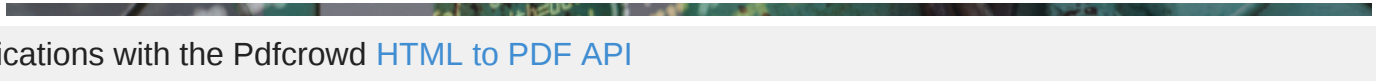
AWS changes its PenTesting permission requirement, Appsecco found out exactly what is allowed and what is not

Riyaz Walikar Follow
May 3 · 4 min read

A blogpost on the communication between us and AWS Support team to expand on some ambiguity within the AWS Customer Service Policy for Pen testing after the change in their process that removes the requirement of seeking permission before an assessment.



Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Background

If you are a security consulting company offering vulnerability discovery and attack related services, you would be familiar with the requirement from AWS regarding filling up and submission of a Vulnerability / Penetration Testing Request Form on the AWS portal.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

In this form an AWS customer had to provide information, using a root account, to AWS regarding the scheduled Penetration Testing exercise. This information was around the source of the attacks, expected peak bandwidth, start date and time, end date and time and other details relevant to the pentest.

AWS recently changed this process removing the requirement to seek permission from AWS before beginning testing for the following 8 services

- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateways
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

The complete policy can be found at — https://aws.amazon.com/security/penetration-testing/

The Ambiguity

At Appsecco, we frequently work with clients who have a large AWS presence and who seek our vulnerability assessment and penetration testing services. The removal of the form submission requirement meant one less thing to worry about in our engagement with our clients.

However, the section on **Prohibited Activities** and the **AWS Policy Regarding the Use of Security Assessment Tools and Services** section had us concerned as it said *Request flooding (login request flooding, API request flooding)* and *Resource request flooding (eg. HTTP request flooding, Login request flooding, API request flooding)* was prohibited, respectively in those sections.

In our understanding this included testing for weak credentials for Web Application login forms and directory/content discovery on Web Servers.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

We explained our understanding to the AWS Support team using the “AWS Security Simulated Event” email address listed on the Customer Service Policy for Pen Testing and receieved a response. The following are the questions we asked and the responses from AWS.

Our questions

1. Whether Login Request Flooding listed under Prohibited Activities includes automated testing for weak credentials for Web Application login forms (hosted on EC2), specifically tests listed under https://www.owasp.org/index.php/Testing_for_Brute_Force_(OWASP-AT-004) even if they are kept well under 10,000 Requests Per Second (RPS). (currently at about 300 RPS)
2. Whether hunting for hidden files and directories under web application folders is allowed, even if they are kept well under 10,000 RPS (currently at about 300 RPS)
3. Whether any other security test that we may conduct that is not meant to be a Denial of Service making requests of less than 1000 RPS, is allowed or not.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Response from AWS

1. Our restrictions on login request flooding are intended to prevent disabling of login and authentication services by overwhelming them with login attempts. Automated testing for weak or commonly used credentials and other forms of brute force vulnerability testing is authorized so long as the traffic is at a rate slow enough that every request can be processed to completion.
2. Hunting for hidden files and directories is permitted so long as the target of your testing has authorized this activity.
3. Other forms of security testing and scanning not explicitly prohibited by our penetration testing policy are allowed. As a general rule, if the target is aware of your activity and your path of ingress does not include flooding or otherwise attempting to overwhelm the target with data it is permitted.

Conclusion

From the responses it is clear that an automated test is allowed as long as

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- the traffic is at a rate slow enough that every request can be processed to completion
- the target of our testing has authorized the activity

As a general rule, if the target is aware of your activity and your path of ingress does not include flooding or otherwise attempting to overwhelm the target with data it is permitted.

. . .

At Appsecco we provide advice, testing, training and insight around software and website security, especially anything that's online, and its associated hosting infrastructure — Websites, e-commerce sites, online platforms, mobile technology, web-based services etc.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

AWS | Vulnerability Assessment | Penetration Testing | Brute Force Attack | Denial Of Service

76 claps

WRITTEN BY

Riyaz Walikar

Follow

Chief Offensive Security Officer, @Appseccouk

Appsecco

Follow

Making sense of application security for everyone. Follow us to get a pragmatic view of the landscape including hacks, attacks, modern defence techniques. We cover ideas on securing applications, training the modern workforce in secure development and testing.

Write the first response

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

More From Medium

Related reads

Rootpipe Reborn (Part I)

codecolorist in...
Apr 13 · 6 min read ★

219

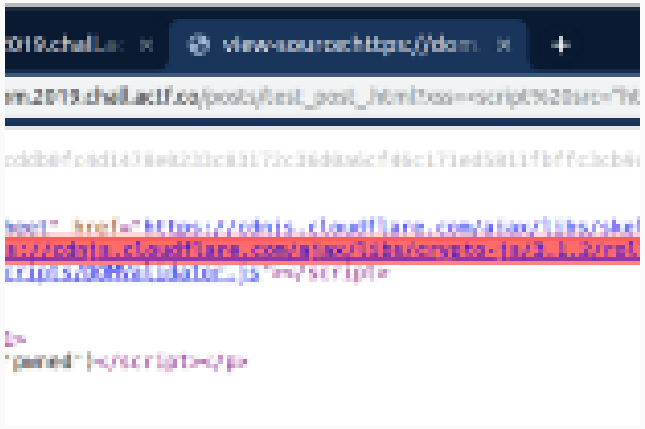
Related reads

How Slack Hires a Red Team (and you can too!)

John Sonnenschein in...
May 7 · 8 min read ★

84

Related reads



XSS-Auditor — the protector of unprotected

terjanq in InfoSec Writ...
Apr 25 · 4 min read ★

316

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD