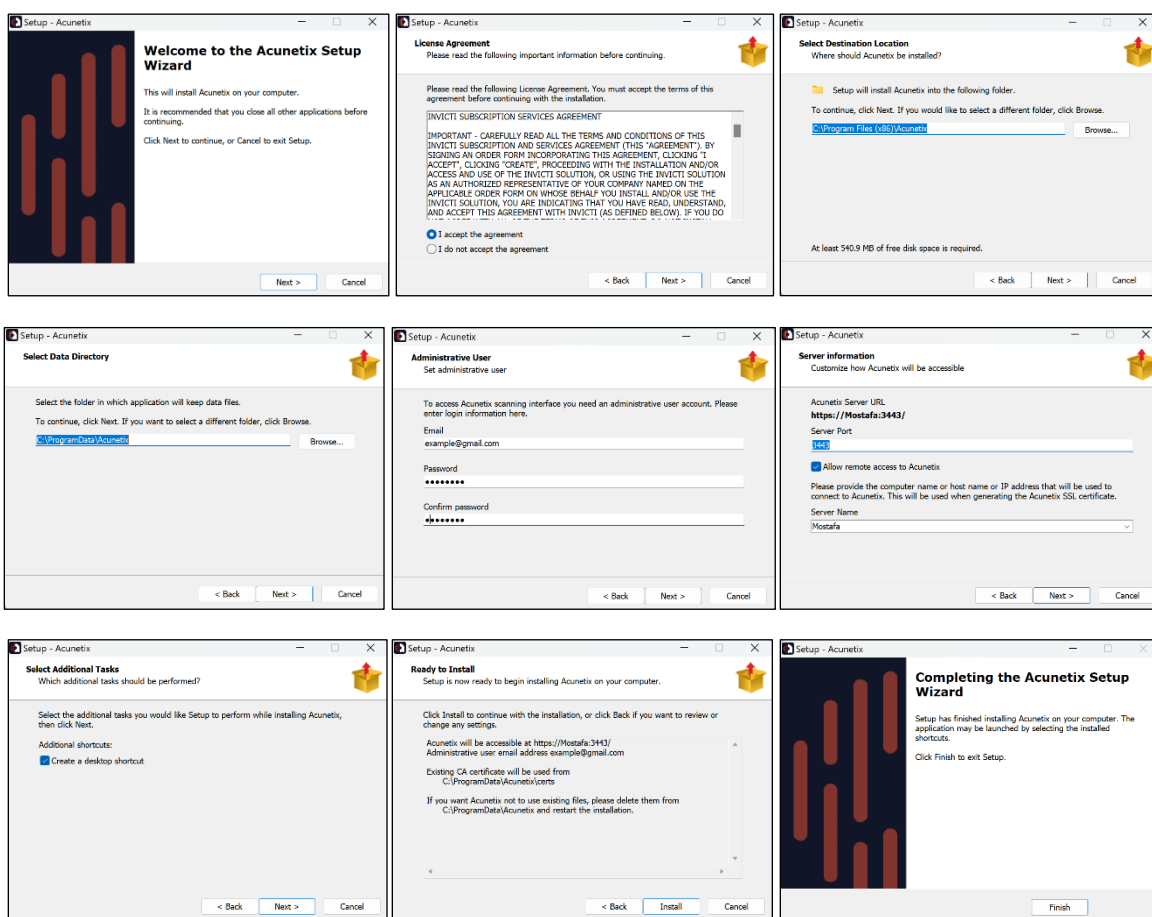


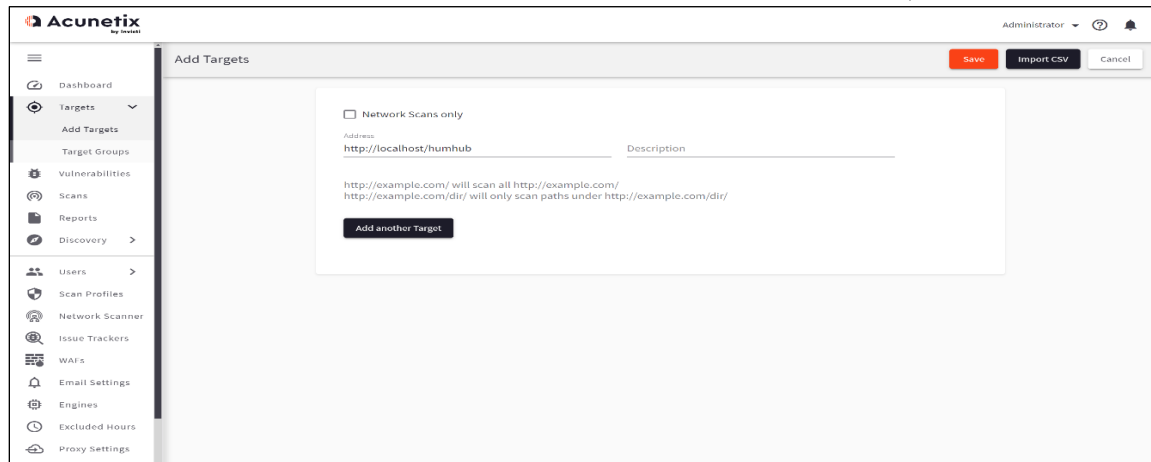
# گام دوم: بررسی امنیت شبکه اجتماعی HumHub

## با استفاده از Acunetix

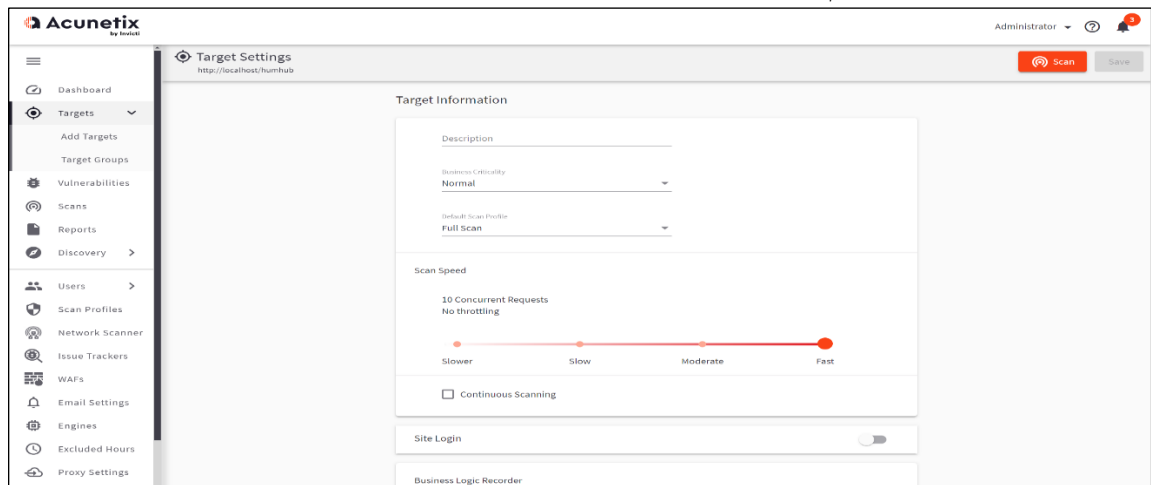
1- مراحل نصب را طبق تصاویر زیر انجام می‌دهیم.



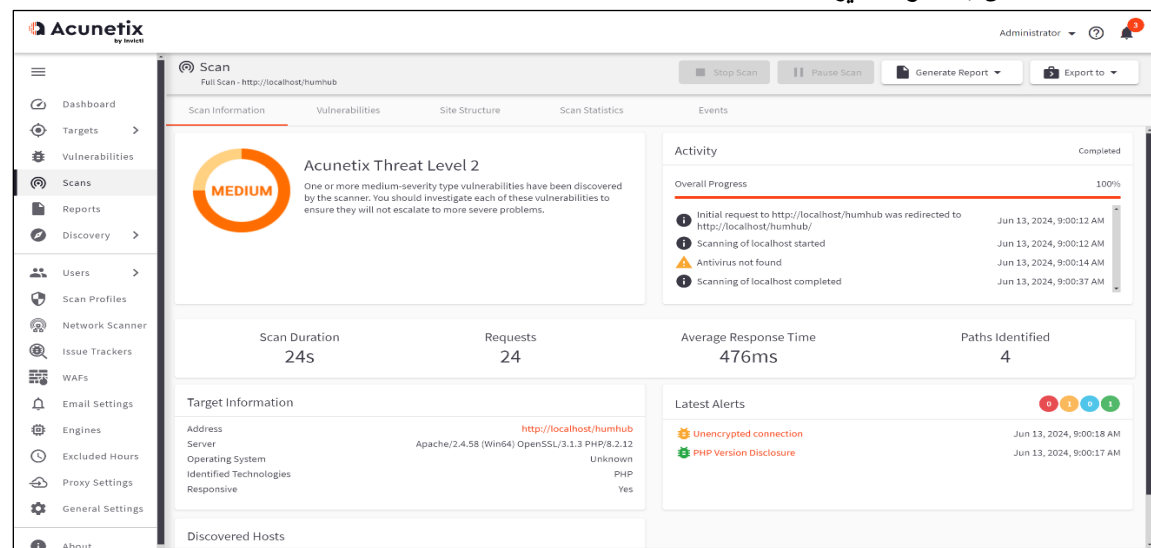
2- بر روی Add Target کلیک می‌کنیم و آدرس را (<http://localhost/humhub>) وارد می‌کنیم. سپس بر روی Save کلیک می‌کنیم.



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 از پروتکل https است.

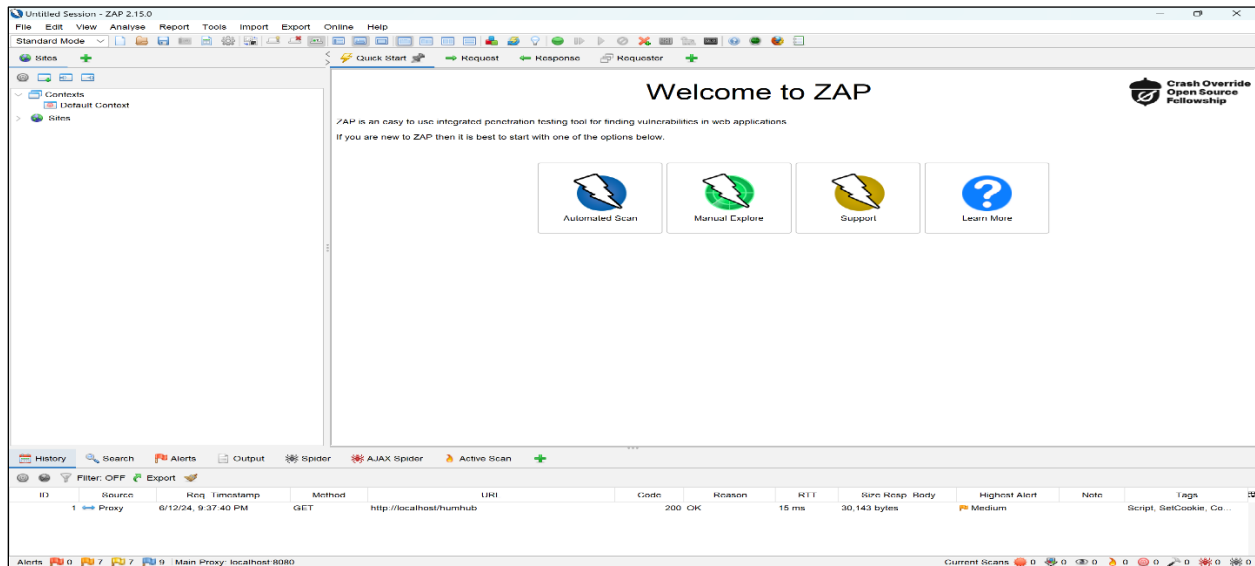
The screenshot displays the Acunetix web application security scanner interface. The left sidebar contains navigation links: Dashboard, Targets, Vulnerabilities, Scans, Reports, Discovery, Users, Scan Profiles, Network Scanner, Issue Trackers, WAFs, Email Settings, Engines, Excluded Hours, Proxy Settings, General Settings, and About. The main content area is titled 'Scan' and shows a 'Full Scan' of 'http://localhost/humhub'. The 'Vulnerabilities' tab is active, displaying a table of findings:

Severity	Vulnerability	URL	Parameter	Status	Confidence %
Medium	Unencrypted connection	http://localhost/		Open	100
Informational	PHP Version Disclosure	http://localhost/		Open	95

Below the table, it indicates 'Items per page: 20' and '1 - 2 of 2'. A detailed view of the 'Unencrypted connection' vulnerability is shown on the right. It includes the URL 'http://localhost/', a description stating that the scan target was connected over an unencrypted connection, and a note that a potential attacker can intercept and modify data. It also lists the discovery tool as '/RPA/no\_https.js' and provides sections for 'HTTP Request', 'HTTP Response', 'The impact of this vulnerability', and 'How to fix this vulnerability'.

# با استفاده از ZAP

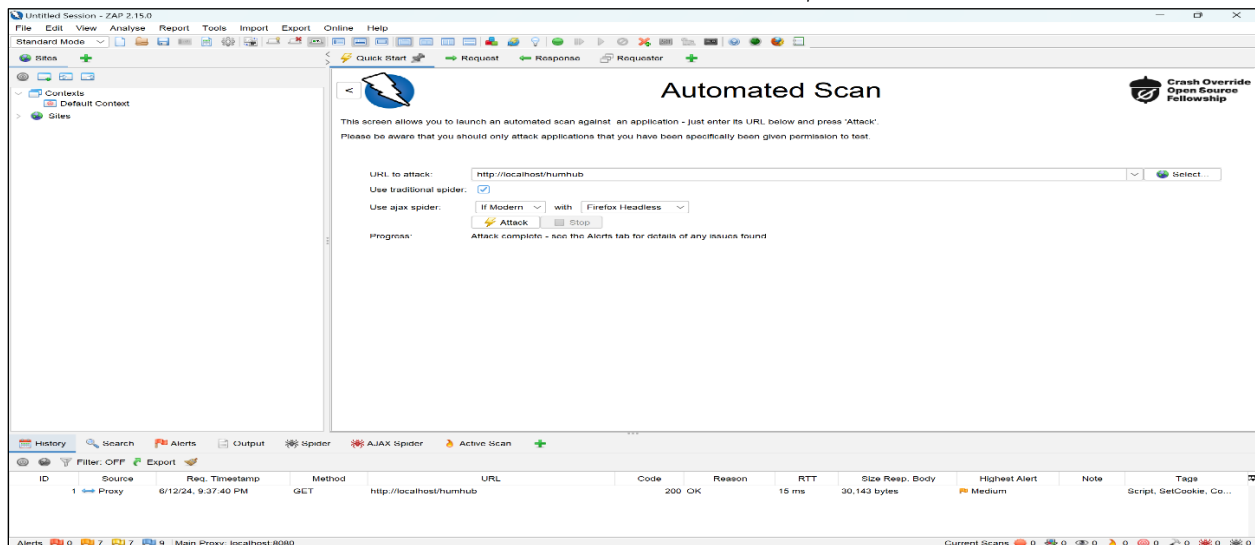
1- پس از نصب موفقیت آمیز برنامه، آن را اجرا می کنیم.



2- بر روی Automated Scan کلیک می کنیم.

3- URL شبکه اجتماعی یعنی <http://localhost/humhub> را وارد می کنیم.

4- بر روی Attack کلیک می کنیم.



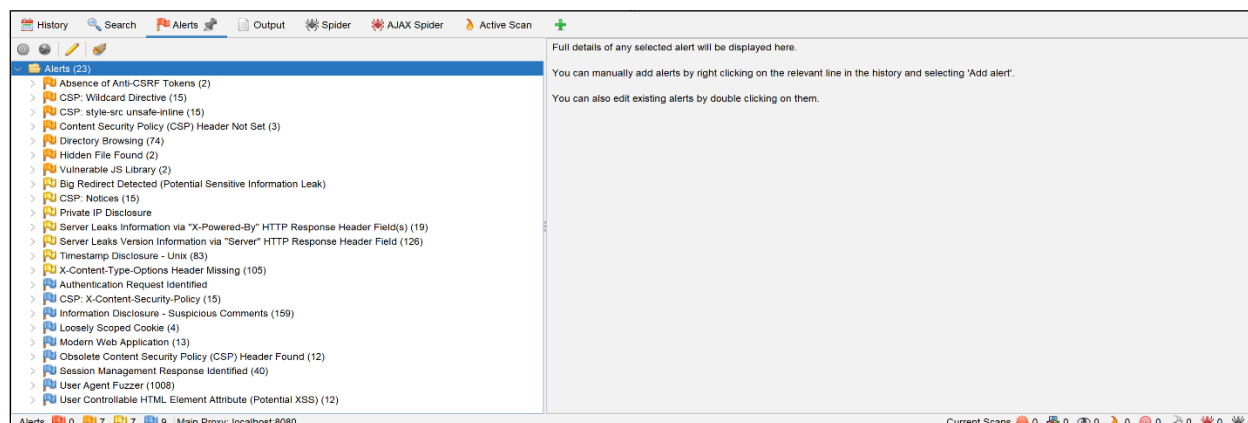
5- منتظر می مانیم تا فرایند بررسی به اتمام برسد.

6- به تب Alerts می رویم.

7- مشاهده می شود که 23 مورد شناسایی شده است.

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

از 23 مورد، 7 مورد High، 7 مورد Medium و 9 مورد Informational می باشد.



### 1- بررسی Absence of Anti-CSRF Tokens

هیچ نشانه Anti-CSRF در فرم HTML submission 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.

#### راه حل

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 مجموعه ای از هدرهای استاندارد HTTP را ارائه می کند که به صاحبان وب سایت اجازه می دهد منابع محتوای تأیید شده ای را که مرورگرها باید مجاز به بارگذاری در آن صفحه باشند، اعلام کنند - انواع تحت پوشش عبارتند از JavaScript، CSS، فریم های HTML، فونت ها، تصاویر و اشیاء قابل جاسازی مانند اپلت های جاوا. اکتیو ایکس، فایل های صوتی و تصویری.

## راه حل

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

### 3- بررسی Vulnerable JS Library

از کتابخانه Bootstrap ورژن 3.4.1 استفاده شده است که آسیب پذیر است.

## راه حل

آپدیت کردن آن به آخرین ورژن