Product Newsletter

March 2019 Edition

We hope you have noticed our announcement about our new pathbreaking scanner. You can check out the press release here.

APPTRANA

Recently we have added several features that help our large customers use Apptrana more efficiently. Some major features that went live were

ROLE BASED ACCESS CONTROL

Enterprises with diversified teams can now take advantage of RBAC and provide selective rights to different teams/ members. 3 types of users can be created in AppTrana.

1

Administrator

These users have complete control, and these are the only users who could create other users.

2

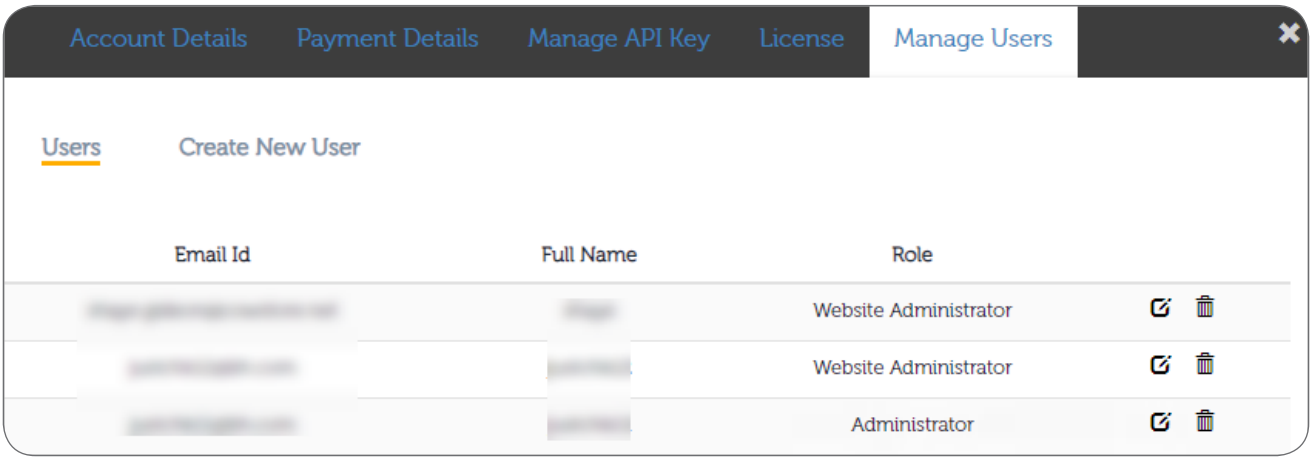
Website Administrator

These users have visibility and can make changes to websites associated to them. They will not be able to see websites not assigned to them and will not be able to change or upgrade plans.

3

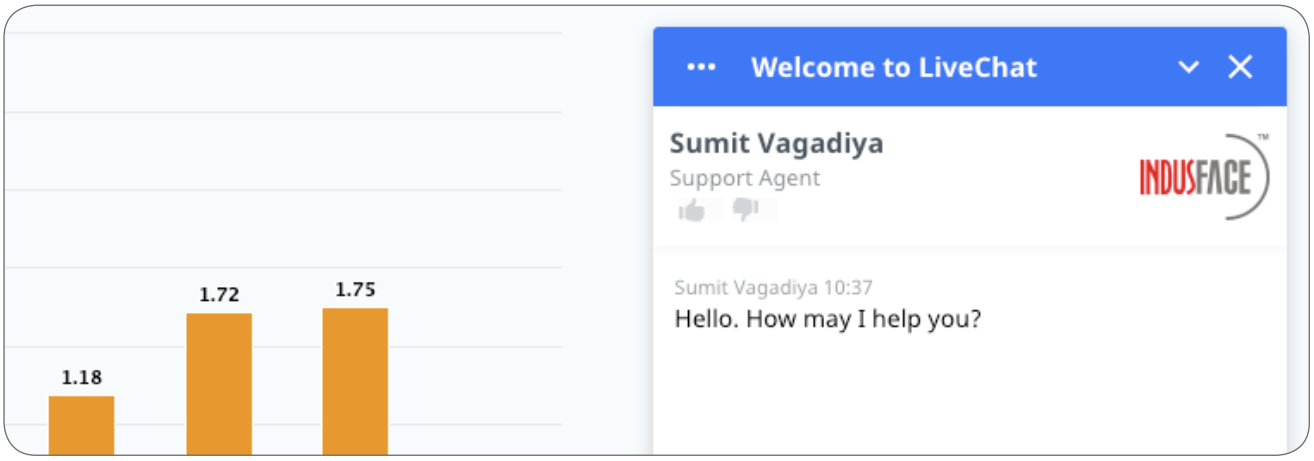
View Only Administrator

These users have visibility to websites assigned to them but won't be able to make any changes.



LIVE CHAT

With Live chat embedded in the portal, any user can directly reach out to our support team and get their queries addressed instantly. Chat is monitored 24*7 by our expert monitoring team and they would be happy to assist you.

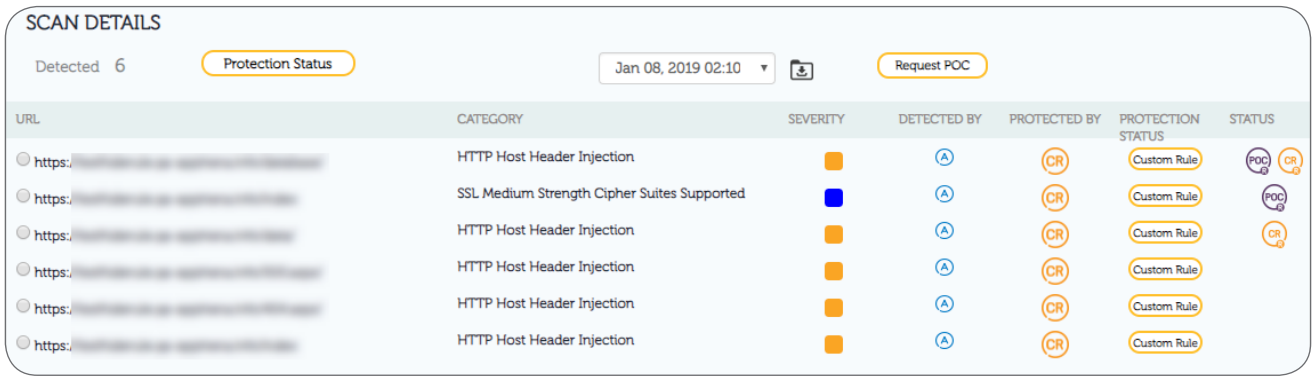


PROTECTION STATUS CHANGES

New enhancements to how protection status are shown for vulnerabilities found is now more actionable with direct visibility to applicable rules that can be turned on to get further protection.

Changes made were

- Protection status in detect page:
  - Different tabs were consolidated into 2 tabs Detected Tab & Protection Status Tab.
    - **Detected Tab -** Provides the details of vulnerability found
    - **Protection Status Tab –** Provides details of protection applied to the vulnerabilities including details if the vulnerability can be protected through custom rules or not.
  - Following states are shown under protected by.
    - **AR** – means the vulnerabilities can be protected by advance rules
    - **PR** - means the vulnerabilities can be protected by premium rules
    - **CR** – means the vulnerabilities can be protected by custom rules
    - **N/A** – means this cannot be fixed through WAF.
  - Protection status column – tells if the rules are actually applied and if protection is on.



WEB APPLICATION SCANNING

On the WAS side, our effort was to build upon the new scanner that we recently released and add features that would provide:

Some of the major advances made on WAS side are as follows:

SIGNATURE UPDATE

Signatures were added to find the following vulnerabilities:

1 Session ID scoped to parent domain

Session cookie is scoped to the parent domain instead of a sub-domain. If a cookie is scoped to a parent domain, then this cookie will be accessible by the parent domain and by any other sub-domains of the parent domain. This could lead to security problems.

2 XML RPC Vulnerability

XML-RPC is remote procedure calling using HTTP as the transport and XML as the encoding. An attacker can abuse this interface to brute force authentication credentials using API calls.

3 HSTS Missing from HTTPS Server

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTP (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period during which the user agent shall access the server in only secure fashion. If this is missing, then insecure agents would be able to connect.

GUIDED SCANS

Config driven guided scan support was introduced. Guides are lists of actions that will be taken automatically when all elements defined in that set of actions is encountered during crawl. Multiple guides can be defined per site. This will help crawler go to pages which it could not go before because of need of special actions. For example, say there is a multi-step wizard, where certain fields and inputs need to be provided to reach the next step, unless crawler knows what these actions are there is no way it goes further.

Now in such cases guided scan config can be added which tells crawler exactly what actions need to be taken. For customers needing such ability are requested to contact our support team, they would write the necessary config for your site and add it.

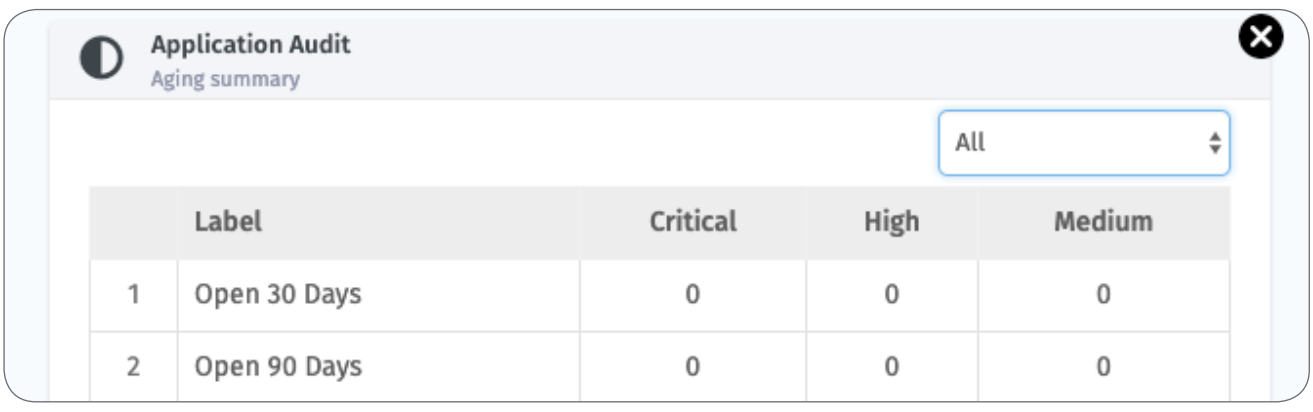
SCAN CONFIGS

Also, we had enabled the ability to add certain site-specific configs which would help customers create certain exceptions like

- **Exclude URI from attack**
  We have seen cases where there can be certain URI's that customers want to crawl to as it is through this that other pages can be reached but do not want attack to happen. In such cases customers can get certain URI whitelisted from attacks. This can be done by reaching out to support@indusface.com
- **Crawl to foreign domain.**
  By default, crawler does not crawl foreign domain, but in cases of SSO logins etc, it becomes important to crawl certain foreign domain URI's. Now this can be done through special config for a website. Please reach out to support to enable this.

AGING SUMMARY

We have added aging summary widget for AA, MM and VA scans. With this, customers can easily identify vulnerabilities that are older than certain time period. Which would help customers prioritize the fix for vulnerabilities.



BIFURCATION OF MANUAL AND AUTOMATED VULNERABILITY AS A WIDGET IN DASHBOARD

With this, customers can clearly see the vulnerabilities found through Manual PT vs Automated scans in the application audit widgets in the portal using the Manual PT & Automated scan filters available in the widgets The changes are done both in the dashboard page and application audit page.