

Sprint Result

Mother Nature Strikes



Lightening strikes your data center, taking it offline. If this is not mitigated, you'll only get half of the work done next sprint that you would like to, as you will be restoring the machine the entire time. Thus, when planning for your next sprint, only plan for half of the PBI's that you would normally plan for.

Sprint Result

Competition Strikes



Your lead developer is hired by a new startup, Appear, Inc. to develop a new computing platform, code named Golden Delicious. The largest PBI in the previous sprint did not get completed. Adjust the order of your tasks and place arrow above the longest task, which is highest priority for the current task.

Sprint Result

No Attack



3

Sprint Result

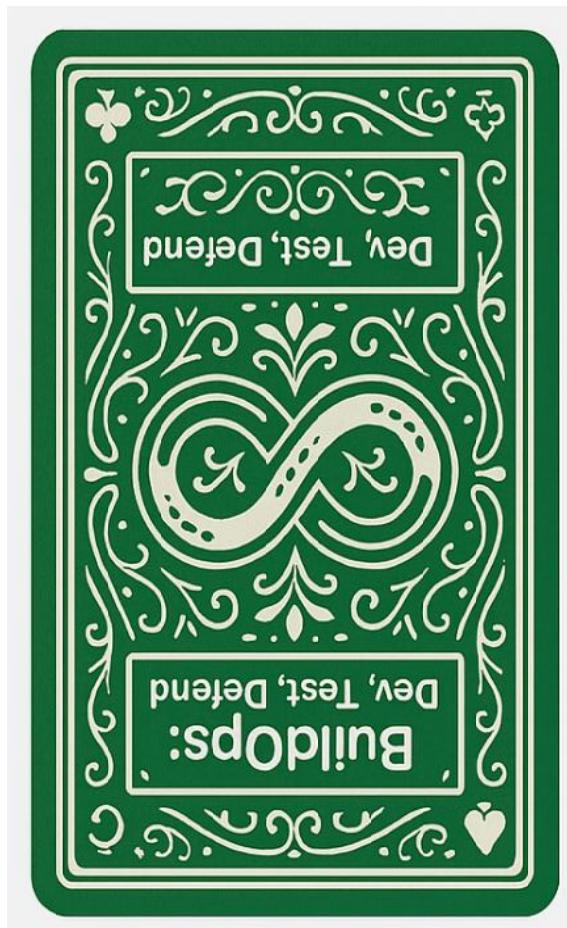
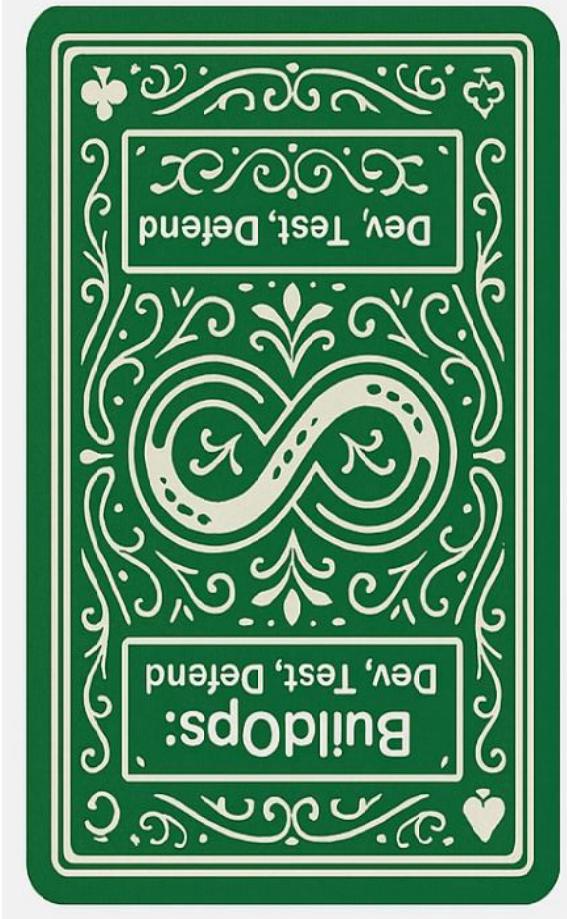
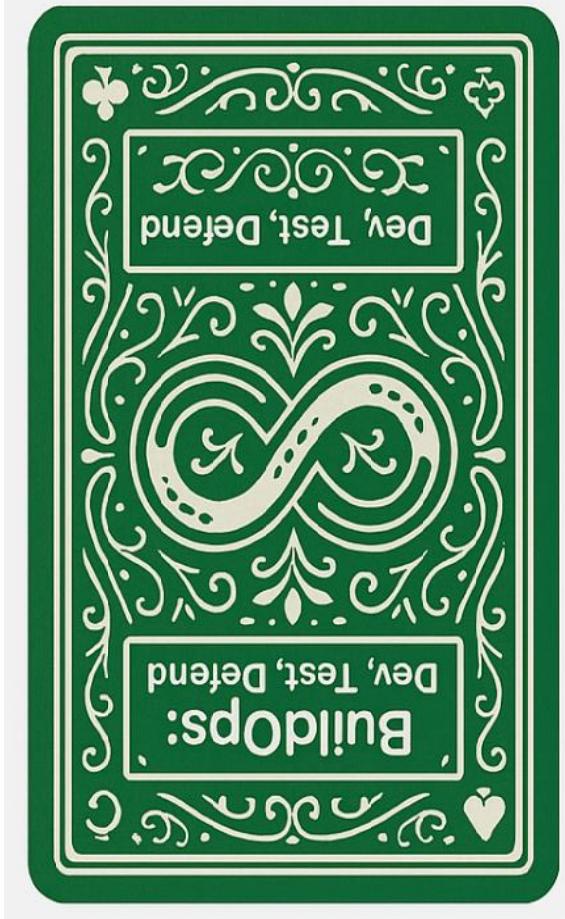
Lottery Winner



4

You won the lottery. Your project got done early and to celebrate your boss sends you to Hawaii for a weeks vacation at a major cyber security conference. But, because you are gone, reduce the number of story points in the next sprint by 4.

The attackers were lured by other things and other sites. Do not draw any attack cards for this sprint.





Sprint Result

Extra Productive

5

Your team was very productive this sprint. Add an extra 3 story points to the next sprint.



Sprint Result

Estimation Error

6

There was an error in estimation and the team did not get as many story points completed as planned. Select the lowest priority PBI from the sprint and indicate they did not get completed.



Sprint Result

Big Estimation Error

7

There was an error in estimation and the team did not get as many story points completed as planned. Select the two lowest priority PBIs from the sprint and indicate they did not get completed.

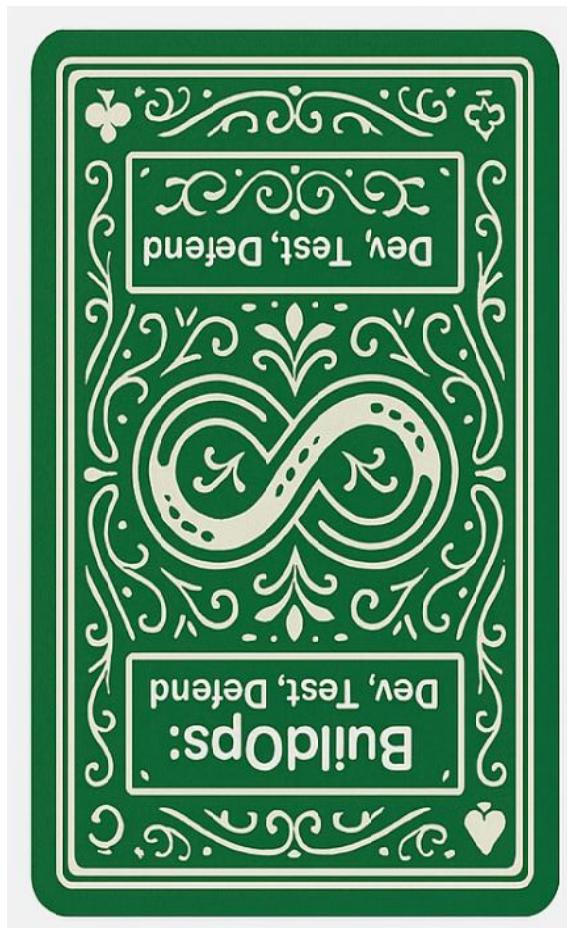
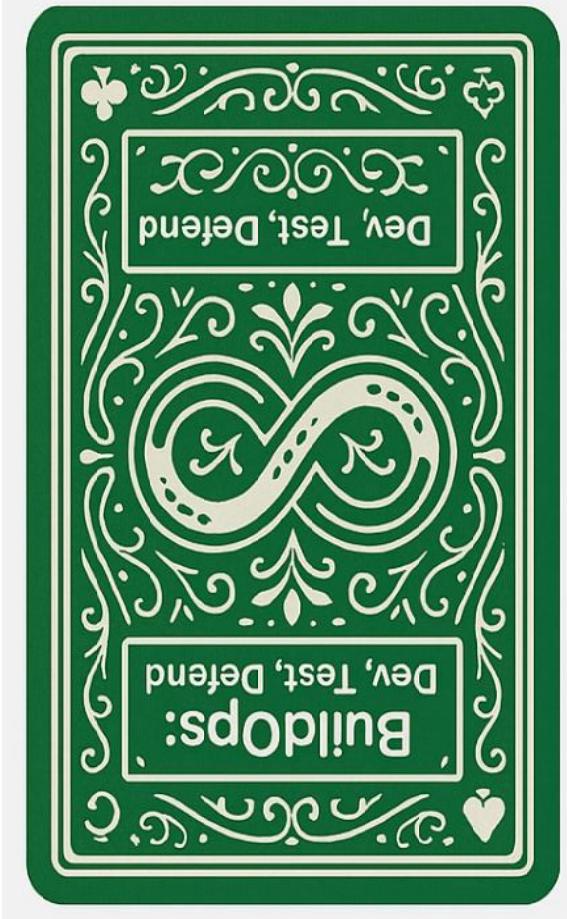
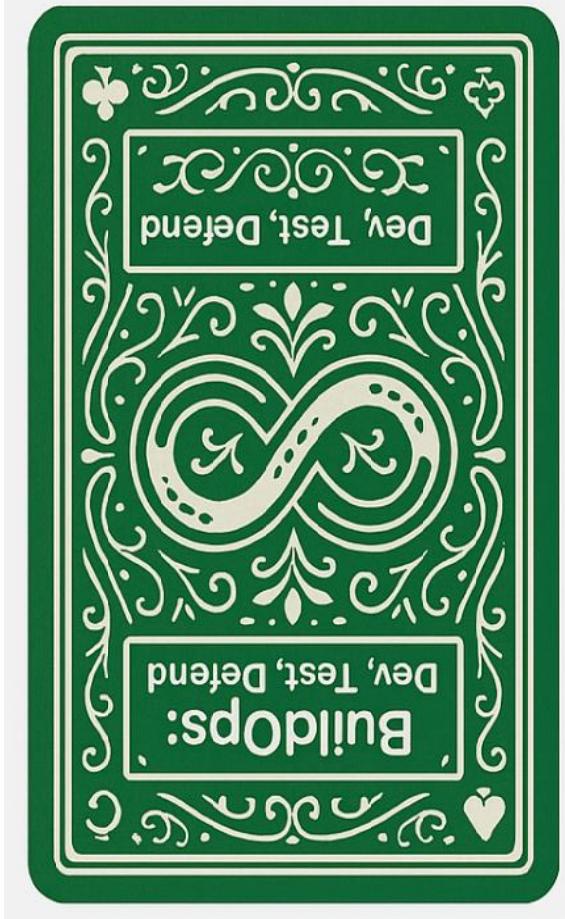


Sprint Result

Normal Sprint

8

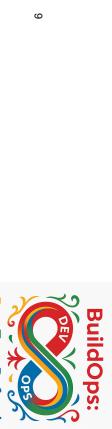
The sprint was completed normally. You completed everything that was planned in an appropriate fashion. Great job!





Sprint Result Baby Showers

One of your developers is having a baby and will be out on maternity / paternity leave next sprint. Reduce the number of PBI's that will be completed by 25% to account for this loss.



Sprint Result Burnout Detected

The team got its work finished, but struggled and you are detecting burnout. To avoid burnout, reduce the number of story points in the next sprint by half to combat this and use team building activities to counteract burnout.



Sprint Result Effective Sprint

11



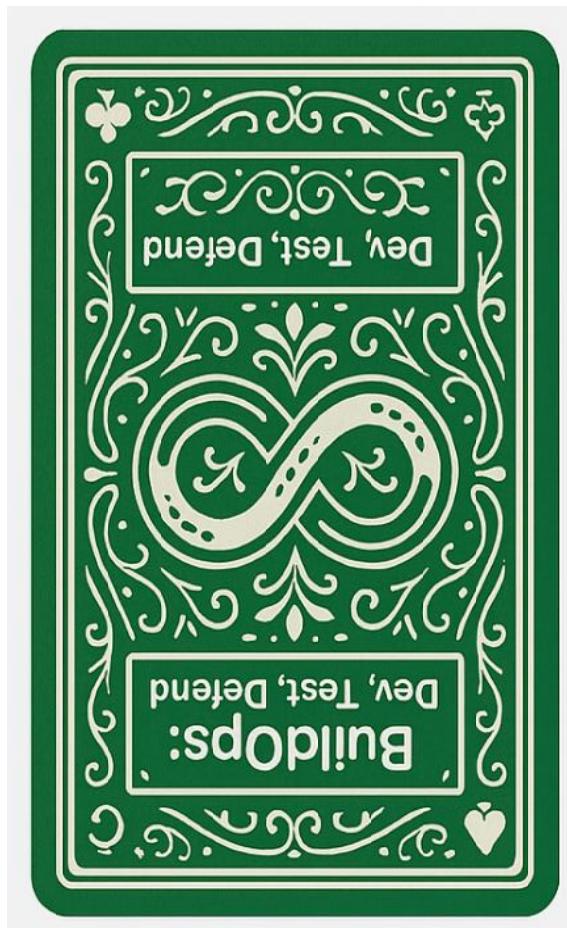
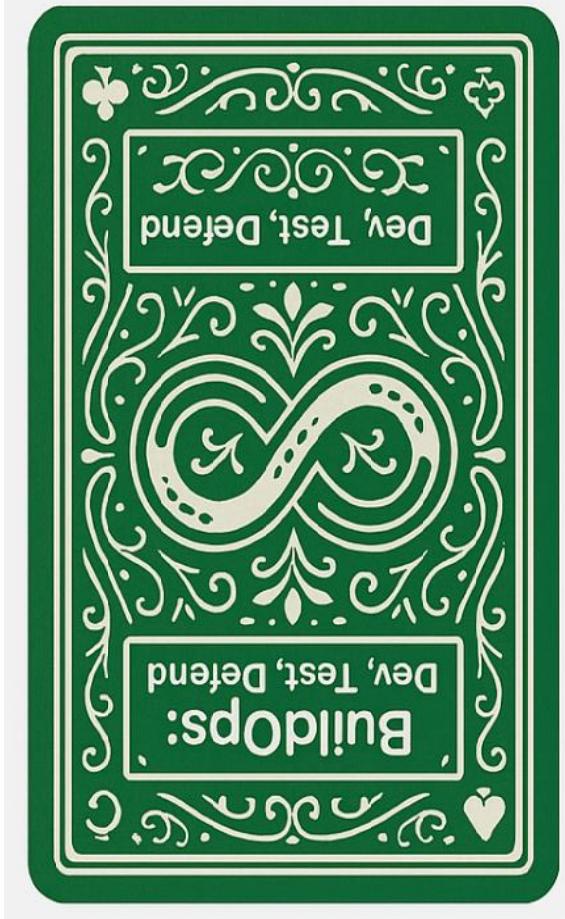
Sprint Result Normal Sprint

12

The team has completed its retrospective and feels it can be more productive next sprint. In planning the next sprint, add two additional story points to planning beyond what normally is planned for.

The sprint was completed normally. You completed everything that was planned in an appropriate fashion. Great job!

10



Cloud Migration



As a **CTO**, I want **the application moved from out local data center into the cloud and architected to ensure redundancy across multiple zones so that the system is more robust in the event of a failure of computing infrastructure..**

Story Points: 6 Customer Value: 35

Common Platform



As a **CTO**, I want **the application to use a common code base for both iOS and Android Deployments so that the developers do not need to maintain two separate applications, one for Android and one for iOS..**

Story Points: 8 Customer Value: 35

User Relationships



As a **User**, I want **the application to support multiple users to safely access a single account and perform operations on a single account so that spouses can jointly manage transactions and a parent can aid a child using money zoom while away at college.**

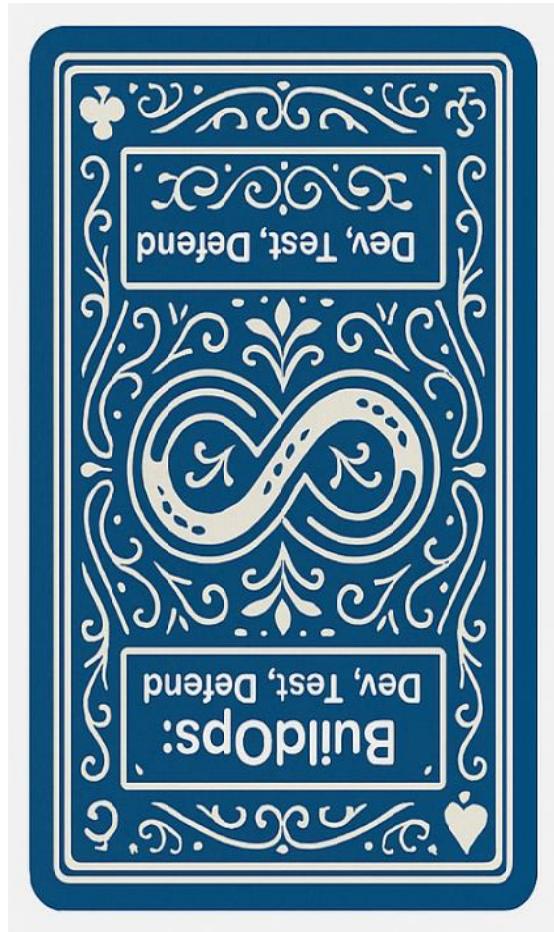
Story Points: 6 Customer Value: 60

Currency Conversion



As a **User**, I want **the application to support transfers made in a foreign currency and converted to American Dollars so that the user can use the application while vacationing in Canada, Mexico, and the Bahamas..**

Story Points: 8 Customer Value: 50





Advertisement Targeting

5

As a **Vendor**, I want *the application* to allow me to access *users transfer habits and purchasing with the application* so that *the users of the application can be targeted with advertisements and other offers from vendors, increasing the value of the product..*

Story Points: 4 Customer Value: 100



In-App Chat for Transfers

7

As a **User**, I want *to include a message with my transfer and be able to chat with the recipient so that I can communicate with the person receiving my payment..*

Story Points: 6 Customer Value: 50



Transaction Categorization and Budgeting

6

As a **User**, I want *my transactions to be automatically categorized and allow me to set budgets so that so that I can track and control my expenses.*

Story Points: 6 Customer Value: 60

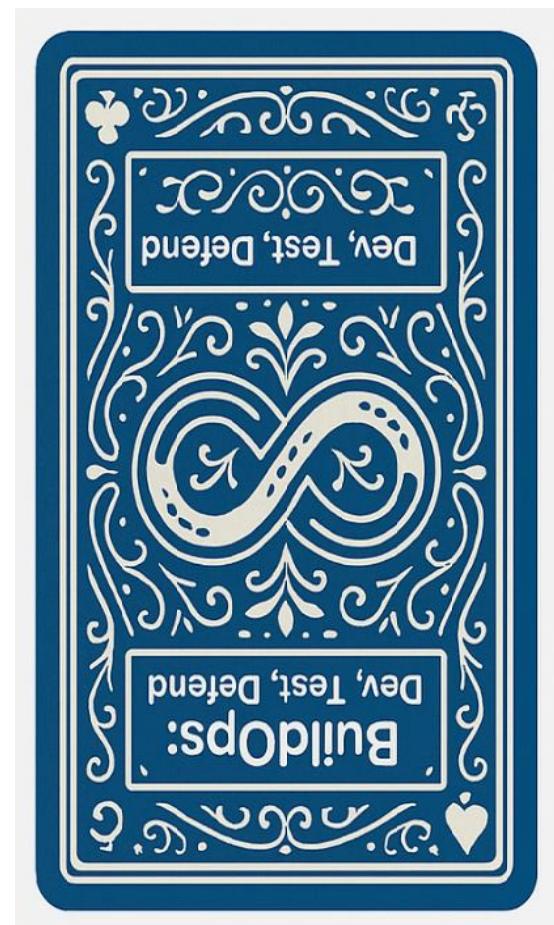
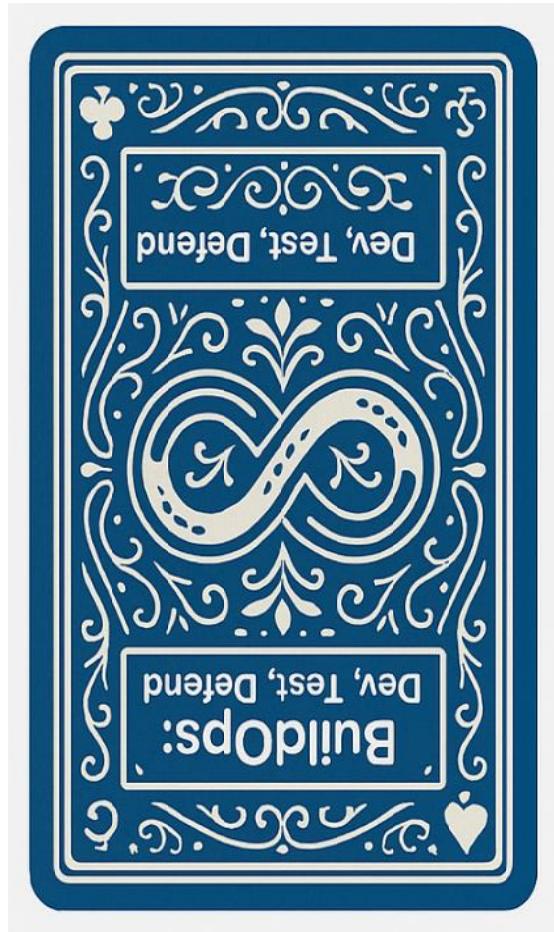


Scheduled Payments

8

As a **user**, I want *to schedule recurring payments so that I don't have to remember and manually pay them each time.*

Story Points: 4 Customer Value: 50



Digital Receipts for Bill Payments

9



As a **user**, I want **to receive digital receipts for each payment** so that **I have proof of payment for my records or tax purposes.**

Story Points: 3 Customer Value: 50

Microservices Architecture

11



As a **CTO**, I want **the system to be redesigned to use a microservices architecture and platform engineering** so that **the system is easier to maintain and can be extended easier and also is more robust.**

Note: If Cloud Migration has already been performed, this PBI will only require 6 story points instead of 9..

Story Points: 9 Customer Value: 60

Integration with Budgeting Software

10

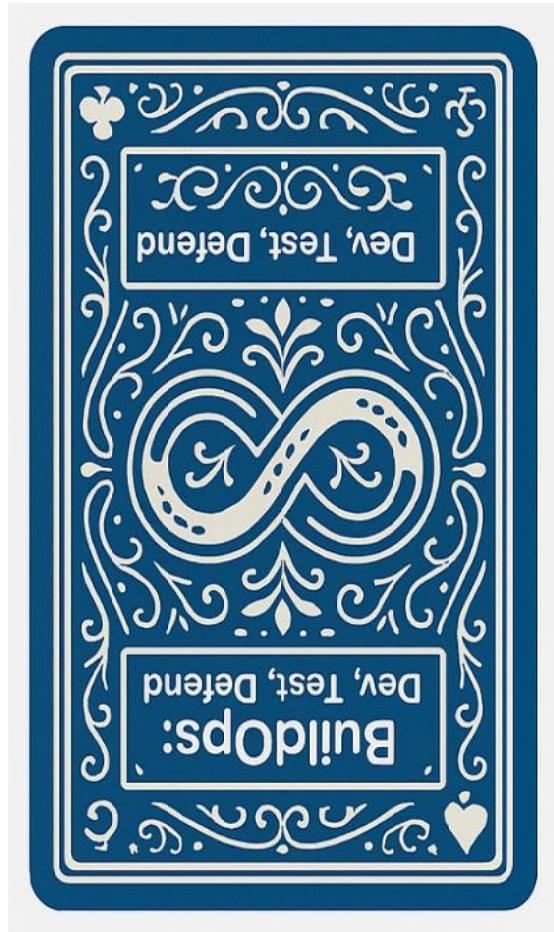


As a **user**, I want **the system to be able to interact with budgeting and financial tracking software (aka Quicken, Microsoft Money, Banktivity, YNAB)** so that **I can use the existing tracking software that I am familiar with to budget and track expenses over time.**

Story Points: 8 Customer Value: 80

Story Points: Customer Value:

As a , I want so that .





Round 1

No Attack

The attackers were lured by other things. You got lucky!

Points Lost: 0

Mitigation(s): None



Round 1

False Alarm

You thought you were under attack, but it merely was a false alarm from a required external penetration test.

Points Lost: 0

Mitigation(s): None



Round 1

Deleting Kiddie

3



Round 1

DoSing Kiddie

4

A malicious actor gets to server by accident – maliciously deletes all data.

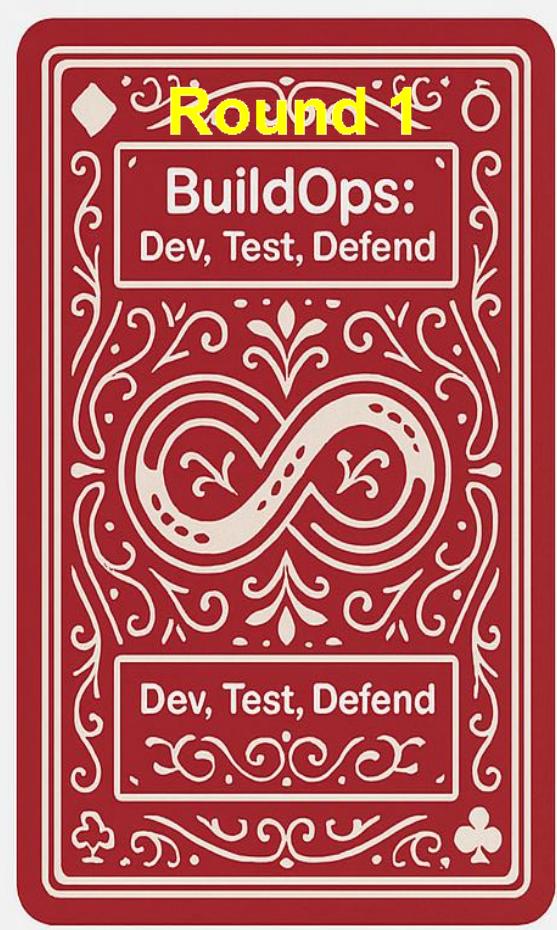
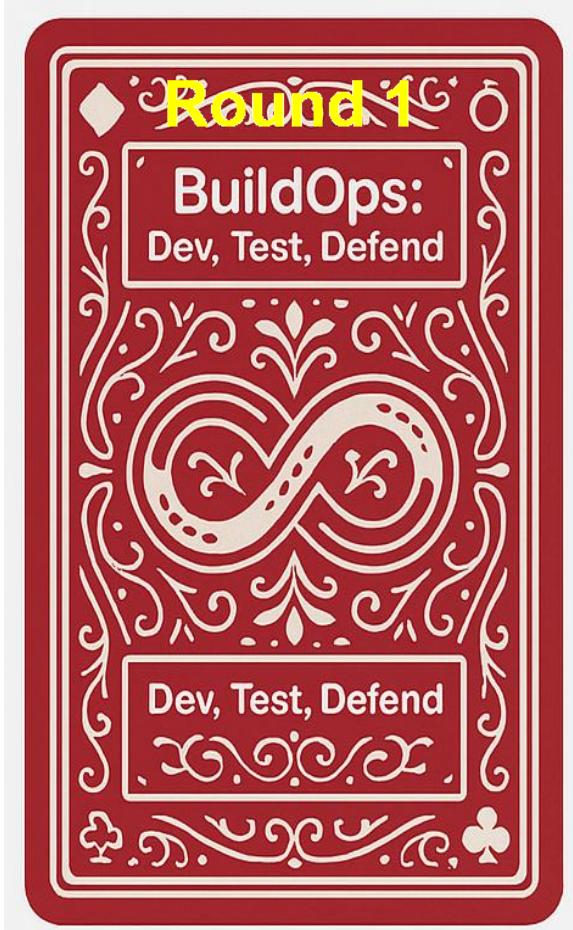
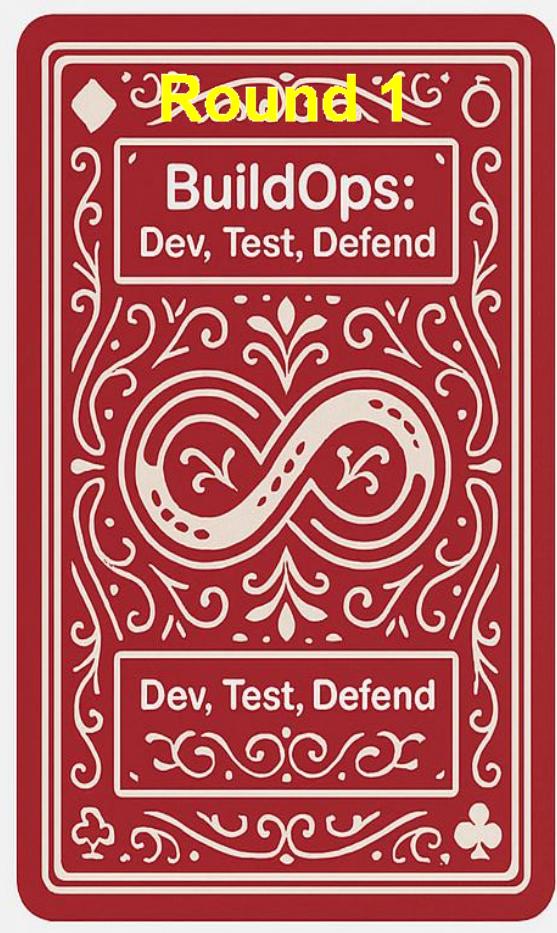
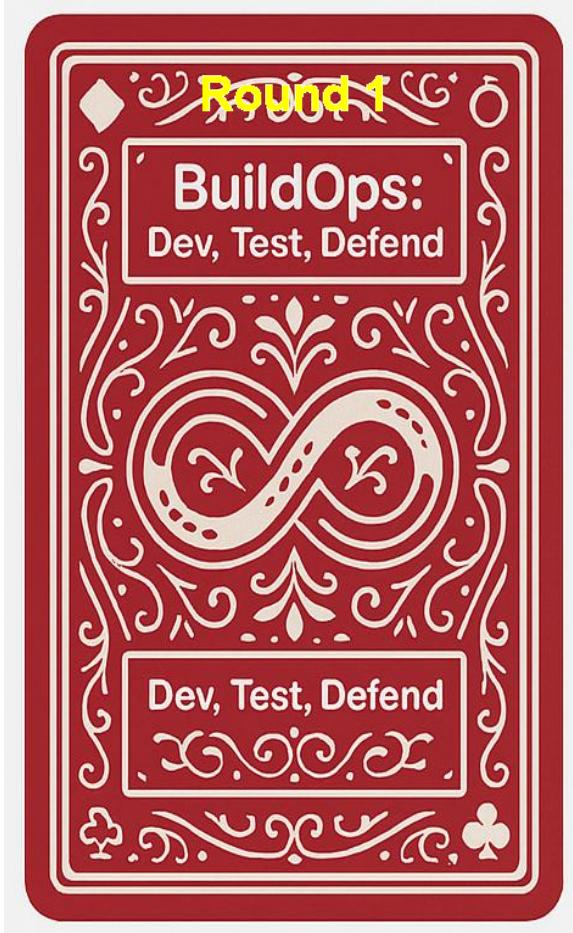
A malicious actor gets to server by accident and uses for ddos attacks on other servers

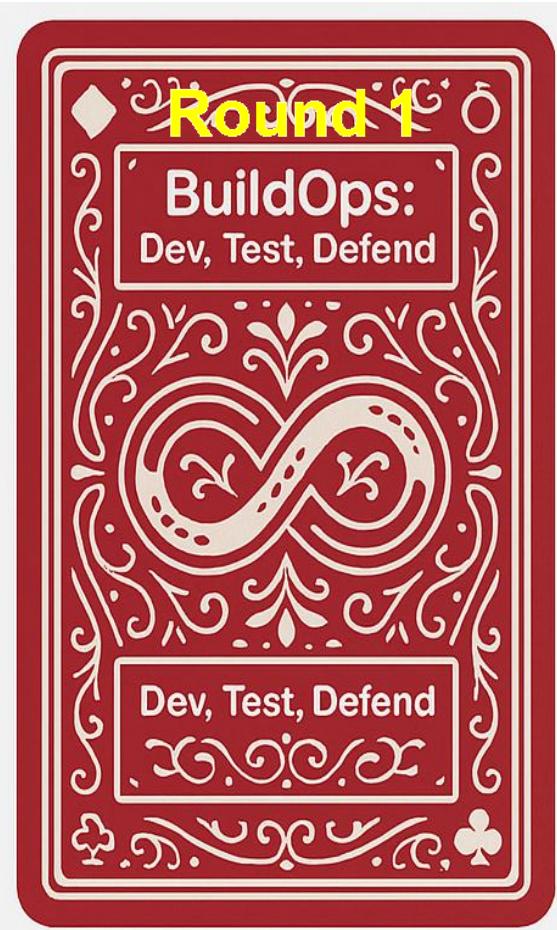
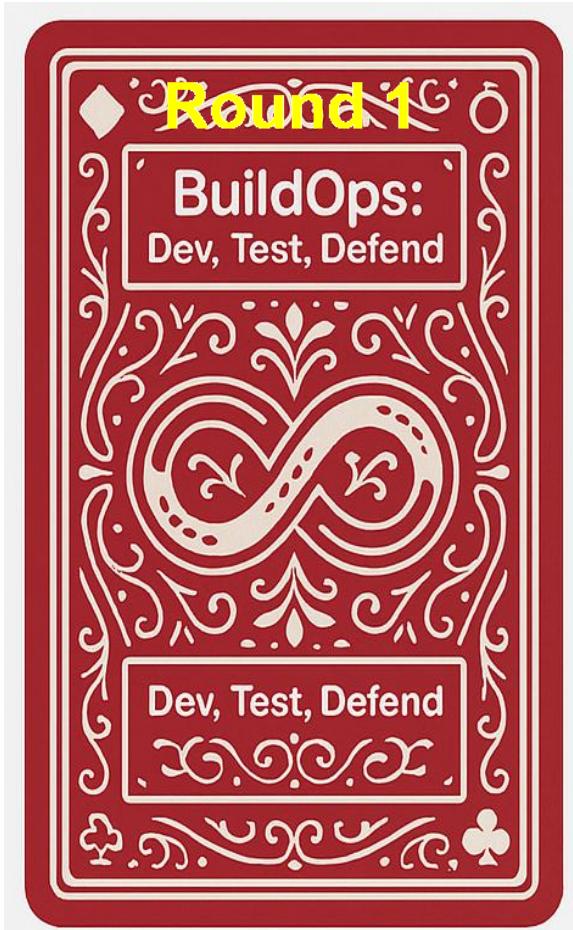
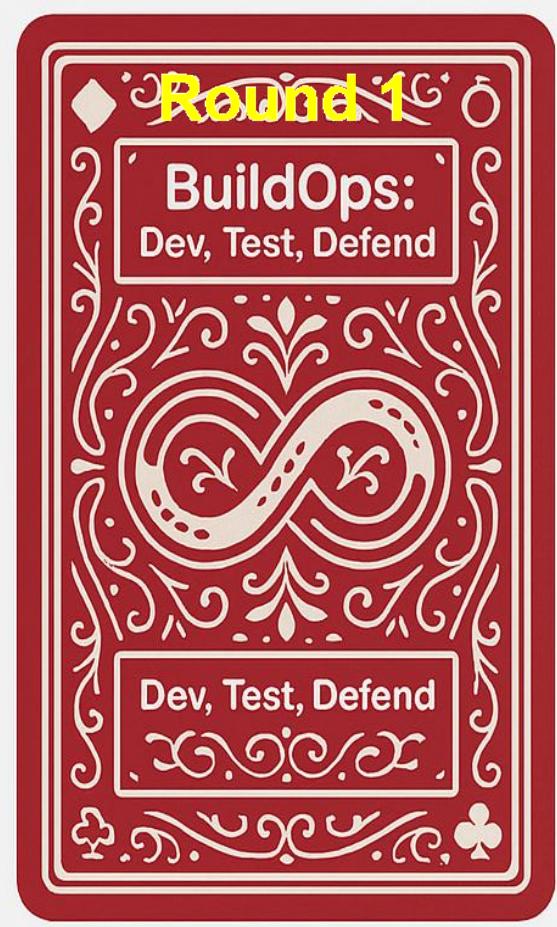
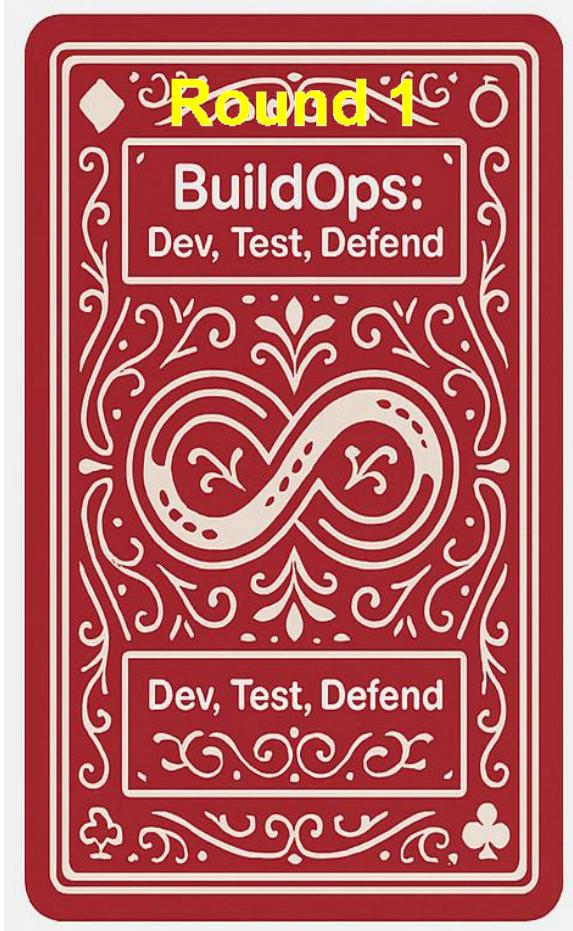
Points Lost: 30

Mitigation(s): Data Backup
Server Patches

Points Lost: 60

Mitigation(s): Server Penetration Testing
Network Protection





Round 1

Mother Nature Again



A power outage hits your data center, resulting in lowered performance for your system.

If the system has been moved to the cloud, you are fine. Otherwise, customers are somewhat unhappy, but the system is still operational.

Points Lost: 40

Mitigation(s): Cloud Migration
Only Cloud Migration

Round 2

Just Looking Attack



The attackers were lured by other things. You got lucky!

Points Lost: 0

Mitigation(s): None

Round 2

No Attack



Round 2

Hacking Kiddie



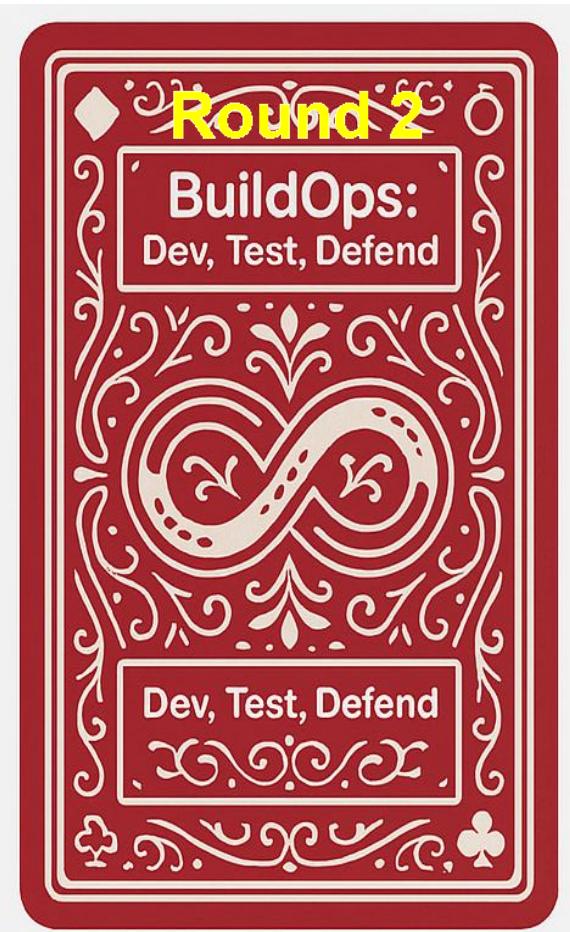
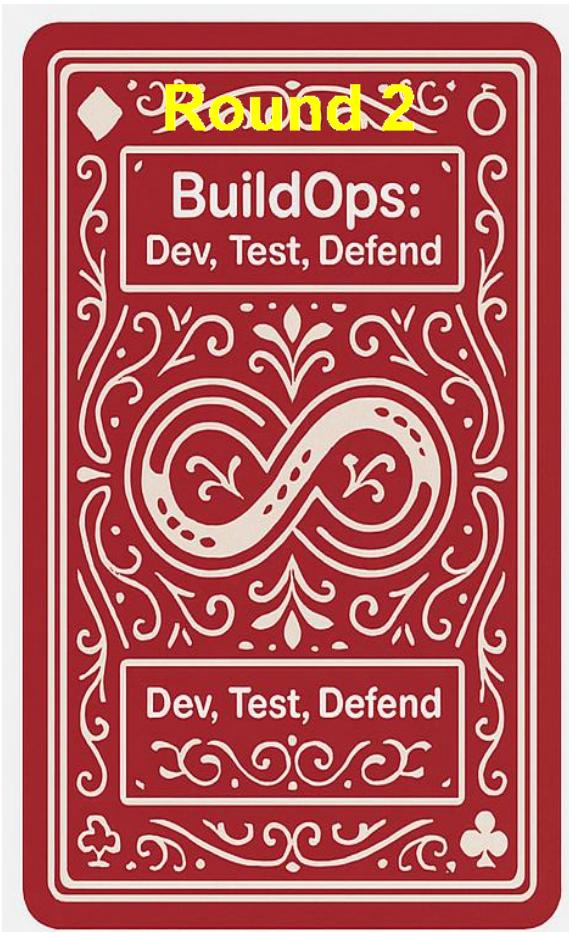
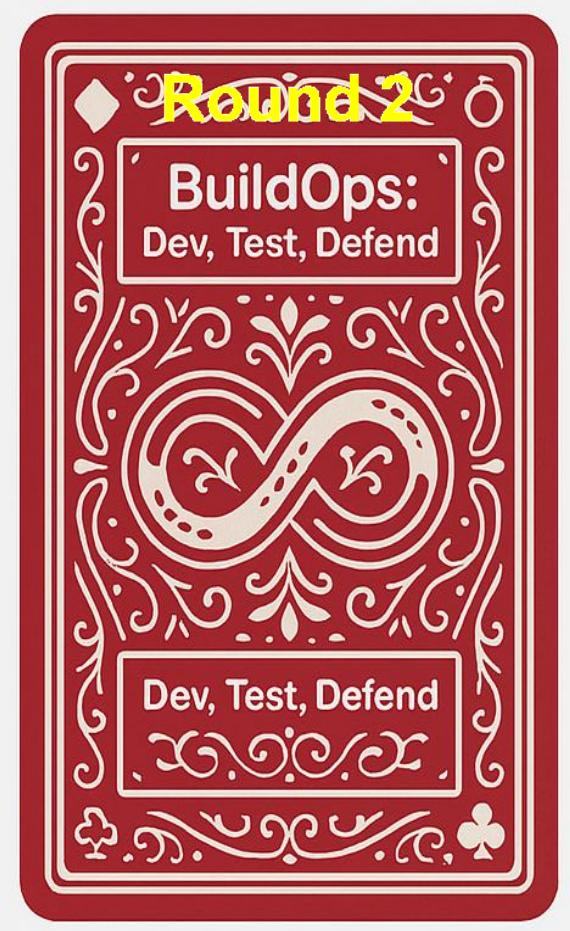
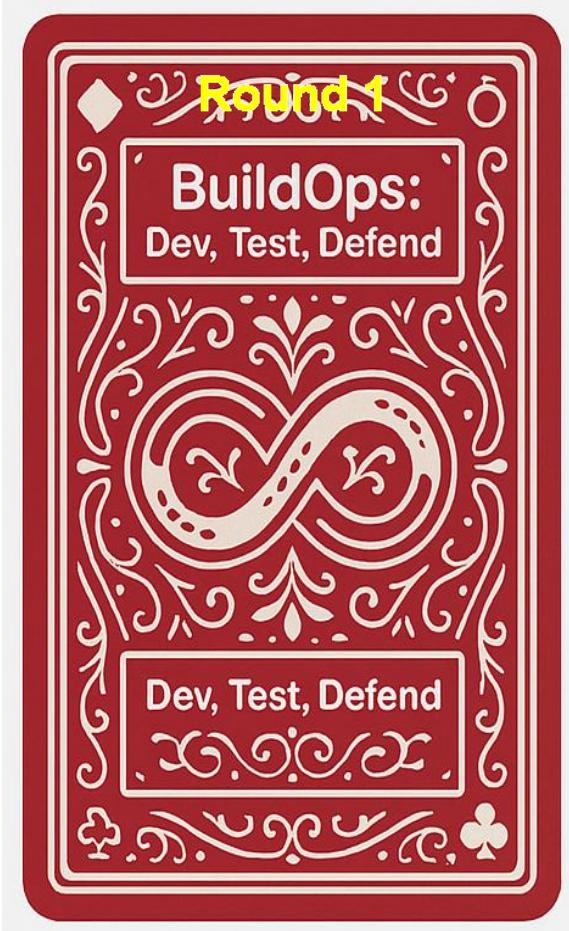
A hacker gains access to your system and gets to server by accident. The attacker exfiltrates unencrypted data from the database and downloads other material, publishing it on the web.

Points Lost: 10

Mitigation(s): Authentication Hardening
Prevent Access to Office

Points Lost: 60

Mitigation(s): Server Penetration Testing
Network Protection



Round 2

Phishing Kiddie

13



An attacker sends spam email, gets subscribers to download rogue version or enter credentials in spoofed website, and now has login credentials on your system.

Points Lost: 50

Mitigation(s): Incident Communication
Two Factor Authentication

Round 2



Improperly Trained Dev

15

Round 2

Amateur Developer

14



A developer that you have hired accidentally publishes the access keys to the repos you are using for your code base. An adversary discovers this and plants malicious code inside of the codebase.

Points Lost: 30

Mitigation(s): Server Penetration Testing
Encrypt & Hide Data on Server

Round 2



Recognition

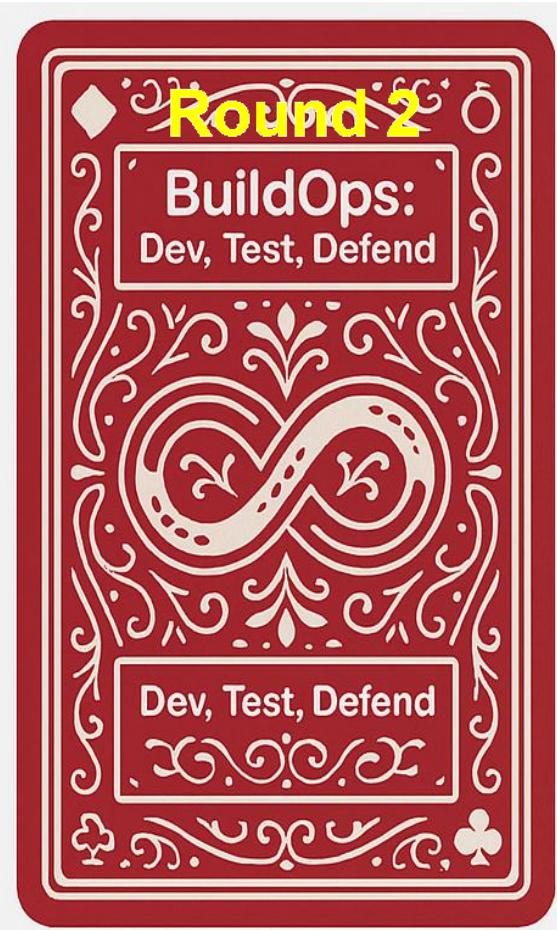
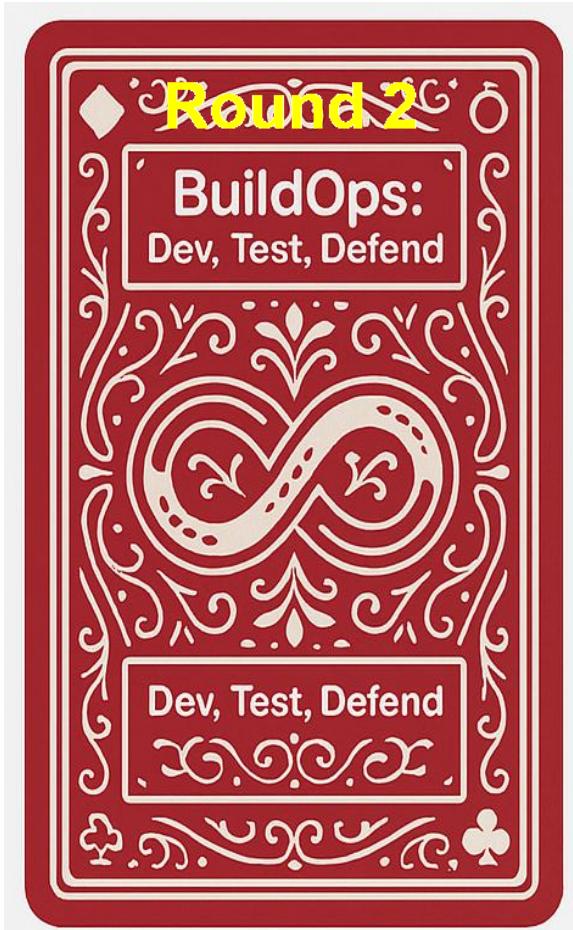
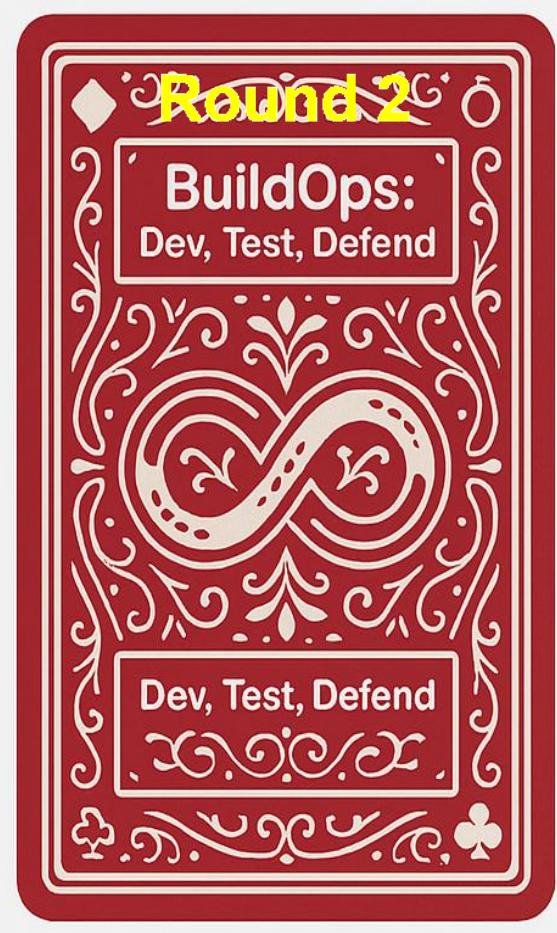
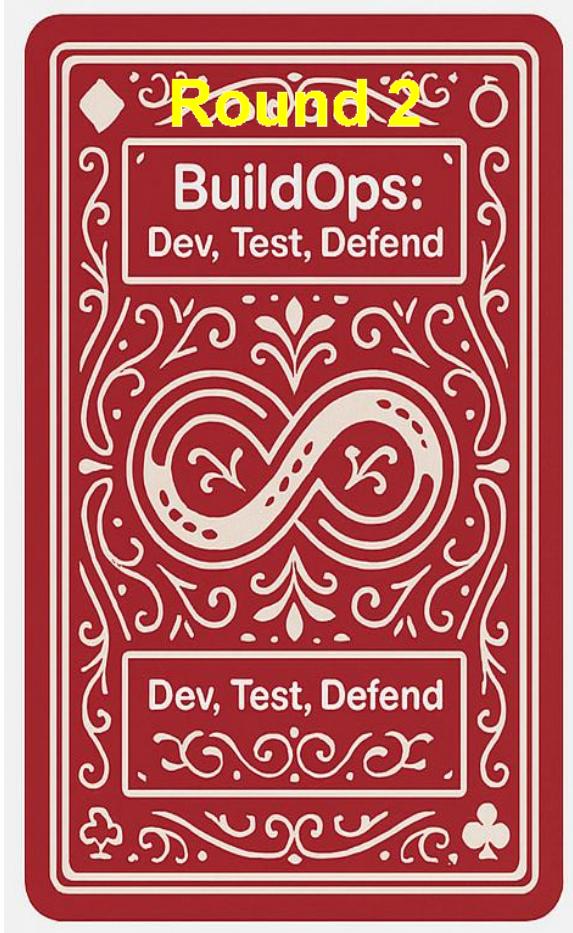
16

An attack is made, and they discover that the server is vulnerable to SQL injection through several of its diagnostics API's.

Your site has been acknowledged as an overly secure site and is published in Wired magazine as an exemplar website.

Points Lost: 30

Mitigation(s): Security Review of Server Code
Server Penetration Testing



Round 3

MITM Kiddie

17



An attacker spoofs Wi-Fi access point in airport – Gains credentials – randomly hacks accounts.

Points Lost: 25

Mitigation(s): Secure Network Communication

Two Factor Authentication

Round 3

MITM Mafia

19



An attacker spoofs Wi-Fi access point in airport uses dodgy root certificates to validate all banking services - gains credentials - steals small amount from each.

Points Lost: 25

Mitigation(s): SSL Pinning for Enhanced HTTPS

Security

Two Factor Authentication

Round 3

Aggrieved Hacker

18



An attacker gains access to server – downloads or modifies server data – publicizes the data resulting in personal information being published.

Points Lost: 60

Mitigation(s): Server Penetration Testing

Encrypt & Hide Data on Server

Round 3

Mafia Team

20

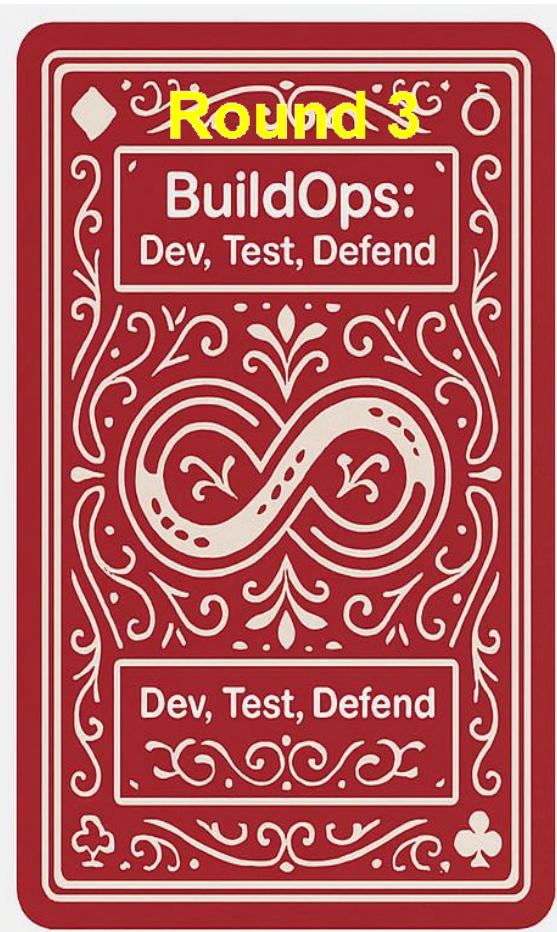
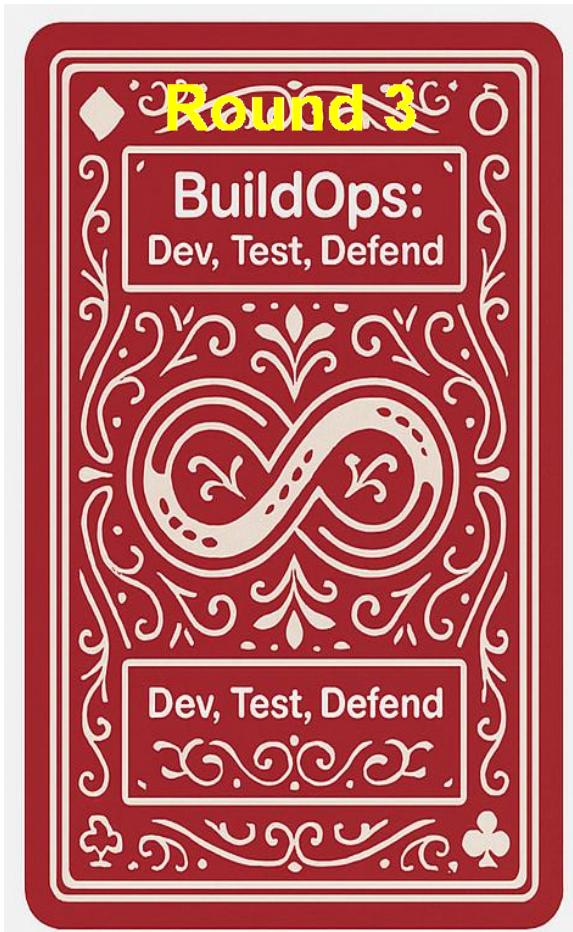
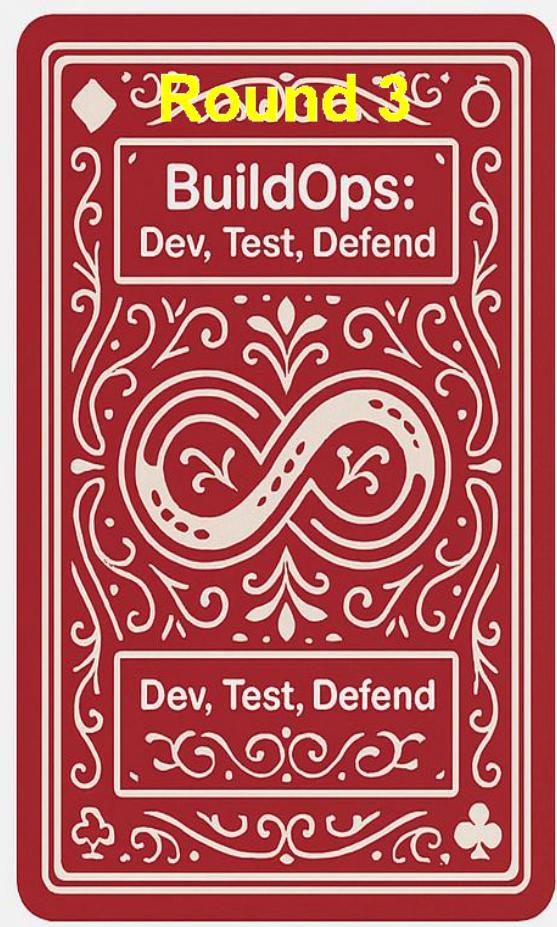
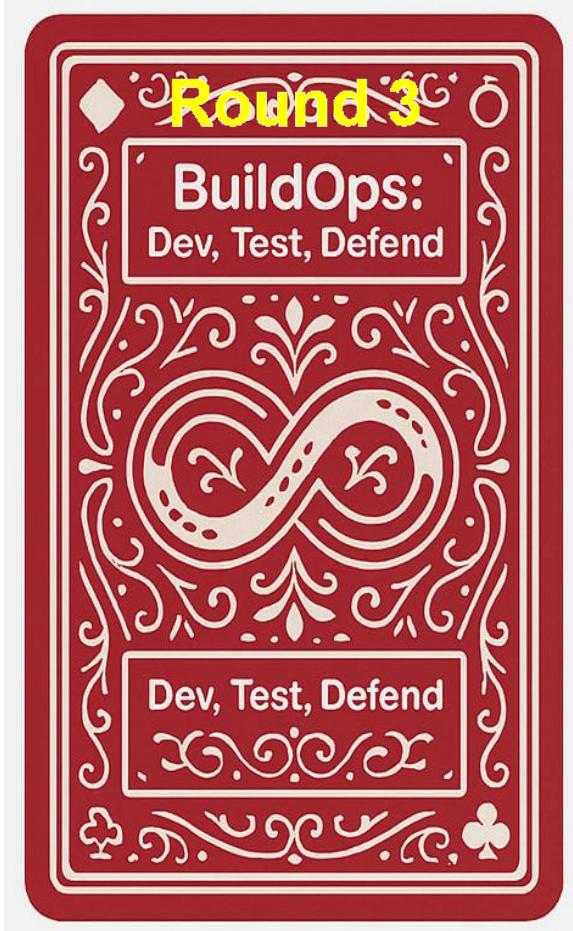


Physically gains access to office, get passwords from server logs, small theft from tens of thousands of accounts.

Points Lost: 80

Mitigation(s): Network Protection

Filter server logs



Round 3

21

Mafia Adv Prog Team



A set of advanced hackers gain access to server though zero day exploit, installed hacked version, transfer money out of accounts.

Points Lost: 100

Mitigation(s): Network Monitoring for Server



Round 3

23

Zero Day

A Zero day vulnerability has been identified in the cloud platform the project has migrated to.
If the platform has been moved to the cloud, there is no defense against this vulnerability except for the single item listed. If the platform has not been moved to the cloud, you are not vulnerable.

Points Lost: 50

Mitigation(s): Encrypt & Hide Data on Server

Round 3

22

Mafia APT



An attacker gets malware on device via email – sends back credentials found in logs to command and control server – used to clean out all compromised accounts.

Points Lost: 100

Mitigation(s): Filter server logs
Two Factor Authentication



Round 3

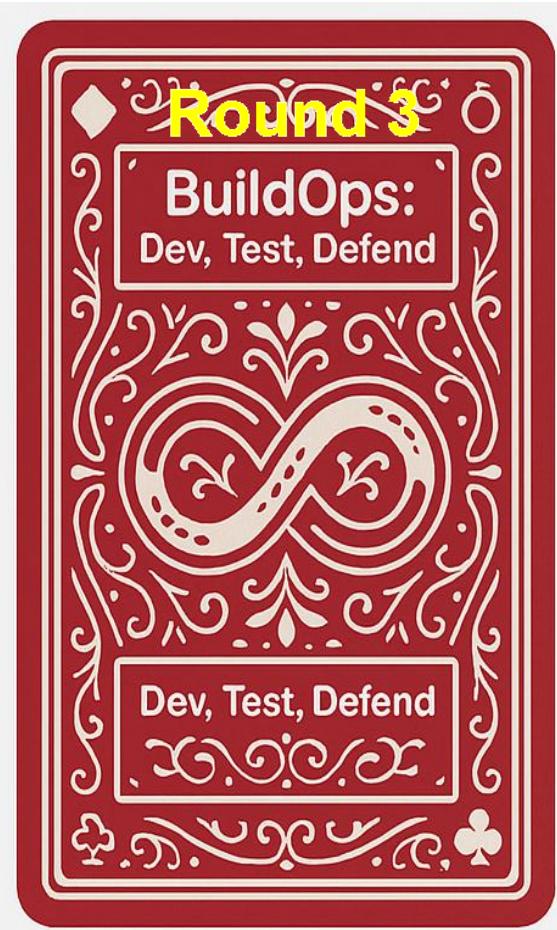
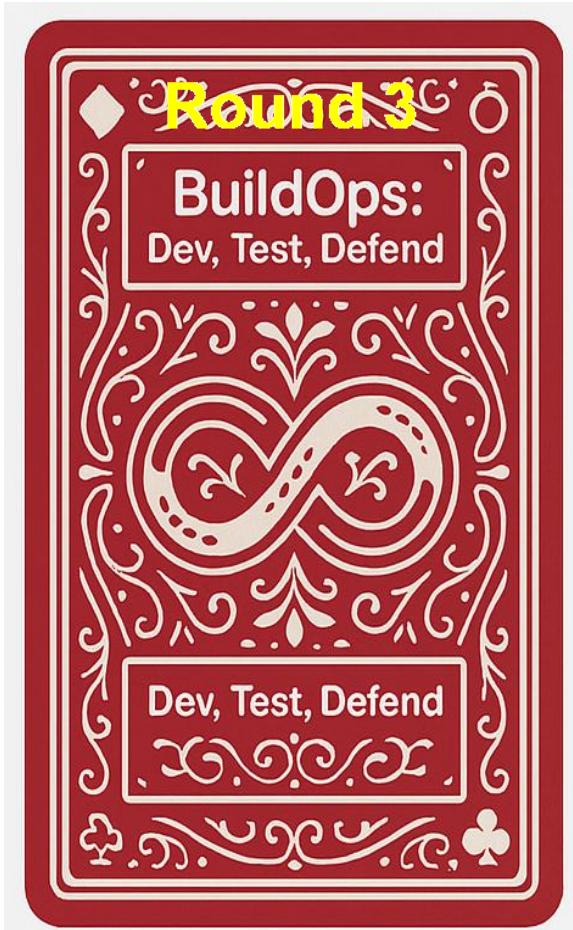
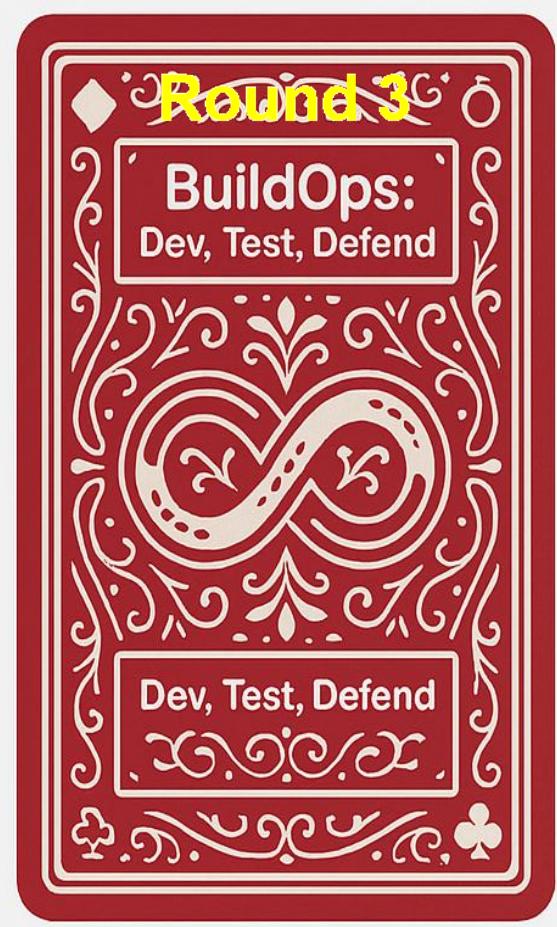
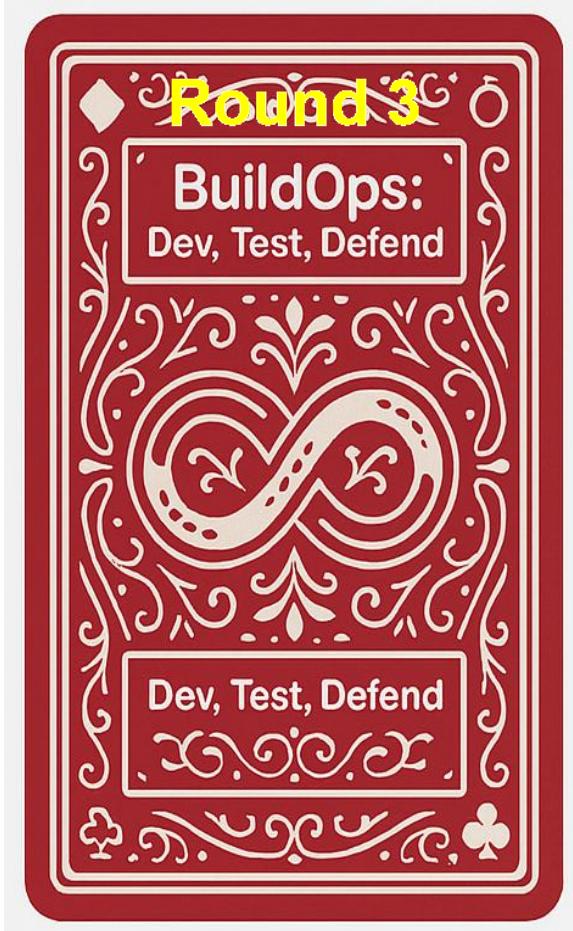
24

Vendor Faking

A vendor has been faked within the system and is attacking automatic payments.
If the automatic payment system PBI has been implemented, you are vulnerable unless the mitigations have been applied.

Points Lost: 60

Mitigation(s): Two Factor Authentication



Round 3

Cross Platform Injection

25



Chat Feature Data Leak

26

Shared code across iOS and Android increases exposure to bugs or injection paths. This exploit has been used against your system, as an attacker has discovered a way to perform a cross platform injection attack.

If a common platform PBI has been implemented, you are vulnerable and at this point, there is no mitigation.

Points Lost: 60

Mitigation(s): None

Round 3

Receipt Fraud Attack

27



Platform Attack

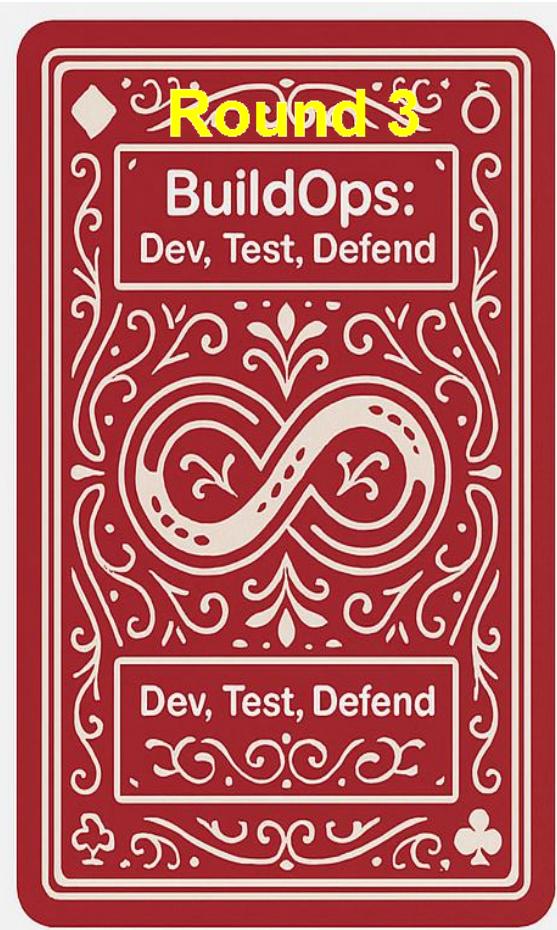
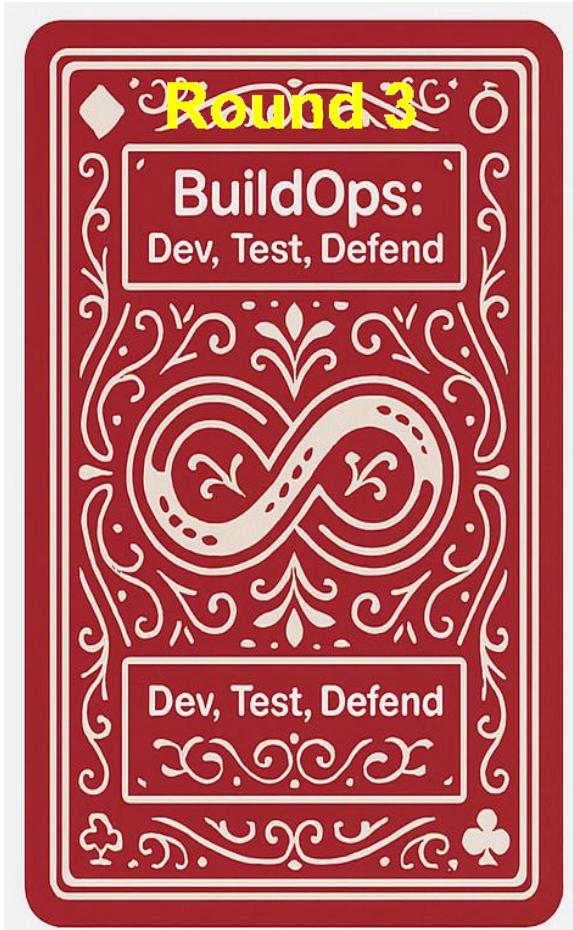
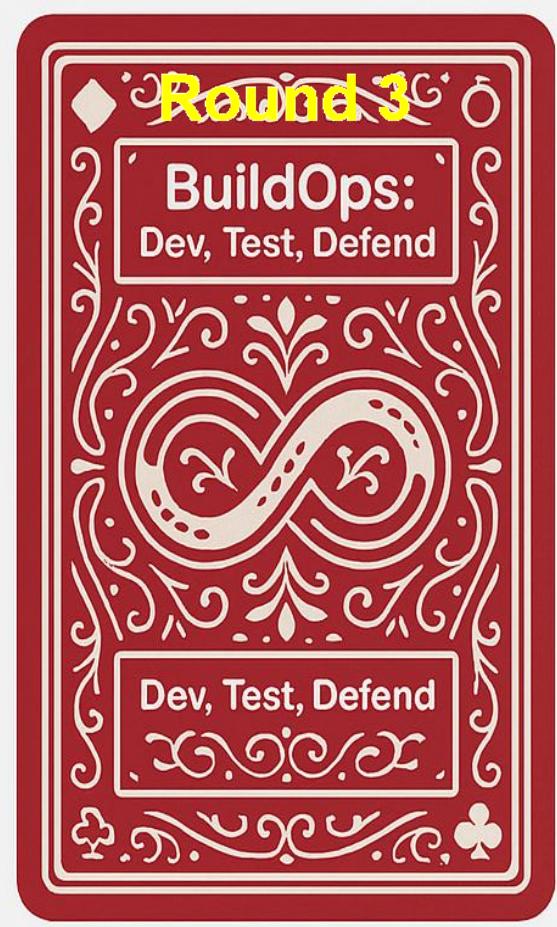
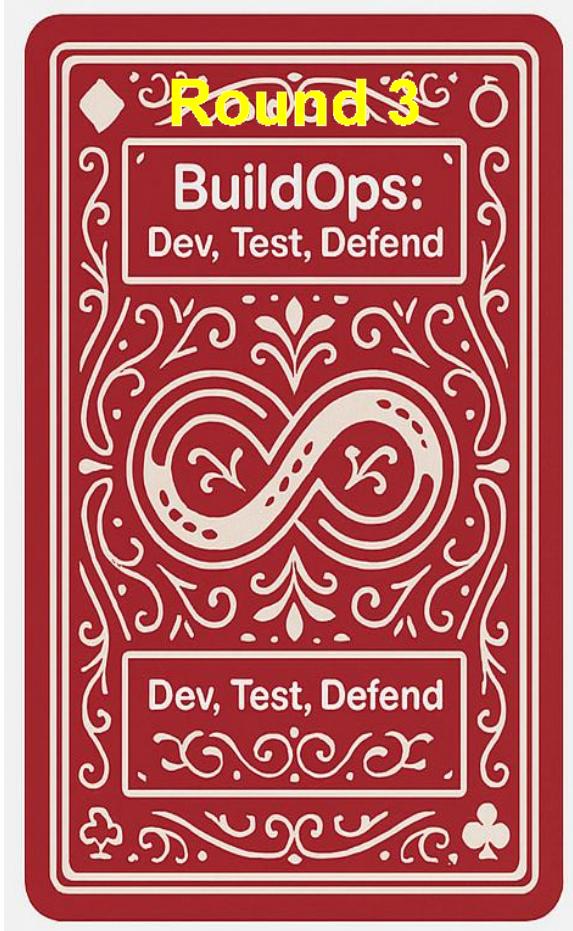
28

Malicious users have attacked your system, generating fake receipts and modifying legitimate ones, sending fraudulent proof of purchases to vendors or providing you with receipts that are fraudulent.

If Digital Receipts for Payments have been enabled, you are vulnerable.

Points Lost: 80

Mitigation(s): None



Data Backup

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

Story Points: 1 Customer Value: 10

2

Logging and Monitoring

Sprint: 1



3



4

Password Security Rules

Sprint: 1



5

Password Change

Sprint: 1

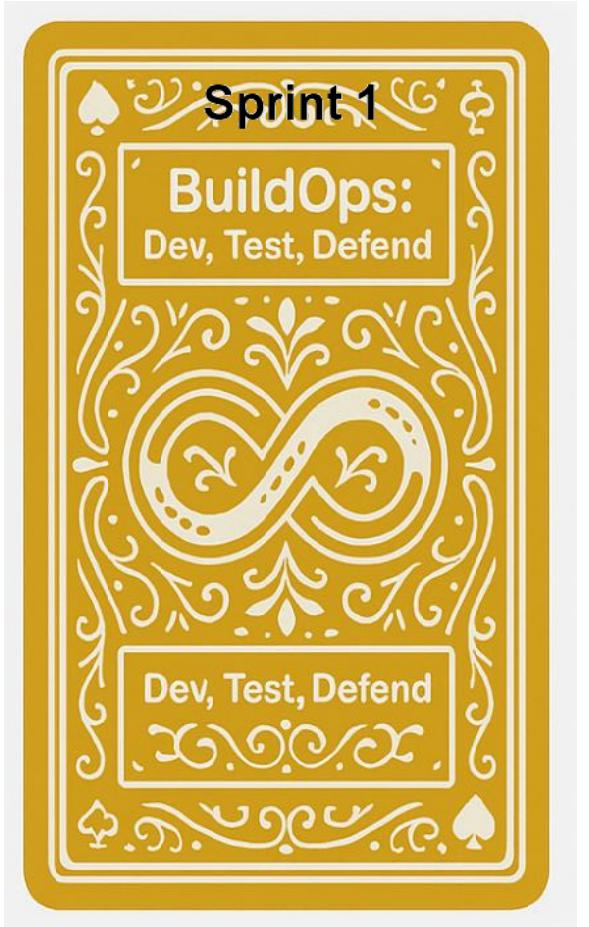
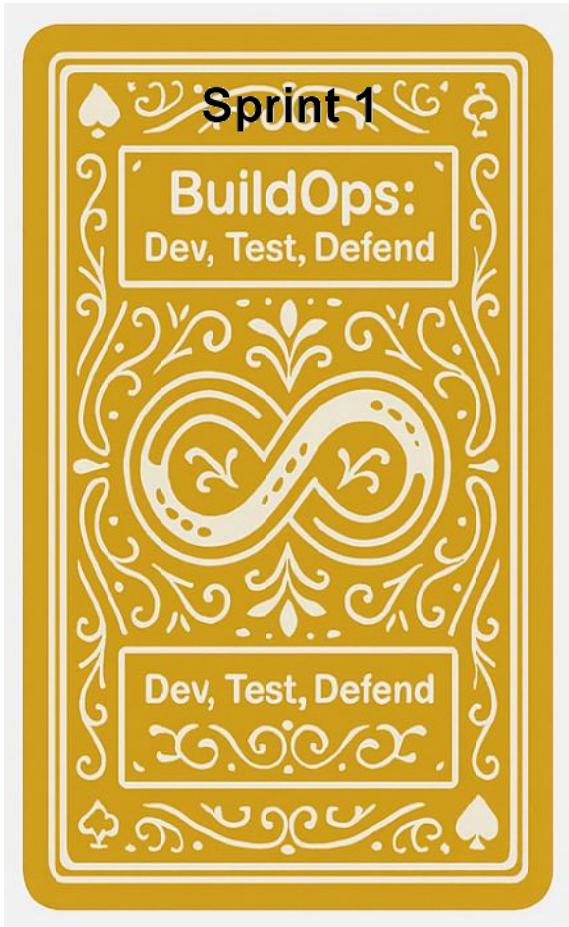
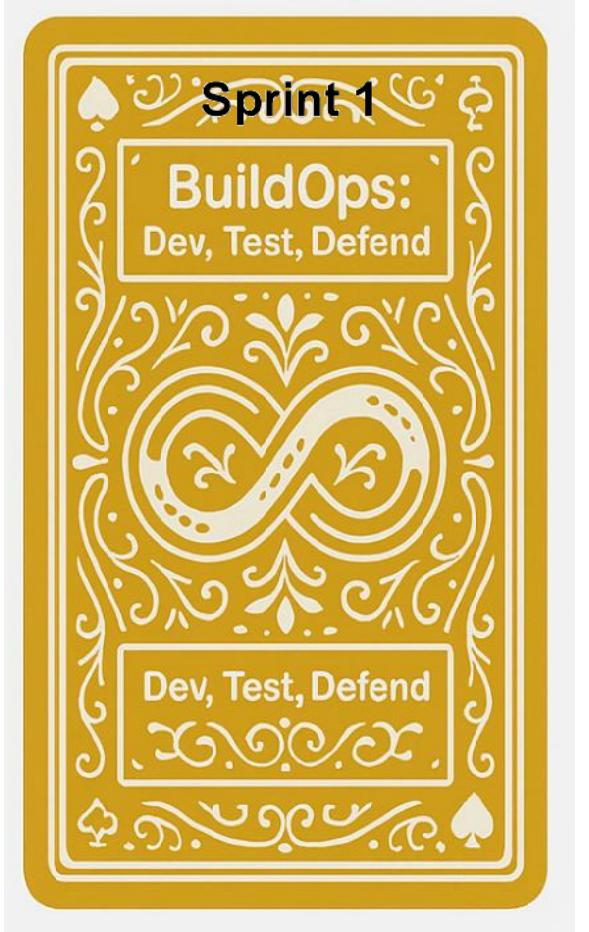
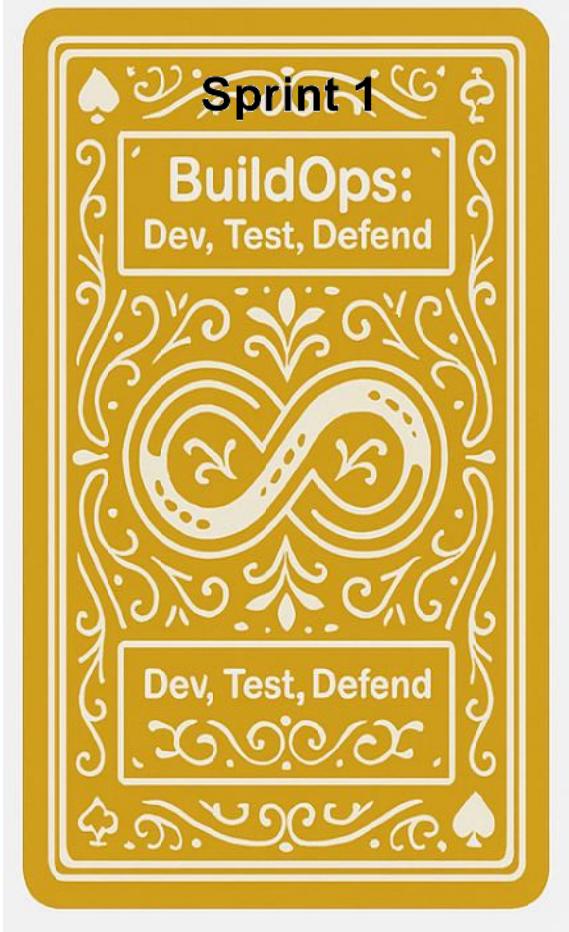


6

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

Story Points: 2 Customer Value: 15



Security Review of Application

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

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

Story Points: 4 Customer Value: 5

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*.

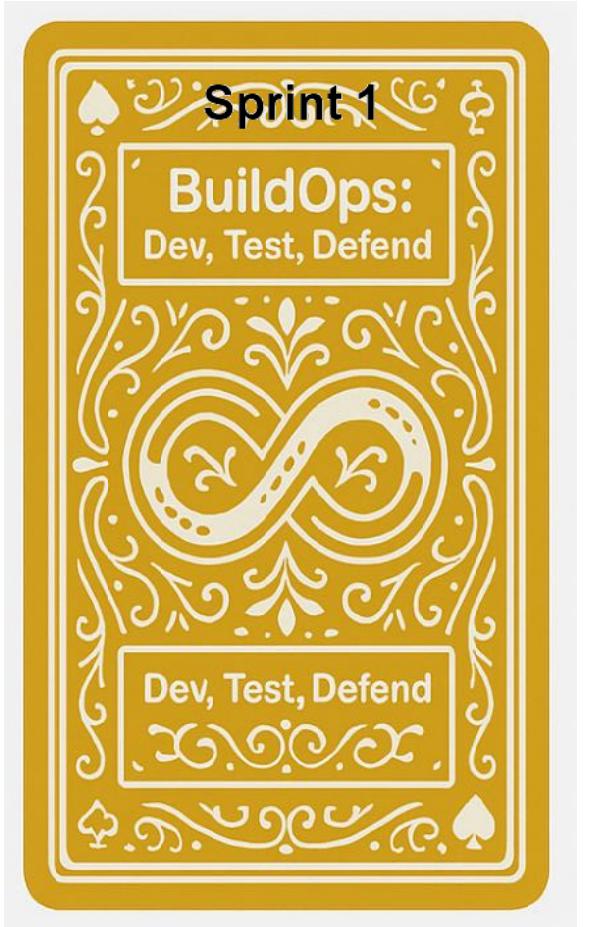
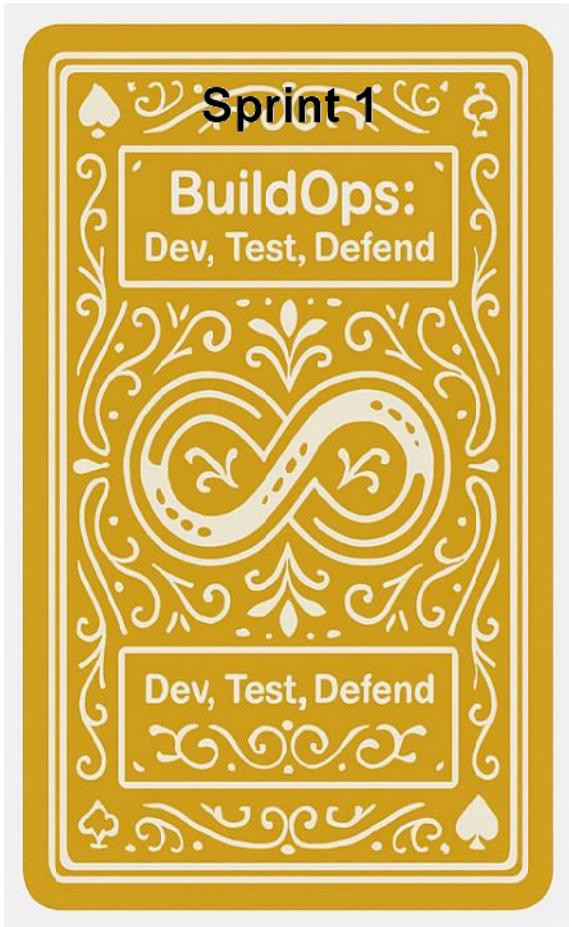
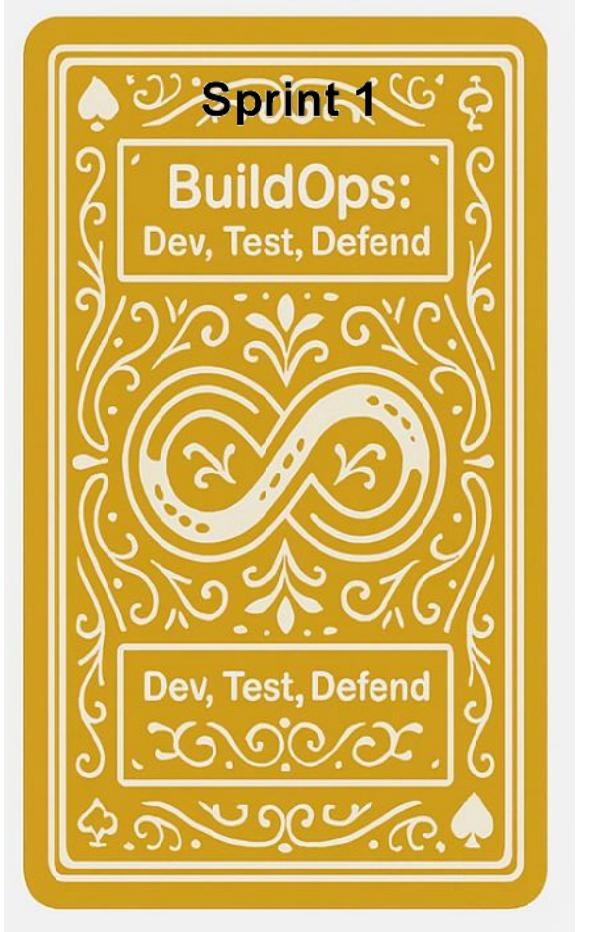
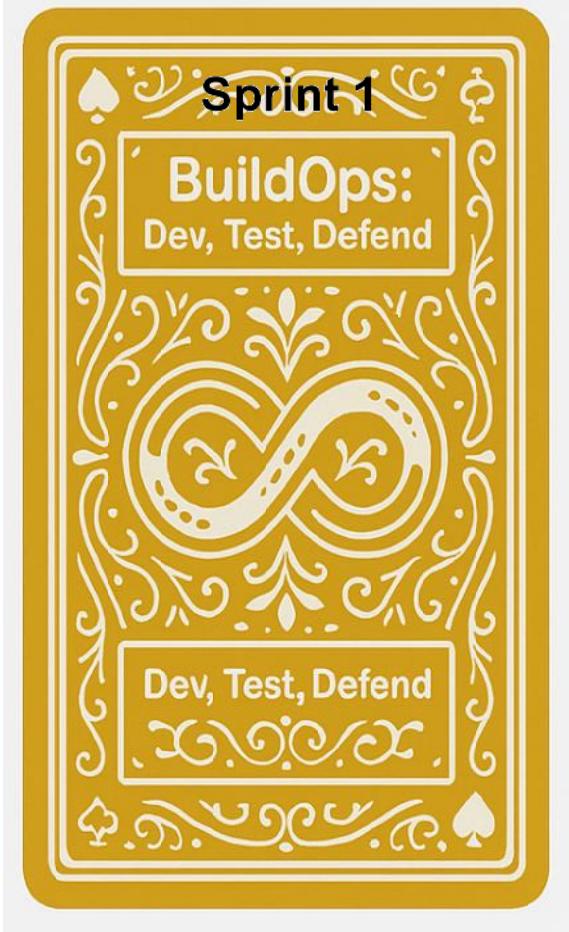
As a *Product Owner*, I want *an external security expert to perform code and design reviews of the app* so that *we can fix any vulnerabilities early*.

Secure Network Communication

Sprint: 1

6





Two Factor Authentication

Sprint: 2

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

Story Points: 4 Customer Value: 10



Network Protection

Sprint: 2

1

2

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**.

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

Story Points: 4 Customer Value: 10

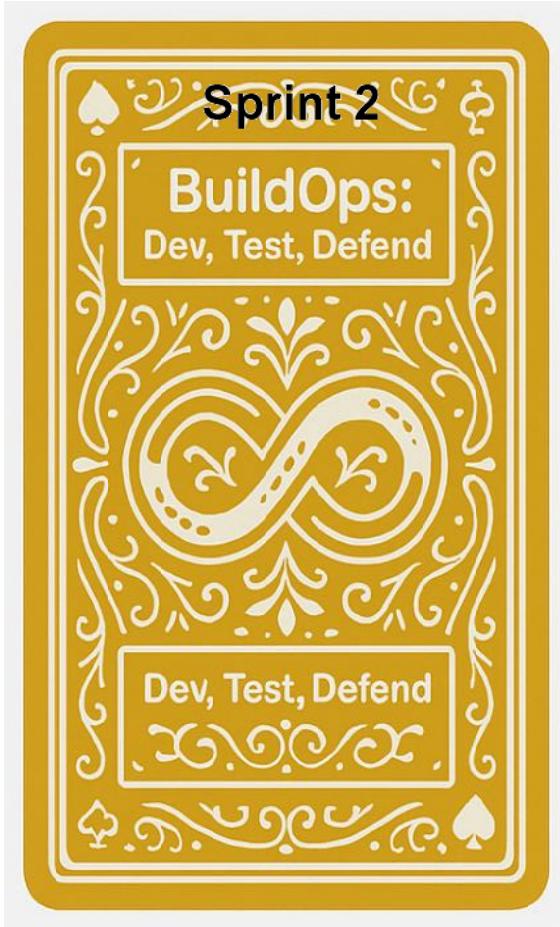
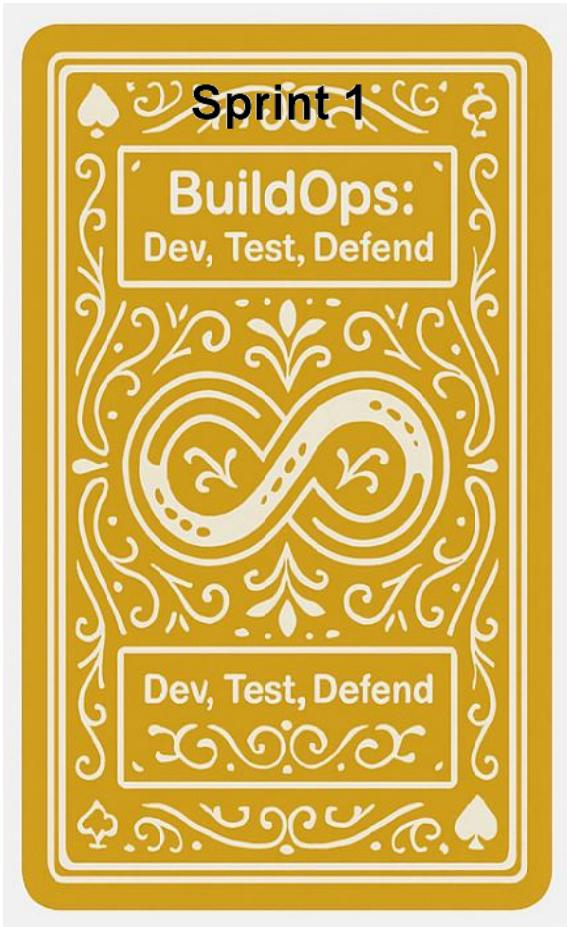
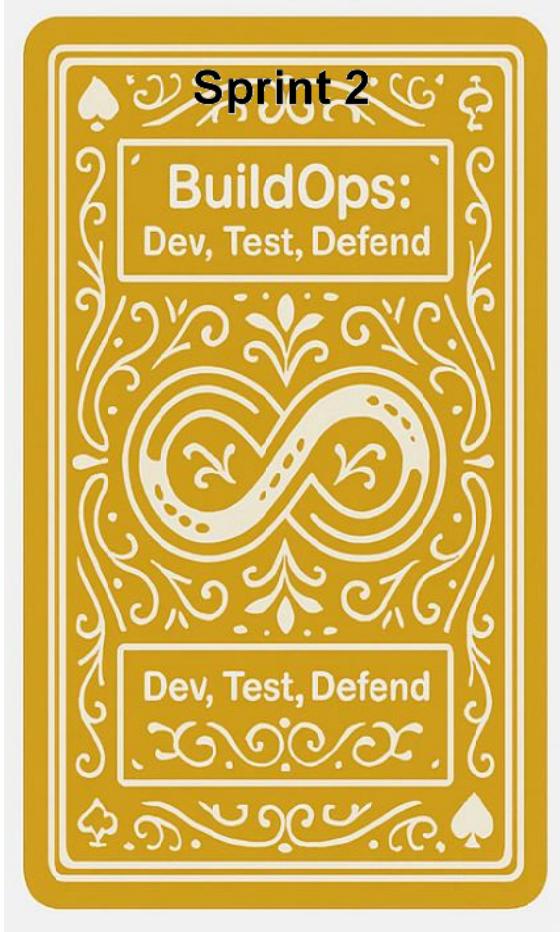
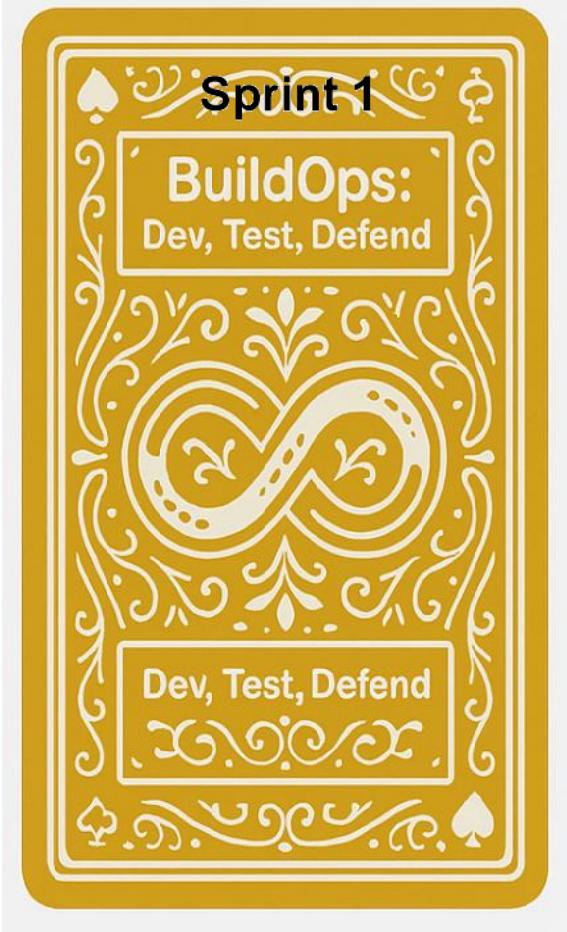
0

Server Patches

Sprint: 1



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**.



Incident Communication

Sprint: 2

3



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**.

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: 3 Customer Value: 5

Story Points: 4 Customer Value: 15



Sprint:



As a , I want so that .

As a , I want so that .

Story Points: Customer Value:

Story Points: Customer Value:

4



Hardware Security Module

Sprint: 2

1



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**.

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: 3

Customer Value: 5

Story Points: 4

Customer Value: 15



Sprint:



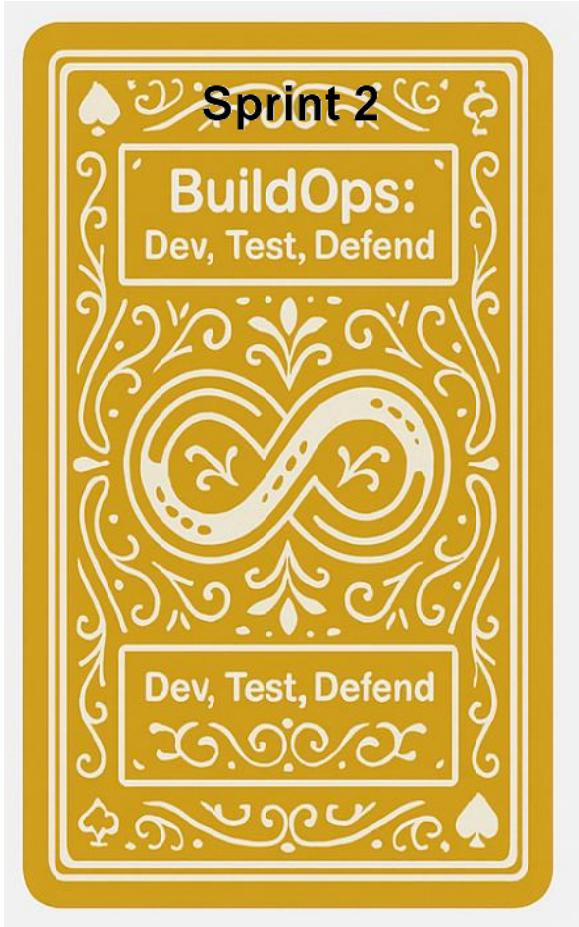
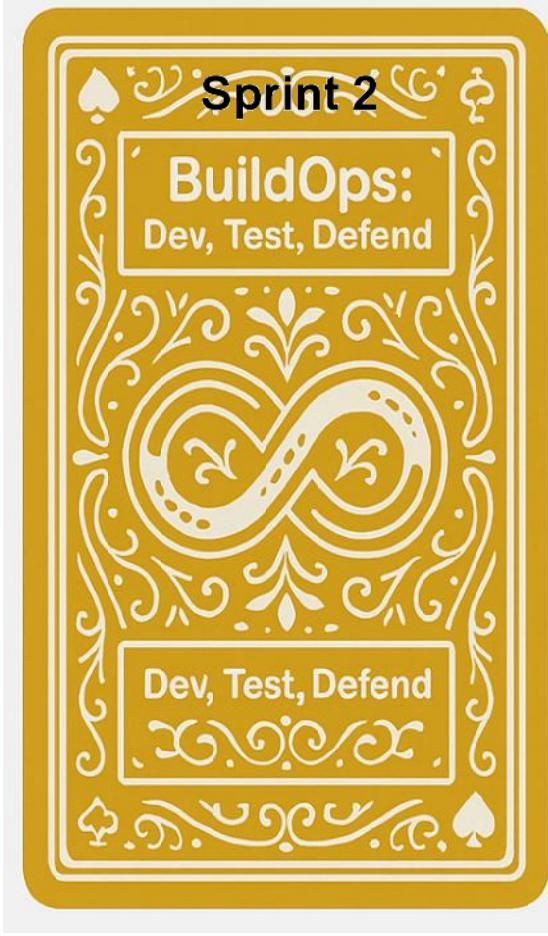
As a , I want so that .

As a , I want so that .

Story Points: Customer Value:

Story Points: Customer Value:

1



Network Monitoring for Server

Sprint: PT



1

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



7

Honeytrap in server

Sprint: PT



8

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: 15

Story Points: 4 Customer Value: 5

6

Encrypt & Hide Data on Server

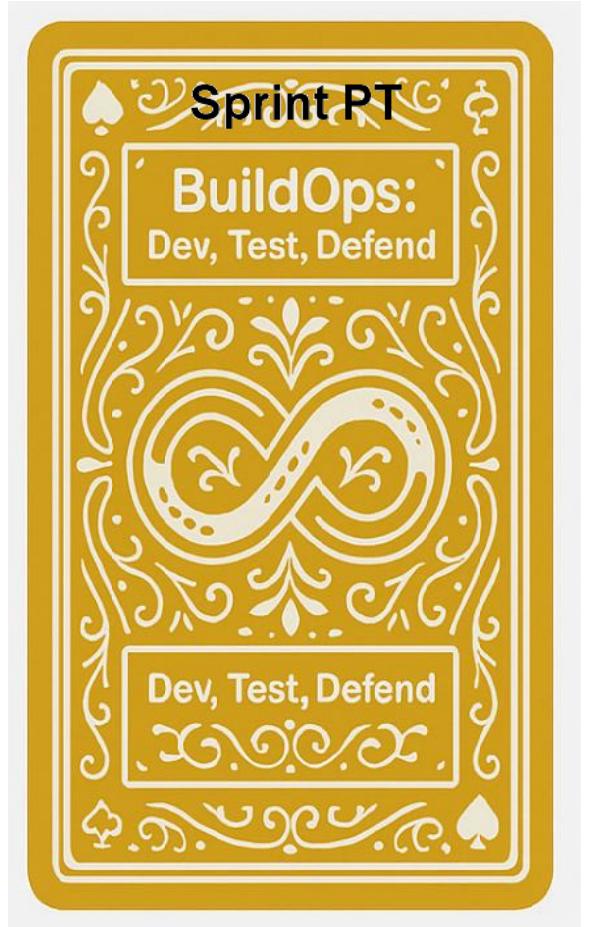
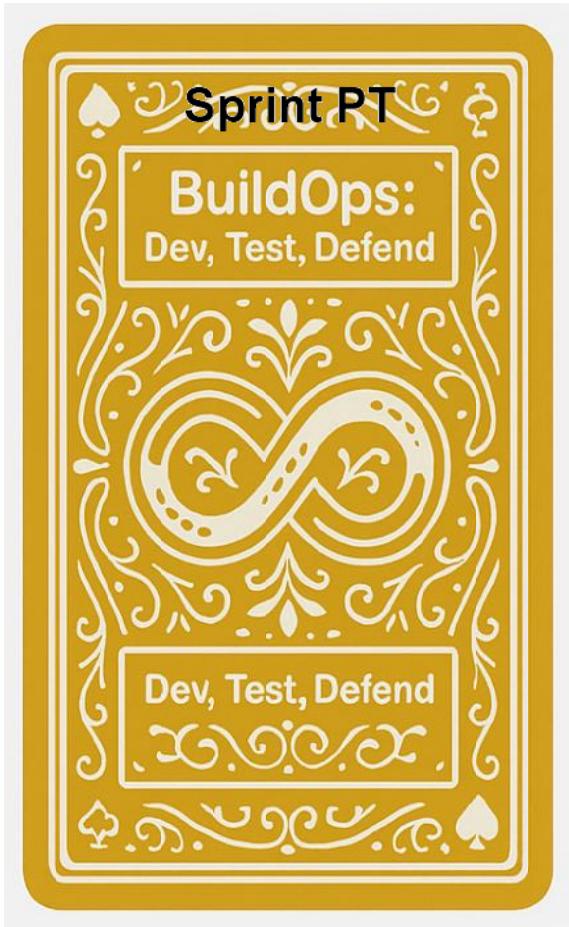
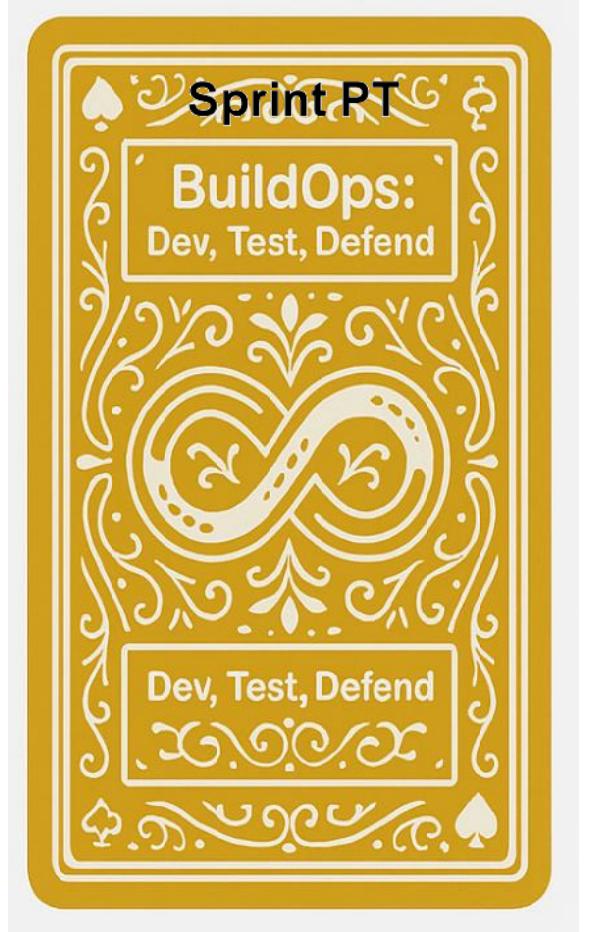
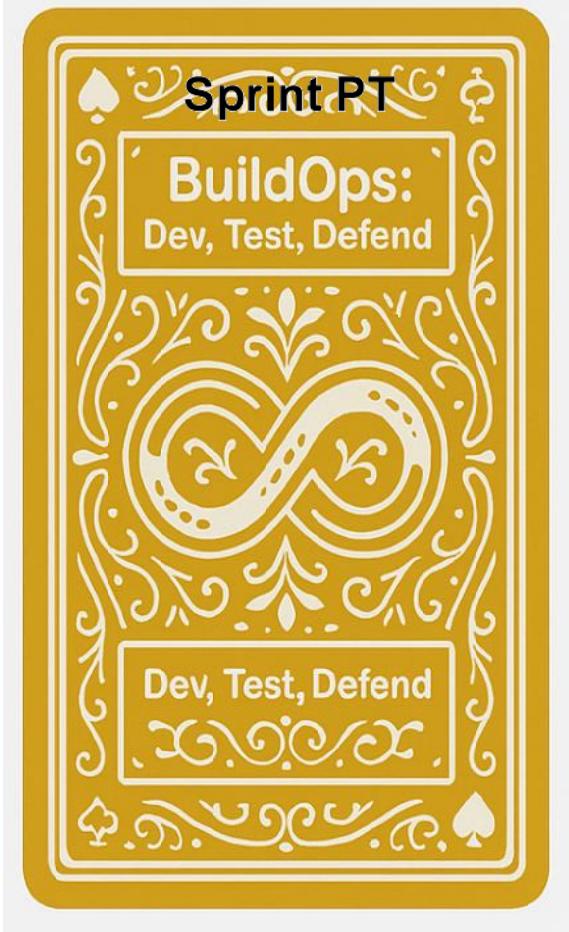
Sprint: PT



1

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



SSL Pinning for Enhanced HTTPS

Security

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

Sprint: RSC



As a **security analyst (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

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

Sprint: RSC



As a **security analyst (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

2 0

1 9

1 9

2 0

