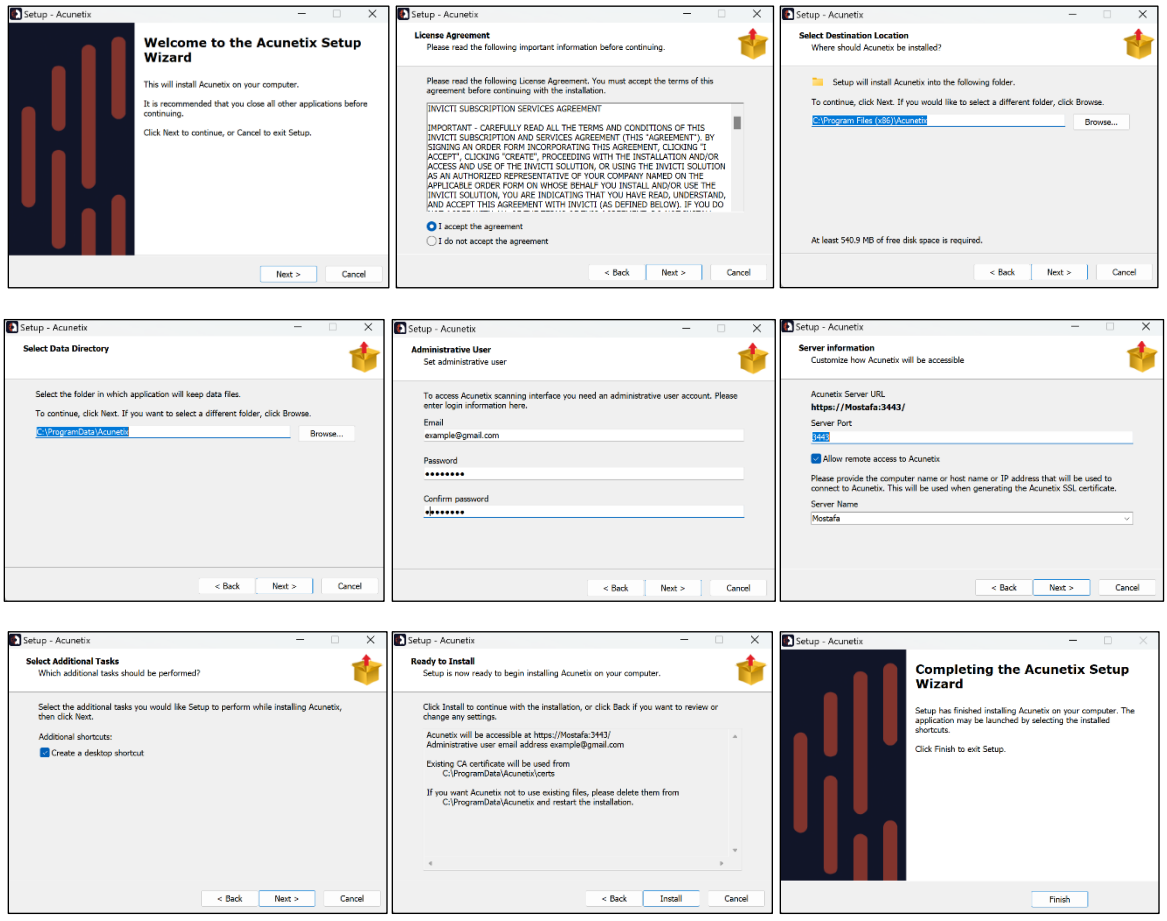
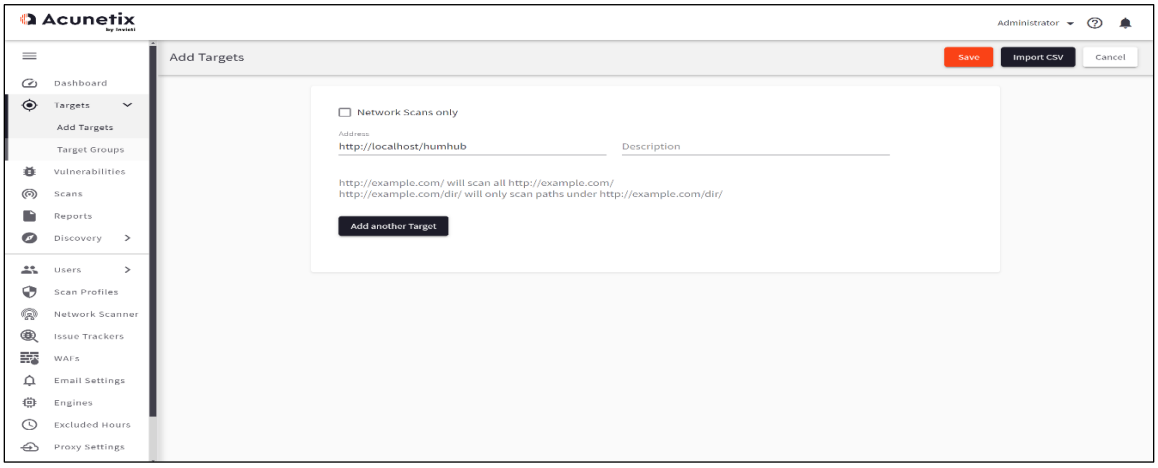
گام دوم: بررسی امنیت شبکه اجتماعی HumHub

با استفاده از Acunetix

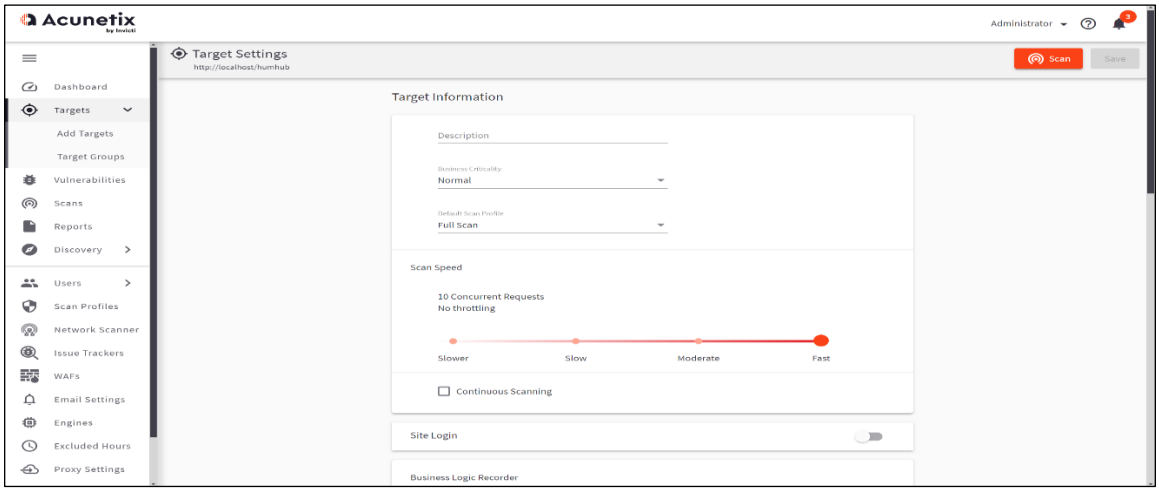
1- مراحل نصب را طبق تصاویر زیر انجام می‌دهیم.



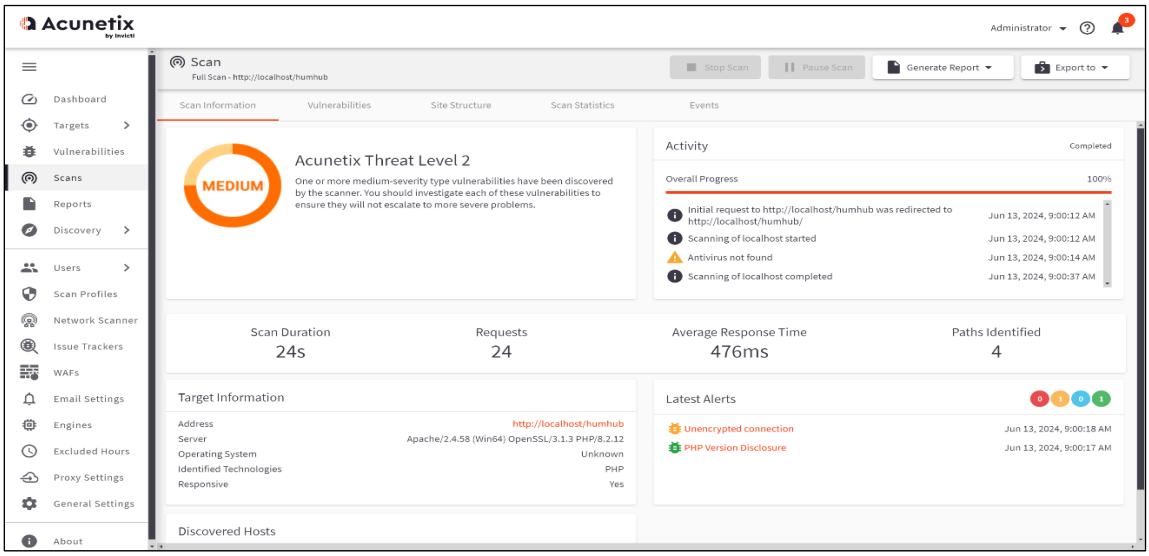
2- بر روی Add Target کلیک می‌کنیم و آدرس را (http://localhost/humhub) وارد می‌کنیم. سپس بر روی Save کلیک می‌کنیم.



3- بر روی Scan کلیک می‌کنیم.



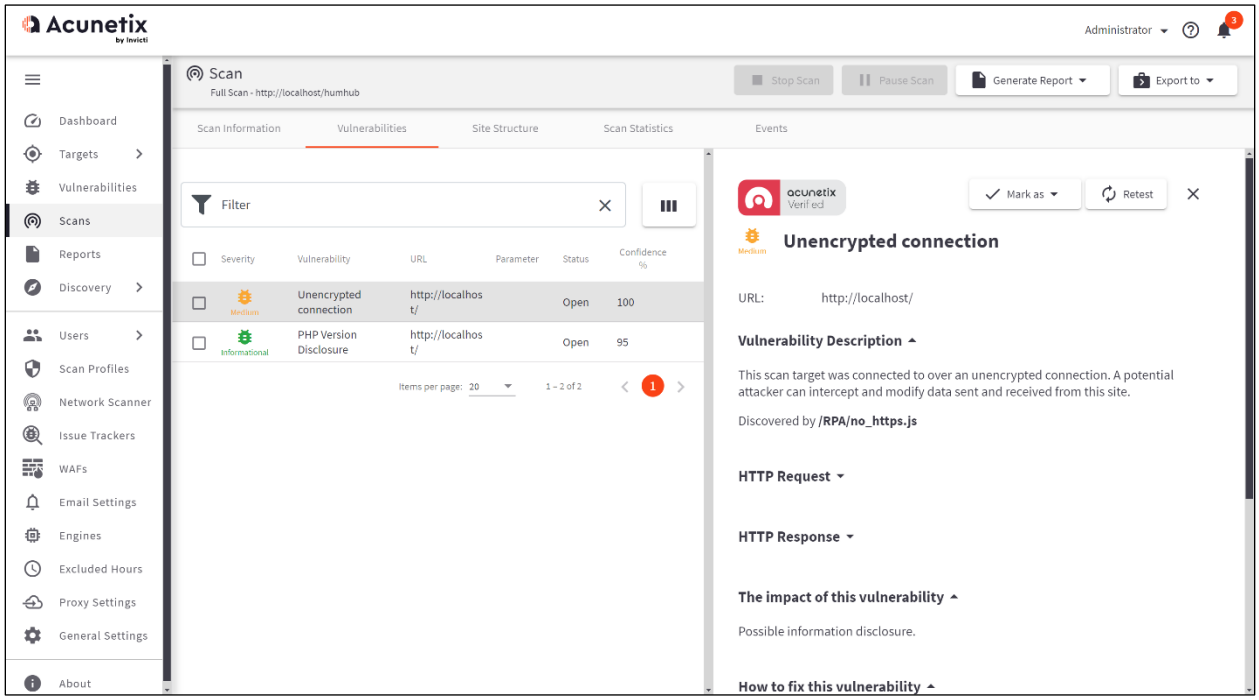
4- نتیجه اسکن به صورت زیر است.



یک Vulnerability از نوع Medium و یکی از نوع Informational پیدا شد.

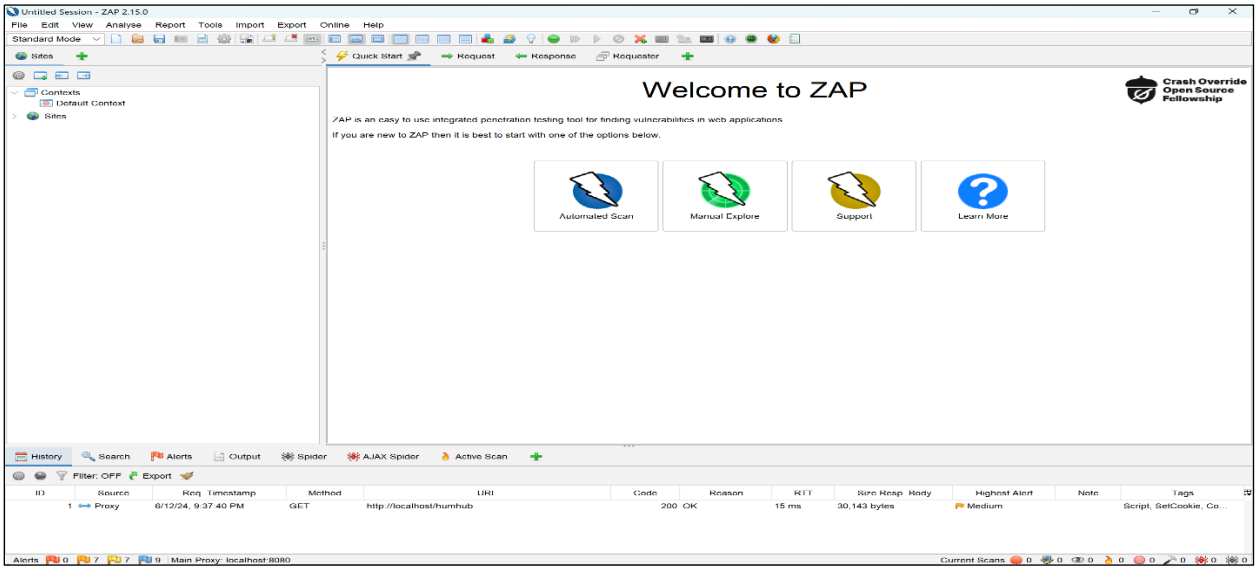
بررسی **Unencrypted connection**

این آسیب‌پذیری به دلیل استفاده از پروتکل http به جای https است. این موضوع امکان دزدی اطلاعات را از کاربران فراهم می‌کند. همچنین راه حل آن استفاده ازپروتکل https است.



با استفاده از ZAP

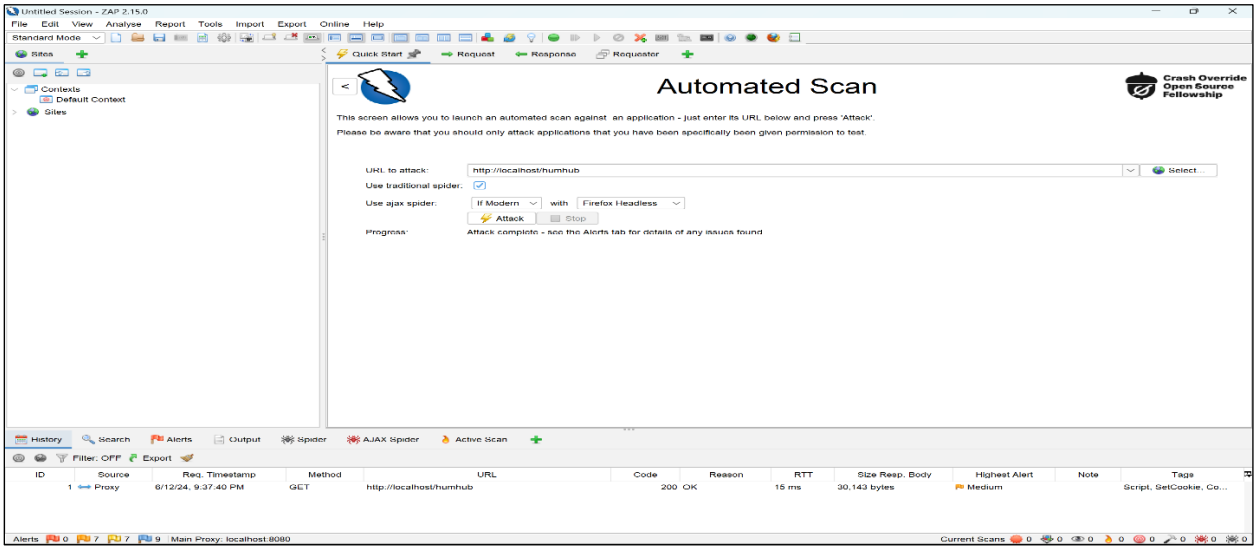
1- پس از نصب موفقیت‌آمیز برنامه، آن را اجرا می‌کنیم.



2- بر روی Automated Scan کلیک می‌کنیم.

3- URL شبکه اجتماعی یعنی http://localhost/humhub را وارد می‌کنیم.

4- بر روی Attack کلیک می‌کنیم.



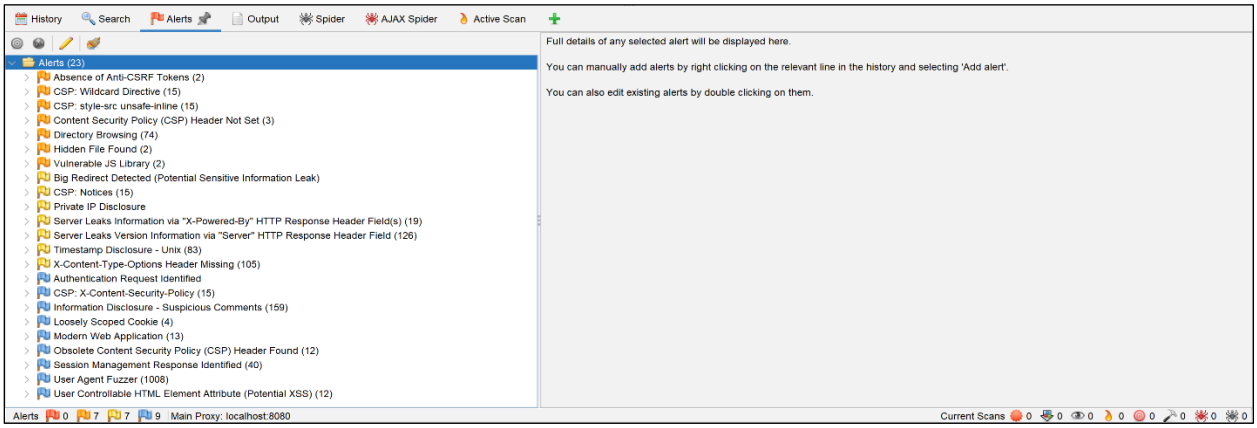
5- منتظر می‌مانیم تا فرایند بررسی به اتمام برسد.

6- به تب Alerts می‌رویم.

7- مشاهده می‌شود که 23 مورد شناسایی شده است.

دسته بندی Alert ها به صورت (High – Medium – Low – Informational – False Positive) می‌باشد.

از 23 مورد، 7 مورد High، 7 مورد Medium و 9 مورد Informational می‌باشد.



1- بررسی Absence of Anti-CSRF Tokens

هیچ نشانه Anti-CSRF در فرم HTML sunmission یافت نشد. جعل درخواست بین سایتی حمله ای است که شامل وادار کردن قربانی به ارسال درخواست HTTP به مقصد مورد نظر بدون اطلاع یا قصد او برای انجام یک عمل به عنوان قربانی است. علت اصلی، عملکرد برنامه با استفاده از اقدامات URL/فرم قابل پیش بینی به روشی قابل تکرار است. ماهیت حمله این است که CSRF از اعتمادی که یک وب سایت به کاربر دارد سوء استفاده می کند. در مقابل، (XSS) از اعتمادی که کاربر به یک وب سایت دارد سوء استفاده می کند. مانند XSS، حملات CSRF لزوماً بین سایتی نیستند، اما می توانند باشند. جعل درخواست های متقاطع سایت به نام های CSRF، XSRF، حمله با یک کلیک، Session Riding، Confused deputy و Sea surf نیز شناخته می شود.

راه‌حل

باید از یک Framework بررسی شده استفاده کنیم که اجازه بروز این ضعف را نمی دهد یا ساختارهایی ارائه می دهد که اجتناب از این ضعف را آسان تر می کند. به عنوان مثال، استفاده از anti – CSRF Package مانند OWASP CSRFGuard.

2- بررسی CSP: Wildcard Directive

سیاست امنیتی محتوا (CSP) یک لایه امنیتی اضافه شده است که به شناسایی و کاهش انواع خاصی از حملات کمک می کند. شامل (اما نه محدود به) Cross Site Scripting (XSS) و حملات تزریق داده. این حملات برای همه چیز از سرقت داده تا تخریب سایت یا توزیع بدافزار استفاده می شود. CSP مجموعه‌ای از هدرهای استاندارد HTTP را ارائه می‌کند که به صاحبان وب‌سایت اجازه می‌دهد منابع محتوای تأیید شده‌ای را که مرورگرها باید مجاز به بارگذاری در آن صفحه باشند، اعلام کنند - انواع تحت پوشش عبارتند از JavaScript، CSS، فریم‌های HTML، فونت‌ها، تصاویر و اشیاء قابل جاسازی مانند اپلت‌های جاوا. اکتیو ایکس، فایل های صوتی و تصویری.

راه‌حل

اطمینان حاصل کردن از این که وب سرور، سرور برنامه، Load Balancer و غیره به درستی کانفیگ شده‌اند و هدر Content – Security – Policy (Header) را دارند.

3- بررسی **Vulnerable JS Library**

از کتابخانه Bootstrap ورژن 3.4.1 استفاده شده است که آسیب‌پذیر است.

راه‌حل

آپدیت کردن آن به آخرین ورژن