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

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

Points Lost: 30

Mitigation(s): Data Backup
Server Patches

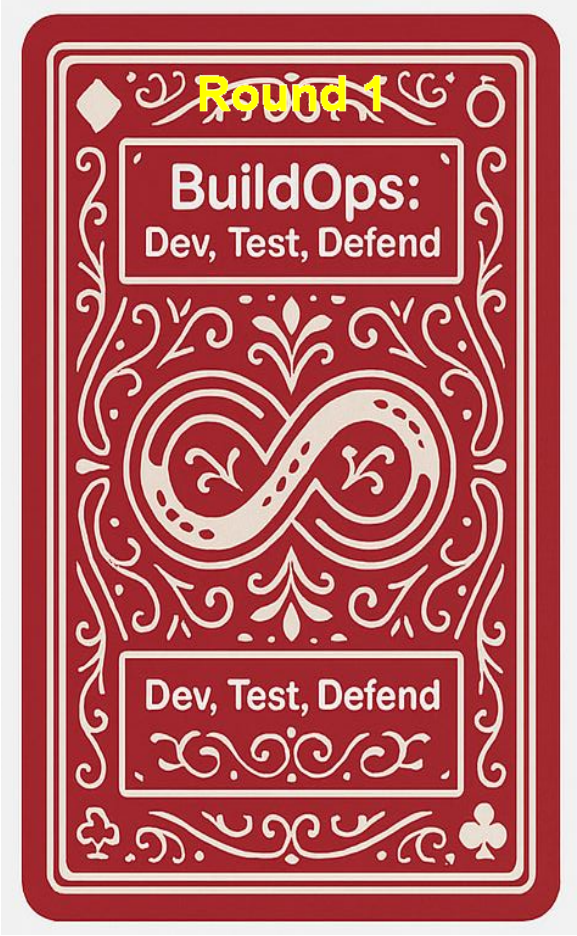
Round 1

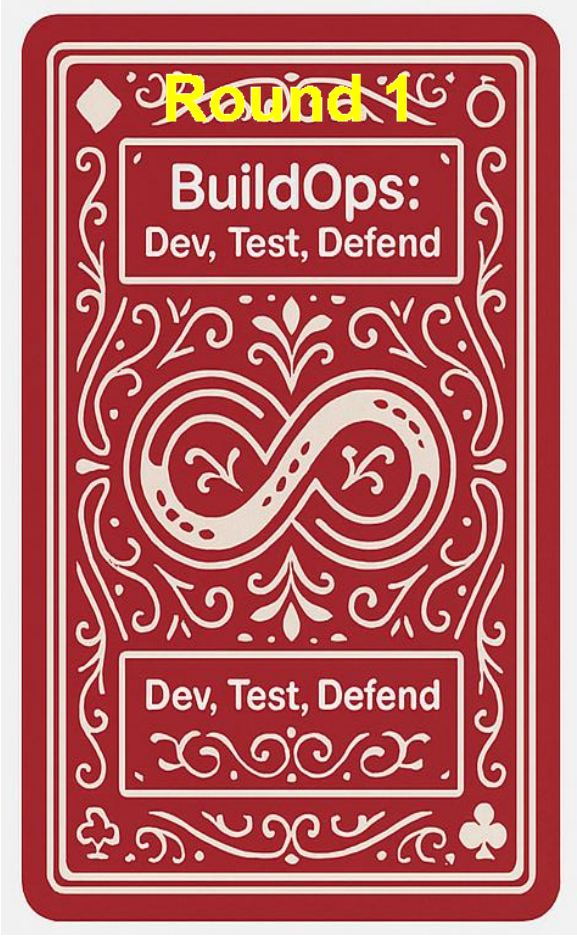
DoSing Kiddie

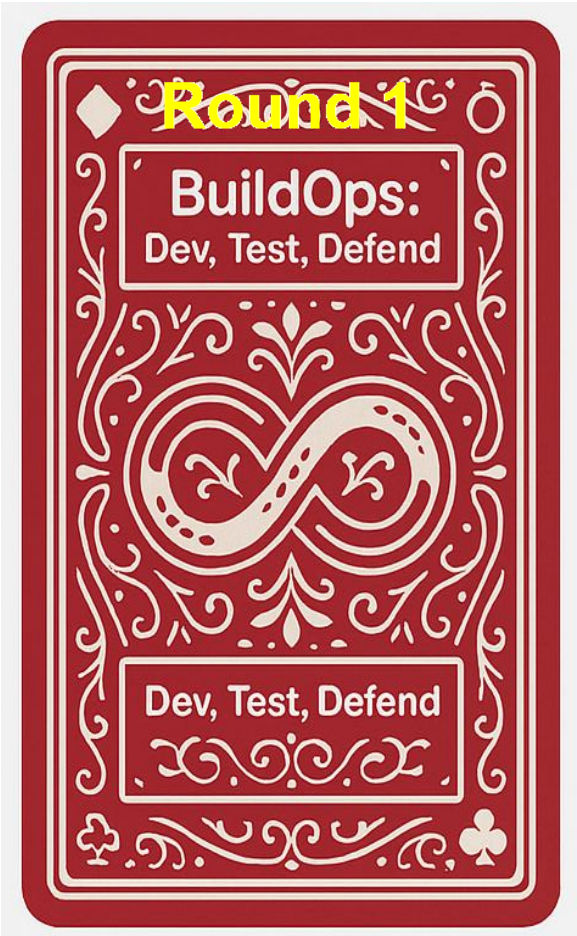
A malicious actor gets to server by accident and uses for ddos attacks on other servers

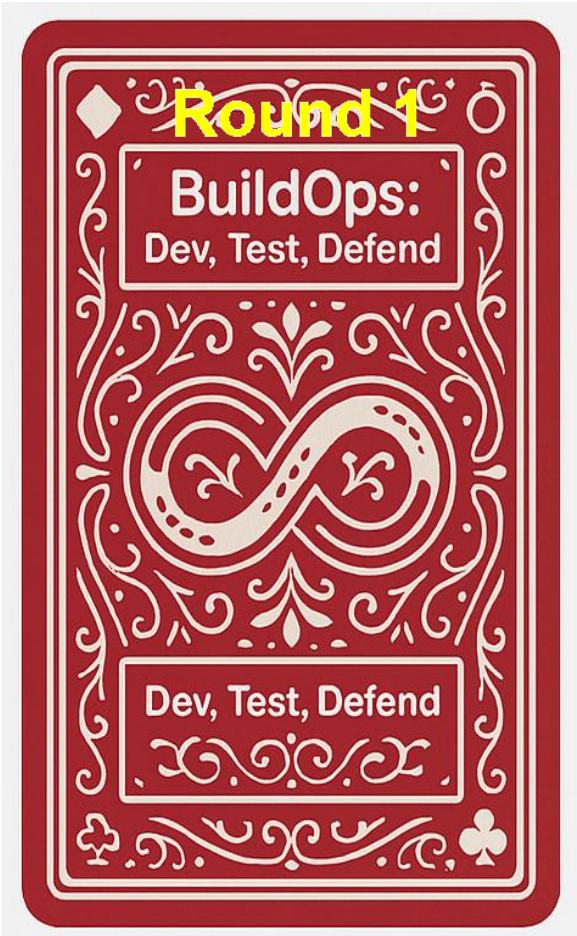
Points Lost: 60

Mitigation(s): Server Penetration Testing
Network Protection


Round 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend

Round 1

Darknet Reader

5

A user discovers a set of credentials for a key employee on the dark web that was published a year ago. They use them to try and hack your system.

Points Lost: 25

Mitigation(s): Password Change
Two Factor Authentication

Round 1

Mother Nature

6

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.

Points Lost: 25

Mitigation(s): Data Backup
Cloud Migration

Round 1

Bad Outsourcing

7

An attacker is able to use a simple SQL injection attack to discover the root password for the system. From this, they take it offline resulting in a service outage.

Points Lost: 40

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

Round 1

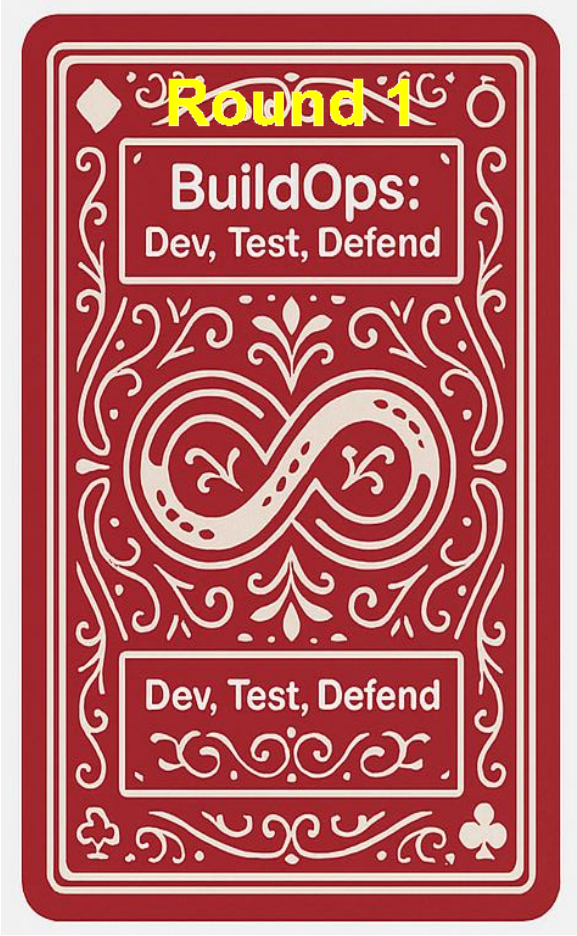
Coffee Shop Hacker

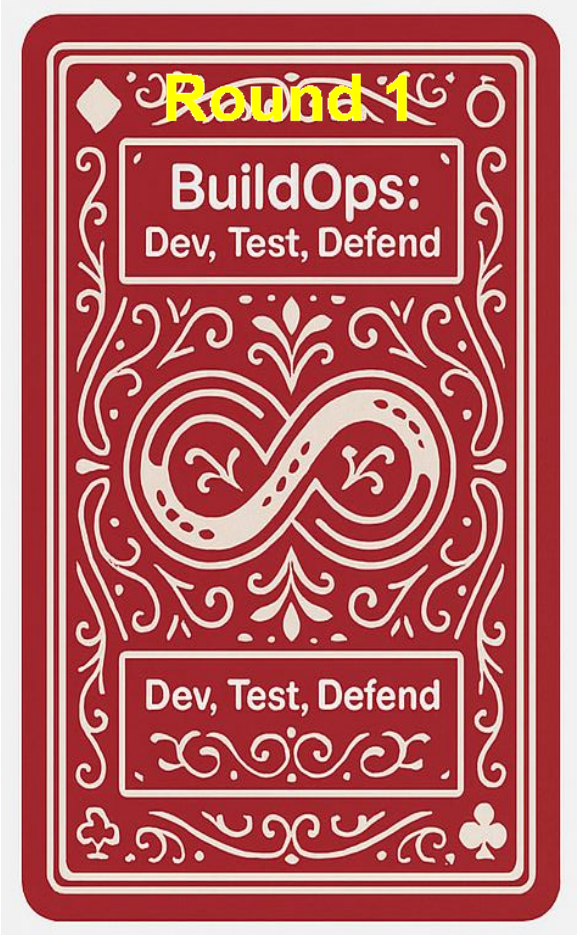
8

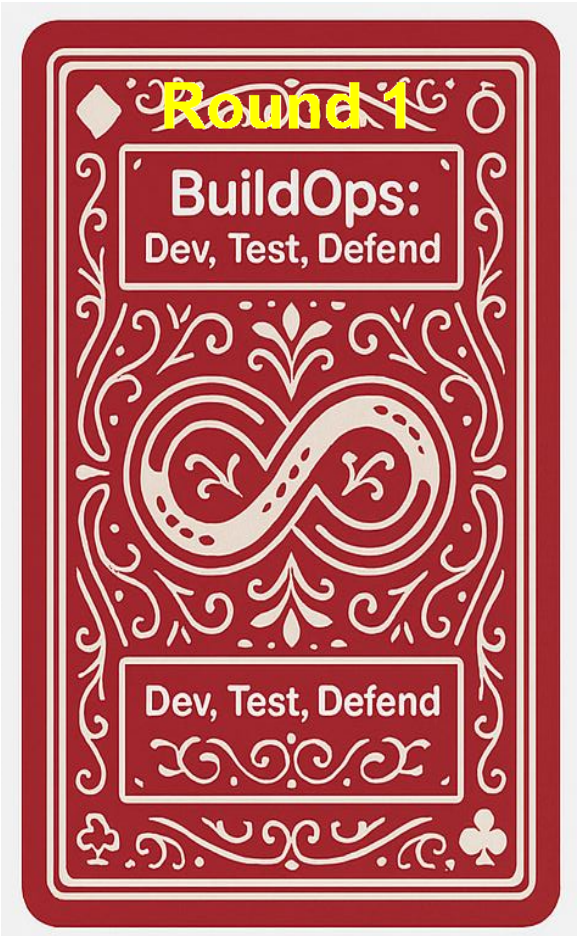
A major client of yours has had their Wi-Fi hacked at their coffee shop. Lots of packets are captured, and the attackers attempt to use them to break into other systems.

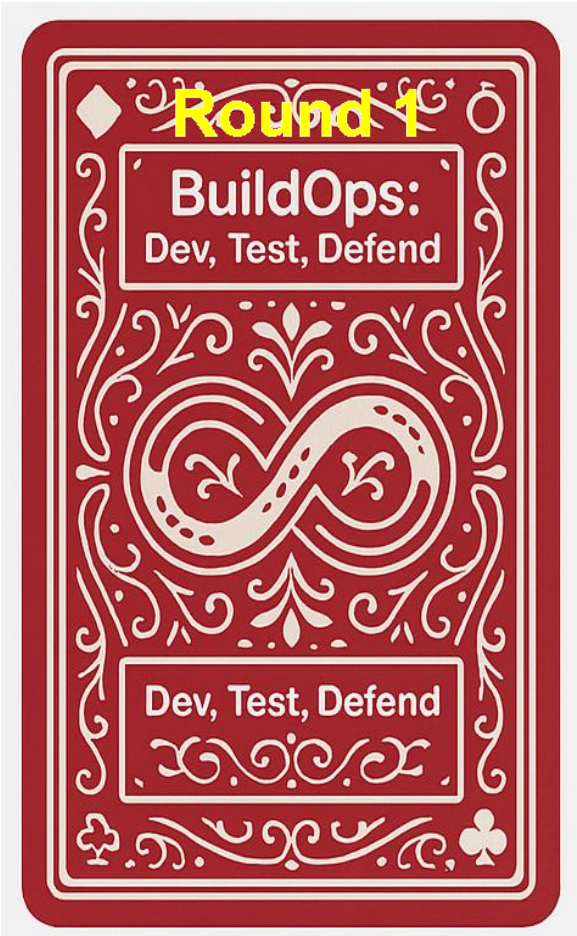
Points Lost: 30

Mitigation(s): Secure Network Communication
Two Factor Authentication


Round 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend

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

No Attack

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

Points Lost: 0

Mitigation(s): None

Round 2

Just Looking Attack

An attacker gets into your system, but doesn't do anything. They do not try to steal any data, the merely poke around.

Points Lost: 10

Mitigation(s): Authentication Hardening

Prevent Access to Office

Round 2

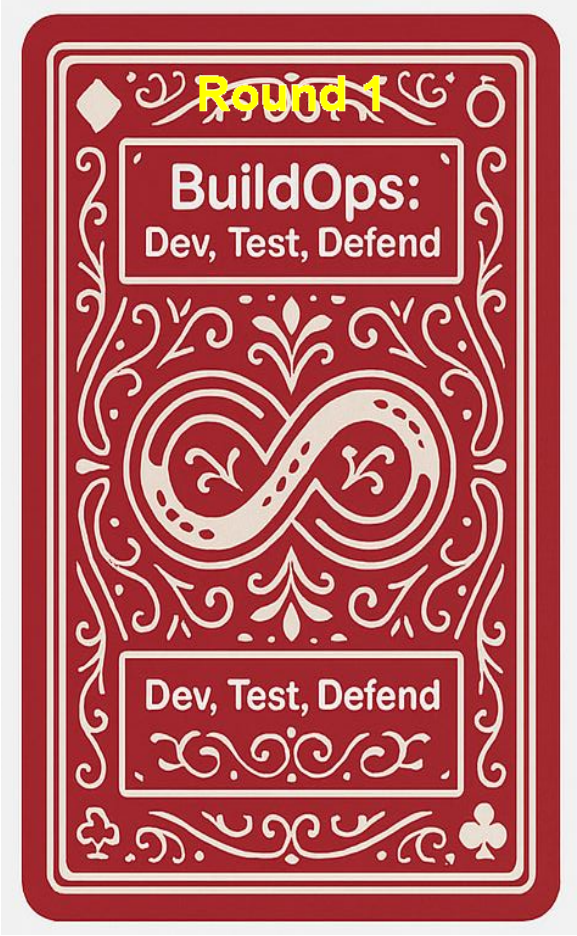
Hacking Kiddie

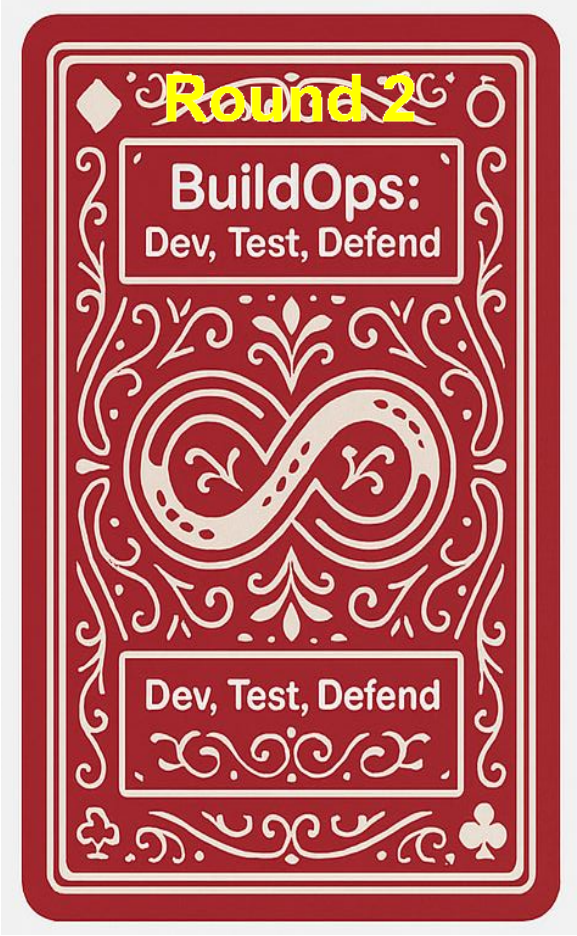
A hacker gains access to your system and gets to server by accident. The attacker exfiltrates unencrypted data from the database and downloads other material, publishing it on the web.

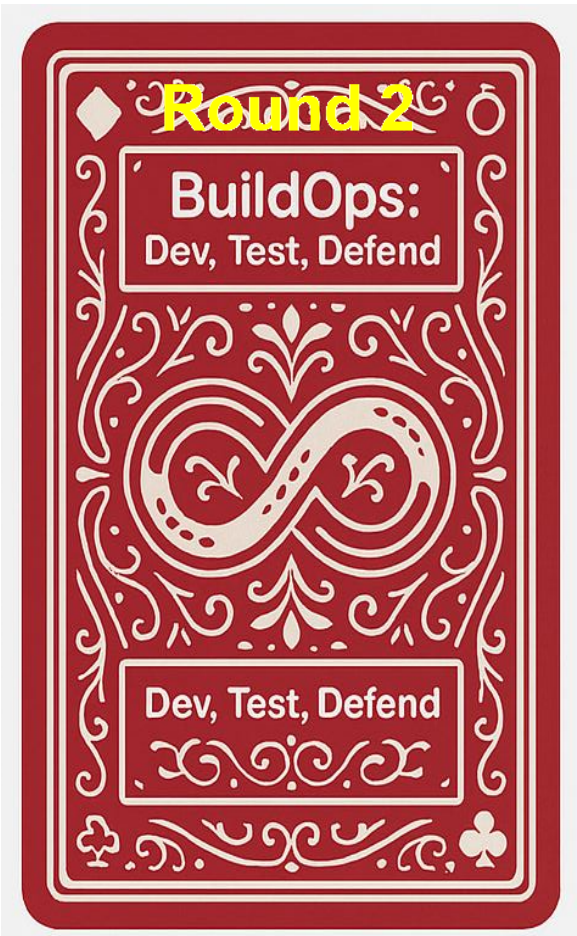
Points Lost: 60

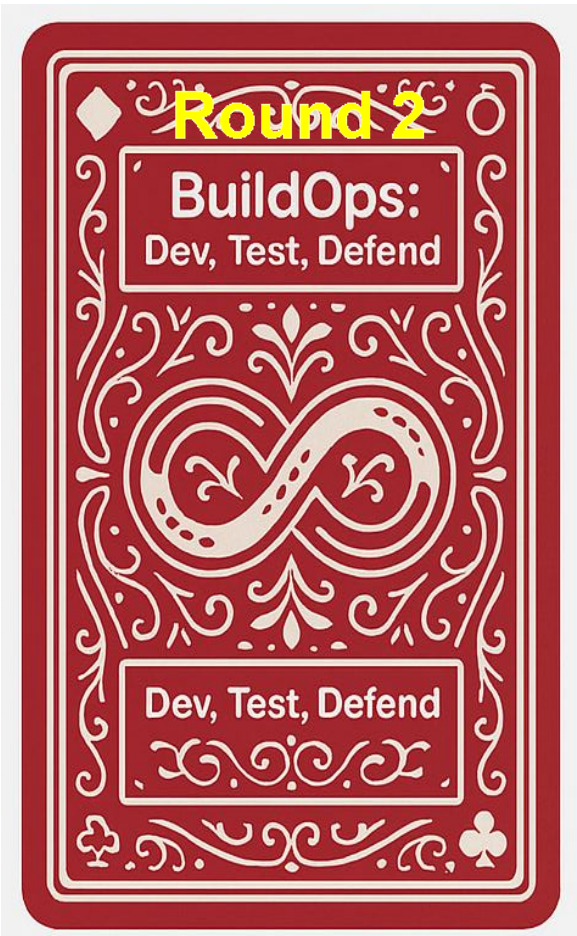
Mitigation(s): Server Penetration Testing

Network Protection


Round 1
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 2
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 2
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 2
BuildOps:
Dev, Test, Defend
Dev, Test, Defend

Round 2

Phishing Kiddie

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

Points Lost: 50

Mitigation(s): Incident Communication
Two Factor Authentication

Round 2

Amateur Developer

A developer that you have hired accidently 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

Improperly Trained Dev

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

Points Lost: 30

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

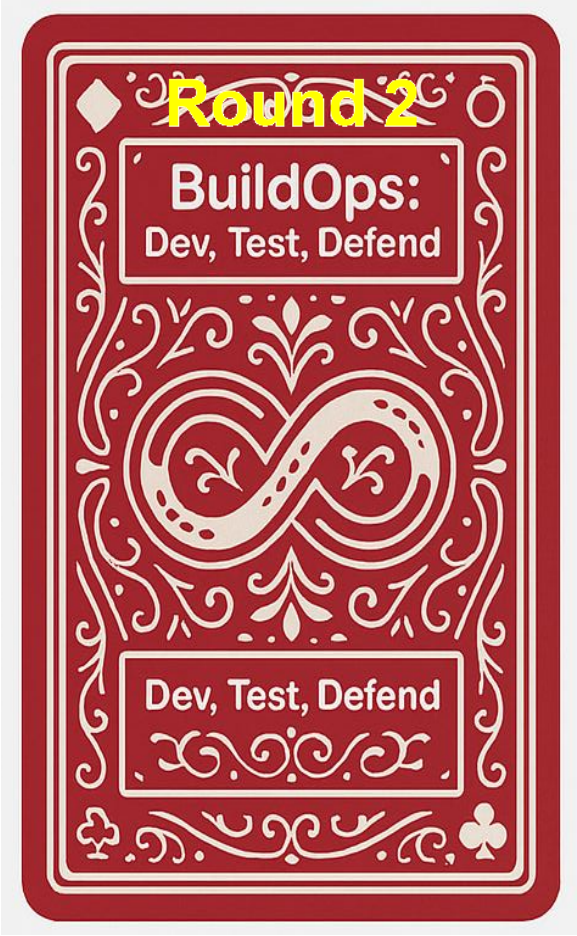
Round 2

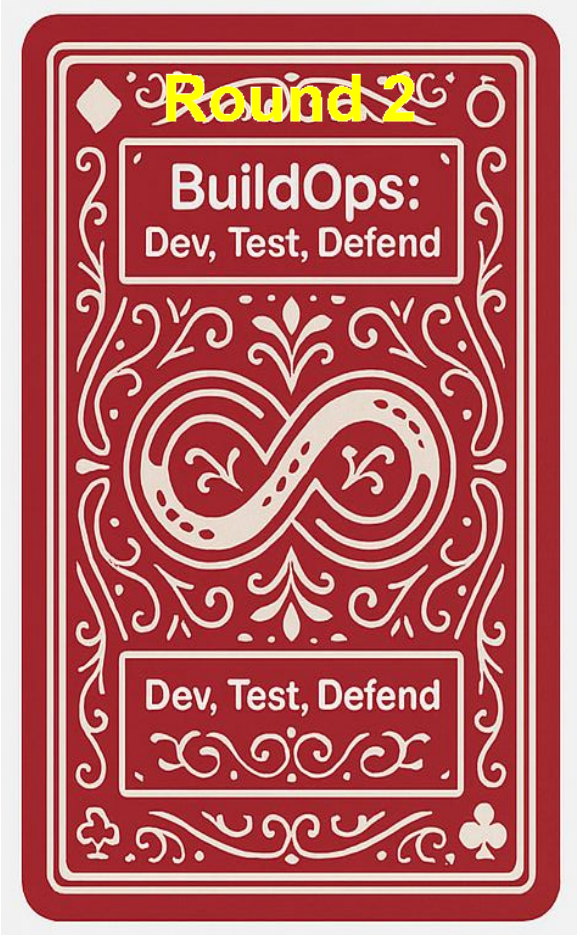
Recognition

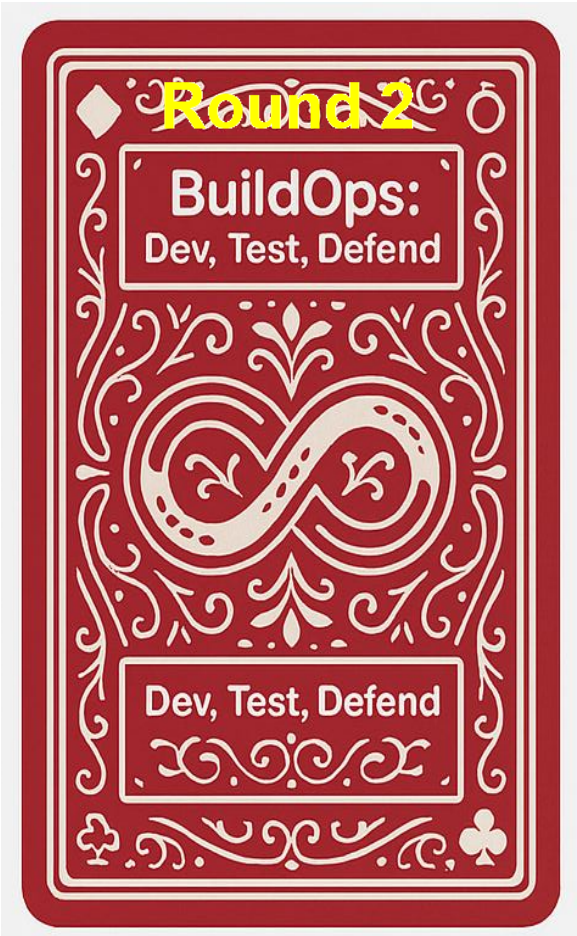
Your site has been acknowledged as an overly secure site and is published in Wired magazine as an exemplar website.

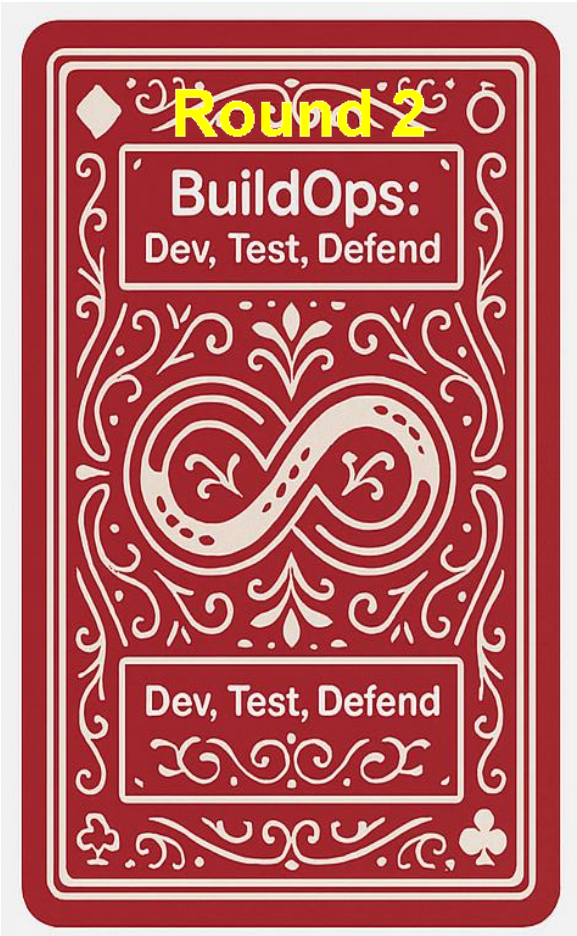
Points Lost: 0

Mitigation(s): None


Round 2
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 2
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 2
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 2
BuildOps:
Dev, Test, Defend
Dev, Test, Defend

Round 3

MITM Kiddie

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

Aggrieved Hacker

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

MITM Mafia

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: 80

Mitigation(s): SSL Pinning for Enhanced HTTPS Security

Two Factor Authentication

Round 3

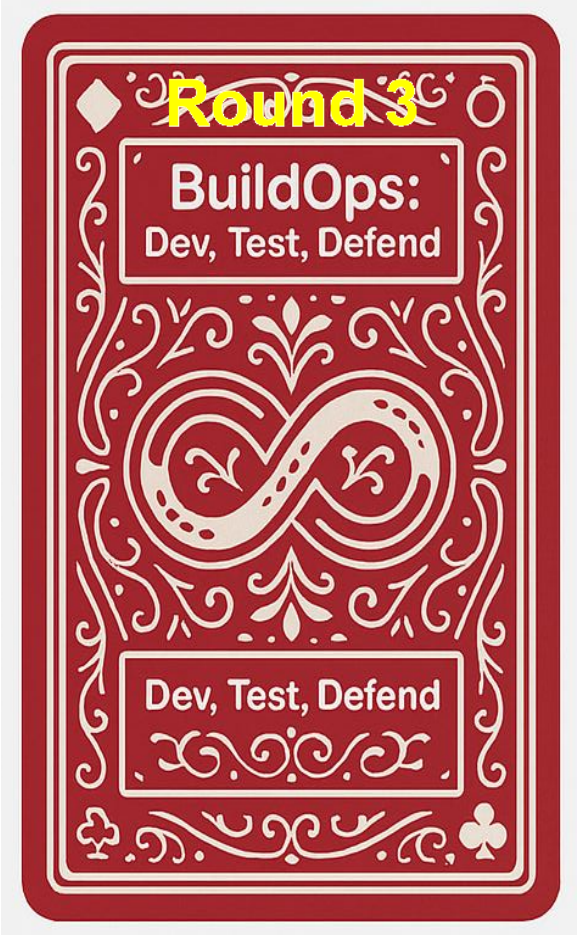
Mafia Team

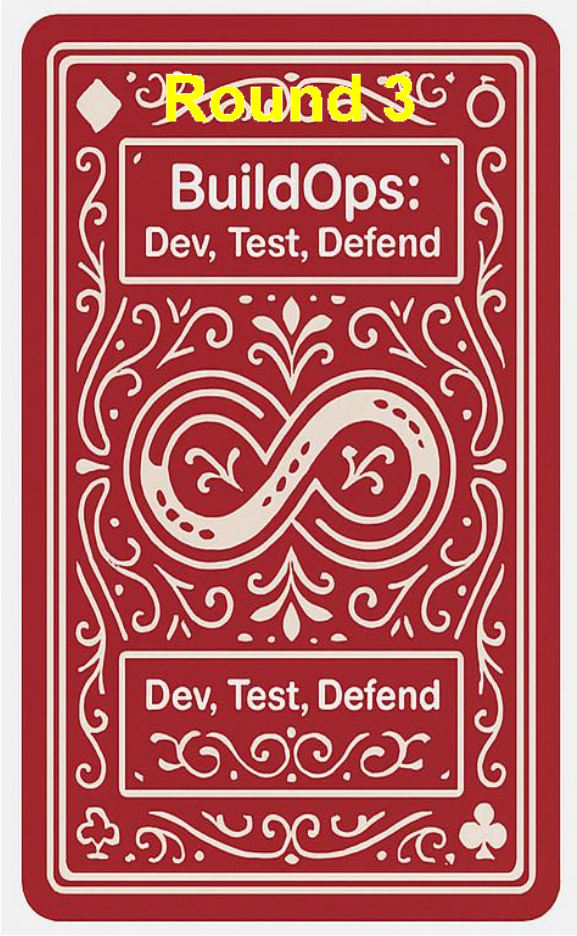
Physically gains access to office, get passwords from server logs, small theft from tens of thousands of accounts.

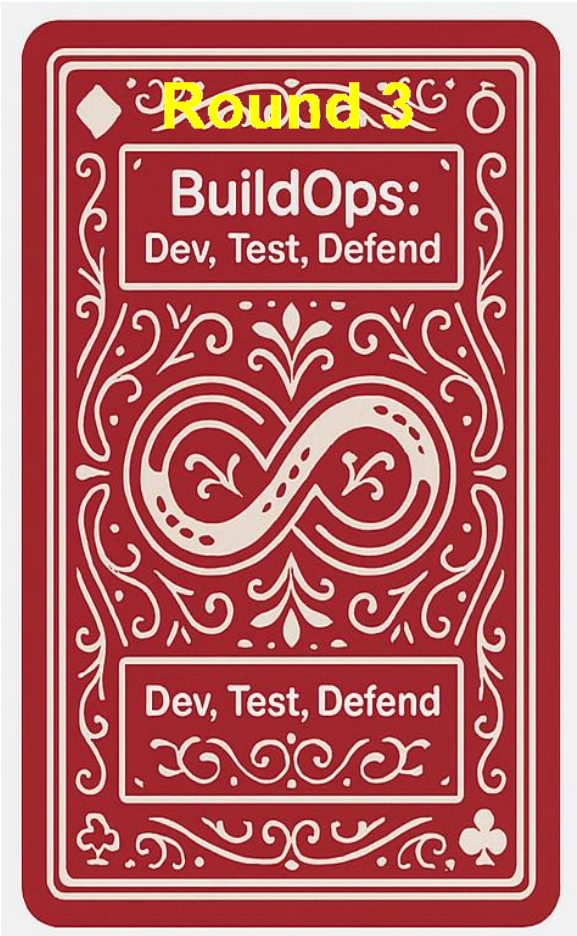
Points Lost: 80

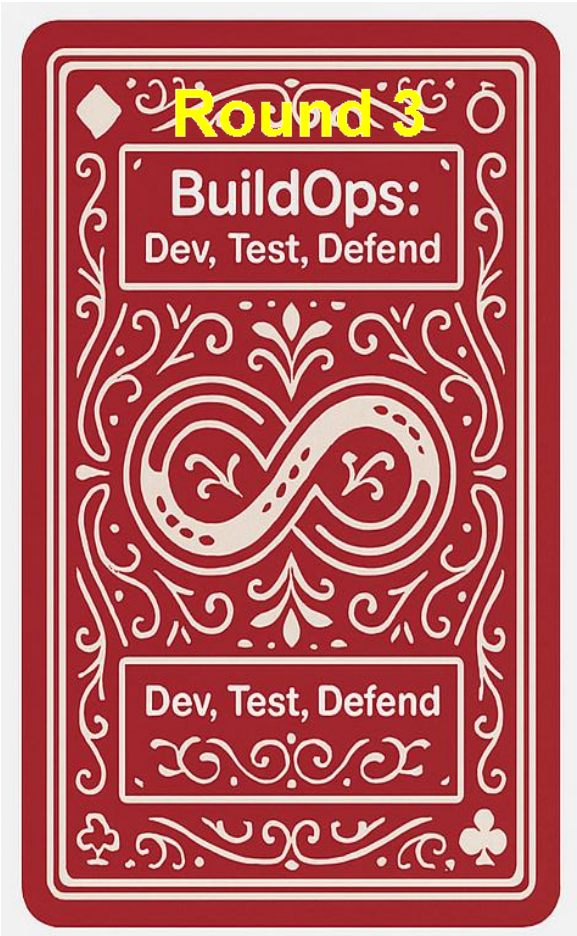
Mitigation(s): Network Protection

Filter server logs


Round 3
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 3
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 3
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 3
BuildOps:
Dev, Test, Defend
Dev, Test, Defend

Round 3

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

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

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

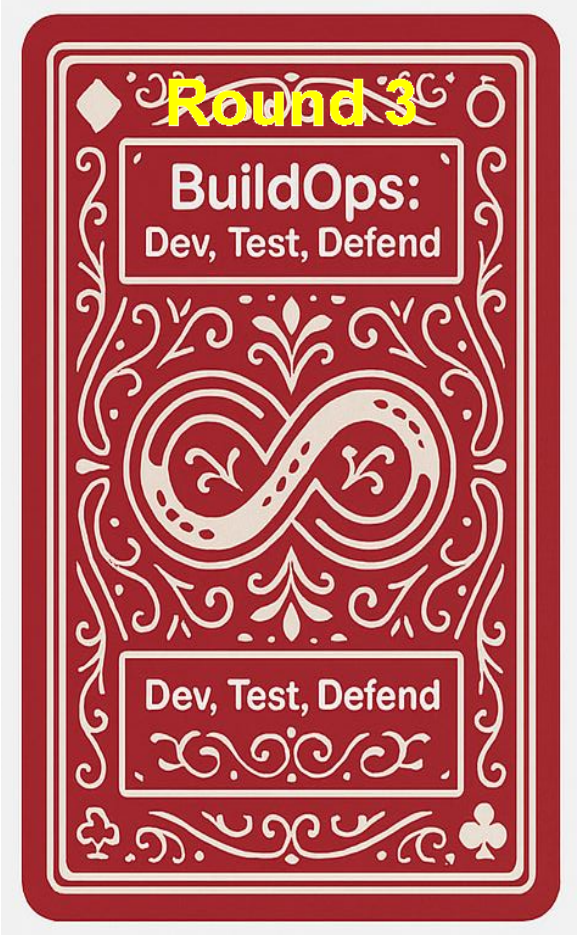
Vendor Faking

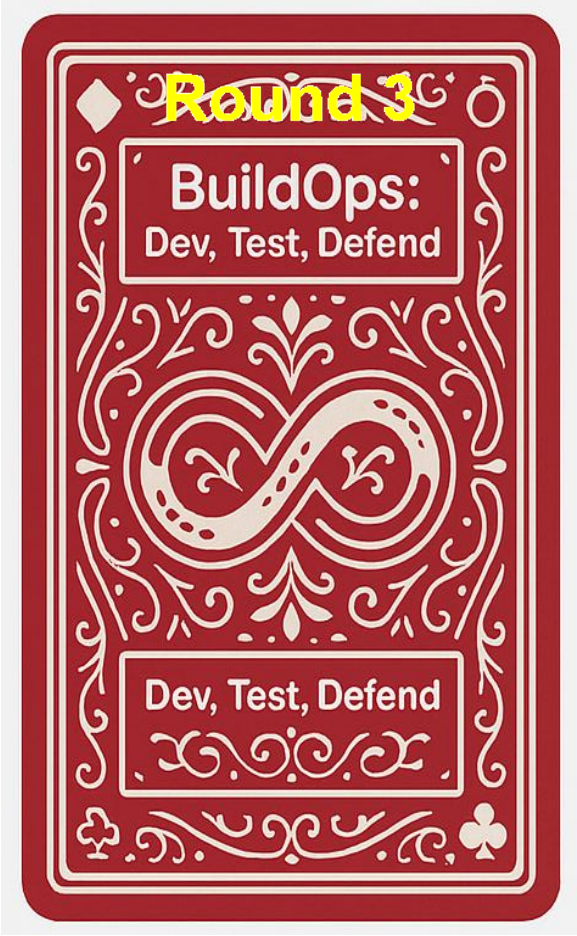
A vendor has been faked within the system and is attacking automatic payments.

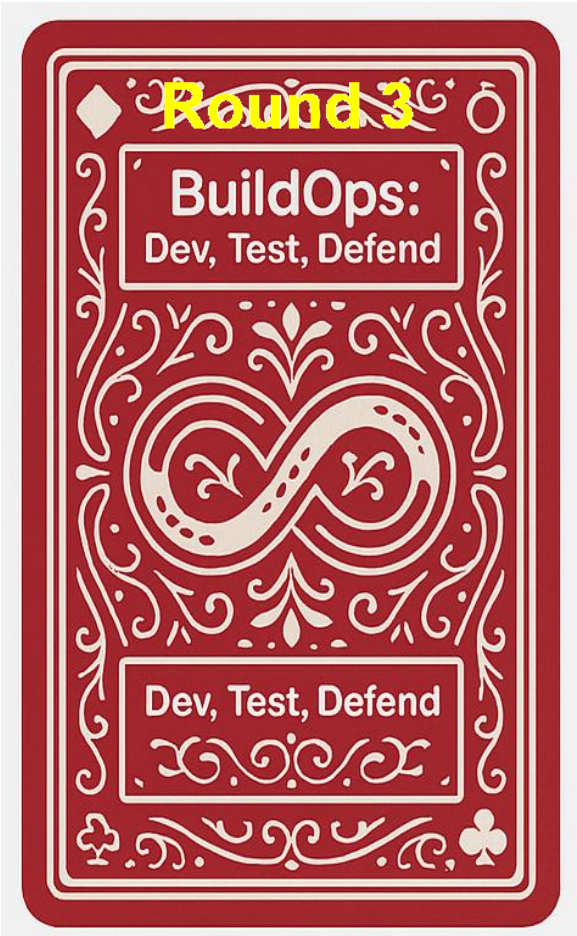
If the automatic payment system PBI has been implemented, you are vulnerable unless the mitigations have been applied.

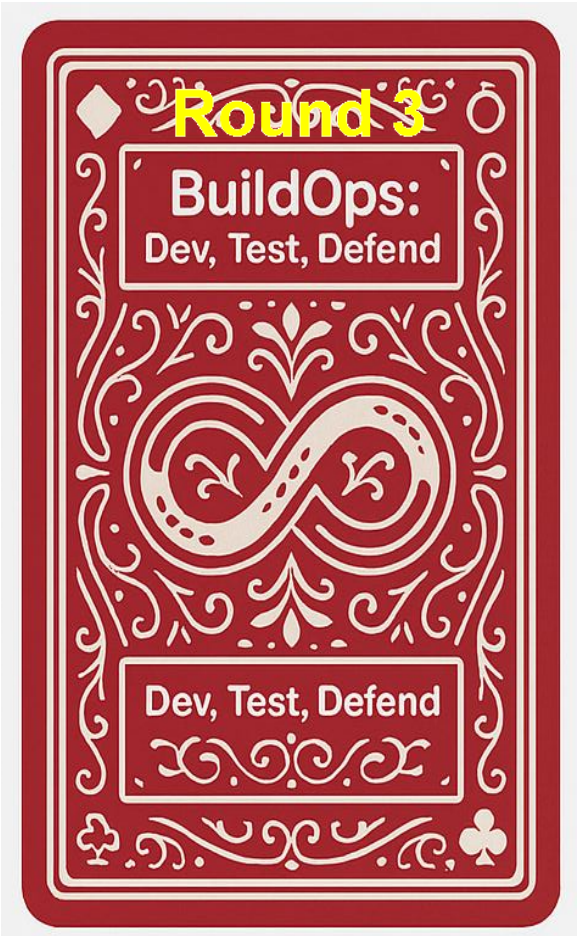
Points Lost: 60

Mitigation(s): Two Factor Authentication


Round 3
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 3
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 3
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 3
BuildOps:
Dev, Test, Defend
Dev, Test, Defend

Round 3

Cross Platform Injection

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

Chat Feature Data Leak

Unencrypted or improperly stored messages reveal sensitive communication.

If you have enabled the Chat feature, you are vulnerable to this attack.

Points Lost: 50

Mitigation(s): None

Round 3

Receipt Fraud Attack

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

Round 3

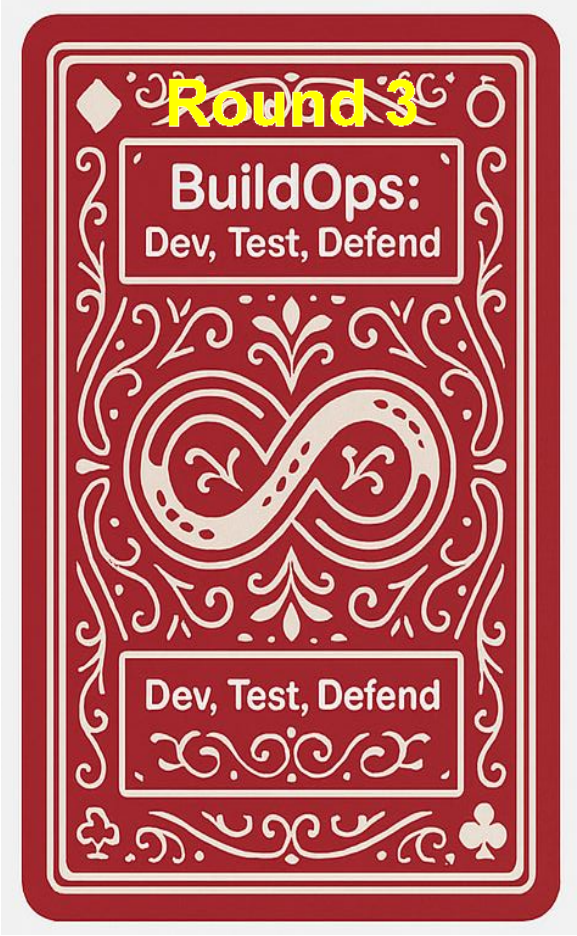
Platform Attack

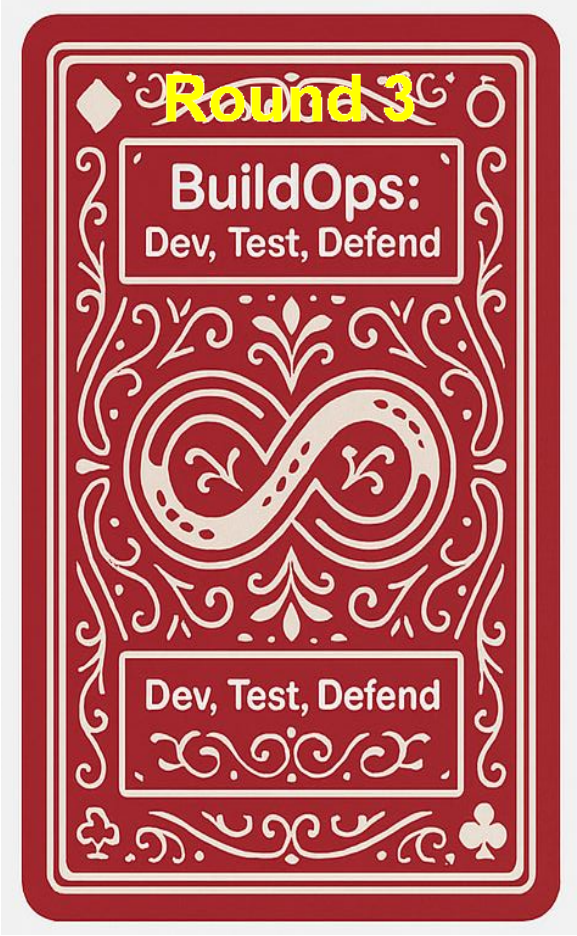
A malicious user has identified a vulnerability in the platform that is being used for your microservices architecture.

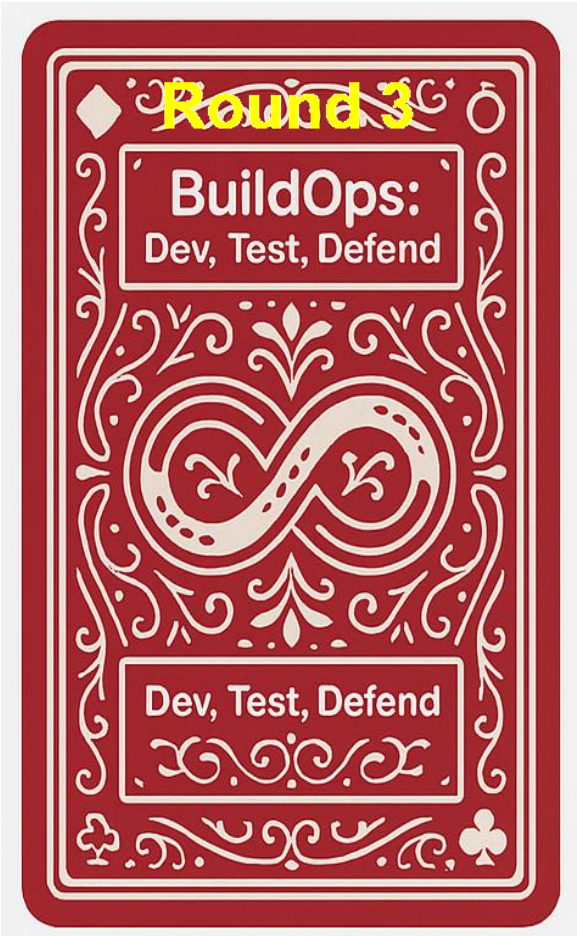
If you have switched to a microservices architecture, you are vulnerable. If you have not made the switch, you are not vulnerable. If vulnerable, you will spend 3 story points next sprint mitigating this.

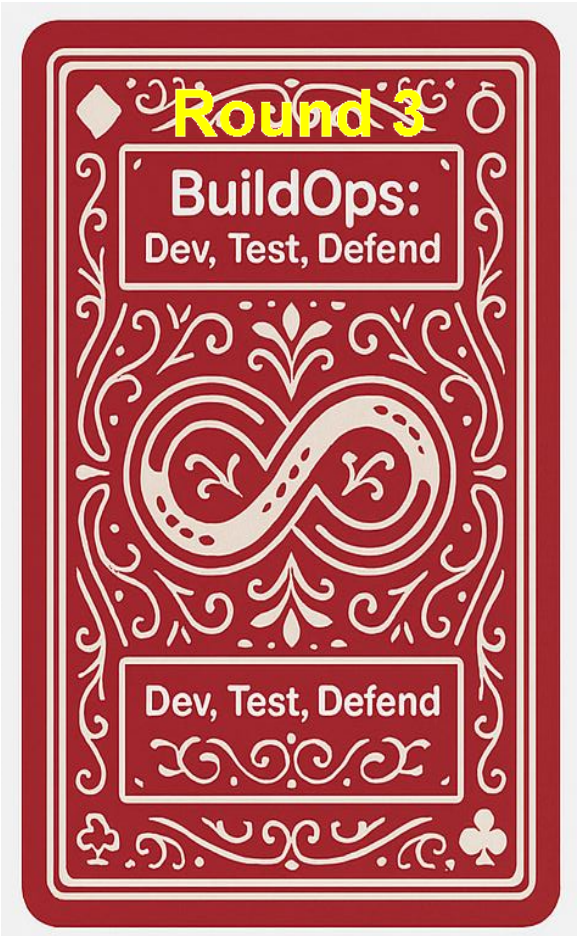
Points Lost: 60

Mitigation(s): None


Round 3
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 3
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 3
BuildOps:
Dev, Test, Defend
Dev, Test, Defend


Round 3
BuildOps:
Dev, Test, Defend
Dev, Test, Defend