Security Assessment Request Form

In order to get approval for performing in depth security scans targeting Pagely hosted sites or services you must complete the following form and submit it back to our security or support team. We will review and submit the completed form to our data center provider (Amazon Web Services) and get back to you within 3-5 business days with confirmation if the request has been approved or not, you should not begin any security scanning until you have received approval from Pagely staff.

For a smooth request process:

- Submit this form at least 1 week before any testing is scheduled to begin.
- Upon completion of the scan, you must send a copy of the report generated related to the scanning or testing to security@pagely.com for record keeping purposes and review.
- If you have any questions related to the findings in the report, you may open a support ticket via https://support.pagely.com/ and attach the report findings along with your questions or concerns.

Name of the professional service being utilized to perform the tests:

Contact information for the professional service being utilized:

Contact phone number and email for your staff during the testing window:

Server or website which will be the target of the testing:

Source IP addresses that the security assessment will originate from:

Approximate bandwidth expected utilized during the test:

Start Date: (date, hour and time zone)

End Date: (date, hour and time zone)

Formal Agreement:

Security Assessment (the “testing”):
(a) will be limited to the source and destination IP addresses, network bandwidth, and instance-level resources (such as CPU, memory and input/output) specified in your AWS Vulnerability/Penetration Testing Request Form, and the times and other conditions specified in the authorization email that will be sent to email addresses provided above,
(b) will not involve t2.nano, m1.small or t1.micro instances (as described on the AWS website, located at http://aws.amazon.com),
(c) is subject to the terms of the Amazon Web Services Customer Agreement between AWS and Company (available at http://aws.amazon.com/agreement/) (the “Agreement”),
(d) and will abide by AWS’s policy regarding the use of security assessment tools and services (included below).

Furthermore, Testing is not authorized until AWS validates the information and sends an authorization email to the requesting party containing an authorization number. Authorization can take up to 48 business hours. Any discoveries of vulnerabilities or other issues that are the direct result of AWS must be conveyed to aws-security@amazon.com within 24 hours of completion of the Testing. Your performance of the Testing and the results will be considered AWS Confidential Information under Section 9 of the Agreement.
Amazon Web Services, Inc.
Amazon Web Services (AWS) - Cloud Computing Services
Amazon Web Services offers reliable, scalable, and inexpensive cloud computing services. Free to join, pay only for what you use.

AWS’s policy regarding the use of security assessment tools and services allows significant flexibility for performing security assessments of your AWS assets while protecting other AWS customers and ensuring quality-of-service across AWS.
AWS understands there are a variety of public, private, commercial, and/or open-source tools and services to choose from for the purposes of performing a security assessment of your AWS assets.
The term “security assessment” refers to all activity engaged in for the purposes of determining the efficacy or existence of security controls amongst your AWS assets, eg. port-scanning, vulnerability scanning/checks, penetration testing, exploitation, web application scanning, as well as any injection, forgery, or fuzzing activity, either performed remotely against your AWS assets, amongst/between your AWS assets, or locally within the virtualized assets themselves.

You are NOT limited in your selection of tools or services to perform a security assessment of your AWS assets. However, you ARE prohibited from utilizing any tools or services in a manner that perform Denial-of-Service (DoS) attacks or simulations of such against ANY AWS asset, yours or otherwise. Prohibited activities include, but may not be limited to:

- Protocol flooding (eg. SYN flooding, ICMP flooding, UDP flooding)
- Resource request flooding (eg. HTTP request flooding, Login request flooding, API request flooding)

A security tool that solely performs a remote query of your AWS asset to determine a software name and version, such as “banner grabbing,” for the purpose of comparison to a list of versions known to be vulnerable to DoS, is NOT in violation of this policy.

Additionally, a security tool or service that solely crashes a running process on your AWS asset, temporary or otherwise, as necessary for remote or local exploitation as part of the security assessment, is NOT in violation of this policy. However, this tool may NOT engage in protocol flooding or resource request flooding, as mentioned above.

A security tool or service that creates, determines the existence of, or demonstrates a DoS condition in ANY other manner, actual or simulated, is expressly forbidden.

Some tools or services include actual DoS capabilities as described, either silently/inherently if used inappropriately or as an explicit test/check or feature of the tool or service. Any security tool or service that has such a DoS capability, must have the explicit ability to DISABLE, DISARM, or otherwise render HARMLESS, that DoS capability. Otherwise, that tool or service may NOT be employed for ANY facet of the security assessment.

It is the sole responsibility of the AWS customer to ensure the tools and services employed for performing a security assessment are properly configured and successfully operate in a manner that does not perform DoS attacks or simulations of such. It is the sole responsibility of the AWS customer to independently validate that the tool or service employed does not perform DoS attacks, or simulations of such, PRIOR to security assessment of any AWS assets. This AWS customer responsibility includes ensuring contracted third-parties perform security assessments in a manner that does not violate this policy.

Furthermore, you are responsible for any damages to AWS or other AWS customers that are caused by your penetration testing activities.

AWS Policy Regarding the Use of Security Assessment Tools and Services Agreement*

Please fill out your name and sign below

I, _____ hereby state that I have read and agree to the terms of the above policy as it related to the requested security assessment to be performed; as well as answered truthfully and accurately for all related questions in this document.

Signature: _____ Date: _____