Sencitive Files & Directoreis

معرفی File ها و directory های مهم عمومی سایت ها و مسیر های احتمالی

صفحه Admin

برای استفاده از خیلی از آسیب پذیری ها نیازمند داشتن آدرس صفحه ی Admin یا همان صفحه ی ورود به پنل مدیریت هستیم

به عنوان مثال

آسیب پذیری های مربوط به forget password

آسیب پذیری sqlinjection

استفاده از cheet shit های sqlinjection

انجام عملیات brute force

پس این فایل یکی از مهمترین فایل های هر سایت است

اما مسیر هایی که عموما این فایل در آن ها یافت می شود چیست ؟

Example.com/admin

/login

/signin

/log

/manage

/manager

/adm

/default

/user , users

/member , members

/adm

/a

- خیلی از اوقات لازم است حتما شما format این فایل ها را نیز مشخص نمایید به عنوان مثال اگر سایت شما با زبان برنامه نویسی php طراحی شده باشد این آدرس می تواند /admin.php باشد

- یک سری ابزار های اختصاصی مانند admin-finder و یا directory- finder موجودند که تعداد زیادی از این کلمات پیشفرض را در خود دارند و آن ها را برای هر سایت که شما انتخاب نمایید امتحان می نمایند و نتیجه را به شما می گویند

- ممکن است اصلا صفحه مدیریت سایت به صورت یکی از فایل های سایت ظاهر نشود بلکه صفحه ی اصلی یکی از زیر دامنه های سایت اصلی باشد که این زیر دامنه ها نیز می توانند به نام همین فایل های مشخص شده در بالا باشند

- یکی دیگر از مکان هایی که امکان دارد صفحه ورود مدیریت سایت باشد آدرس سایت در port هایی غیر از port های اصلی سایت مانند 80 و 443 باشد مانند port 81 یا 8081 و یا هر port دیگر الیته معمولا port هایی که خود سرویس خاصی را ارائه می هند برای این امر انتخاب نمی شوند مانند port 3306 که ارائه دهنده سرویس mysql است

Robots.txt

Robots.txt که تقریبا در همه ی سایت ها یافت می شود همیشه در آدرس ذیل قرار دارد

Example.com/robots.txt

محتوای این فایل آدرس دیگر file ها و directory های مهم هرسایت را مشخص نموده است الیته ممکن است فایلی در سایت از نظر ما اهمیت ویژه ای داشته باشد ولی آدرس آن در robots.txt نیامده باشد پس نباید به این سایت اکتفا نمود

روش کلی تشخیص وجود directory

یکی از روش هایی که اطمینان از وجود یک directory را برای ما حاصل می نماید واکنش سایت به نام directory است به عنوان مثال اگر سایتی دارای directory به نام plugins باشد و ما در request زیر را به عنوان url قرار دهیم سایت برای تایید این مسئله یک علامت / در انتهای آن قرار خواهد داد

Request : Http://example.com/plugins

Response : http://eample.com/plugins/

الیته با پیشرفت امنیت در سال های اخیر خیلی از برنامه نویسان ترفندی را پیش گرفته اند که اگر شما هر کلمه ای را به عنوان نام ورودی به سایت بدهید سایت چه واقعا حاوی آن directory باشد چه نباشد علامت / را در انتهای آن قرار می دهد بنابراین برای حصول اطمینان از درستی عملکرد سایت در قرایند بالا یک نام بیهوده که اطمینان دارید directory به این نام وجود ندارد را امتحان نمایید

معرفی فایل های اختصاصی cms ها

Wordpress

پیدا نمودن user ها

پیدا نمودن user ها در این cms روش های متنوعی دارد

- یکی از این روش ها مراجعه به آدرس wp-json/wp/v2/users می باشد که در آن جا تمام username ها و userId ها مشخص است

Wp-json به طور کلی قالی است که اطلاعات جامع زیادی از سایتی که یا آن سر و کار دارید در اختیار شما قرار می دهد

- روش author

در این روش متغیر author را برابر یا userID های احتمالی user های word press قرار می دهیم

مثال

Request: example.com/?author=1

Response: example.com/author=admin

در این مثال سایت به ما پاسخ داده است که username کاربری که userID آن برابر یا 1 است admin می باشد

- Wpscan

ابزاری به نام wpscan مختص اسکن آسیب پذیری ها و ویژگی های سایت هایی که از wordpress cms استفاده می نمایند تهیه شده است که توانایی پیدا نمودن username ها را دارد

نحوه ی کار با این ابزار در کلاس wordpress hacking تدریس خواهد شد

- Hackertarget

سایت هایی مانند hackertarget دارای ویژگی هایی مانند اسکن خصوصیات سایت هایی که دارای wordpress-cms هستند

که یکی از نتایج اسکن آن ها نام تمام username هاست

- صفحه login

صفحه login مختص به سایت های wordpress در آدرس های wp-login و wp-admin قرار دارند البته در تعداد کمی از سایت ها به صورت authentication ظاهر می شوند

در صفحه login شما می توانید user name ها را حدس بزنید به این ترتیب که اگر هم user و هم password که شما در این صفحه وارد نموده اید اشتباه باشد به شما پیغام username or password is wrong می دهد ولی اگر username صحیح باشد و password اشتباه به شما پیغام this password for this username is wrong را نمایش می دهد

- نویسنده مطلب

این روش بیشتر در سایت هایی شبیه به سایت های خبری جوابگو است

منظور از نویسنده در اینجا الزاما نویسنده خبر نیست بلکه منظور کاربری است که این مطلب را درون سایت بارگذاری نموده است می باشد

معمولا در انتهای هر خبر یا مطلب نام نویسنده به صورت لینک وجود دارد که تمامی خبر ها و یا مطالب آن نویسنده را در یک صفحه جمع نموده است

نامی که برای نویسنده در لینک تشکیل شده در url موجود است معمولا یک username است

پیدا نمودن version

-

پیدا نمودن plugin ها و theme ها

Joomla

پیدا نمودن user ها

پیدا نمودن version

پیدا نمودن plugin ها و theme ها

معرفی crowling و crowler ها

Acunetix

burpsuit

معرفی fuzzing و fuzzer ها

Dirbuster

Burpsuit

آسیب پذیری های در این رابطه

.svn

.git