داره و اون جلوگیری از هک شدن وبسایت از طریق sql injection هست .

دسترسی کاربران را بسته به دامنه آنها محدود کنید

کد:

```
#   1block visitors referred from indicated domains
  2IfModule mod_rewrite.c>
  3RewriteEngine on
  4RewriteCond %{HTTP_REFERER} scumbag.com [NC,OR]
  5RewriteCond %{HTTP_REFERER} wormhole.com [NC,OR]
  6RewriteRule .* - [F]
  7
 8ifModule>
```

ایجاد محدودیت در آپلود فایل :

با کد زیر حداکثر حجم فایل قابل آپلود رو ۲۰ مگابایت تنظیم کردیم.

```
php_value upload_max_filesize 20M
```

ایجاد محدودیت در حجم پست ارسالی :

با کد زیر میشه حداکثر حجم هر پست رو ۲ مگابایت تعیین کرد:

```
php_value post_max_size 2M
```

نمایش پیغام requast time در بازه زمانی مشخص:

requast time حداکثر زمانی درخواست فراخوانی یک صفحه هست :

```
php_value max_execution_time 200
```

حداکثر زمان دریافت اطلاعات POST و GET :

```
php_value max_input_time 250
```

فعال کردن قابلیت Gzip :

وقتی کاربری از طریق مروگر سایتش درخواست نمایش سایت شما رو میده این درخواست به سرور شما ارسال میشه و سرور فایلهایی که برای نمایش سایت شما لازم هست رو جمع میکنه و به مرورگر کاربر میفرسته و سایت شما نمایش داده میشه، ولی اگه از قابلیت Gzip استفاده کنید هنگام درخواست سرور فایلهای مورد نیاز رو به صورت فشرده در می یاره و این فایل فشرده رو به مرورگر ارسال میکنه و بعد از خارج شدن از حالت فشرده در سیستم کاربر سایت شما نمایش داده میشه. در حقیقت میزان حجمی که باید توسط مرورگر برای نمایش سایت شما دریافت شه کمتر میشه واین یعنی افزایش قابل توجه سرعت بارگزاری سایت. برای اینکه چک کنید که ها ست شما از این قابلیت پشتیبانی میکنه از این ابزار استفاده کنید. اگه پشتیبانی نمیکنه باید هاست رو عوض کنید و اگر پشتیبانی کرد کد زیر رو برای فعال شدنش روی سایت خودتون در فایل htaccess قرار بدین (این کدی هست که من برای سایت خودم استفاده میکنم شما میتونین پسوند های مورد نظر خودتون رو با پسوند های درج شده در اینجا تعویض کنین)

```
#BEGIN Compress text files
<ifModule mod_deflate.c>
 <filesMatch "\.(css|js|x?html?|php|woff|ttf|png|jpg|gif)"$>
 SetOutputFilter DEFLATE
</filesMatch>
</ifModule>
#END Compress text files
```

تصویر پیشفرض

با استفاده از این کد اگر یکی از تصاویر وبسایتتون دچار مشکلی شد و به هر دلیلی لود نشد تصویری که اینجا معرفی میکنید جایگزین اون میشه . با استفاده این کد ظاهری حرفه ای تر به وبسایتتون بدین

```
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule ^images/.*.jpg$ /images/default.jpg [L]
```

با جایگزین کردن images/default.jpg/ با آدرس تصـــویر پیشـــفرض و تغییر دادن /images و jpg. محـل تصـــــاویر و فرمـت تصـــــاویری رو کـه می خواهیـد در صـــورت اشـــکـال بـا images/default.jpg/ جایگزین بشه ، کد رو اختصاصی و آماده استفاده در سرور خودتون کنید

جلوگیری از hotlinking

سارقان مطلب و bandwidth با کپی کردن لینک فایل های درون سرور شما (مثالا تصاویر ، موزیک ها ، کلیپ های فلش و ...) به پیشرفت سایت خودشان کمک می کنند و به جای آن از پهنای باید شما استفاده می کنند که می تواند باعث کندی لود شدن صفحات سایت شما و یا حتی در برخی موارد تمام شدن پهنا باند ماهیانه شما بشه . برای اینکه جلوی این افراد رو بگیرید از کد زیر استفاده کنید .

```
$^! RewriteCond %{HTTP_REFERER}
RewriteCond %{HTTP_REFERER} !^http://(www.)?domain.com/ .*$ [NC]
RewriteRule .(gif|jpg|swf|flv|png)$ /feed/ [R=302,L]
```

در کد بالا domain.com رو با دامین سایت خودتون عوض کنید

منتقل کردن از چند دامین به یک دامین دیگر

```
$^! RewriteCond %{HTTP_REFERER}
RewriteCond %{HTTP_REFERER} !^http://(www.)?domain.com/ .*$ [NC]
```

RewriteRule .(gif|jpg|swf|flv|png)$ /feed/ [R=302,L]

اگر از چند دامین برای آدرس دهی با سایتتان ا ستفاده می کنید این امر ممکن ا ست که هر دو دامین را به یک دامین دیگر روی سرور بفرستید

فقط به جای http://www.domain.net و domain.net دو دامین خودتون رو بنویســـید و به جای http://domain.net آدرس جدید رو بنویسید

فراموش نکنید که :

* mod_rewrite از درون فایل htaccess اجرا می شود

* دستورات در فایل htaccess به حروف بزرگ و کوچک حساسند

* همیشه قبل از دست کاری فایل htaccess از اون نسخه پشتیبان تهیه کنید

اجازه دهی و جلوگیری از دسترسی ها

شما به سادگی با استفاده از این فایل می توانید از ورود آدرس آی پی های خاص به وب سایت خود جلوگیری کنید. دقت کنید که در آدرس های زیر، آدرس سوم بخش چهارم را ندارد و حتما می توانید حدس بزنید که چرا:

order allow,deny
deny from 255.0.0.0
.deny from 123.45.6
allow from all

جلوگیری از لیست کردن پوشه ها در مرورگر

ممکن است بعضی اوقات در وب سایت خود پوشه های بازی داشته باشید که تنظیم شده اند تا به صورت پیش فرض قابل مرور باشند. این بدین معناست که کاربر ها می توانند تمامی فایل های لیست شده در آن و ساختار کامل آن را توسط مرورگر خود مشاهده کنند، به عنوان مثال پوشه ی تصاویر و...

اما بعضی توسعه دهنده ها نمی خواهند چنین اتفاقی بیفتد و قصد جلوگیری از مرور پوشه های خود توسط دیگران را دارند.

خوشبختانه دستور مورد استفاده در چنین شرایطی بسیار ساده است:

```
1 Options -Indexes
```

این دستور را می توانید در فایل .Htaccess هر پوشه ای که قصد جلوگیری از مرور آن را دارید قرار دهید.

امن سازی با رمز عبور

یکی دیگر از کاربردهای استفاده از فایل .Htaccess را می توان قابلیت امن سازی بخش های خاصی از وب سایت دانست.

برای این کار می بایست فایلی را برای قرارگیری اطلاعات مربوط به ورود تولید کنید و آن را مورد استفاده قرار دهید، این کار باعث جلوگیری از بسیاری از حملات صورت گرفته به وب سایت شما خواهد شد.

یک نمونه از کدهای تولید شده را می توانید در این قسمت مشاهده کنید:

```
AuthType Basic
"AuthName "This Area is Password Protected
AuthUserFile /full/path/to/.htpasswd
Require valid-user
```

چند نکته در خصوص وردپرس

امن سازی وردپرس با استفاده از .Htaccess

پیشنهاد می کنم با استفاده از قواعد بخش قبل، دستورات زیر را برای امن سازی ورود به صفحه ی wp-login.php انجام دهید:

```
<Files wp-login.php>
Order Deny,Allow
Deny from All
Satisfy Any
"AuthName "Protected By AskApache
AuthUserFile /web/askapache.com/.htpasswda1
AuthType Basic
Require valid-user
<Files/>
```

بالا بردن امنیت فایل wp-config در htaccess :

برای جلوگیری از سرقت اطلاعات فایل حیاتی و جلوگیری از دسترسی به اطلاعات پایگاه داده سایت کد زیر رو در فایل قرار بدین

```
<files wp-config.php>
order allow,deny
deny from all
<files/>
```

افزایش امنیت محتوای فولدر wp-includes :

کافیه کد زیر رو در htaccess قرار بدین :

```
.Block the include-only files #
RewriteEngine On
```

```
/ RewriteBase
RewriteRule ^wp-admin/includes/ - [F,L]
RewriteRule !^wp-includes/ - [S=3]
RewriteRule ^wp-includes/[^/]+\.php$ - [F,L]
RewriteRule ^wp-includes/js/tinymce/langs/.+\.php - [F,L]
RewriteRule ^wp-includes/theme-compat/ - [F,L]
```

حل مشکل تعداد آیتم های فهرست وردپرس :

اگه دقت کرده با شین هنگام ساخت فهر ست د سته ها به صورت د ستی از یه جایی به بعد دیگه هر چی اضـــافه میکنین بعد ذخیره می بینین اضـــافه نشـــده برای حل این محدودیت کد زیر رو تو فایل htaccess قرار بدین :

```
<IfModule mod_php.c>
php_value suhosin.post.max_vars 7000
php_value suhosin.request.max_vars 7000
< / IfModule>
```

حذف category از آدرس وردپرسی شما :

شاید شما هم دو ست دا شته با شید کلمه /category/ رو از آدرس وردپر سی خودتون حذف کنید. این کار علاوه بر اینکه باعث جمع و جور شدن url شما میشه تاحدودی هم در سئو سایتتون موثر هســـت. البته با تغییر پیوند یکتای مربوط به category هم میشـــه که این کار رو افزونه های ســـئو برای شما انجام میدن و این کد رو محض یک راه حل بیرون از چهارچوب اصولی قرار دادم .

```
RewriteRule ^category/(.+)$ http://www.yourblog.com/$1 [R=301,L]
```

قواعد بازنویسی آدرس های HTTP

بازنویســـی قواعد آدرس های HTTP یکی از مهم ترین و پرکاربردترین اســـتفاده های .Htaccess محسوب می شود که امروزه بسیار مورد استفاده قرار می گیرد، به این مثال نگاهی بیندازید:

```
Options +FollowSymLinks
RewriteEngine On
/ RewriteBase

RewriteRule !\.(html|php)$ - [S=4]
RewriteRule ^([^_]*)_([^_]*)_([^_]*)_([^_]*)_(.*)$ $1-$2-$3-$4-$5
[E=uscor:Yes]
RewriteRule ^([^_]*)_([^_]*)_([^_]*)_(.*)$ $1-$2-$3-$4 [E=uscor:Yes]
RewriteRule ^([^_]*)_([^_]*)_(.*)$ $1-$2-$3 [E=uscor:Yes]
RewriteRule ^([^_]*)_(.*)$ $1-$2 [E=uscor:Yes]

$RewriteCond %{ENV:uscor} ^Yes
RewriteRule (.*) http://d.com/$1 [R=301,L]
```

دستور RewriteEngine و RewriteBase همیشه می توانند روی چنین مقادیر دقیقی تنظیم شود اما شما می بایست ابتدا RewriteEngine را فعال سازید.

روش های زیادی در اینترنت در مورد این موضوع که چگونه می توانید mod_rewrite را در سرور خود فعال سازید وجود دارند.

به نحو دستورات و ساختار آن ها دقت کنید، بعد از دریافت درخواست های HTTP، سریعا آدرس ها با این نحوها و عبارات منظم تطابق می یابند و کاربر را به صفحه ی مورد نظر هدایت می کنند.

دستوراتی مثل [R=301,L] دستورات مهمی هستند که به آن ها پرچم های بازنویسی گفته می شود و می توانید اطلاعات زیادی را در مورد آن ها در اینترنت پیدا کنید.

دستورات بالا ممکن است شما را کمی گیج کرده باشد اما نگران نباشید، من پیشنهاد می کنم نگاهی به این آدرس بیندازید تا به شما در تولید آدرس های مورد نظر کمک کند و همچنین اینجا نیز آموزش بسیار جالبی وجود دارد با یک مثال ساده که می توان به خوبی بازنویسی آدرس ها را با توجه به آن فراگرفت.

```
RewriteRule ^dir/([0-9]+)/?$ /index.php?id=$1 [L]
```

در یادگیری آن عجله نکنید، ممکن است یادگیری تمامی دستورات آن و مسلط شدن روی آن چندین ماه طول بکشد!

تعیین ایندکس و صفحه ی پیشفرض در یک پوشه

همانطور که احتمالا می دانید، Apache هنگام درخواست یک پوشه یا صفحه ی اصلی وب سایت، به سراغ فایل هایی مثل index.html، index.php و... می رود اما شما می تواند با استفاده از یک دستور ساده این موضوع را کمی اصلاح کنید و به ترتیب اولویت خود، فایل هایی که Apache باید به صورت پیش فرض در هر پوشه به دنبال آن ها بگردد را تعیین کنید:

```
1 DirectoryIndex index.html index.cgi index.php
```

اگر هاست شما از این فایل پشتیبانی میکند اما از SSI پشتیبانی نمیکند

کافیست خطوط زیر را وارد کنید تا از SSI هم پشتیبانی شود .

```
AddType text/html .shtml
AddHandler server-parsed .shtml
Options Indexed FollowSymLinks Includes
```

خط اول بیان میکند که کلیه فایل‌ها با پسوند shtml دارا صحت هستند

خط دوم یک handler اضافه میکند خط سوم باعث میشود سرور این فایل‌ها را اجرا کند .

بنابراین شما خودتان بدون نیاز به درخواست از ادمین سرور توانستید SSI را فعال کنید .

اگر هم دو ست دارید فایل‌های SSI بـ صورت جداگانه از فایل‌های html نبا شند میتوانید خطوط زیر را اضافه کنید :

```
AddType text/html .shtml .html . htm
AddHandler server-prased .shtml .html .htm
Options Indexes FollowSymLinks Includes
```

این خطوط باعث میشوند که کلیه فایل‌ها با پسوند html نیز به سرور برای اجرا شدن منتقل شوند

تا اگر کدی که برای SSI باشد داشته باشد را اجرا کند و سپس صفحه شروع به بارگذاری کند .

مجبورسازی برای دانلود فایل ها چندرسانه ای

مرورگر بسیاری از کاربران ممکن است قابلیت پخش بعضی فرمت های چندرسانه ای را به صورت مستقل داشته باشد اما شما شاید به دلایلی بخواهید از این موضوع جلوگیری کنید و کاربر را مجبور به دانلود چنین فرمت هایی کنید.

برای انجام این موضوع می توانید از دستور ساده ی زیر استفاده کرده و فرمت های مدنظر خود را نیز به آن ها اضافه کنید:

```
1  AddType application/octet-stream .zip .mp3 .mp4
```

سندهای خطای شخصی سازی شده

احتمالا در بسیاری از وب سایت ها با صفحات شخصی سازی شده ی 404 و... مواجه شده اید و پرسیده اید که چگونه می توان چنین صفحاتی را طراحی کرد؟

پاسخ این سوال واقعا ساده است.

با نگاهی به دستورات زیر پاسخ خود را خواهید گرفت:

```
ErrorDocument 100 /100_CONTINUE
ErrorDocument 101 /101_SWITCHING_PROTOCOLS
ErrorDocument 102 /102_PROCESSING
ErrorDocument 200 /200_OK
ErrorDocument 201 /201_CREATED
ErrorDocument 202 /202_ACCEPTED
ErrorDocument 203 /203_NON_AUTHORITATIVE
ErrorDocument 204 /204_NO_CONTENT
ErrorDocument 205 /205_RESET_CONTENT
ErrorDocument 206 /206_PARTIAL_CONTENT
ErrorDocument 207 /207_MULTI_STATUS
ErrorDocument 300 /300_MULTIPLE_CHOICES
ErrorDocument 301 /301_MOVED_PERMANENTLY
ErrorDocument 302 /302_MOVED_TEMPORARILY
ErrorDocument 303 /303_SEE_OTHER
ErrorDocument 304 /304_NOT_MODIFIED
ErrorDocument 305 /305_USE_PROXY
ErrorDocument 307 /307_TEMPORARY_REDIRECT
ErrorDocument 400 /400_BAD_REQUEST
ErrorDocument 401 /401_UNAUTHORIZED
ErrorDocument 402 /402_PAYMENT_REQUIRED
ErrorDocument 403 /403_FORBIDDEN
ErrorDocument 404 /404_NOT_FOUND

ErrorDocument 405 /405_METHOD_NOT_ALLOWED
ErrorDocument 406 /406_NOT_ACCEPTABLE
ErrorDocument 407 /407_PROXY_AUTHENTICATION_REQUIRED
ErrorDocument 408 /408_REQUEST_TIME_OUT
ErrorDocument 409 /409_CONFLICT
ErrorDocument 410 /410_GONE
ErrorDocument 411 /411_LENGTH_REQUIRED
ErrorDocument 412 /412_PRECONDITION_FAILED
ErrorDocument 413 /413_REQUEST_ENTITY_TOO_LARGE
```

```
ErrorDocument 414 /414_REQUEST_URI_TOO_LARGE
ErrorDocument 415 /415_UNSUPPORTED_MEDIA_TYPE
ErrorDocument 416 /416_RANGE_NOT_SATISFIABLE
ErrorDocument 417 /417_EXPECTATION_FAILED
ErrorDocument 422 /422_UNPROCESSABLE_ENTITY
ErrorDocument 423 /423_LOCKED
ErrorDocument 424 /424_FAILED_DEPENDENCY
ErrorDocument 426 /426_UPGRADE_REQUIRED
ErrorDocument 500 /500_INTERNAL_SERVER_ERROR
ErrorDocument 501 /501_NOT_IMPLEMENTED
ErrorDocument 502 /502_BAD_GATEWAY
ErrorDocument 503 /503_SERVICE_UNAVAILABLE
ErrorDocument 504 /504_GATEWAY_TIME_OUT
ErrorDocument 505 /505_VERSION_NOT_SUPPORTED
ErrorDocument 506 /506_VARIANT_ALSO_VARIES
ErrorDocument 507 /507_INSUFFICIENT_STORAGE
ErrorDocument 510 /510_NOT_EXTENDED
```

جلوگیری از حملات وب

کد htaccess جلوگیری از حملات dos

برای جلوگیری از بازدید fake و ربات ها بر روی وبسایتتان کد زیر را به انتهای htaccess هاست خود بیافزایید

```
SetEnvIfNoCase User-Agent .* allowed_agent
Order Deny,Allow
Deny from All
Allow from env=allowed_agent
```

جلوگیری از اسکن سایت توسط اسکنر ها

برای جلوگیری از اسکن سایت توسط اسکنر ها میتوانید با ایجاد یک فایل htaccess. و قرار دادن کد های زیر ، مانع اسکن سایت توسط این اسکنر ها شوید.

```
RewriteEngine On
<IfModule mod_rewrite.c>
[RewriteCond %{HTTP_USER_AGENT} ^w3af.sourceforge.net [NC,OR
[RewriteCond %{HTTP_USER_AGENT} dirbuster [NC,OR
[RewriteCond %{HTTP_USER_AGENT} nikto [NC,OR
[RewriteCond %{HTTP_USER_AGENT} SF [OR
[RewriteCond %{HTTP_USER_AGENT} sqlmap [NC,OR
[RewriteCond %{HTTP_USER_AGENT} fimap [NC,OR
[RewriteCond %{HTTP_USER_AGENT} nessus [NC,OR
[RewriteCond %{HTTP_USER_AGENT} whatweb [NC,OR
[RewriteCond %{HTTP_USER_AGENT} Openvas [NC,OR
[RewriteCond %{HTTP_USER_AGENT} jbrofuzz [NC,OR
[RewriteCond %{HTTP_USER_AGENT} libwhisker [NC,OR
[RewriteCond %{HTTP_USER_AGENT} webshag [NC,OR
RewriteCond %{HTTP:Acunetix-Product} ^WVS
[RewriteRule ^.* http://127.0.0.1/ [R=301,L
<IfModule/>
```

کد .htaccess؛ جلوگیری از حملات SQL Injection

کد .htaccess زیر از حملات SQL Injection تا حد زیادی جلوگیری می‌نماید و از خطر در امان خواهید بود (تقریباً)

```
RewriteEngine On
Options +FollowSymLinks
ServerSignature Off

RewriteCond %{REQUEST_METHOD}
^(HEAD|TRACE|DELETE|TRACK) [NC,OR]
RewriteCond %{THE_REQUEST} ^.*(\\r|\\n|%0A|%0D).* [NC,OR]

RewriteCond %{HTTP_REFERER}
^(.*)(<|>|'|%0A|%0D|%27|%3C|%3E|).* [NC,OR]
RewriteCond %{HTTP_COOKIE} ^.*(<|>|'|%0A|%0D|%27|%3C|%3E|).*
[NC,OR]
RewriteCond %{REQUEST_URI} ^/(,|;|:|<|>|">|"<|/|\\\.\.\\).{0,9999}.*
[NC,OR]

RewriteCond %{HTTP_USER_AGENT} ^$ [OR]
RewriteCond %{HTTP_USER_AGENT} ^(java|curl|wget).* [NC,OR]
RewriteCond %{HTTP_USER_AGENT}
^.*(winhttp|HTTrack|clshttp|archiver|loader|email|harvest|extract|grab|miner
).* [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^.*(libwww-
perl|curl|wget|python|nikto|scan).* [NC,OR]
RewriteCond %{HTTP_USER_AGENT}
^.*(<|>|'|%0A|%0D|%27|%3C|%3E|).* [NC,OR]

RewriteCond %{QUERY_STRING}
^.*(;|<|>|'|"|\)|%0A|%0D|%22|%27|%3C|%3E|).*(/\*|union|select|insert|cast|s
et|declare|drop|update|md5|benchmark).* [NC,OR

RewriteCond %{QUERY_STRING} ^.*(localhost|loopback|127\.0\.0\.1).*
[NC,OR]
```

```
RewriteCond %{QUERY_STRING} ^.*\.[A-Za-z0-9].* [NC,OR]#
RewriteCond %{QUERY_STRING}
^.*(<|>|'|%0A|%0D|%27|%3C|%3E|).* [NC]
RewriteRule ^(.*)$ sqlinj.cfm
```

اگر کسی قصد هک کردن وب‌سایت شما را داشته باشید با پیج sqlinj.cfm رو به رو می‌شود. شما می‌توانید یک اسم‌دیگر برای این پیج انتخاب کنید.

از این به بعد در زمینه .htaccess بیشتر پست می‌گذارم

ضمناً این کد جلوی نرم افزار httrack عزیز را هم می‌گیرد و نمی‌گذارد قالب شما را با جاش بردارد!

جلوگیری از حملات تزریق کد (SQL INJECTION) به وسیله htaccess

همونطور که میدونید حملات تزریق کد به علت نقص امنیتی در پایگاه داده معمولا به وجود میاد که البته دیگه با پیشرفت و افزایش امنیت و اصول طراحی استاندارد سایت دیگه این باگ از بین میره.

و امکان هک شـــدن از این طریف نزدیک صـــفر میشـــه اما یک کد قرار میدم که با قرار دادنش در htaccess تا حد خیلی زیادی از حملات sql injection در امان خواهید بود

و در صورتی که کسی بخواد با این روش شما رو هک کنه با صفحه hack.cfm روبرو میشه.

که این صفحه رو خود شما باید طراحی کنید و در هاستتون قرار بدین.

از این کد در سیستم های مدیریت محتوا مثل : وردپرس-جوملا-نیوک-دروپال و انجمن ها و چت روم میشه استفاده کرد

درون فایل htaccess این کد رو قرار بدین :

کد:

```
RewriteEngine On

Options +FollowSymLinks

ServerSignature Off

RewriteCond %{REQUEST_METHOD} ^(HEAD|TRACE|DELETE|TRACK) [NC,OR]

RewriteCond %{THE_REQUEST} ^.*(\\r|\\n|%0A|%0D).* [NC,OR]

RewriteCond %{HTTP_REFERER} ^(.*)(<|>|'|%0A|%0D|%27|%3C|%3E|).* [NC,OR]

RewriteCond %{HTTP_COOKIE} ^.*(<|>|'|%0A|%0D|%27|%3C|%3E|).* [NC,OR]

RewriteCond %{REQUEST_URI} ^/(,|;|:|<|>|">|"<|/|\\\.\.\\).{0,9999}.* [NC,OR]

RewriteCond %{HTTP_USER_AGENT} ^$ [OR]

RewriteCond %{HTTP_USER_AGENT} ^(java|curl|wget).* [NC,OR]
```

```
RewriteCond %{HTTP_USER_AGENT}
^.*(winhttp|HTTrack|clshttp|archiver|loader|email|harvest|extract|grab|miner
).* [NC,OR]

RewriteCond %{HTTP_USER_AGENT} ^.*(libwww-
perl|curl|wget|python|nikto|scan).* [NC,OR]

RewriteCond %{HTTP_USER_AGENT}
^.*(<|>|'|%0A|%0D|%27|%3C|%3E|).* [NC,OR]

RewriteCond %{QUERY_STRING}
^.*(;|<|>|'|"|\)|%0A|%0D|%22|%27|%3C|%3E|).*(/\*|union|select|insert|cast|s
et|declare|drop|update|md5|benchmark).* [NC,OR

RewriteCond %{QUERY_STRING} ^.*(localhost|loopback|127\.0\.0\.1).*
[NC,OR]

RewriteCond %{QUERY_STRING} ^.*\.[A-Za-z0-9].* [NC,OR]#

RewriteCond %{QUERY_STRING} ^.*(<|>|'|%0A|%0D|%27|%3C|%3E|).*
[NC]

RewriteRule ^(.*)$ hack.cfm
```

عوض کردن ایندکس فولدری خاص

اکثر میزبانهای وب فایلی که وظیفه لود شدن در هنگام باز کردن دایرکتوری خاصی را دارد

با نام index قرار میدهند که با استفاده از htaccess میتوانید انرا عوض کنید . خط زیر را به فایل اضافه کنید :

DirectoryIndex filename.html

حتما دیده اید که اگر فایل index.html در دایرکتوری نبود سرور فایل دیگری مثلا index.php را اجرا میکند

روش به اینصورت است که در دستور فوق بعد از filename.html با یک فضای خالی نام‌های دیگر را وارد میکنید .

بنابراین سرور در دایرکتوری ویژه ابتدا به دنبال فایل اولی و سپس به دنبال فایل دومی و به همین ترتیب جستجو میکند .

اگر هم هیچ یک از فایل‌ها پیدا نشد پیغام خطای ٤٠٤ ظاهر میشود .

Redirec توسط htaccess

حتما میدانید که راههای زیادی برای ریدایرکت کردن فایلی خاص به فایل دیگر وجود دارد اما بهترین کار همین است که میگویم

در فایل خط زیر را وارد کنید :

Redirect /OldDir/OldFile.html http://www.domainname.com/newdir

بنابراین دستور به شرح زیر است

Redirect oldlocation newlocation

منتهی یادتان باشد که newlocation باید نام ادرس کامل سایت باشد .

دسترسی کاربران را بسته به User-Agent Header محدود کنید

این روش می تواند در مصرف پهنای باند شما صرفه جویی کند، جلوی بعضی از botها و spider ها را می گیرد :

کد:

```
#block visitors referred from indicated domains
<IfModule mod_rewrite.c>
SetEnvIfNoCase ^User-Agent$
.*(craftbot|download|extract|stripper|sucker|ninja|clshttp|webspider|leache
r|col lector|grabber|webpictures) HTTP_SAFE_BADBOT
SetEnvIfNoCase ^User-Agent$ .*(libwww-perl|aesop_com_spiderman)
HTTP_SAFE_BADBOT
Deny from env=HTTP_SAFE_BADBOT
```

</ifModule>

مسدود کردن مرورگر های آفلاین و روبات های بد !

مرورگرهای آفلاین نرم افزاری با سرعت بالا برای گرفتن اطلاعات از اینترنت است. این برنامه به شما امکان دریافت کامل اطلاعات یک سایت را به صورت طبقه بندی شده می دهد !!!

روبات های بد یا همون Bad Robots هم اسپایدر هایی هستن که باعث خرابکاری می شن و خلاصه برای سایتتون مفید نیستند !

شما می تونید به وسیله ی کد هایی که در پایین بهتون می دم از این ها جلوگیری کنید و به نوعی شر مزاحم های سایت خودتون رو کم کنید !!!

به روت سایت خود رفته و httaccess رو باز کنید !

دقت کنید شاید این فایل مخفی شده باشد .

این کد ها رو در آخرش اضافه کنید !

کد:

```
RewriteEngine On
RewriteCond %{HTTP_USER_AGENT} ^BlackWidow [OR]
RewriteCond %{HTTP_USER_AGENT} ^Bot\ mailto:craftbot@yahoo.com
[OR]
RewriteCond %{HTTP_USER_AGENT} ^ChinaClaw [OR]
```

```
RewriteCond %{HTTP_USER_AGENT} ^Custo [OR]
RewriteCond %{HTTP_USER_AGENT} ^DISCo [OR]
RewriteCond %{HTTP_USER_AGENT} ^Download\ Demon [OR]
RewriteCond %{HTTP_USER_AGENT} ^eCatch [OR]
RewriteCond %{HTTP_USER_AGENT} ^EirGrabber [OR]
RewriteCond %{HTTP_USER_AGENT} ^EmailSiphon [OR]
RewriteCond %{HTTP_USER_AGENT} ^EmailWolf [OR]
RewriteCond %{HTTP_USER_AGENT} ^Express\ WebPictures [OR]
RewriteCond %{HTTP_USER_AGENT} ^ExtractorPro [OR]
RewriteCond %{HTTP_USER_AGENT} ^EyeNetIE [OR]
RewriteCond %{HTTP_USER_AGENT} ^FlashGet [OR]
RewriteCond %{HTTP_USER_AGENT} ^GetRight [OR]
RewriteCond %{HTTP_USER_AGENT} ^GetWeb! [OR]
RewriteCond %{HTTP_USER_AGENT} ^Go!Zilla [OR]
RewriteCond %{HTTP_USER_AGENT} ^Go-Ahead-Got-It [OR]
RewriteCond %{HTTP_USER_AGENT} ^GrabNet [OR]
RewriteCond %{HTTP_USER_AGENT} ^Grafula [OR]
RewriteCond %{HTTP_USER_AGENT} ^HMView [OR]
RewriteCond %{HTTP_USER_AGENT} HTTrack [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Image\ Stripper [OR]
RewriteCond %{HTTP_USER_AGENT} ^Image\ Sucker [OR]
RewriteCond %{HTTP_USER_AGENT} Indy\ Library [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^InterGET [OR]
RewriteCond %{HTTP_USER_AGENT} ^Internet\ Ninja [OR]
RewriteCond %{HTTP_USER_AGENT} ^JetCar [OR]
RewriteCond %{HTTP_USER_AGENT} ^JOC\ Web\ Spider [OR]
RewriteCond %{HTTP_USER_AGENT} ^larbin [OR]
RewriteCond %{HTTP_USER_AGENT} ^LeechFTP [OR]
RewriteCond %{HTTP_USER_AGENT} ^Mass\ Downloader [OR]
RewriteCond %{HTTP_USER_AGENT} ^MIDown\ tool [OR]
RewriteCond %{HTTP_USER_AGENT} ^Mister\ PiX [OR]
RewriteCond %{HTTP_USER_AGENT} ^Navroad [OR]
RewriteCond %{HTTP_USER_AGENT} ^NearSite [OR]
RewriteCond %{HTTP_USER_AGENT} ^NetAnts [OR]
RewriteCond %{HTTP_USER_AGENT} ^NetSpider [OR]
RewriteCond %{HTTP_USER_AGENT} ^Net\ Vampire [OR]
```

```
RewriteCond %{HTTP_USER_AGENT} ^NetZIP [OR]
RewriteCond %{HTTP_USER_AGENT} ^Octopus [OR]
RewriteCond %{HTTP_USER_AGENT} ^Offline\ Explorer [OR]
RewriteCond %{HTTP_USER_AGENT} ^Offline\ Navigator [OR]
RewriteCond %{HTTP_USER_AGENT} ^PageGrabber [OR]
RewriteCond %{HTTP_USER_AGENT} ^Papa\ Foto [OR]
RewriteCond %{HTTP_USER_AGENT} ^pavuk [OR]
RewriteCond %{HTTP_USER_AGENT} ^pcBrowser [OR]
RewriteCond %{HTTP_USER_AGENT} ^RealDownload [OR]
RewriteCond %{HTTP_USER_AGENT} ^ReGet [OR]
RewriteCond %{HTTP_USER_AGENT} ^SiteSnagger [OR]
RewriteCond %{HTTP_USER_AGENT} ^SmartDownload [OR]
RewriteCond %{HTTP_USER_AGENT} ^SuperBot [OR]
RewriteCond %{HTTP_USER_AGENT} ^SuperHTTP [OR]
RewriteCond %{HTTP_USER_AGENT} ^Surfbot [OR]
RewriteCond %{HTTP_USER_AGENT} ^tAkeOut [OR]
RewriteCond %{HTTP_USER_AGENT} ^Teleport\ Pro [OR]
RewriteCond %{HTTP_USER_AGENT} ^VoidEYE [OR]
RewriteCond %{HTTP_USER_AGENT} ^Web\ Image\ Collector [OR]
RewriteCond %{HTTP_USER_AGENT} ^Web\ Sucker [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebAuto [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebCopier [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebFetch [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebGo\ IS [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebLeacher [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebReaper [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebSauger [OR]
RewriteCond %{HTTP_USER_AGENT} ^Website\ eXtractor [OR]
RewriteCond %{HTTP_USER_AGENT} ^Website\ Quester [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebStripper [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebWhacker [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebZIP [OR]
RewriteCond %{HTTP_USER_AGENT} ^Wget [OR]
RewriteCond %{HTTP_USER_AGENT} ^Widow [OR]
RewriteCond %{HTTP_USER_AGENT} ^WWWOFFLE [OR]
RewriteCond %{HTTP_USER_AGENT} ^Xaldon\ WebSpider [OR]
```

```
RewriteCond %{HTTP_USER_AGENT} ^Zeus
RewriteRule ^.* - [F,L]
```

جلوگیری از اجرای فایل در پوشه های با پرمیژن (دسترسی) 777

اگه در سایتتون یک پوشه داشتید که پرم 777 بود و میخواید جلوی خطر احتمالی رو بگیرید

یک .htaccess باز کنید و توش اینو بزنید .

کد PHP:

```
AddHandler cgi-script .php .pl .py .jsp .asp .htm .shtml .sh .cgi .html Options
-ExecCGI
```

جلوگیری از حملات LFI

حدود ۷۰ تا ۸۰ درصد از وبسایت ها مقابل حملات LFI آسیب پذیر هستند، هکر ها از این حفره جهت بهره برداری و گرفتن shell استفاده میکنند، شما میتوانید از طریق .htaccess وبسایت خود را مقابل این حملات ایمن سازی کنید.

در زیر میتوانید یک نمونه از کد php آسیب پذیر در مقابل حملات LFI را مشاهده کنید:

کد:

```
<php?>
LFI Vulnerable Code //
;redirect = $_GET[redirect]$
;include($redirect)
<?
```

کد زیر زیر به لطف ارائه SigSiu.net میتواند شما را مقابل این حملات ایمن کند.

کد:

```
##########Begin - File injection protection, by SigSiu.net
RewriteCond %{REQUEST_METHOD} GET
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=http:// [OR]
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=(\.\.//?)+ [OR]
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=/([a-z0-9_.]//?)+ [NC]
RewriteRule .* - [F]
End - File injection protection ##########
```

در ادامه کد بالا (لوگکت) ممکن است بخواهد از URL encoding بجای http:// استفاده کنید، بدین جهت کد زیر را در خط دوم کد بالا جایگزین کنید:

کد:

```
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=http%3A%2F%2F [OR]
```

افزودن کد زیر به فایل .htaccess میتواند چند لایه امنیتی در مقابل حملاتی که با استفاده از proc/self/environ method نفوذ پذیری را ممکن میکنند (لوگکت) اضافه کند:

کد:

```
#proc/self/environ? no way!
```

RewriteCond %{QUERY_STRING} proc\/self\/environ [NC,OR]

-

کد زیر میتواند از شما در مقابل Apache HTTP Server CVE-2011-3192 Denial Of Service Vulnerability که نخستین بار در August 2011 کشف شد محافظ کند، البته این کد مخصوص کسانیست که امکان به روز رسانی سرور خود را ندارند، اگر از نسخه به روز تر از این تاریخ میزبانی میشوید، اجرای این کد لزومی ندارد.

کد:

```
#drop Range header when more than 5 ranges
#CVE-2011-3192
SetEnvIf Range (,.*?){5,} bad-range=1
RequestHeader unset Range env=bad-range
.#optional logging
#CustomLog insert-path-and-name-of-log common env=bad-range
```

- استفاده از x-frame یکی از غیر اصولی ترین و خطرناک ترین کد هاییست که شما میتوانید بر روی وبسایت خود اجرا کند و یا اگر از سیستم های مدیریت محتوا استفاده میکنید به کاربران خود اجازه دهید تا از این کد استفاده کنند، قصد آموزش اینکه این کد چطور میتواند حفره ای برای نفوذ با شد را در این مقاله نداریم و صرفا به شما آموزش میدهیم که چطور میتوانید از اجرا شدن این کد با اسفاده از .htaccess جلوگیری کنید:

کد:

```
# Don't allow any pages to be framed - Defends against CSRF
Header set X-Frame-Options DENY
```

در ادامه کد بالا که اجرای کد x-frame را غیر فعال میکند، متوانید به جای DENY از SAMEORIGIN جهت اجازه دادن کد x-frame ی که تنها از سایت خودتان اجرا میشود، استفاده کنید.

بدین ترتیب تنها صفحات داخلی وبسایت شما اجازه قرار گرفتن در کد x-frame را خواهند داشت.

در نسـخه های ۸ و ۹ مرورگر اینترنت اکسـپلورر با اسـتفاده از کد زیر از cross site scripting محافظت کنید.

توجه: ا ستفاده از این کد ممکن ا ست کارایی برخی از وب سایت ها را مختل کند، اگر این م شکل برای شما پیش آمد کافیست تا مقدار 1 را به 0 تغییر دهید.

کد:

```
#Turn on IE8-IE9 XSS prevention tools
"Header set X-XSS-Protection "1; mode=block
```

Content Security Policy –

یک لایه افزوده شده امنیت ایست که میتواند شما را در مقابل حملاتی نظیر Cross Site Scripting و data injection ایمن کند، کد زیر اجرای جاوا کد های خارجی را محدود میکند و اجازه اجرا را به آنها نمیدهد، اما اگر در وبسایت خود از سرویسهای نظیر Google Analytics ا ستفاده میکنید این کد جلوی کارایی آن را میگیرد چرا که اسـتفاده از اینگونه سـرویسـها مسـتلزم اجرای جاوا کد میباشد.

کد:

```
.Only allow JavaScript from the same domain to be run #
.Don't allow inline JavaScript to run #
";'Header set X-Content-Security-Policy "allow 'self
```

کد زیر جلوی کاراکترهای غیر استاندارد را خواهد گرفت و این عمل میتواند شما در مقابل حملاتی که با درخواست HTTP نفوذ پذیری را ممکن میکند ایمن کند.

کد:

```
#Prevent use of specified methods in HTTP Request
RewriteCond %{REQUEST_METHOD} ^(HEAD|TRACE|DELETE|TRACK)
[NC,OR]
```

```
#Block out use of illegal or unsafe characters in the HTTP Request
RewriteCond %{THE_REQUEST} ^.*(\\r|\\n|%0A|%0D).* [NC,OR]
#Block out use of illegal or unsafe characters in the Referer Variable of the
HTTP Request
RewriteCond %{HTTP_REFERER}
^(.*)(<|>|'|%0A|%0D|%27|%3C|%3E|%00).* [NC,OR]
#Block out use of illegal or unsafe characters in any cookie associated with
the HTTP Request
RewriteCond %{HTTP_COOKIE} ^.*(<|>|'|%0A|%0D|%27|%3C|%3E|%00).*
[NC,OR]
#Block out use of illegal characters in URI or use of malformed URI
RewriteCond %{REQUEST_URI} ^/(,|;|:|<|>|">|"<|/|\\\.\.\\).{0,9999}.*
[NC,OR]
#Block out  use of empty User Agent Strings
#NOTE - disable this rule if your site is integrated with Payment Gateways
such as PayPal
RewriteCond %{HTTP_USER_AGENT} ^$ [OR]
#Block out  use of illegal or unsafe characters in the User Agent variable
RewriteCond %{HTTP_USER_AGENT}
^.*(<|>|'|%0A|%0D|%27|%3C|%3E|%00).* [NC,OR]
#Measures to block out  SQL injection attacks
RewriteCond %{QUERY_STRING}
^.*(;|<|>|'|"|\)|%0A|%0D|%22|%27|%3C|%3E|%00).*(/\*|union|select|insert|c
[ast|set|declare|drop|update|md5|benchmark).* [NC,OR

#Block out  reference to localhost/loopback/127.0.0.1 in the Query String
RewriteCond %{QUERY_STRING} ^.*(localhost|loopback|127\.0\.0\.1).*
[NC,OR]
#Block out  use of illegal or unsafe characters in the Query String variable
RewriteCond %{QUERY_STRING}
^.*(<|>|'|%0A|%0D|%27|%3C|%3E|%00).* [NC]
```

کد .htaccess غیر فعال کردن TRACE and TRACK

TRACE and TRACK یک روش درخواست هست که باعث میشه اطلاعاتی که از طرف client یا کاربر به ibm http server ارسال میشه ، مجددا به client برگردانده میشه یک مثال ساده :

$telnet 127.0.0.1 8080 Trying... Connected to 127.0.0.1. Escape character is '^]'. TRACE / HTTP/1.0 Host: foo A: b C: d HTTP/1.1 200 OK Date: Mon, 04 Oct 2004 14:07:59 GMT Server: IBM_HTTP_SERVER Connection: close Content-Type: message/http TRACE / HTTP/1.0 A: b C: d Host: foo .Connection closed

#disable TRACE and TRACK in the main scope of httpd.conf RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* – [F] RewriteCond %{REQUEST_METHOD} ^TRACK RewriteRule .* – [F] … <VirtualHost www.example.com> … # disable TRACE and TRACK in the www.example.com virtual host RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* – [F] RewriteCond %{REQUEST_METHOD} ^TRACK RewriteRule .* – [F] # </VirtualHost>

مجبور کردن مرور گر برای تغییر مسیر از HTTP به https

در حالت عادی آدرس سایت شما http://www.yoursite.com هست یعنی بدون رمزنگاری اطلاعات ما بین کاربر و سرور و با پورت 80 سایت بالا میاد

وقتی شما مجوز SSL یا secure locket layer رو از یکی از شرکت های ارائه دهنده ssl میخرید(اس اس ال امکان رمز نگاری اطلاعات رد و بدل شده بین کاربر و سرور رو میده جهت افزایش امنیت اطلاعات و جلوگیری از

هک شدن که خودش یه بحث مفصله و سعی میکنم داخل یک تاپیک حداگانه در مورد پروتکل اس اس ال توضیح بدم)

در واقع سایت شما با دو پروتکل قابل دسترسی هست یکی http که برای همه سیات ها پیشفرض هست و دوم https که با پروت 443 بالا میاد و

وقتی مجوز ssl رو میخرید براتون فعال میشه و کاربر به دو روش میتونه به سایتتون دسترسی داشته باشه

در حالت عادی وقتی آدرس سایتتونو تایپ میکنه با پروتکل http سایت بالا میاد

بوسیله فایل htaccess این امکان هست که بصورت پیشفرض هر وقت کسی آدرس سایت شما رو وارد کرد با پروتکل https سایت لود بشه چرا که ممکنه کاربر ندونه سایت شما از این پروتکل پشتیبانی میکنه(در صورتی که یک مجوز اس اس ال خریده و فعال کرده باشید)

خوب برای اینکه آدرس از http به https بصورت پیشفرض تغییر کنه راه های دیگه ای هم هست مثلا از داخل پنل مدیریت جوملا ، برخی افزونه ها و.. اما اینم بعنوان یک روش تکمیلی و ساده مورد استفاده قرار میگیره

برای اینکار داخل فایل htaccess روت سایت این کد رو وارد کنید و قبلش مطمئن بشید که ماژول RewriteEngine داخل سرور فعال هست.

کد:

```
RewriteEngine on RewriteCond %{SERVER_PORT} !^443$ RewriteRule ^/(.*) https://%{SERVER_NAME}/$1 [NC,R,L]
```

ودر انتها

کد کامل Htaccess

این کد ها برای کسایی که Vbseo + Sitemap دارن :

کد:

```
#Comment the following line (add '#' at the beginning)
.#to disable mod_rewrite functions

#Please note: you still need to disable the hack in
.#the vBSEO control panel to stop url rewrites

RewriteEngine On

#Some servers require the Rewritebase directive to be
#enabled (remove '#' at the beginning to activate)
#Please note: when enabled, you must include the path
#to your root vB folder (i.e. RewriteBase /forums/)
/ RewriteBase#

#RewriteCond %{HTTP_HOST} !^www\.yourdomain\.com
#RewriteRule (.*) http://www.yourdomain.com/forums/$1 [L,R=301]

$RewriteRule ^((urllist|sitemap_).*\.(xml|txt)(\.gz)?)
vbseo_sitemap/vbseo_getsitemap.php?sitemap=$1 [L]

RewriteCond %{REQUEST_URI}
!(admincp/|modcp/|cron|vbseo_sitemap|api\.php)
RewriteRule ^((archive/)?(.*\.php(/.*)?))$ vbseo.php [L,QSA]

RewriteCond %{REQUEST_FILENAME} !-f
```

```
RewriteCond %{REQUEST_FILENAME} !-d
RewriteCond %{REQUEST_URI}
!(admincp/|modcp/|cron|vbseo_sitemap|api|redir\.php)
RewriteRule ^(.+)$ vbseo.php [L,QSA]
RewriteEngine On
$RewriteRule ^((urllist|sitemap).*\.(xml|txt)(\.gz)?)
vbseo_sitemap/vbseo_getsitemap.php?sitemap=$1 [L]


#BEGIN Compress text files
<ifModule mod_deflate.c>
<"$filesMatch "\.(css|js|x?html?|php)>
SetOutputFilter DEFLATE
<filesMatch/>
<ifModule/>
#END Compress text files


#BEGIN Expire headers
<ifModule mod_expires.c>
ExpiresActive On
"ExpiresDefault "access plus 1 seconds
"ExpiresByType image/x-icon "access plus 2592000 seconds
"ExpiresByType image/jpeg "access plus 2592000 seconds
"ExpiresByType image/png "access plus 2592000 seconds
"ExpiresByType image/gif "access plus 2592000 seconds
ExpiresByType application/x-shockwave-flash "access plus 2592000
"seconds
"ExpiresByType text/css "access plus 604800 seconds
"ExpiresByType text/javascript "access plus 216000 seconds
"ExpiresByType application/javascript "access plus 216000 seconds
"ExpiresByType application/x-javascript "access plus 216000 seconds
"ExpiresByType text/html "access plus 600 seconds
"ExpiresByType application/xhtml+xml "access plus 600 seconds
<ifModule/>
```

```
#END Expire headers

#BEGIN Cache-Control Headers
<ifModule mod_headers.c>
<"$filesMatch "\.(ico|jpe?g|png|gif|swf)>
"Header set Cache-Control "max-age=2592000, public
<filesMatch/>
<"$filesMatch "\.(css)>
"Header set Cache-Control "max-age=604800, public
<filesMatch/>
<"$filesMatch "\.(js)>
"Header set Cache-Control "max-age=216000, private
<filesMatch/>
<"$filesMatch "\.(x?html?|php)>
"Header set Cache-Control "max-age=600, private, must-revalidate
<filesMatch/>
<ifModule/>
#END Cache-Control Headers

#BEGIN Turn ETags Off
<ifModule mod_headers.c>
Header unset ETag
<ifModule/>
FileETag None
#END Turn ETags Off

BEGIN Remove Last-Modified Header #
<ifModule mod_headers.c>
Header unset Last-Modified
<ifModule/>
#END Remove Last-Modified Header
```

```
<IfModule mod_mime.c>
AddType text/css .css
AddType application/x-javascript .js
AddType text/richtext .rtf .rtx
AddType image/svg+xml .svg .svgz
AddType text/plain .txt
AddType text/xsd .xsd
AddType text/xsl .xsl
AddType video/asf .asf .asx .wax .wmv .wmx
AddType video/avi .avi
AddType image/bmp .bmp
AddType application/java .class
AddType video/divx .divx
AddType application/msword .doc .docx
AddType application/x-msdownload .exe
AddType image/gif .gif
AddType application/x-gzip .gz .gzip
AddType image/x-icon .ico
AddType image/jpeg .jpg .jpeg .jpe
AddType application/vnd.ms-access .mdb
AddType audio/midi .mid .midi
AddType video/quicktime .mov .qt
AddType audio/mpeg .mp3 .m4a
AddType video/mp4 .mp4 .m4v
AddType video/mpeg .mpeg .mpg .mpe
AddType application/vnd.ms-project .mpp
AddType application/vnd.oasis.opendocument.database .odb
AddType application/vnd.oasis.opendocument.chart .odc
AddType application/vnd.oasis.opendocument.formula .odf
AddType application/vnd.oasis.opendocument.graphics .odg
AddType application/vnd.oasis.opendocument.presentation .odp
AddType application/vnd.oasis.opendocument.spreadsheet .ods
AddType application/vnd.oasis.opendocument.text .odt
AddType audio/ogg .ogg
AddType application/pdf .pdf
AddType image/png .png
```

```
AddType application/vnd.ms-powerpoint .pot .pps .ppt .pptx
AddType audio/x-realaudio .ra .ram
AddType application/x-shockwave-flash .swf
AddType application/x-tar .tar
AddType image/tiff .tif .tiff
AddType audio/wav .wav
AddType audio/wma .wma
AddType application/vnd.ms-write .wri
AddType application/vnd.ms-excel .xla .xls .xlsx .xlt .xlw
AddType application/zip .zip
<IfModule/>
<IfModule mod_expires.c>
ExpiresActive On
"ExpiresByType text/css "access plus 1 month
"ExpiresByType application/x-javascript "access plus 1 month
"ExpiresByType text/richtext "access plus 1 day
"ExpiresByType image/svg+xml "access plus 1 day
"ExpiresByType text/plain "access plus 1 day
"ExpiresByType text/xsd "access plus 1 day
"ExpiresByType text/xsl "access plus 1 day
"ExpiresByType video/asf "access plus 1 month
"ExpiresByType video/avi "access plus 1 month
"ExpiresByType image/bmp "access plus 1 month
"ExpiresByType application/java "access plus 1 month
"ExpiresByType video/divx "access plus 1 month
"ExpiresByType application/msword "access plus 1 month
"ExpiresByType application/x-msdownload "access plus 1 month
"ExpiresByType image/gif "access plus 1 month
"ExpiresByType application/x-gzip "access plus 1 month
"ExpiresByType image/x-icon "access plus 1 month
"ExpiresByType image/jpeg "access plus 1 month
"ExpiresByType application/vnd.ms-access "access plus 1 month
"ExpiresByType audio/midi "access plus 1 month
"ExpiresByType video/quicktime "access plus 1 month
"ExpiresByType audio/mpeg "access plus 1 month
"ExpiresByType video/mp4 "access plus 1 month
```

"ExpiresByType video/mpeg "access plus 1 month
"ExpiresByType application/vnd.ms-project "access plus 1 month
ExpiresByType application/vnd.oasis.opendocument.database "access plus
"1 month
ExpiresByType application/vnd.oasis.opendocument.chart "access plus 1
"month
ExpiresByType application/vnd.oasis.opendocument.formula "access plus
"1 month
ExpiresByType application/vnd.oasis.opendocument.graphics "access plus
"1 month
ExpiresByType application/vnd.oasis.opendocument.presentation "access
"plus 1 month
ExpiresByType application/vnd.oasis.opendocument.spreadsheet "access
"plus 1 month
ExpiresByType application/vnd.oasis.opendocument.text "access plus 1
"month
"ExpiresByType audio/ogg "access plus 1 month
"ExpiresByType application/pdf "access plus 1 month
"ExpiresByType image/png "access plus 1 month
"ExpiresByType application/vnd.ms-powerpoint "access plus 1 month
"ExpiresByType audio/x-realaudio "access plus 1 month
"ExpiresByType application/x-shockwave-flash "access plus 1 month
"ExpiresByType application/x-tar "access plus 1 month
"ExpiresByType image/tiff "access plus 1 month
"ExpiresByType audio/wav "access plus 1 month
"ExpiresByType audio/wma "access plus 1 month
"ExpiresByType application/vnd.ms-write "access plus 1 month
"ExpiresByType application/vnd.ms-excel "access plus 1 month
"ExpiresByType application/zip "access plus 1 month
<IfModule/>

<IfModule mod_deflate.c>
<IfModule mod_setenvif.c>
BrowserMatch ^Mozilla/4 gzip-only-text/html
BrowserMatch ^Mozilla/4.0[678] no-gzip
BrowserMatch bMSIE !no-gzip !gzip-only-text/html
BrowserMatch bMSI[E] !no-gzip !gzip-only-text/html

<IfModule/>

<IfModule mod_headers.c>
Header append Vary User-Agent env=!dont-vary
<IfModule/>

<IfModule mod_.c>
AddOutputByType DEFLATE text/css application/x-javascript text/html text/richtext image/svg+xml text/plain text/xsd text/xsl text/xml image/x-icon
<IfModule/>

<IfModule/>

<"$FilesMatch "\.(css|js|CSS|JS)>
<IfModule mod_headers.c>
"Header set Pragma "public
"Header append Cache-Control "public, must-revalidate, -revalidate
<IfModule/>

FileETag MTime Size
<IfModule mod_headers.c>
"Header set X-Powered-By "W3 Total Cache/0.9.1.3
<IfModule/>

<FilesMatch/>

FilesMatch >
<"$"\.(rtf|rtx|svg|svgz|txt|xsd|xsl|RTF|RTX|SVG|SVGZ|TXT|XSD|XSL|)
<IfModule mod_headers.c>
"Header set Pragma "public
"Header append Cache-Control "public, must-revalidate, -revalidate
<IfModule/>

FileETag MTime Size
<IfModule mod_headers.c>
"Header set X-Powered-By "W3 Total Cache/0.9.1.3
<IfModule/>

<FilesMatch/>

FilesMatch >
"\.(asf|asx|wax|wmv|wmx|avi|bmp|class|divx|doc|docx|exe|gif|gz|gzip|ico|jpg

```
|jpeg|jpe|mdb|mid|midi|mov|qt|mp3|m4a|mp4|m4v|mpeg|mpg|mpe|mpp|odb
|odc|odf|odg|odp|ods|odt|ogg|pdf|png|pot|pps|ppt|pptx|ra|ram|swf|tar|tif|tiff|w
av|wma|wri|xla|xls|xlsx|xlt|xlw|zip|ASF|ASX|WAX|WMV|WMX|AVI|BMP|CLA
SS|DIVX|DOC|DOCX|EXE|GIF|GZ|GZIP|ICO|JPG|JPEG|JPE|MDB|MID|MI
DI|MOV|QT|MP3|M4A|MP4|M4V|MPEG|MPG|MPE|MPP|ODB|ODC|ODF|O
DG|ODP|ODS|ODT|OGG|PDF|PNG|POT|PPS|PPT|PPTX|RA|RAM|SWF|T
<"$AR|TIF|TIFF|WAV|WMA|WRI|XLA|XLS|XLSX|XLT|XLW|ZIP)
<IfModule mod_headers.c>
"Header set Pragma "public
"Header append Cache-Control "public, must-revalidate, -revalidate
<IfModule/>

FileETag MTime Size
<IfModule mod_headers.c>
"Header set X-Powered-By "W3 Total Cache/0.9.1.3
<IfModule/>

<FilesMatch/>


<Ifmodule mod_php4.c>
php_value upload_max_filesize 2M
php_value max_execution_time  30
php_value max_input_time  60
php_value memory_limit  32M
php_value post_max_size  8M
php_flag register_globals  off
php_flag display_errors  off
php_flag file_uploads  on
php_flag log_errors  off
php_flag output_buffering  off
php_flag register_argc_argv  on
php_flag magic_quotes_gpc  off
php_flag magic_quotes_runtime  off
php_flag magic_quotes_sybase  off
php_flag mysql.allow_persistent  off
php_flag register_long_arrays  on
php_flag allow_url_fopen  on
```

```
php_flag cgi.force_redirect  on
php_flag enable_dl  on
<Ifmodule/>

<Ifmodule mod_php5.c>
php_value upload_max_filesize 2M
php_value max_execution_time  30
php_value max_input_time  60
php_value memory_limit  32M
php_value post_max_size  8M
php_flag register_globals  off
php_flag display_errors  off
php_flag file_uploads  on
php_flag log_errors  off
php_flag output_buffering  off
php_flag register_argc_argv  on
php_flag magic_quotes_gpc  off
php_flag magic_quotes_runtime  off
php_flag magic_quotes_sybase  off
php_flag mysql.allow_persistent  off
php_flag register_long_arrays  on
php_flag allow_url_fopen  on
php_flag cgi.force_redirect  on
php_flag enable_dl  on
<Ifmodule/>
```

کسایی هم که وی بی سئو و سایت مپ ندارن این رو آخر httaccess خودشون اضافه کنن .

کد:

```
BEGIN Compress text files #
<ifModule mod_deflate.c>
<"$filesMatch "\.(css|js|x?html?|php)>
SetOutputFilter DEFLATE
```

<filesMatch/>

<ifModule/>

END Compress text files #

BEGIN Expire headers #
<ifModule mod_expires.c>
ExpiresActive On
"ExpiresDefault "access plus 1 seconds
"ExpiresByType image/x-icon "access plus 2592000 seconds
"ExpiresByType image/jpeg "access plus 2592000 seconds
"ExpiresByType image/png "access plus 2592000 seconds
"ExpiresByType image/gif "access plus 2592000 seconds
ExpiresByType application/x-shockwave-flash "access plus 2592000
"seconds
"ExpiresByType text/css "access plus 604800 seconds
"ExpiresByType text/javascript "access plus 216000 seconds
"ExpiresByType application/javascript "access plus 216000 seconds
"ExpiresByType application/x-javascript "access plus 216000 seconds
"ExpiresByType text/html "access plus 600 seconds
"ExpiresByType application/xhtml+xml "access plus 600 seconds
<ifModule/>

END Expire headers #

BEGIN Cache-Control Headers #
<ifModule mod_headers.c>
<"$filesMatch "\.(ico|jpe?g|png|gif|swf)>
"Header set Cache-Control "max-age=2592000, public
<filesMatch/>

<"$filesMatch "\.(css)>
"Header set Cache-Control "max-age=604800, public
<filesMatch/>

<"$filesMatch "\.(js)>
"Header set Cache-Control "max-age=216000, private
<filesMatch/>

```
<"$filesMatch "\.(x?html?|php)>
"Header set Cache-Control "max-age=600, private, must-revalidate
<filesMatch/>
<ifModule/>
END Cache-Control Headers #

BEGIN Turn ETags Off #
<ifModule mod_headers.c>
Header unset ETag
<ifModule/>
FileETag None
END Turn ETags Off #

BEGIN Remove Last-Modified Header #
<ifModule mod_headers.c>
Header unset Last-Modified
<ifModule/>
END Remove Last-Modified Header #


<IfModule mod_mime.c>
AddType text/css .css
AddType application/x-javascript .js
AddType text/richtext .rtf .rtx
AddType image/svg+xml .svg .svgz
AddType text/plain .txt
AddType text/xsd .xsd
AddType text/xsl .xsl
AddType video/asf .asf .asx .wax .wmv .wmx
AddType video/avi .avi
AddType image/bmp .bmp
AddType application/java .class
AddType video/divx .divx
AddType application/msword .doc .docx
AddType application/x-msdownload .exe
```

```
AddType image/gif .gif
AddType application/x-gzip .gz .gzip
AddType image/x-icon .ico
AddType image/jpeg .jpg .jpeg .jpe
AddType application/vnd.ms-access .mdb
AddType audio/midi .mid .midi
AddType video/quicktime .mov .qt
AddType audio/mpeg .mp3 .m4a
AddType video/mp4 .mp4 .m4v
AddType video/mpeg .mpeg .mpg .mpe
AddType application/vnd.ms-project .mpp
AddType application/vnd.oasis.opendocument.database .odb
AddType application/vnd.oasis.opendocument.chart .odc
AddType application/vnd.oasis.opendocument.formula .odf
AddType application/vnd.oasis.opendocument.graphics .odg
AddType application/vnd.oasis.opendocument.presentation .odp
AddType application/vnd.oasis.opendocument.spreadsheet .ods
AddType application/vnd.oasis.opendocument.text .odt
AddType audio/ogg .ogg
AddType application/pdf .pdf
AddType image/png .png
AddType application/vnd.ms-powerpoint .pot .pps .ppt .pptx
AddType audio/x-realaudio .ra .ram
AddType application/x-shockwave-flash .swf
AddType application/x-tar .tar
AddType image/tiff .tif .tiff
AddType audio/wav .wav
AddType audio/wma .wma
AddType application/vnd.ms-write .wri
AddType application/vnd.ms-excel .xla .xls .xlsx .xlt .xlw
AddType application/zip .zip
<IfModule/>

<IfModule mod_expires.c>
ExpiresActive On
"ExpiresByType text/css "access plus 1 month
"ExpiresByType application/x-javascript "access plus 1 month
```

"ExpiresByType text/richtext "access plus 1 day
"ExpiresByType image/svg+xml "access plus 1 day
"ExpiresByType text/plain "access plus 1 day
"ExpiresByType text/xsd "access plus 1 day
"ExpiresByType text/xsl "access plus 1 day
"ExpiresByType video/asf "access plus 1 month
"ExpiresByType video/avi "access plus 1 month
"ExpiresByType image/bmp "access plus 1 month
"ExpiresByType application/java "access plus 1 month
"ExpiresByType video/divx "access plus 1 month
"ExpiresByType application/msword "access plus 1 month
"ExpiresByType application/x-msdownload "access plus 1 month
"ExpiresByType image/gif "access plus 1 month
"ExpiresByType application/x-gzip "access plus 1 month
"ExpiresByType image/x-icon "access plus 1 month
"ExpiresByType image/jpeg "access plus 1 month
"ExpiresByType application/vnd.ms-access "access plus 1 month
"ExpiresByType audio/midi "access plus 1 month
"ExpiresByType video/quicktime "access plus 1 month
"ExpiresByType audio/mpeg "access plus 1 month
"ExpiresByType video/mp4 "access plus 1 month
"ExpiresByType video/mpeg "access plus 1 month
"ExpiresByType application/vnd.ms-project "access plus 1 month
ExpiresByType application/vnd.oasis.opendocument.database "access plus
"1 month
ExpiresByType application/vnd.oasis.opendocument.chart "access plus 1
"month
ExpiresByType application/vnd.oasis.opendocument.formula "access plus
"1 month
ExpiresByType application/vnd.oasis.opendocument.graphics "access plus
"1 month
ExpiresByType application/vnd.oasis.opendocument.presentation "access
"plus 1 month
ExpiresByType application/vnd.oasis.opendocument.spreadsheet "access
"plus 1 month

```
ExpiresByType application/vnd.oasis.opendocument.text "access plus 1
"month
"ExpiresByType audio/ogg "access plus 1 month
"ExpiresByType application/pdf "access plus 1 month
"ExpiresByType image/png "access plus 1 month
"ExpiresByType application/vnd.ms-powerpoint "access plus 1 month
"ExpiresByType audio/x-realaudio "access plus 1 month
"ExpiresByType application/x-shockwave-flash "access plus 1 month
"ExpiresByType application/x-tar "access plus 1 month
"ExpiresByType image/tiff "access plus 1 month
"ExpiresByType audio/wav "access plus 1 month
"ExpiresByType audio/wma "access plus 1 month
"ExpiresByType application/vnd.ms-write "access plus 1 month
"ExpiresByType application/vnd.ms-excel "access plus 1 month
"ExpiresByType application/zip "access plus 1 month
<IfModule/>

<IfModule mod_deflate.c>
<IfModule mod_setenvif.c>
BrowserMatch ^Mozilla/4 gzip-only-text/html
BrowserMatch ^Mozilla/4.0[678] no-gzip
BrowserMatch bMSIE !no-gzip !gzip-only-text/html
BrowserMatch bMSI[E] !no-gzip !gzip-only-text/html
<IfModule/>

<IfModule mod_headers.c>
Header append Vary User-Agent env=!dont-vary
<IfModule/>

<IfModule mod_.c>
AddOutputByType DEFLATE text/css application/x-javascript text/html
text/richtext image/svg+xml text/plain text/xsd text/xsl text/xml image/x-icon
<IfModule/>

<IfModule/>

<"$FilesMatch "\.(css|js|CSS|JS)>
<IfModule mod_headers.c>
"Header set Pragma "public
```

"Header append Cache-Control "public, must-revalidate, -revalidate
<IfModule/>

FileETag MTime Size
<IfModule mod_headers.c>
"Header set X-Powered-By "W3 Total Cache/0.9.1.3
<IfModule/>

<FilesMatch/>

FilesMatch >
<"$"\.(rtf|rtx|svg|svgz|txt|xsd|xsl|RTF|RTX|SVG|SVGZ|TXT|XSD|XSL|)
<IfModule mod_headers.c>
"Header set Pragma "public
"Header append Cache-Control "public, must-revalidate, -revalidate
<IfModule/>

FileETag MTime Size
<IfModule mod_headers.c>
"Header set X-Powered-By "W3 Total Cache/0.9.1.3
<IfModule/>

<FilesMatch/>

FilesMatch >
"\.(asf|asx|wax|wmv|wmx|avi|bmp|class|divx|doc|docx|exe|gif|gz|gzip|ico|jpg
|jpeg|jpe|mdb|mid|midi|mov|qt|mp3|m4a|mp4|m4v|mpeg|mpg|mpe|mpp|odb
|odc|odf|odg|odp|ods|odt|ogg|pdf|png|pot|pps|ppt|pptx|ra|ram|swf|tar|tif|tiff|w
av|wma|wri|xla|xls|xlsx|xlt|xlw|zip|ASF|ASX|WAX|WMV|WMX|AVI|BMP|CLA
SS|DIVX|DOC|DOCX|EXE|GIF|GZ|GZIP|ICO|JPG|JPEG|JPE|MDB|MID|MI
DI|MOV|QT|MP3|M4A|MP4|M4V|MPEG|MPG|MPE|MPP|ODB|ODC|ODF|O
DG|ODP|ODS|ODT|OGG|PDF|PNG|POT|PPS|PPT|PPTX|RA|RAM|SWF|T
<"$AR|TIF|TIFF|WAV|WMA|WRI|XLA|XLS|XLSX|XLT|XLW|ZIP)
<IfModule mod_headers.c>
"Header set Pragma "public
"Header append Cache-Control "public, must-revalidate, -revalidate
<IfModule/>

FileETag MTime Size
<IfModule mod_headers.c>

"Header set X-Powered-By "W3 Total Cache/0.9.1.3
<IfModule/>

<FilesMatch/>

<Ifmodule mod_php4.c>
php_value upload_max_filesize 2M
php_value max_execution_time 30
php_value max_input_time 60
php_value memory_limit 32M
php_value post_max_size 8M
php_flag register_globals off
php_flag display_errors off
php_flag file_uploads on
php_flag log_errors off
php_flag output_buffering off
php_flag register_argc_argv on
php_flag magic_quotes_gpc off
php_flag magic_quotes_runtime off
php_flag magic_quotes_sybase off
php_flag mysql.allow_persistent off
php_flag register_long_arrays on
php_flag allow_url_fopen on
php_flag cgi.force_redirect on
php_flag enable_dl on
<Ifmodule/>

<Ifmodule mod_php5.c>
php_value upload_max_filesize 2M
php_value max_execution_time 30
php_value max_input_time 60
php_value memory_limit 32M
php_value post_max_size 8M
php_flag register_globals off
php_flag display_errors off
php_flag file_uploads on

```
php_flag log_errors  off
php_flag output_buffering  off
php_flag register_argc_argv  on
php_flag magic_quotes_gpc  off
php_flag magic_quotes_runtime  off
php_flag magic_quotes_sybase  off
php_flag mysql.allow_persistent  off
php_flag register_long_arrays  on
php_flag allow_url_fopen  on
php_flag cgi.force_redirect  on
php_flag enable_dl  on
<Ifmodule/>
```

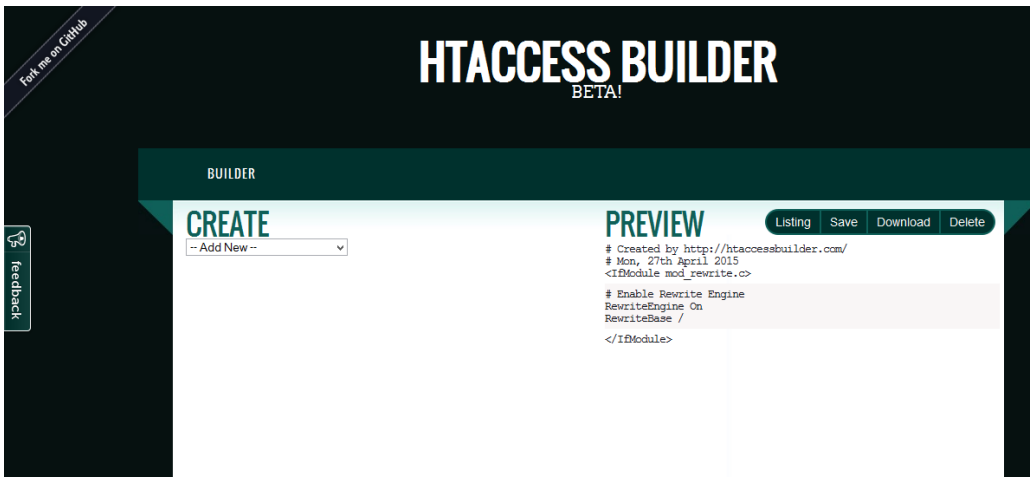
ابزارهای تولید خودکار دستورات .Htaccess

حال که با دستورات اصلی فایل .Htaccess آشنا شدید قصد دارم تعدادی از ابزارهای تولید خودکار دستورات را به شما معرفی کنم:

•

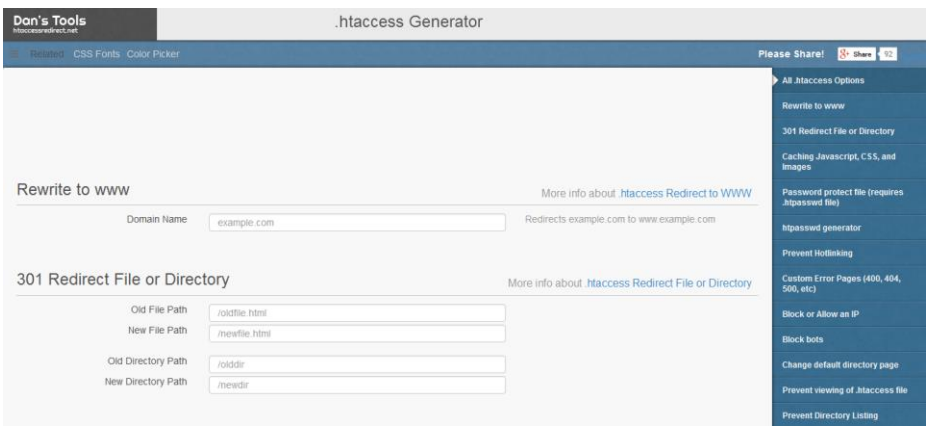
Htaccess Builder

http://htaccessbuilder.com



- htaccess redirect generator.

http://wwwhtaccessredirect.net

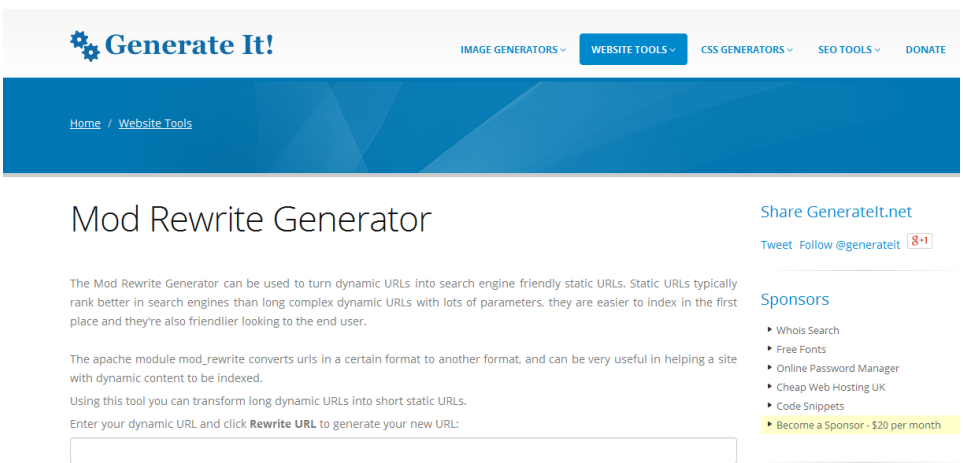


- htaccessEditor – Create a .htaccess File

http://www.htaccesseditor.com/en.shtml

- Mod Rewrite Generator by GenerateIt.net

http://www.generateit.net/mod-rewrite/index.php



منابع

http://www.askapache.com/category/htaccess/

https://www.branded3.com/blog/htaccess-mod_rewrite-ultimate-guide/

http://serverfault.com/questions/214512/redirect-change-urls-or-redirect-http-to-https-in-apache-everything-you-ever
http://wiki.apache.org/httpd/Htaccess
http://httpd.apache.org/docs/current/howto/htaccess.html