MILAD HACKING

Ashiyane Digital Security Team

بسم الله الرحمان الرحیم

پروردگارا

مرا مدد کن تا دانش اندکم

نه نردبانی باشد برای فزونی غرور و تکبر

و نه حلقه ای برای اسارت

و نه دستمایه ای برای تجارت ،

بلکه گامی باشد برای انسانیت و متفاوت ساختن

زندگی خود و دیگران

خرداد 92

MILAD HACKING

Ashiyane Digital Security Team

سلام خدمت همه دوستانی که این کتاب رو میخونن

بعد از کلی تحقیق و مطالعه که در ضمینه هک کردم تصمیم گرفتم این کتاب رو بنویسم تا دوستانی که میخوان امنیت سایت هاشون رو بالا ببرن و باگ های سایت هاشون رو کشف کنن بهشون کمک کوچکی کرده باشم و موجب افزایش امنیت سایت های ایرانی بشه .

چند روز پیش وقتی باگی رو توی Cms یا سیستم مدیریت محتوا Mojenoo که یگ سیستم مدیریت محتوا ایرانی هست و100 ها سایت دولتی ایران از این سیستم مدیریت محتوا استفاده میکردند و به راحتی قابل نفوذ بود این باگ رو ثبت کردم تا هر چه زود تر پیچ بشه و توی این سیستم مدیریت محتوا وجود نداشته باشه.

شما میتونید جزئیات دقیق این باگ کشف شده رو در لینک زیر که در سایت بزرگ و جهانی ثبت باگ cxsecurity ثبت شده است ببینید.

http://cxsecurity.com/issue/WLB-2013050189

زیاد نمیخوام شلوغش کنم الان بعضی از دوستان میگن یه باگ کشف کرده داره همه جا میگه و..... سایر موارد.

خوب ما برای این که بخوایم بفهمیم سایت ما چه باگ هایی داره چند راه داریم.

MILAD HACKING
Ashiyane Digital Security Team

اول این که میشه به صورت دستی این کار رو کرد که این باید تو هک وارد باشی تا روش های این که تست باگ وجود داره در سایت رو تست کنیم.

روش دوم استفاده از سایت های انلاین هست که سایت ها میان سایت رو اسکن میکنن و باگی رو که داره برامون به نمایش میگزارند.

روش سوم و روشی که مد نظر من تو این اموزش هست استفاده از یک نرم افزار اسکنر که میاد سایت رو اسکن میکنه و باگ هایی که روی سایت ما هست رو به ما اطلاع میده.

اسکنر های زیادی به صورت نرم افزاری هستن ولی یکی از محبوب ترین ها اسکنر Acunetix یا Acunetix Web Vulnerability Scanner هست که با کمی سرچ و وب گردی میشه پیداش کرد.

این نرم افزار 3 نسخه داره تا جایی که من اطلاع دارم نسخه های 6 و 7 و8 که نسخه 8 این برنامه اخرین نسخه هست شاید یه مدت دیگه این نسخه جدید تر روانه بازار بشه

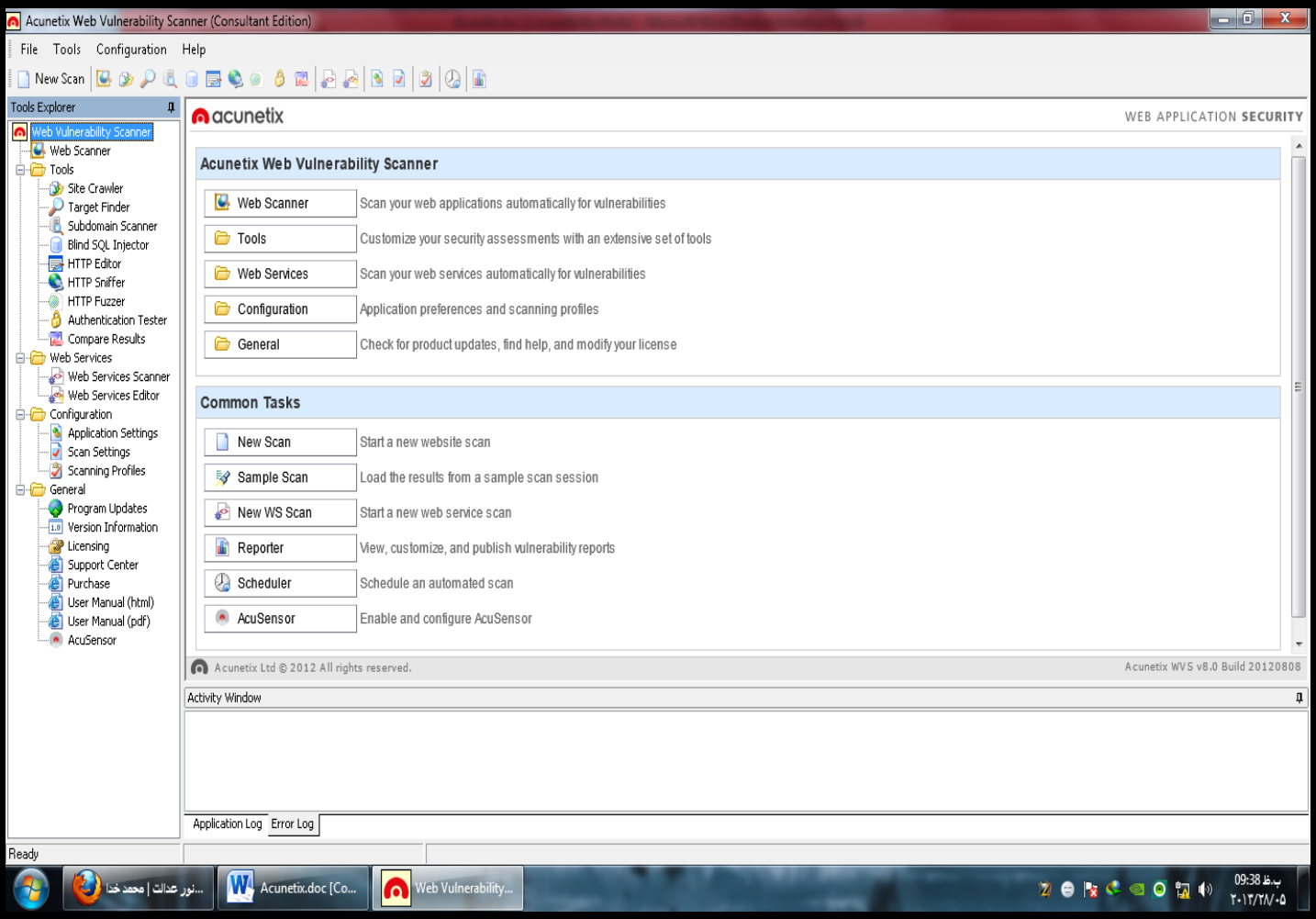
این برنامه رو سایت www.acunetix.com طراحی کرده و بسیار محبوب در بین هکر ها هست.

هکر میاد با این برنامه سایت رو اسکن میکنه و از باگ های کشف شده برای نفوذ استفاده میکنه.

MILAD HACKING

Ashiyane Digital Security Team

خوب این تصویری کلی از محیط برنامه



من یه تارگ رو برای اسکن و ازمایش کردم که یک سایت خارجی هست.

ادرس: www.spiritual-kids.nl

خوب من این تارگ رو میخوام با این برنامه اسکن کنم و باگ هاش رو پیدا کنم

توجه : تارگ در اینجا به معنای هدف میباشد!

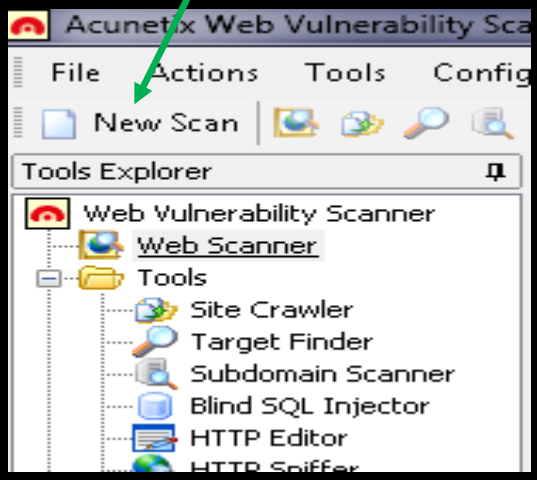
MILAD HACKING

Ashiyane Digital Security Team

من مرحله به مرحله توضیح میدم این اموزش باید به صورت فیلم بود که من به صورت کتابی به شما یاد میدم

خوب ما نرم افزار رو اجرا میکنیم.

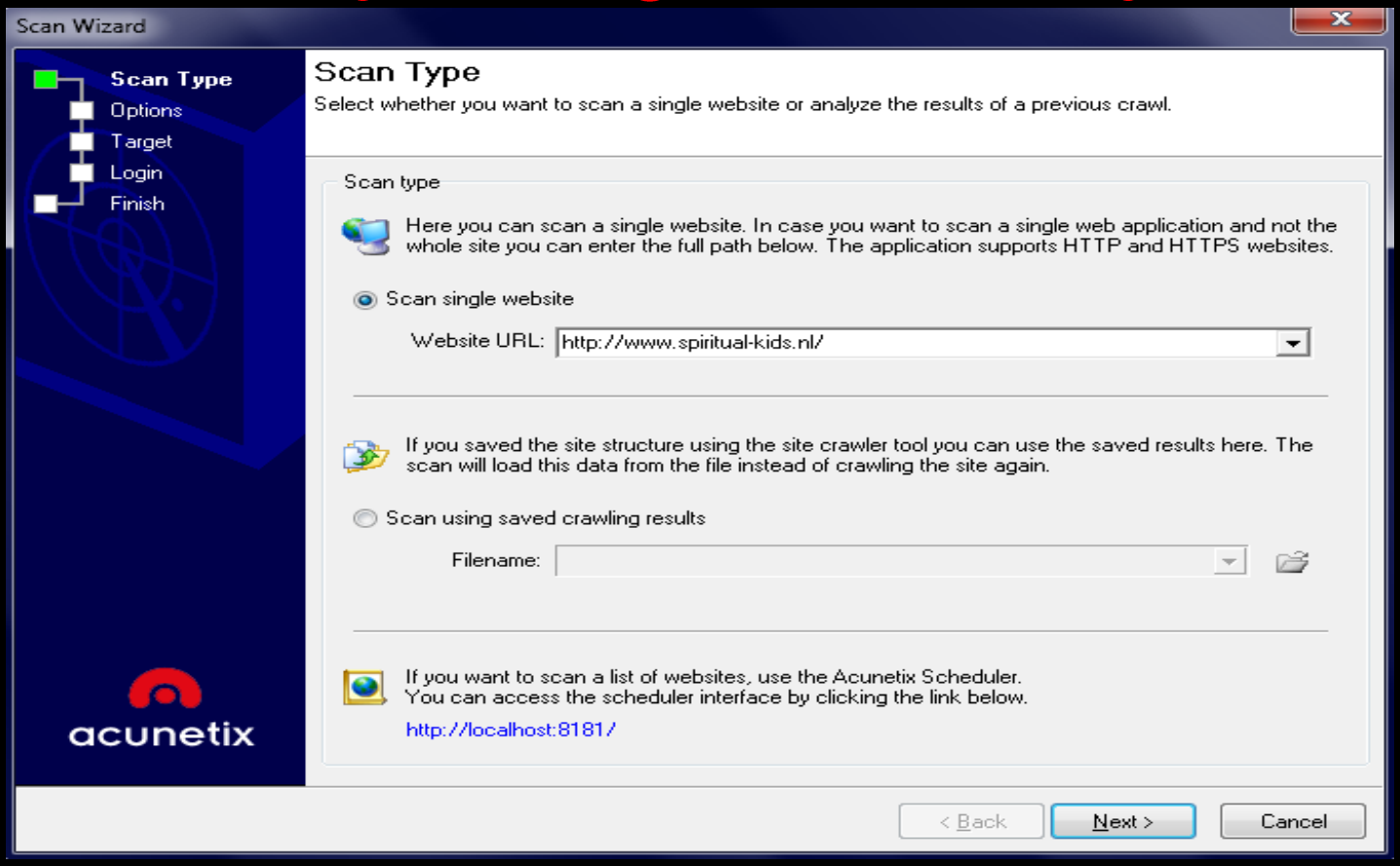
سمت چپ نوشته New Site مثل تصویر زیر



من روش کلیک میکنم تصویر زیر باشه میشه

MILAD HACKING

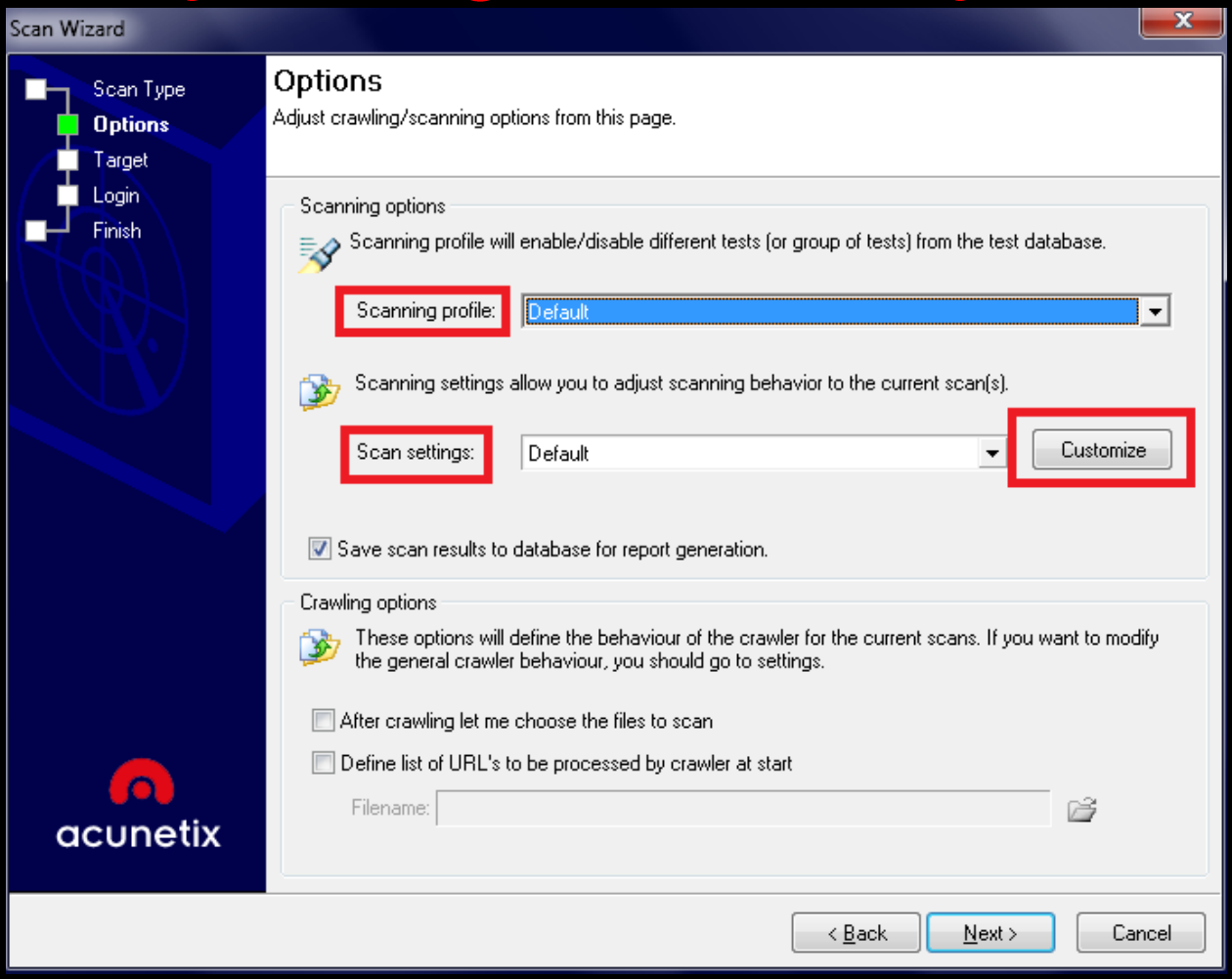
Ashiyane Digital Security Team



تو قسمت Website url: ادرس سایتی که میخوایم اسکن کنیم و باگ ها رو شناسایی کنیم وارد میکنیم و سپس با کلیک روی Next به مرحله بعدی میریم تا تصویر زیر باز بشه.

MILAD HACKING

Ashiyane Digital Security Team

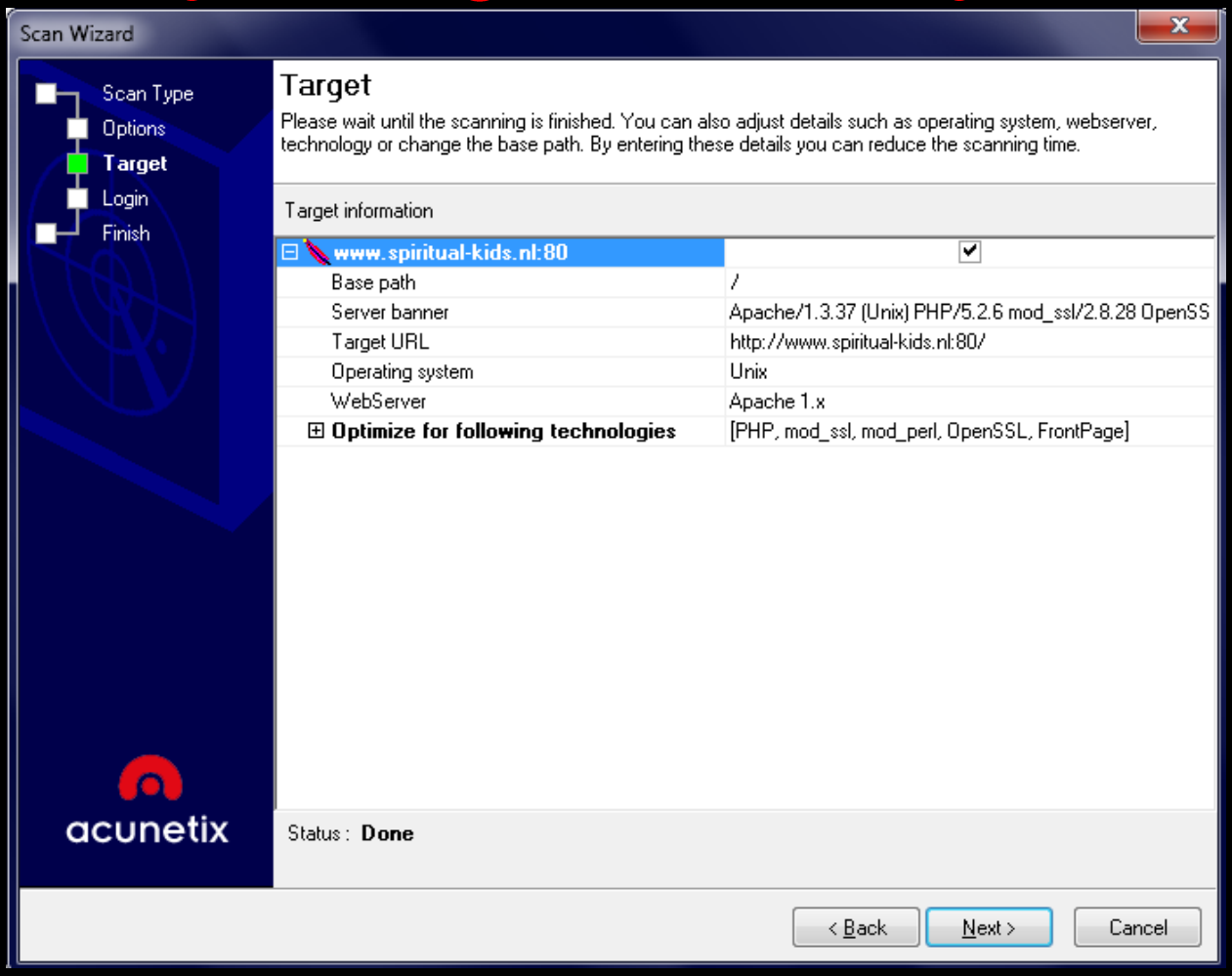


تو این قسمت چند تا تنظیم داره که اولیش Scaning profile هست تو این بخش میتونید تنظیم کنید که دنبال چه باگی بگرده که ببینه سایت ما اون باگ رو داره یا نه

تو قسمت Scan settings هم میشه سرعت و ... بعضی ها رو تو زمان اسکن تنظیم کرد که زیاد مهم نیست ما روی Next کلیک میکنیم تا وارد مرحله بعدی شویم.

MILAD HACKING

Ashiyane Digital Security Team

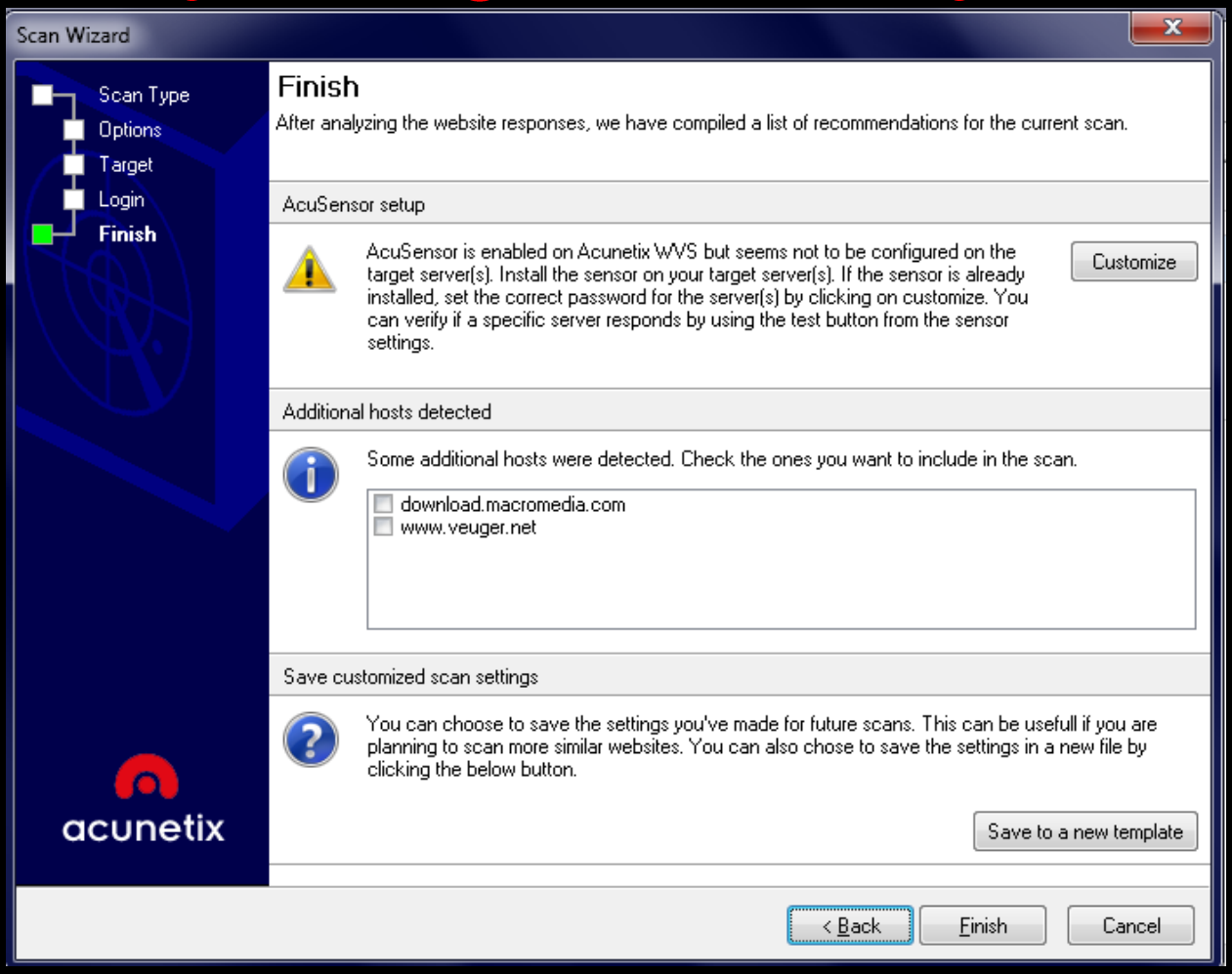


خوب تو این جا نرم افزار میاد دنبال زبان Cms و .... میگرده و بعد از چند ثانیه میتونیم با کلیک بر روی Next وارد مرحله بعد بشیم.

مرحله بعدی تصویر زیر هست.

MILAD HACKING

Ashiyane Digital Security Team



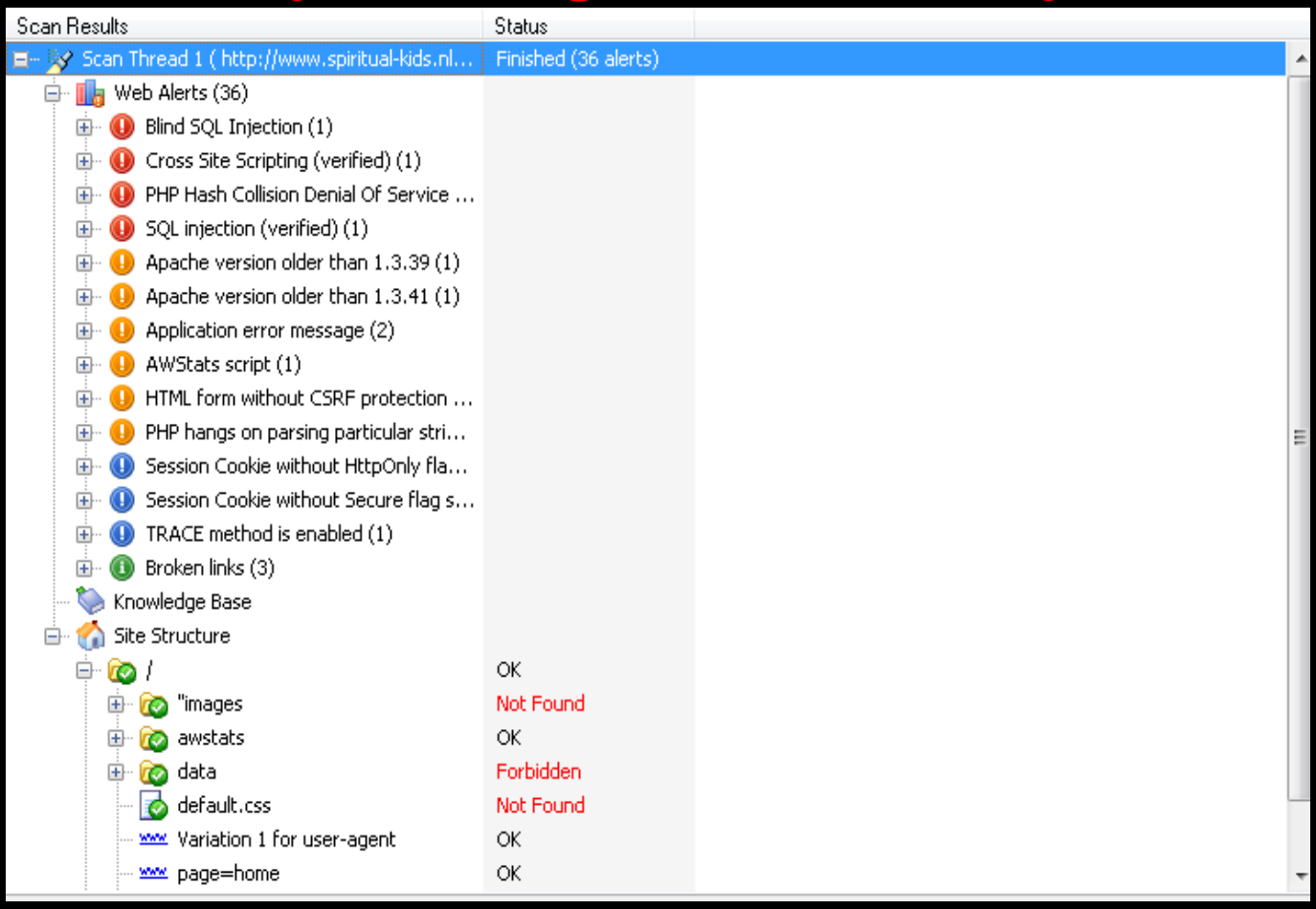
خوب تو این قسمت کار خاصی نمیخواد انجام بدیم و روی Finish کلیک میکنیم تا اسکن به صورت اتوماتیک شروع بشه.

خوب تمومه بعدا از تموم شدن اسکن نتیجه رو به صورت زیر نشون میده.

ولی نه این که نتیجه همیشه یکسان باشه نتایج با هم فرق میکنه که سایت چه باگ هایی داشته باشه.

MILAD HACKING

Ashiyane Digital Security Team



خوب همون طور که از تصویر معلومه این سایت کلی باگ خطر ناک داره .

باگی که با رنگ قرمز نمایش داده میشه باگ های خطر ناک هست.

باگ رنگ نارجی باگ های مدیوم هست ولی باز خطر هک با این باگ هم هست.

باگ های رنگ سبز و ابی بدرد هک نمیخورن و بی فایده هستند.

==========

خوب در مورد باگ ها کمی توضیح میدم

MILAD HACKING

Ashiyane Digital Security Team

باگ SQL INJECTION

همونطور که میدونید در اغلب برنامه های تحت وب از بانک اطلاعاتی استفاده میشه که اطلاعاتی نظیر اسامی ، اطلاعات کاربردی یک سایت ، اطلاعات کاربران و مدیران و ... در آن قرار میگیره .

این برنامه ها اطلاعاتی که کاربران میخواهند وارد کنند را از طریق کد هایی که برنامه نویس نوشته دریافت میکنند و بر اساس آنها Query جدیدی تعریف میکنند و به دیتابیس یا همون بانک اطلاعاتی ارسال میکنند . و ارتباط Databaseبا کاربر از طریق همین Query ها برقرار میشود .

اکثر این برنامه ها از زبان SQL برای این ارتباط استفاده میکنند و جالبه که بدونید این فرایند که Query ها بر اساس اطلاعاتی که کاربران برای آنها تایین میکنند و مستقیماً در فیلدهای ورودی صفته وب وارد میکنند می تواند راهی برای نفوذ یک هکر باشد.

به عبارت دیگر اگر برنامه ای که توسط برنامه نویس نوشته شده ، اطلاعات یک فیلد رو که با همان دستورات کاربر وارد شده رو جلوی یک دستور SQL بگذارد و آن را برای اجرا کردن به بانک اطلاعاتی بفرستد در اینصورت یک هکر که با زبان SQL آشنا باشد می تواند محتویات این فیلدها را طوری با دستورات SQL پر کند که

MILAD HACKING

Ashiyane Digital Security Team

ممکن است به یک فرمان مخرب تبدیل شده و پس از اجرا ، اهداف نفوذگر را برآورده نماید.

باگ ها SQL از طریق برنامه نویسی غلت و اشتباه برنامه نویس سایت اون باگ بوجود میاد و هکر ها هم از این فرصت ها استفاده میکنن و از طریق اون خرابی که ما بهش میگیم باگ اطلاعات سایت رو بدست میارن و در اخر نفوذ و...

میتونم بگم روی تعداد زیادی از سایت های که وجود داره باگ SQL موجود است !
مثلا بیشتر سایت های دولتی ما یا کشور های دیگر از این نوع باگ ها برخوردارن !
مثل : سایت های دانشگاها , سایت های بانک ها , سایت های دولتی , و ....

باگ XSS یا (Cross site script)

این نوع حملات اکثرا برای دزدین کوکی قربانی اسفاده میشه که هکر با تزریق کد به سایت و فرستادن یو آر ال به قربانی کوکی های قربانی در محلی که هکر مشخص کرده سیو میشود

این نو حملات کاربرد زیادی داره ولی بیشترین کاربردش دزدیدن کوکی هاست.

MILAD HACKING
Ashiyane Digital Security Team

باگ CSRF

CRSF مخفف Cross-site Request Forgeries است . درخواستی که از طریق یک سایت دیگر می اید.

این باگ به صورتی هست که مثلا من یک کد مخرب رو توی ای فریم قالب وبلاگ یا سایتم قرار میدم و وقتی شما واردش شدی این کد مخرب اجرا میشه و یه دسترسی به پنل ادمین اضافه میشه همون چیزی که هکر میخواد.

یا مثلا از FTP میشه کانکت شد و یک شل اپلود کرد و ... تمام کامل هک میشه سایت.

فکر میکنم همین 3 باگ رو توضیح مختصری دادم کافی باشه و علاقمند باشید میتونید با مراجعه به مراجع و کتاب های نوشته شده اطلاعات خوبی به دست بیاورد

Author:Milad Hacking

E-mail: Mi1374_MILAD@YAHOO.COM