Logging and Monitoring

Sprint: 1

1

As a ***Developer***, I want ***the app to log all user and system actions to the server*** so that ***I can diagnose security issues when they occur***.

Story Points: 2 **Customer Value:** 5

Data Backup

Sprint: 1

2

As a ***System Administrator***, I want ***to schedule regular backups of server data to an offsite location*** so that ***we can restore operations quickly in case of a failure or breach***.

Story Points: 1 **Customer Value:** 10

Password Security Rules

Sprint: 1

3

As a ***User***, I want ***the app to enforce passwords that include uppercase, lowercase, and numbers with a minimum of 8 characters*** so that ***my account is more secure***.

Story Points: 1 **Customer Value:** 15

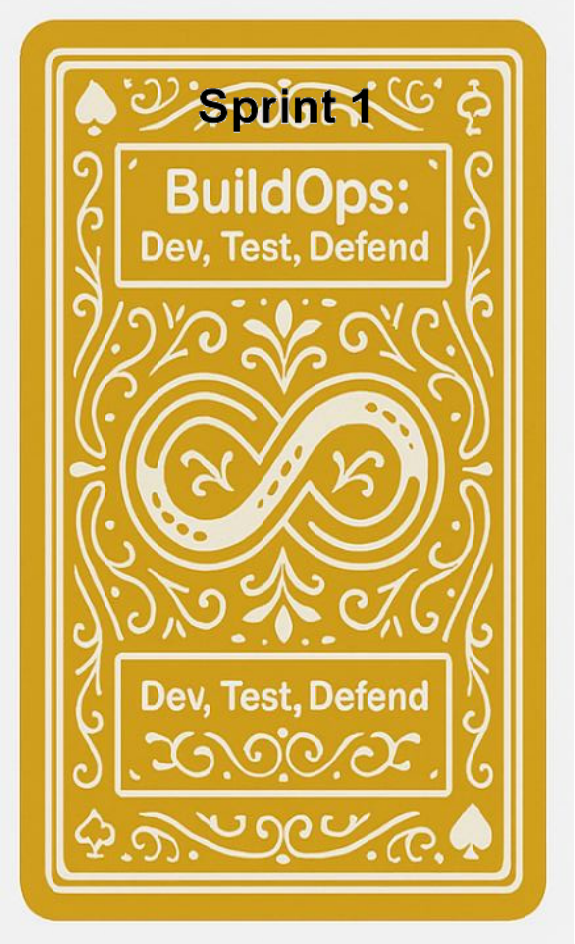
Password Change

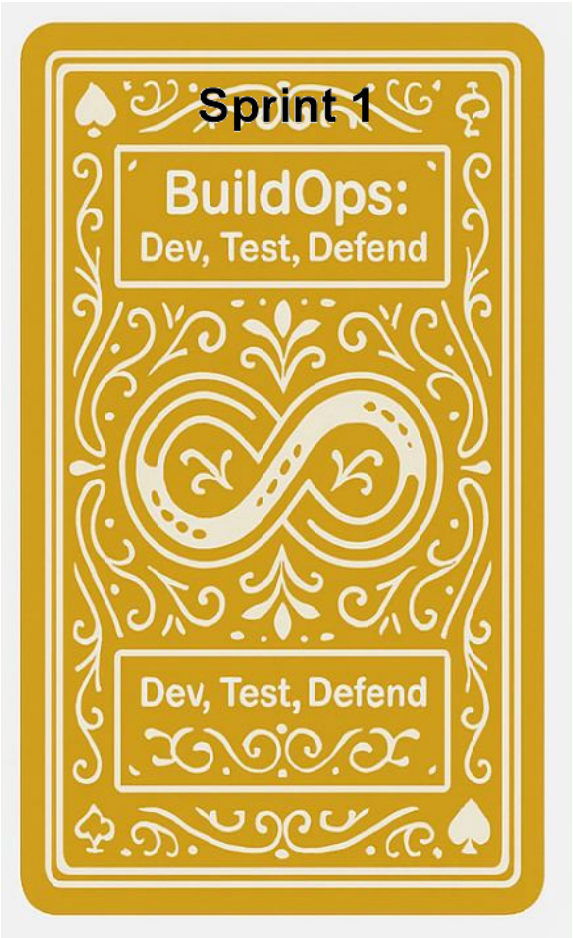
Sprint: 1

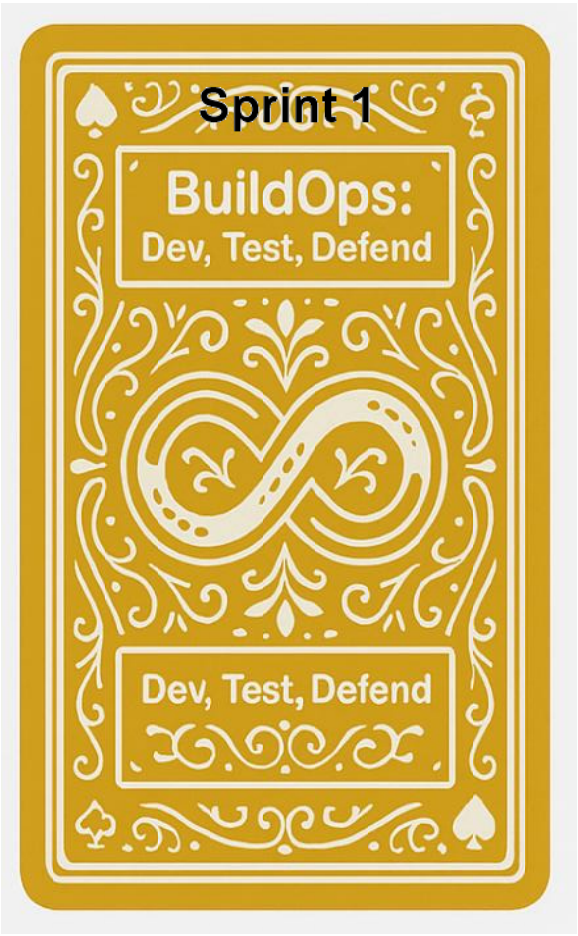
4

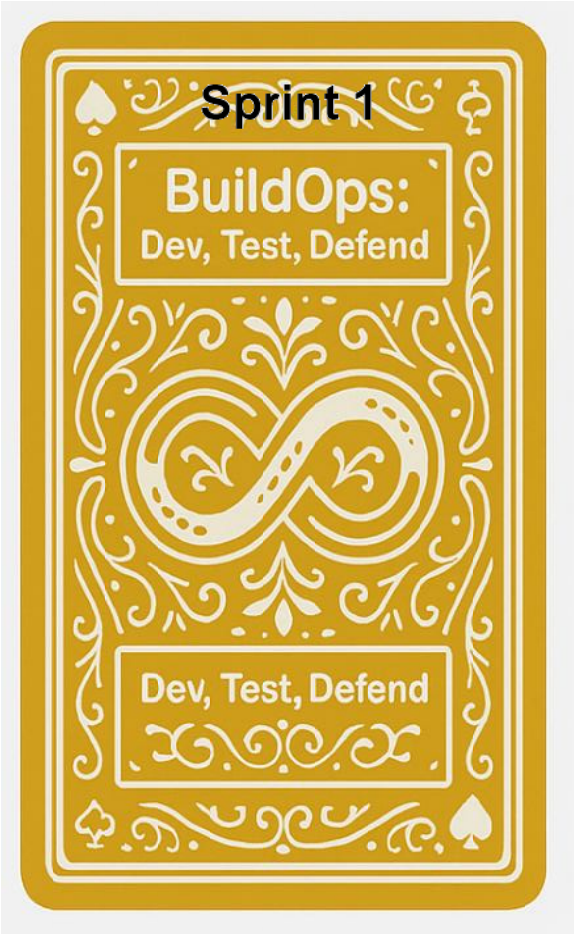
As a ***Security Officer***, I want ***the app to require users to change their passwords regularly*** so that ***compromised credentials cannot be used long-term***.

Story Points: 2 **Customer Value:** 15


Sprint 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend

Secure Network Communication

Sprint: 1

5

As a ***User***, I want ***all app-server communications to use HTTPS*** so that ***my data cannot be intercepted by attackers***.

Story Points: 2 **Customer Value:** 20

Security Review of Application

Sprint: 1

6

As a ***Product Owner***, I want ***an external security expert to perform code and design reviews of the app*** so that ***we can fix any vulnerabilities early***.

Story Points: 4 **Customer Value:** 10

Device Integrity Check

Sprint: 1

7

As a ***Developer***, I want ***the app to detect and block usage on jailbroken or rooted devices*** so that ***we can reduce the risk of compromised environments***.

Story Points: 2 **Customer Value:** 15

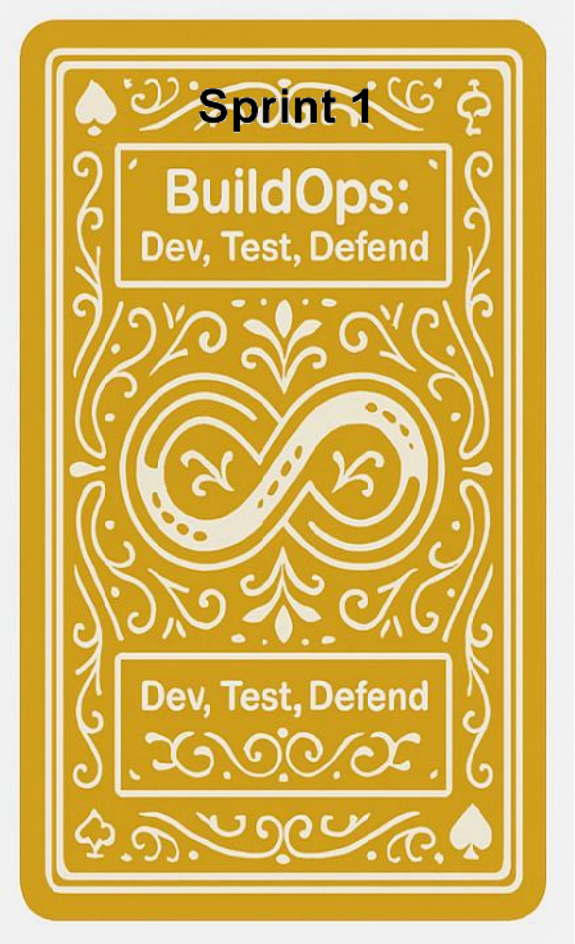
Server Penetration Testing

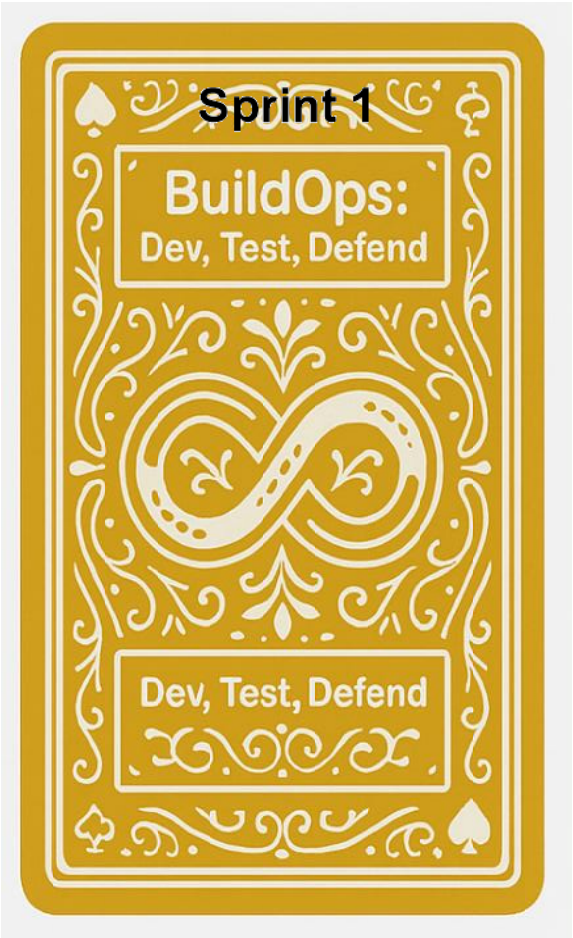
Sprint: 1

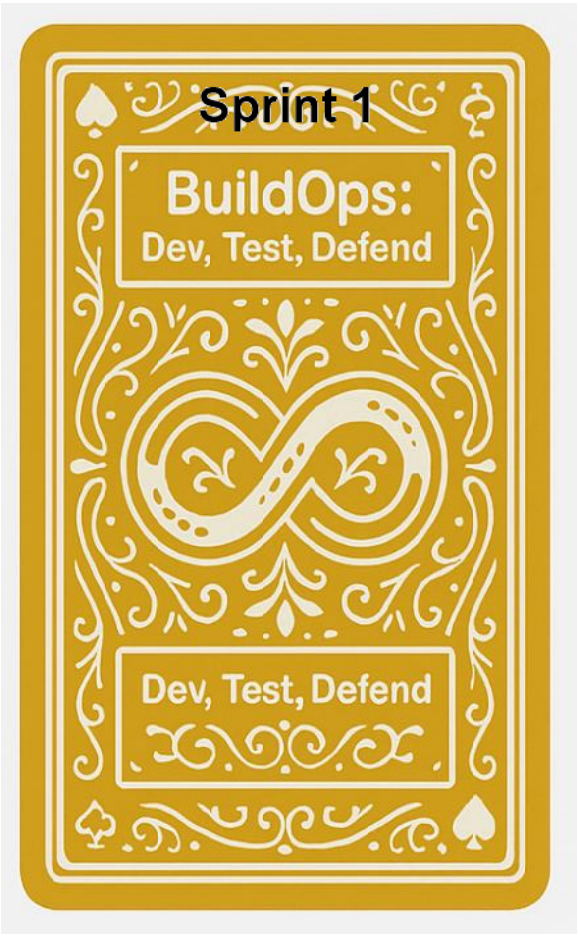
8

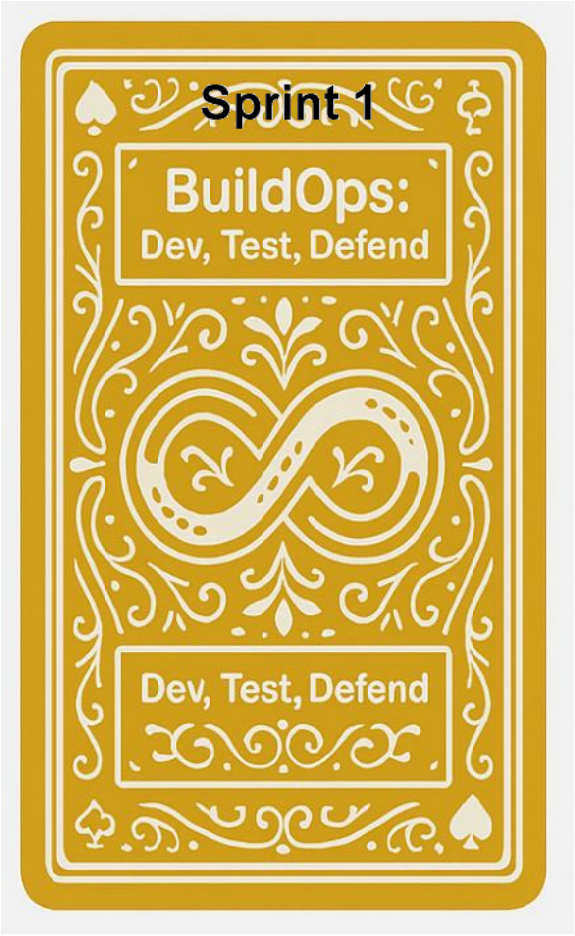
As a ***CTO***, I want ***an external security expert to attempt to breach the server*** so that ***we can identify and patch security weaknesses***.

Story Points: 4 **Customer Value:** 5


Sprint 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend

Server Patches

Sprint: 1

9

As a ***CTO***, I want ***the IT team ensure that all software versions are current and patched*** so that ***we can ensure that all known vulnerabilities have been removed and all functions are operating properly.***.

Story Points: 2 **Customer Value:** 5

Two Factor Authentication

Sprint: 2

10

As a ***User***, I want ***the login process to include a verification code sent to my phone or authentication app*** so that ***my account is protected even if my password is stolen***.

Story Points: 4 **Customer Value:** 10

Security Review of Server Code

Sprint: 2

11

As a ***Product Owner***, I want ***an external security expert to review the server configuration and code*** so that ***we can mitigate backend vulnerabilities***.

Story Points: 4 **Customer Value:** 5

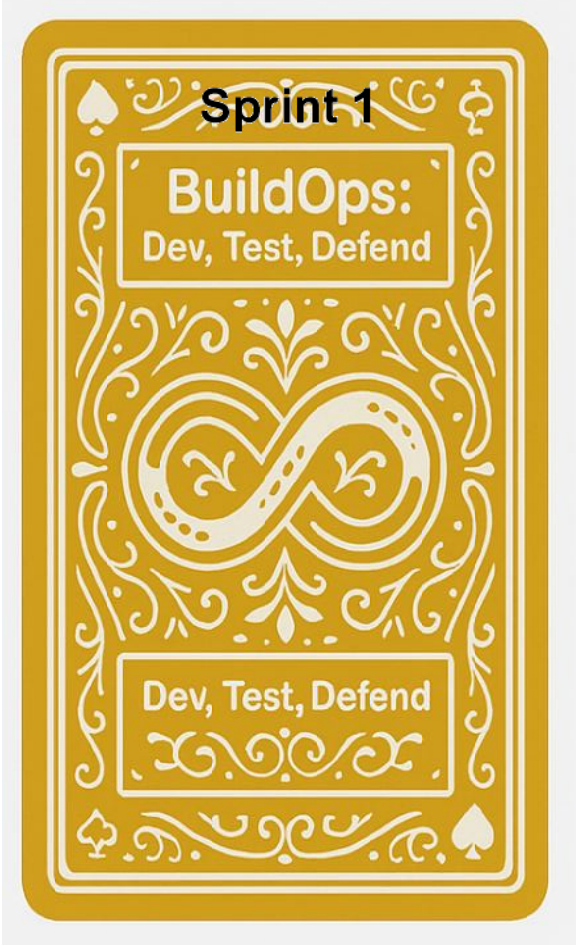
Network Protection

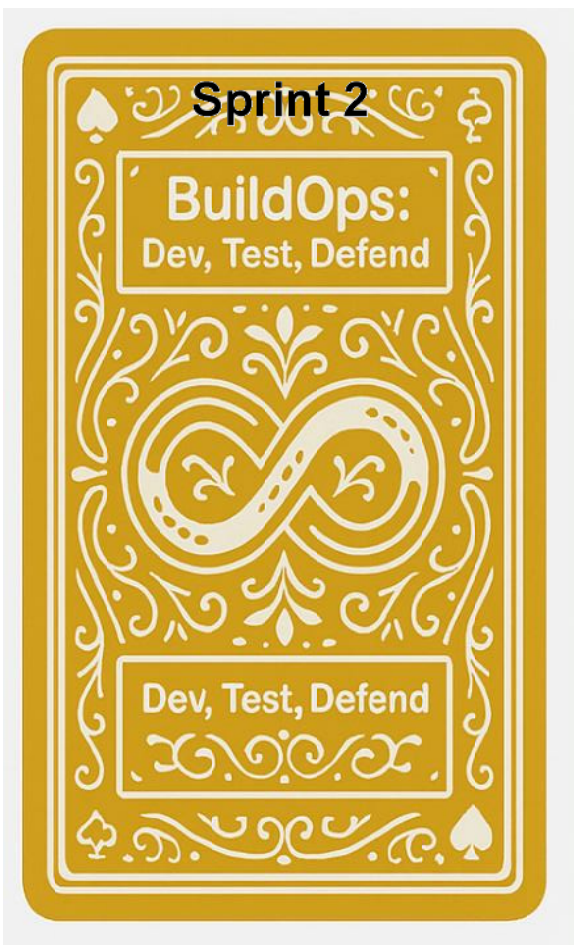
Sprint: 2

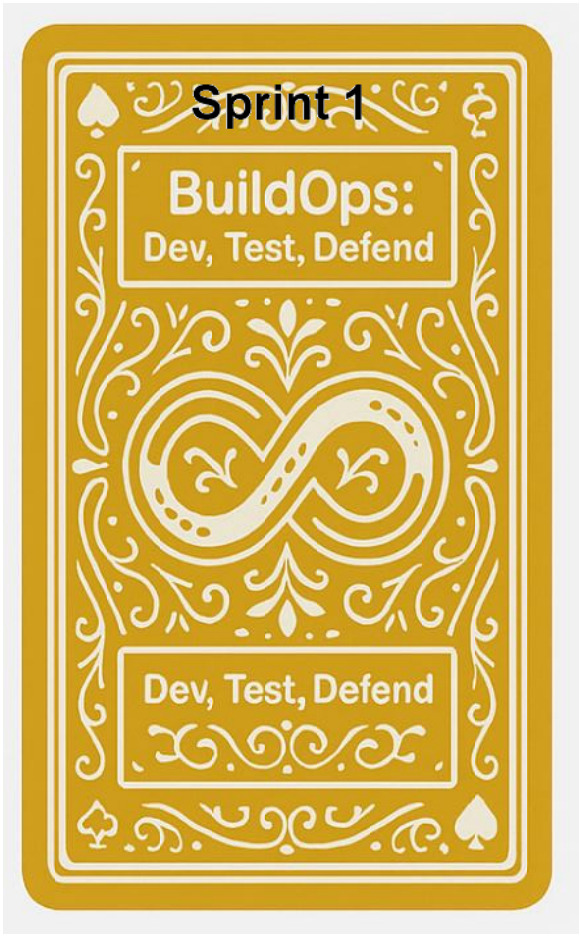
12

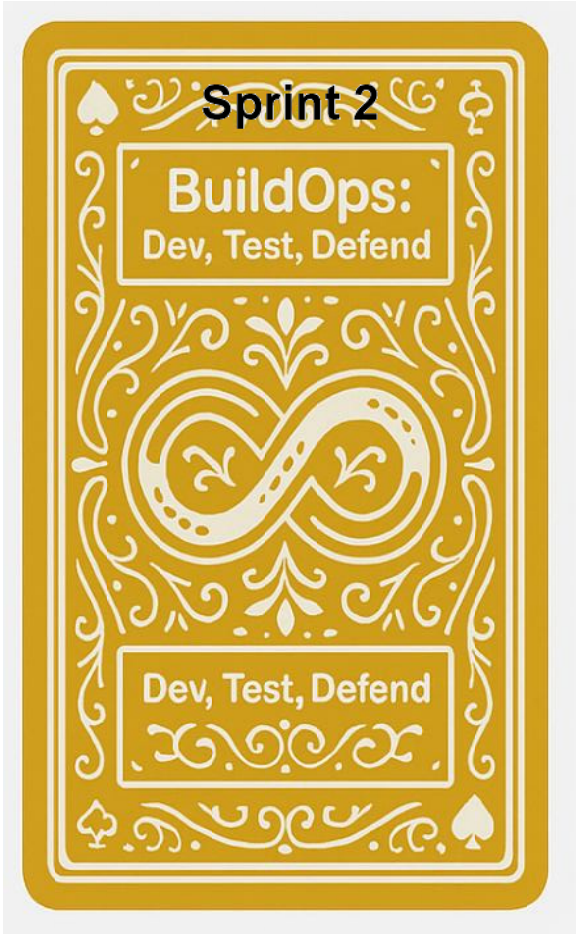
As a ***IT Administrator***, I want ***firewall systems and phishing filters in place for office networks*** so that ***internal systems are protected from external threats***.

Story Points: 4 **Customer Value:** 10


Sprint 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint 2
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint 2
BuildOps:
Dev, Test, Defend
Dev, Test, Defend

Hardware Security Module

Sprint: 2

As a ***Security Engineer***, I want ***all sensitive credentials and encryption keys to be stored in a Hardware Security Module (HSM)*** so that ***they are not exposed to unauthorized access***.

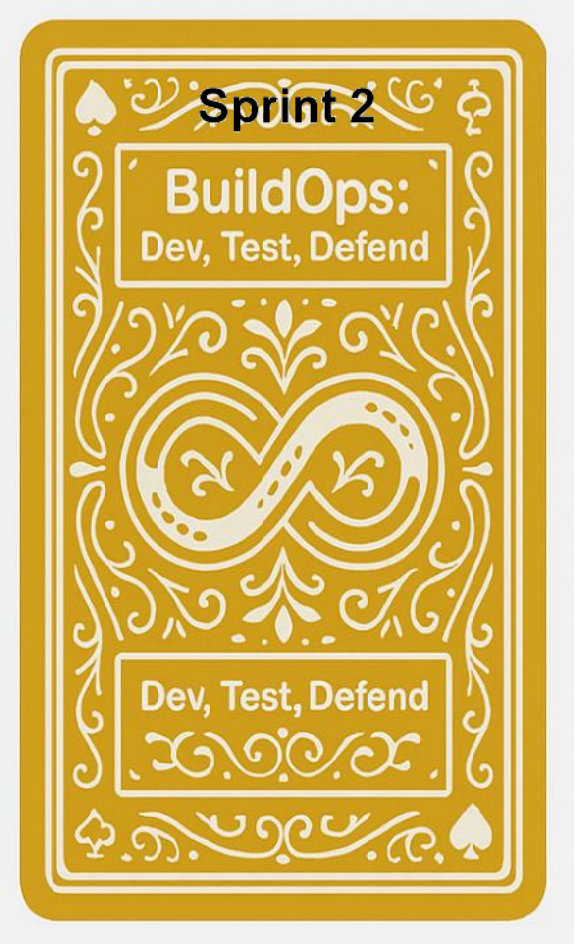
Story Points: 3 **Customer Value:** 5

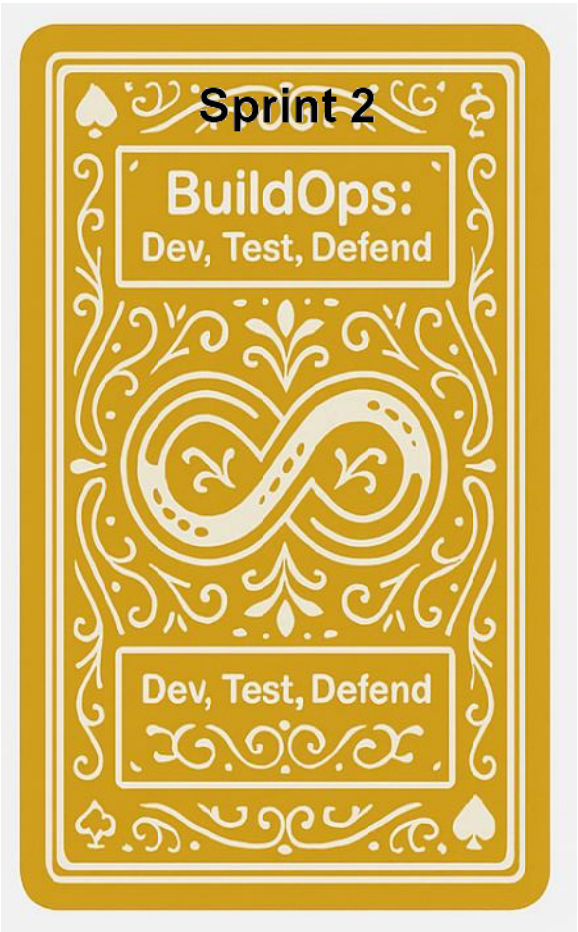
Incident Communication

Sprint: 2

As a ***Marketing Lead***, I want ***a communications plan for security breaches*** so that ***we can respond to incidents transparently and protect the brand***.

Story Points: 4 **Customer Value:** 15


Sprint 2
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint 2
BuildOps:
Dev, Test, Defend
Dev, Test, Defend

Encrypt & Hide Data on Server

15

Sprint: PT

As a ***Penetration Tester***, I want ***the server data to be properly encrypted, unlocked only by software 'keys' in the server process, and backups to be stored offline only in an encrypted format*** so that ***an attacker who gains access to the computer system running the server won't be able to read any server data.***.

Story Points: 2 **Customer Value:** 10

Network Monitoring for Server

16

Sprint: PT

As a ***Penetration Tester***, I want ***to put in a specialist 'network monitoring' system around the server access to detect unusual network traffic that suggests an attack*** so that ***the operations team can detect a potential attack and mitigate it before it is successful.***.

Story Points: 8 **Customer Value:** 10

Honeytrap in server

17

Sprint: PT

As a ***Penetration Tester***, I want ***the development team to place a honeypot in the system to make it look as if there's nothing much for a hacker to find there but what they'll find appears to be live data*** so that ***adversaries have a more challenging time hacking the network and are not able to traverse the network as quickly.***.

Story Points: 4 **Customer Value:** 5

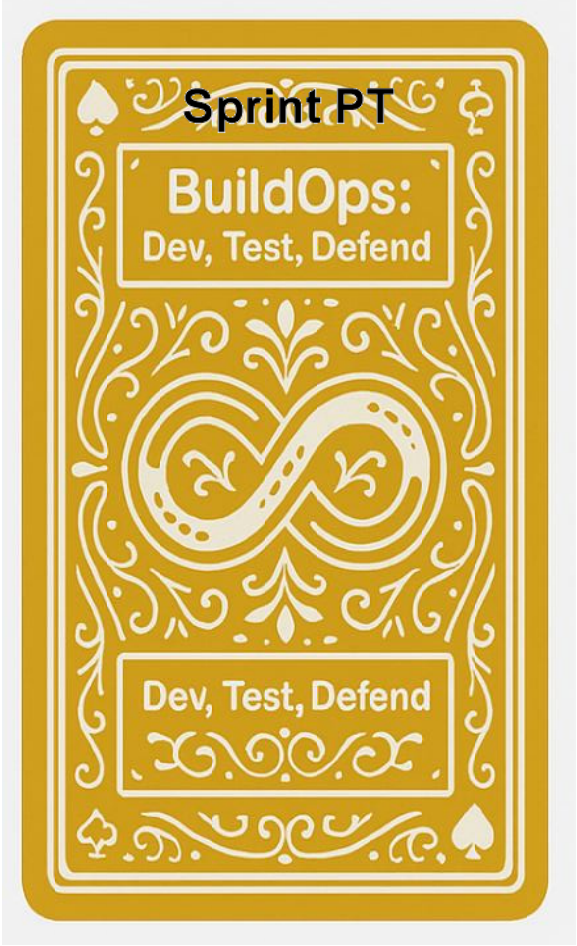
Filter server logs

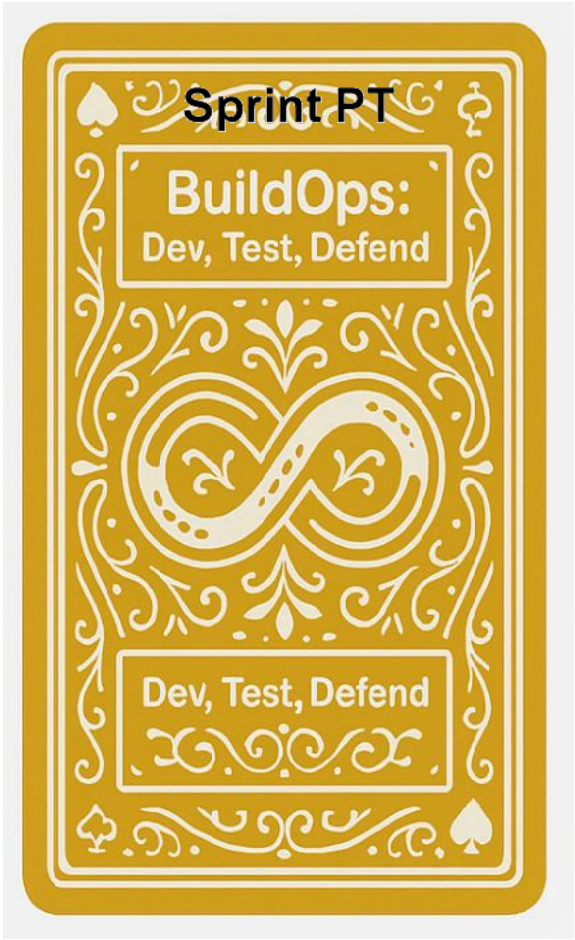
18

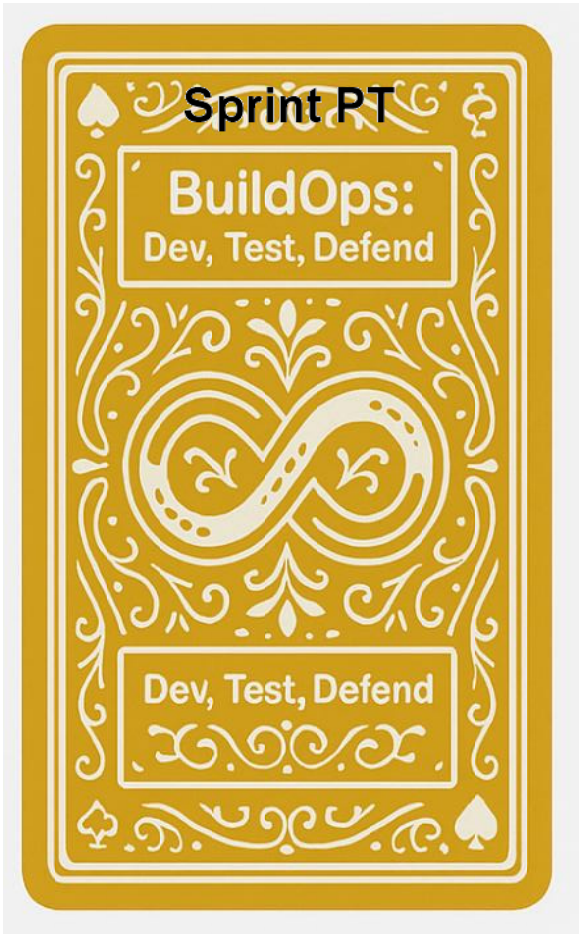
Sprint: PT

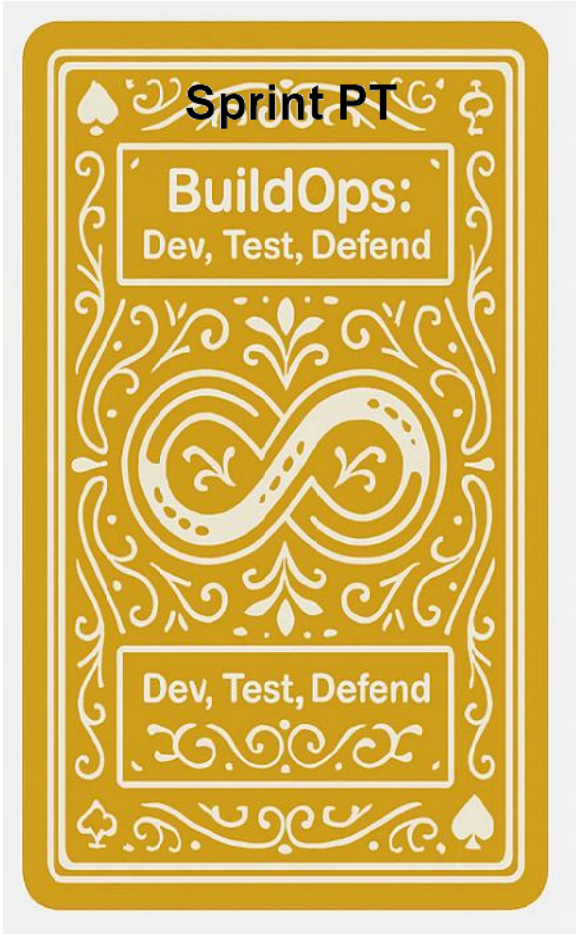
As a ***Penetration Tester***, I want ***the development team to change the logging on the system to ensure that the logs are anonymous and all entries are de-identified*** so that ***an adversary is not able to use the logs to attack the system.***.

Story Points: 4 **Customer Value:** 15


Sprint PT
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint PT
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint PT
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint PT
BuildOps:
Dev, Test, Defend
Dev, Test, Defend

SSL Pinning for Enhanced HTTPS Security

19

Sprint: RSC

As a ***Developer (Code Reviewer)***, I want ***to implement SSL Pinning in the app*** so that ***attackers cannot impersonate our server and intercept communications, even if HTTPS is compromised.***.

Story Points: 4 **Customer Value:** 10

Prevent OS Keylogging via App

20

Sprint: RSC

As a ***security analysist (Code Reviewer)***, I want ***ensure that the app does not trigger any operating system functions that log keystrokes or user input*** so that ***sensitive user data is not exposed.***.

Story Points: 2 **Customer Value:** 15

Block Outdated App Versions

21

Sprint: RSC

As a ***System Administrator (Code Reviewer)***, I want ***prevent outdated app versions from accessing the server and guide users to upgrade*** so that ***security patches and features are consistently applied.***.

Story Points: 2 **Customer Value:** 15

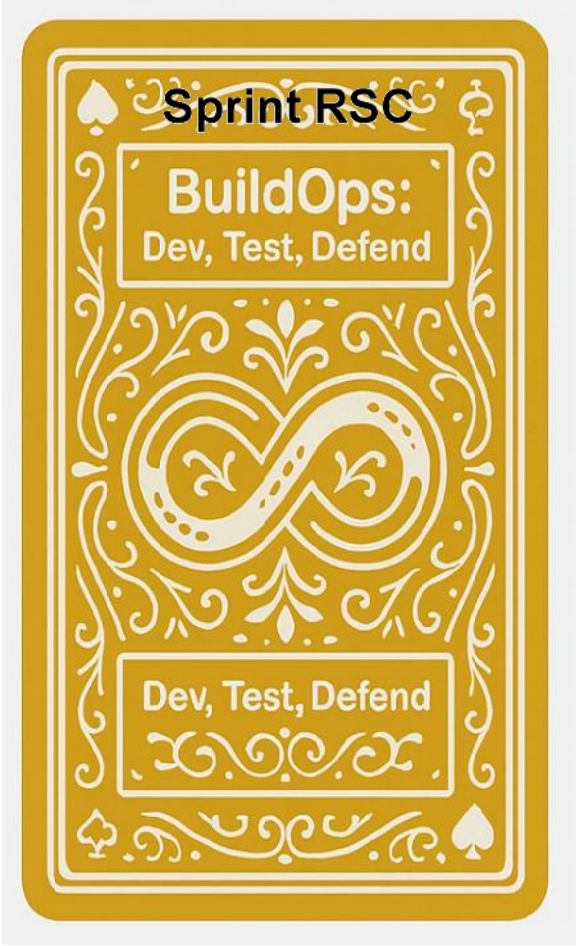
Strengthen Login Security

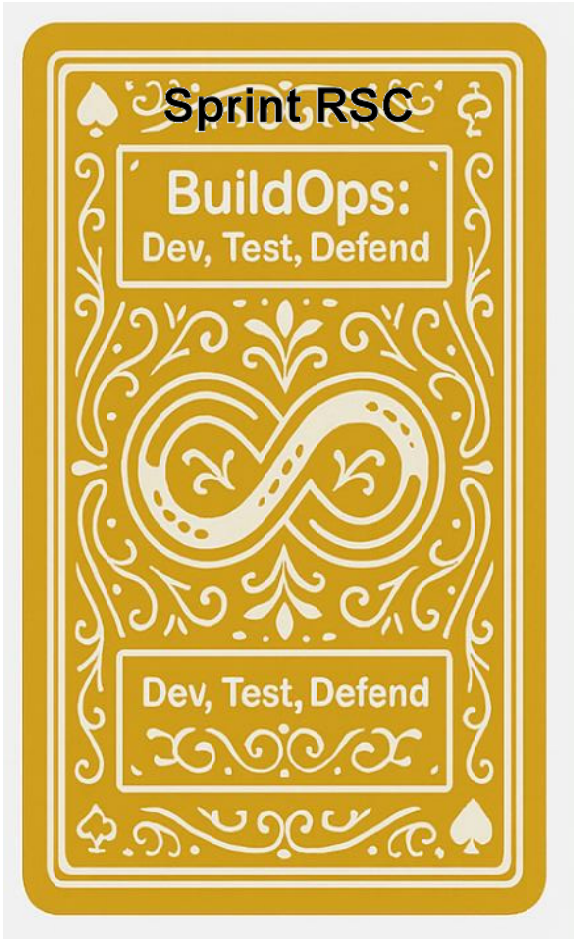
22

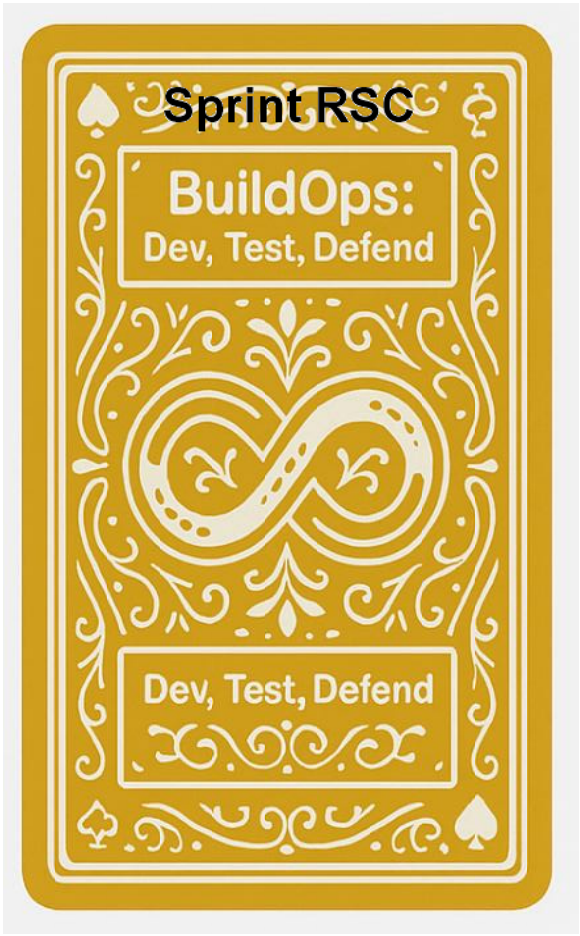
Sprint: RSC

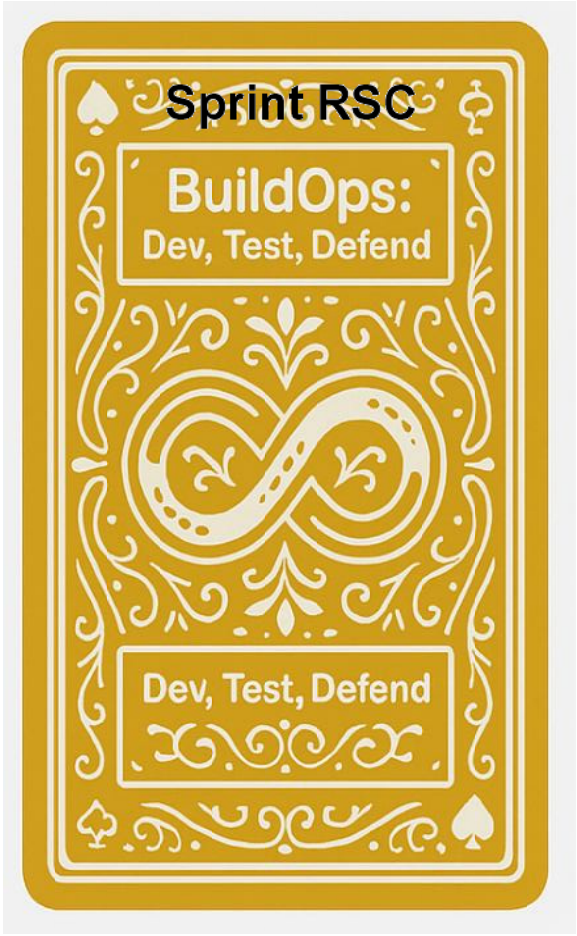
As a ***security analysist (Code Reviewer)***, I want ***the login system to obscure username validity and block login after five failed attempts*** so that ***attackers cannot easily guess credentials through brute force.***.

Story Points: 4 **Customer Value:** 10


Sprint RSC
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint RSC
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint RSC
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Sprint RSC
BuildOps:
Dev, Test, Defend
Dev, Test, Defend