aws summit



0 E T 4 Ø 5

Threat modelling to evaluate the security and resilience of your generative AI workloads

Atul Dambalkar

Senior Solutions Architect AWS India

Ankush Agarwal

Solutions Architect AWS India



What is a threat model?

SHOSTACK'S 4-QUESTION FRAME



What are we working on?



What can go wrong?



What are we going to do about it?



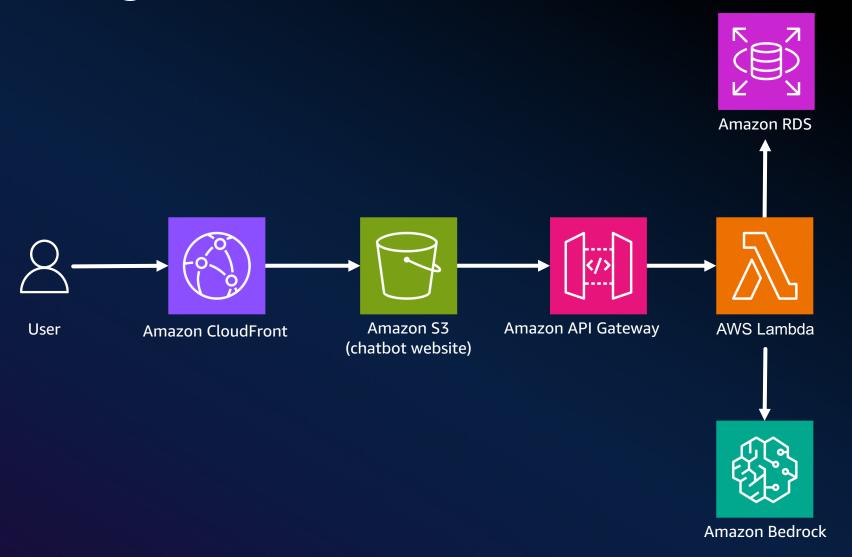
Did we do a good enough job?

What are we working on?

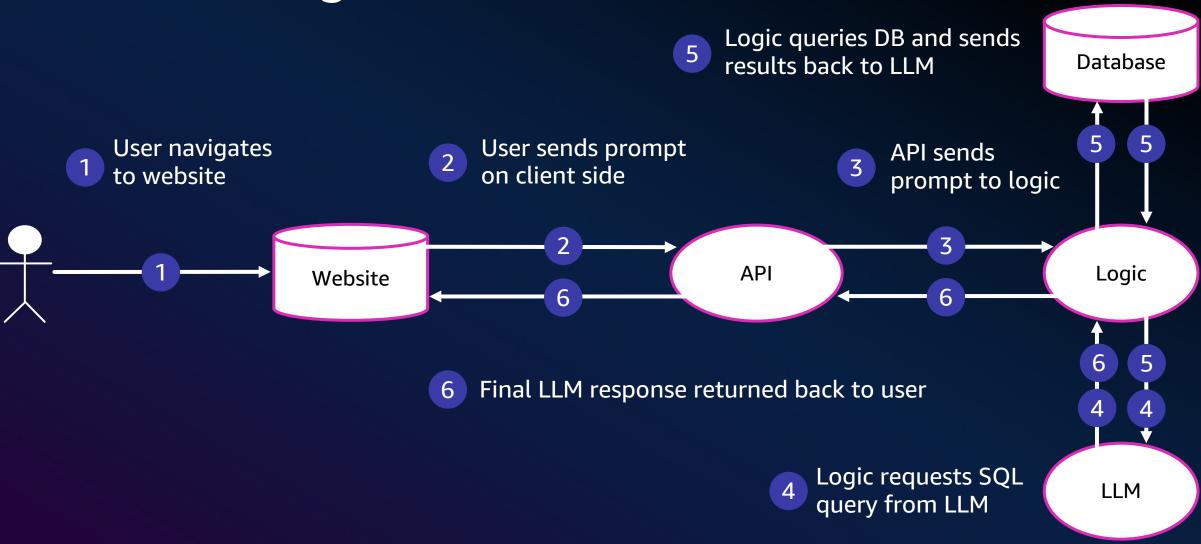
What medications am I currently taking?

You started taking Propranolol a year ago for heart palpitations.

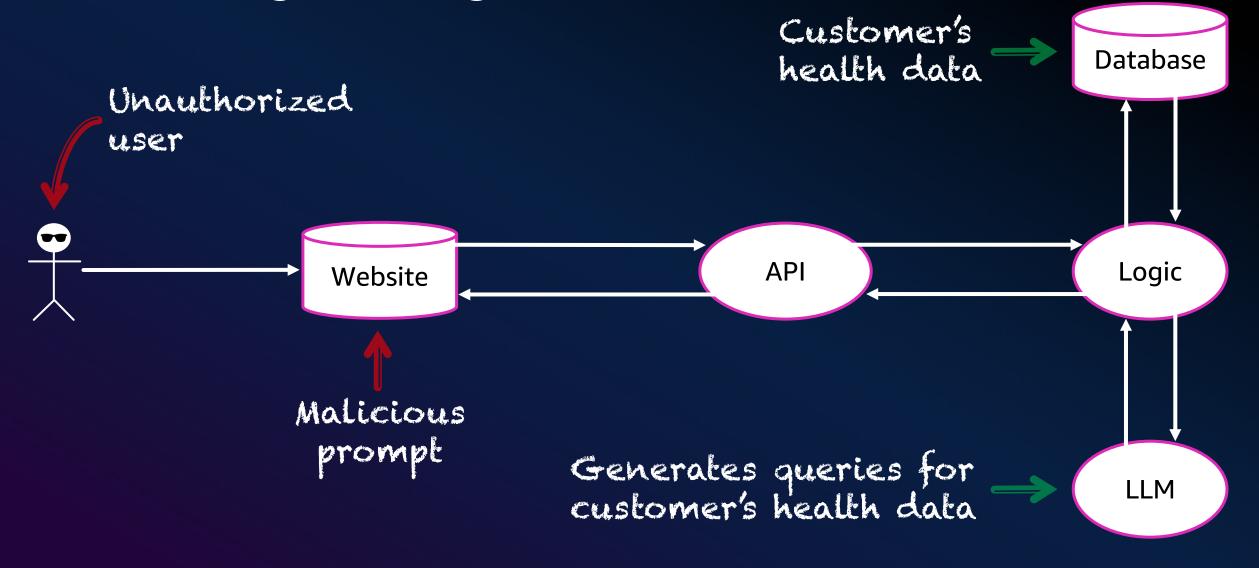
Chat here...



Data flow diagram



What can go wrong?





Threat statement

→ A [threat source] with [pre-requisites],
 can [threat action],
 which leads to [threat impact],
 negatively impacting [goal] of [impacted assets].



Threat statement

An external threat actor with access to the public facing application,

can inject malicious prompts which overwrite existing system prompts,

resulting in healthcare data from other patients being returned,

impacting the confidentiality of the data in the database.



Demo



Develop mitigations

Application LLM uses prompt SQL query result Prompt passed to to generate SQL passed to user via accepts any LLM from logic prompt from user LLM response query Define acceptable Predefine and check Validate output is Sanitize for known use with system against acceptable relevant to user parameters **SQL** statements prompt

Examples



Did we do a good enough job?

Verify Mitigations

Pentesting

→ Per release

→ Recurring

Validate Process

Compare

Other threat frameworks

Review

└── Accuracy

└ Completeness

└── Clarity



How can we operationalize and continuously improve resilience?



Foundational resilience Continuous resilience

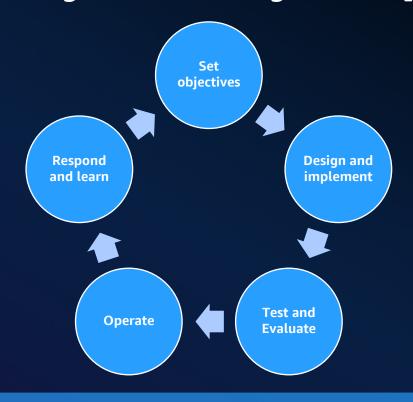


The resilience lifecycle





The resilience lifecycle – Key Outputs



Key outputs

Identified priorities

Better operational practices

Learning/mitigation capabilities



Practices at each step



Setting objectives



Workload prioritization and tiering



Objective metrics identification



AWS continuous resilience services

Set objectives



Design & implement



Test & evaluate



Operate

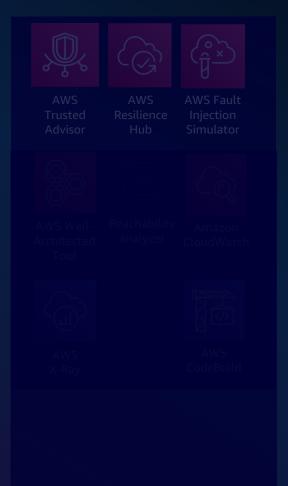


Respond & learn



Set objectives













Design and implement



Architecture recommendation



Foundational resilience services and features



CI/CD



Logging



Dependency mapping



Code reviews and frameworks



Backup and disaster recovery



Training



AWS continuous resilience services

Set objectives



Design & implement



Test & evaluate



Operate



Respond & learn



Set objectives







AWS Well-Architected Framework



Amazon

CloudWatch



AWS Trusted Advisor



AWS Well-Architected Tool



AWS X-Ray



AWS CodePipeline



AWS Elastic Disaster Recovery



Amazon CodeGuru



Flow logs





















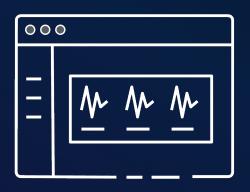




Test and Evaluate



Tracing



Performance benchmarking



Fault injection and GameDays



Load testing

AWS continuous resilience services

Set objectives



Design & implement



Test & evaluate



Operate



Respond & learn



Set objectives









AWS Trusted Advisor



AWS Resilience Hub



AWS Fault Injection Simulator









































AWS Well-Architected Tool









AWS X-Ray



AWS CodeBuild

Operate









Synthetic traffic

Alarming

Operational reviews

Load testing

AWS continuous resilience services

Set objectives



Design & implement



Test & evaluate



Operate



Respond & learn



Set objectives



















































Amazon OpenSearch Service









Respond and learn









Auto remediation

Escalation paths

Event management

Correction of errors



AWS continuous resilience services

Set objectives



Design & implement



Test & evaluate



Operate



Respond & learn



Set objectives















































AWS Config



AWS Systems Manager



Route 53 Application **Recovery Controller**





Build beyond

Redeem your free 7-day trial of AWS Skill Builder



Thank you!

Atul Dambalkar

Senior Solutions Architect AWS India

Ankush Agarwal

Solutions Architect AWS India



Please complete the session survey in the mobile app