ThreatModeler
Identify • Classify • Prioritize • Mitigate

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2017

AWS Threat Model - 1

03/27/2017

Threats

Threat	Source	Risk	Status	Date Created
Weak Identity, Credential and Access Management	Amazon EBS	Very High	Open	03/27/2017
Account Hijacking	Amazon EBS	Very High	Open	03/27/2017
Confidential Data Exposure	Amazon RDS	Very High	Open	03/27/2017
Weak Identity, Credential and Access Management	Amazon RDS	Very High	Open	03/27/2017
Account Hijacking	Amazon RDS	Very High	Open	03/27/2017
Malicious Insiders	Amazon RDS	Very High	Open	03/27/2017
Permanent Data Loss	Amazon RDS	Very High	Open	03/27/2017
Insecure Communication	Amazon RDS	Very High	Open	03/27/2017
Weak Identity, Credential and Access Management	ELB	Very High	Open	03/27/2017
Account Hijacking	ELB	Very High	Open	03/27/2017
Insecure Communication	ELB	Very High	Open	03/27/2017
Weak Identity, Credential and Access Management	Amazon CloudFront	Very High	Open	03/27/2017
Denial of Service	Amazon CloudFront	Very High	Open	03/27/2017
Sensitive Data Exposure	Amazon S3	Very	Open	03/27/2017

		High		
Confidential Data Exposure	Amazon S3	Very High	Open	03/27/2017
Weak Identity, Credential and Access Management	Amazon S3	Very High	Open	03/27/2017
Denial of Service	Amazon S3	Very High	Open	03/27/2017
Man in the Middle Attack	Gateway	Very High	Open	03/27/2017
WiFi Jamming	Gateway	High	Open	03/27/2017
Weak Identity, Credential and Access Management	Amazon EC2	Very High	Open	03/27/2017
System and Application Vulnerability	Amazon EC2	Very High	Open	03/27/2017
Account Hijacking	Amazon EC2	Very High	Open	03/27/2017
Malicious Insiders	Amazon EC2	Very High	Open	03/27/2017
Denial of Service	Amazon EC2	Very High	Open	03/27/2017
Exploiting Incorrectly Configured SSL Security Levels	HTTPS	Low	Open	03/27/2017
Clickjacking	Web App	Very High	Open	03/27/2017
HTTP Response Splitting	Web App	High	Open	03/27/2017
Cross Site Request Forgery aka Session Riding	Web App	Very High	Open	03/27/2017
SQL Injection	Web App	High	Open	03/27/2017
Blind SQL Injection	Web App	High	Open	03/27/2017
Reflected Cross Site Scripting - WASC	Web App	High	Open	03/27/2017
Persistent Cross Site Scripting - WASC	Web App	High	Open	03/27/2017
Accessing and or Intercepting and or Modifying HTTP Cookies	Web App	High	Open	03/27/2017
Session Hijacking	Web App	Very High	Open	03/27/2017
Session Credential Falsification through Forging	Web App	Medium	Open	03/27/2017
Reusing Session IDs aka Session Replay	Web App	High	Open	03/27/2017
Session Fixation	Web App	High	Open	03/27/2017
File Manipulation	Web App	Medium	Open	03/27/2017
Accessing, Modifying or Executing Executable Files	Web App	Very High	Open	03/27/2017

Create files with the same name as files protected with a higher classification	Web App	Very High	Open	03/27/2017
Manipulating Writeable Configuration Files	Web App	Very High	Open	03/27/2017
Manipulating Input to File System Calls	Web App	Very High	Open	03/27/2017
Dictionary-based Password Attack	Web App	High	Open	03/27/2017
Password Brute Forcing	Web App	High	Open	03/27/2017
Password Recovery Exploitation	Web App	High	Open	03/27/2017
Exploit Common or default Usernames and Passwords	Web App	High	Open	03/27/2017