SECURE DELIVERY

Gamification of Threat Modelling

An introduction to

OWASP **Cornucopia**

&

copi BETA!

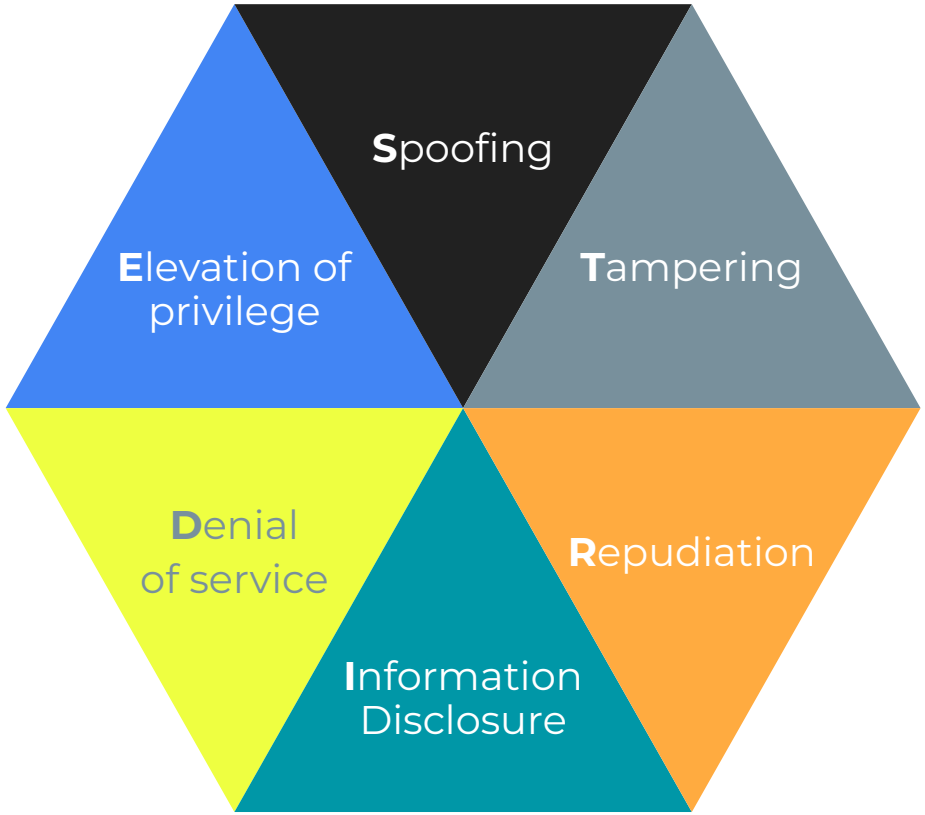
Threat Modelling

- The United States' Executive Order 14028[1]
- OWASP's Top 10:2021 Insecure Design #4[2]

1. Recommended Minimum Standard for Vendor or Developer Verification of Code
2. OWASP Top 10:2021

Traditional Threat Modelling with STRIDE

The purpose of threat modelling is to understand security possible issues before discovering them in your product. Threat models give you pressure points to focus on.



Spoofing

Pretending to be something other than what you are. The inverse characteristic we want to ensure is **Authenticity**.

Tampering

Modifying or manipulation of data within the application the way to ensure this can happen is testing **Integrity**.

Repudiation

A threat or a design feature? It's a security issue that we may not know who performed what action so **Non-repudiation** is desirable.

Information disclosure

The primary threat of any system that has data of value. The required feature, **Confidentiality**, is part of the core CIA triad.

Denial of service

Another major threat and one often employed against systems. Again the required characteristic is in the triad, **Availability**.

Elevation of privilege

This threat covers being able to do more than you should and at the core of access control, **Authorisation** is the desired state.

Waterfall Development Process

Development methodology that preceded Agile and that is still practised where Agile is not (for whatever reason).

STEP ONE

Gather the requirements of the solution ensuring you don't miss any...

STEP TWO

Design a working solution and ensure that it covers all everything ... security too.

STEP THREE

Build the solution and make sure that during that process we take security seriously.

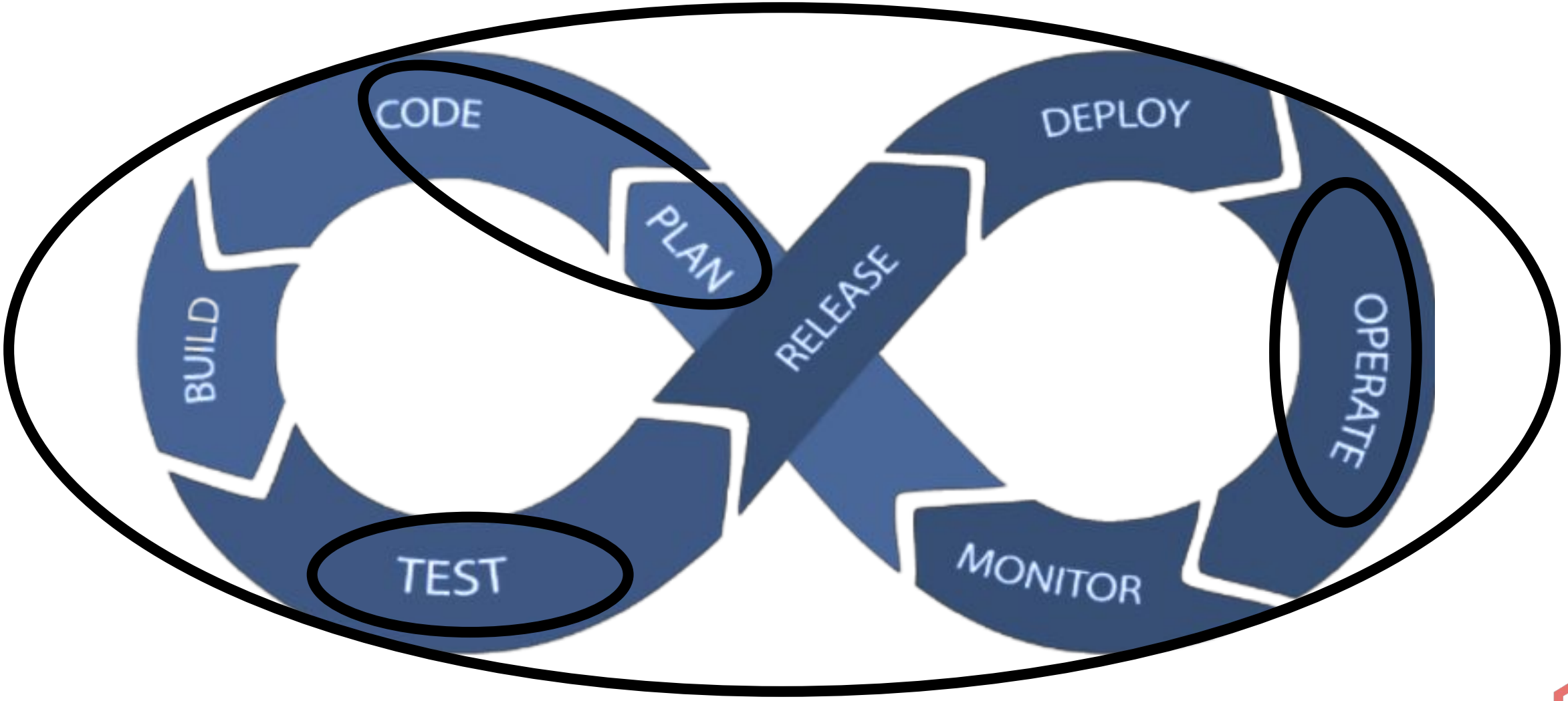
STEP FOUR

Comprehensively test the solution. That it functionally does as designed ... securely.

STEP FIVE

Deploy the solution. Securely, of course. And hope that it still meets the requirements.

Agile Development Process



The Four Questions

- What are we working on?
- What could go wrong?
- What are we going to do about it?
- Did we do a good job?

Agile Threat Modelling

DESIGN TIME

TAKES TIME

CHANGES IN TIME

IT'S ABOUT TIME: WHEN, AMOUNT & HOW OFTEN

At design time, when the use cases are understood but before building starts. It's in that special point in time that you can design for security. It takes time to do. The larger the piece of design work the more time you need to spend on it. And as we start to build, that's when you realise that more threat modelling needs to be done.

Agile Threat Modelling - Design Time

DESIGN TIME

TAKES TIME

CHANGES IN TIME

MODELLED TOO LATE

Threat modelling is generally done by security professionals. And they are usually invited to look at designs ... completed designs

IT'S ABOUT TIME: WHEN, AMOUNT & HOW OFTEN

At design time, when the use cases are understood but before building starts. It's in that special point in time that you can design for security. It takes time to do. The larger the piece of design work the more time you need to spend on it. And as we start to build, that's when you realise that more threat modelling needs to be done.

“Threat modeling: the sooner the better, but never too late.”

Steven Wierckx
Avi Douglen
(OWASP Threat Modelling Project)

https://owasp.org/www-community/Application_Threat_Modeling/

Agile Threat Modelling - Takes Time

DESIGN TIME

MODELLED TOO LATE

Threat modelling is generally done by security professionals. And they are usually invited to look at designs ... completed designs

TAKES TIME

TOO MUCH TIME

Doing threat modelling with a large part of a design leads to a large number of threats being found ... often too many to deal with

CHANGES IN TIME

IT'S ABOUT TIME: WHEN, AMOUNT & HOW OFTEN

At design time, when the use cases are understood but before building starts. It's in that special point in time that you can design for security. It takes time to do. The larger the piece of design work the more time you need to spend on it. And as we start to build, that's when you realise that more threat modelling needs to be done.

“… you probably want to find too many threats, rather than too few…”

Adam Shostack

https://adam.shostack.org/blog/2017/08/magical-approaches-to-threat-modeling/

Agile Threat Modelling - Changes in Time

DESIGN TIME

MODELLED TOO LATE

Threat modelling is generally done by security professionals. And they are usually invited to look at designs ... completed designs

TAKES TIME

TOO MUCH TIME

Doing threat modelling with a large part of a design leads to a large number of threats being found ... often too many to deal with

CHANGES IN TIME

INACCURATE MODELS

Upfront designs change as products evolve. If your threat modelling doesn't also evolve then you have nothing at all

IT'S ABOUT TIME: WHEN, AMOUNT & HOW OFTEN

At design time, when the use cases are understood but before building starts. It's in that special point in time that you can design for security. It takes time to do. The larger the piece of design work the more time you need to spend on it. And as we start to build, that's when you realise that more threat modelling needs to be done.

“All models are wrong, but some models are useful…”

George Box

https://en.wikipedia.org/wiki/All_models_are_wrong/

“… the question is, is the model good enough for this particular application?”

George Box

https://en.wikipedia.org/wiki/All_models_are_wrong/

Agile Threat Modelling - Requirements

DESIGN TIME

MODELLED TOO LATE

AS EARLY AS POSSIBLE

TAKES TIME

TOO MUCH TIME

USING THE TIME WE HAVE

CHANGES IN TIME

INACCURATE MODELS

GOOD ENOUGH MODEL

IT'S ABOUT TIME: WHEN, AMOUNT & HOW OFTEN

At design time, when the use cases are understood but before building starts. It's in that special point in time that you can design for security. It takes time to do. The larger the piece of design work the more time you need to spend on it. And as we start to build, that's when you realise that more threat modelling needs to be done.

Agile Threat Modelling - Requirements

DESIGN TIME

MODELLED TOO LATE

AS EARLY AS POSSIBLE

Story Scrubbing
or
Backlog Grooming

TAKES TIME

TOO MUCH TIME

USING THE TIME WE HAVE

This is timeboxed
combined
with NRF & acceptance

CHANGES IN TIME

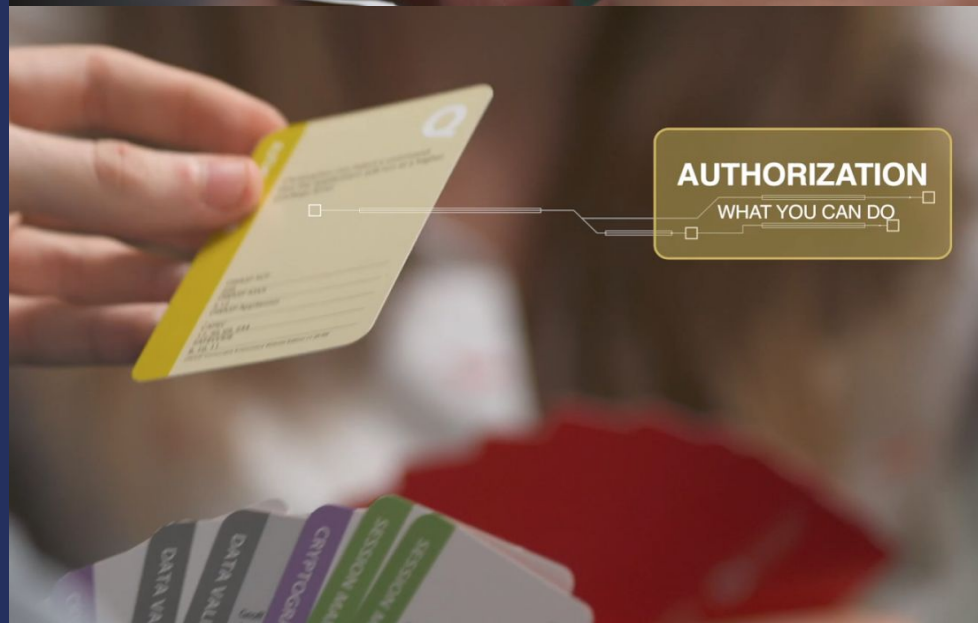
INACCURATE MODELS

GOOD ENOUGH MODEL

We stop
when we are just about
“close … enough”

Gamify threat modelling with Cornucopia and Elevation of Privilege

These two, popular threat modelling card games help to focus teams' thinking and educate on threat modelling concepts while playing. Our online platform for running Cornucopia and Elevation of Privilege card games remotely makes this available to all teams globally.



Gamification using OWASP Cornucopia

There are a couple of other gamification of Threat Modelling tools out there (for example the Microsoft / OWASP Elevation of Privilege that Adam designed) but there are (in my opinion) none quite as well designed for developers or as well connected as Cornucopia.

The game combines several excellent projects:

- OWASP ASVS
- OWASP SCP
- OWASP AppSensor
- SAFECODE / CAPEC

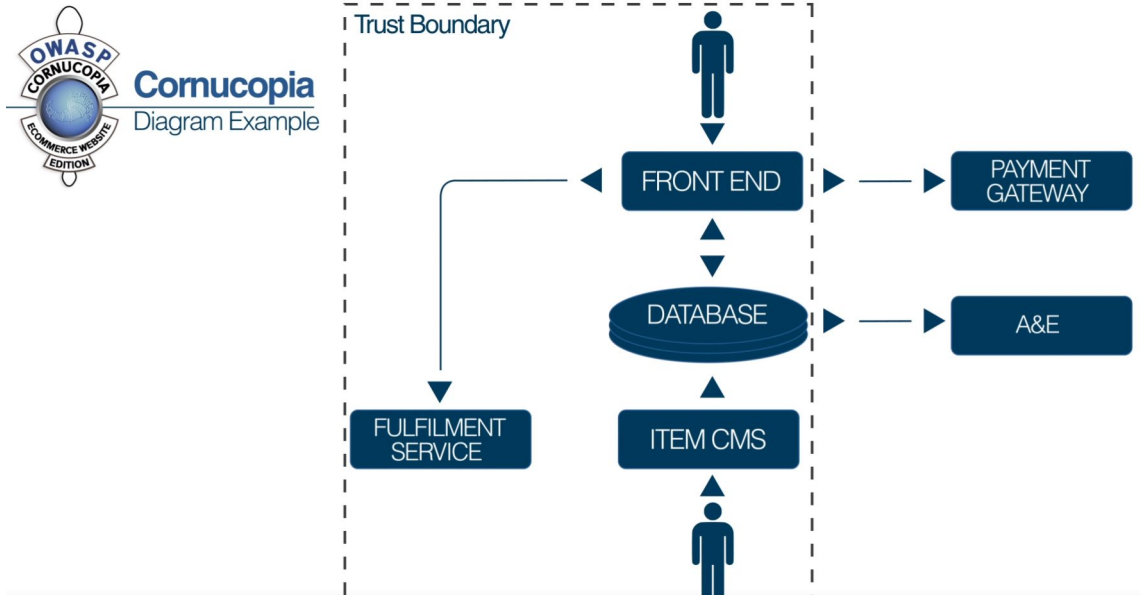
Cornucopia Inputs

Most importantly you need the people building the features to discuss the security impact on and of those features.

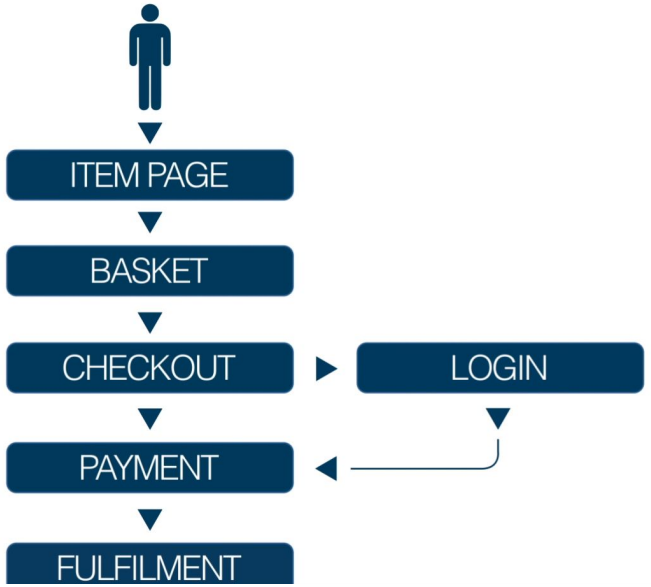
Diagrams that describe the functioning of the application, if available, otherwise draw just what you need. How data flows through that system provides insights into potential attacks.

Architectural designs are valuable to this process. They help us understand the systems in play. But again you can draw the parts involved as you discuss them.

Architectural Designs



Data Flow Diagrams

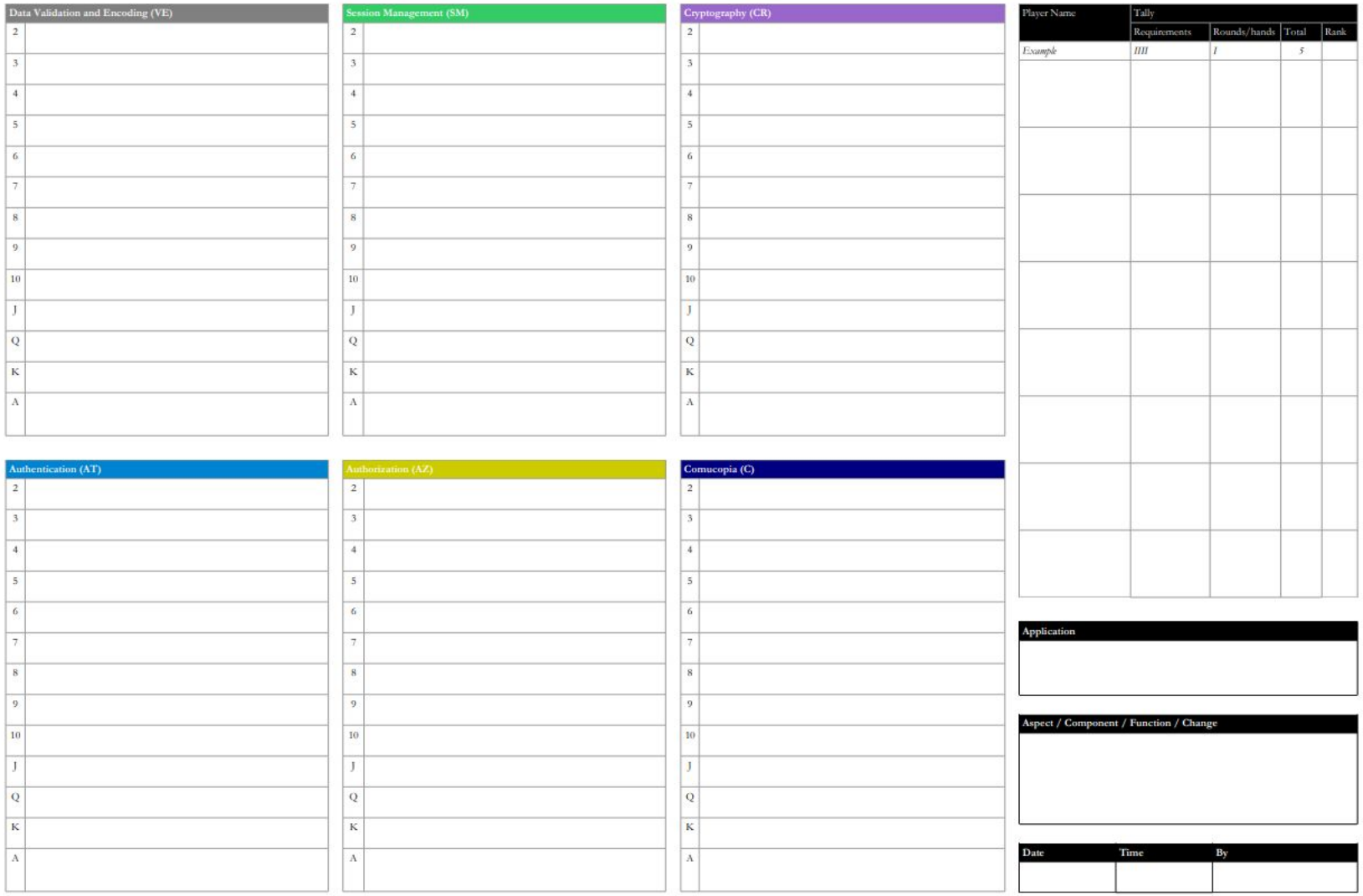


Cornucopia

Outputs

Agile Threat Modelling:

- Acceptance Criteria for Stories
- Security / story context
- Updated diagrams (perhaps)



Data Validation and Encoding (VE)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Session Management (SM)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Cryptography (CR)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Player Name	Tally			
	Requirements	Rounds/hands	Total	Rank
Example	*IIII*	*1*	*5*	

Authentication (AT)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Authorization (AZ)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Cornucopia (C)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Application

Aspect / Component / Function / Change

Date	Time	By

OWASP Cornucopia Score Sheet: https://wiki.owasp.org/images/6/69/Cornucopia-scoresheet.pdf

Cornucopia Outcomes

Additionally you will find that you see an improvement in general good practices like:

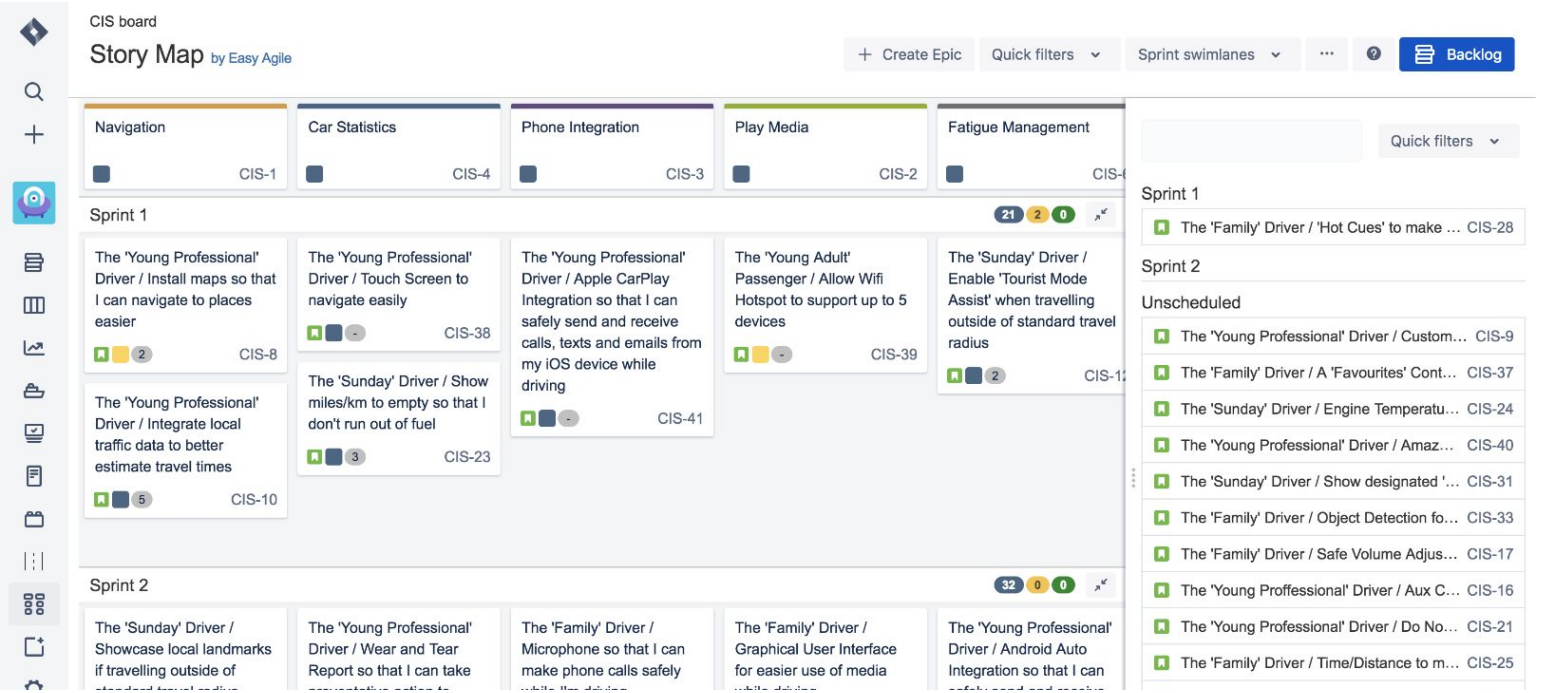
- More accurate design docs;
- Better knowledge sharing; and
- Less hidden tech-debt

Security:

User stories are created from the cards successfully played. Those stories lead to design features or investigations that secure the product when they are implemented.

Compliance:

Doing Threat Modelling is a requirement of many organisation, especially those following SAMM or that are regulated. While Security and Compliance are not the same thing they can be complementary.

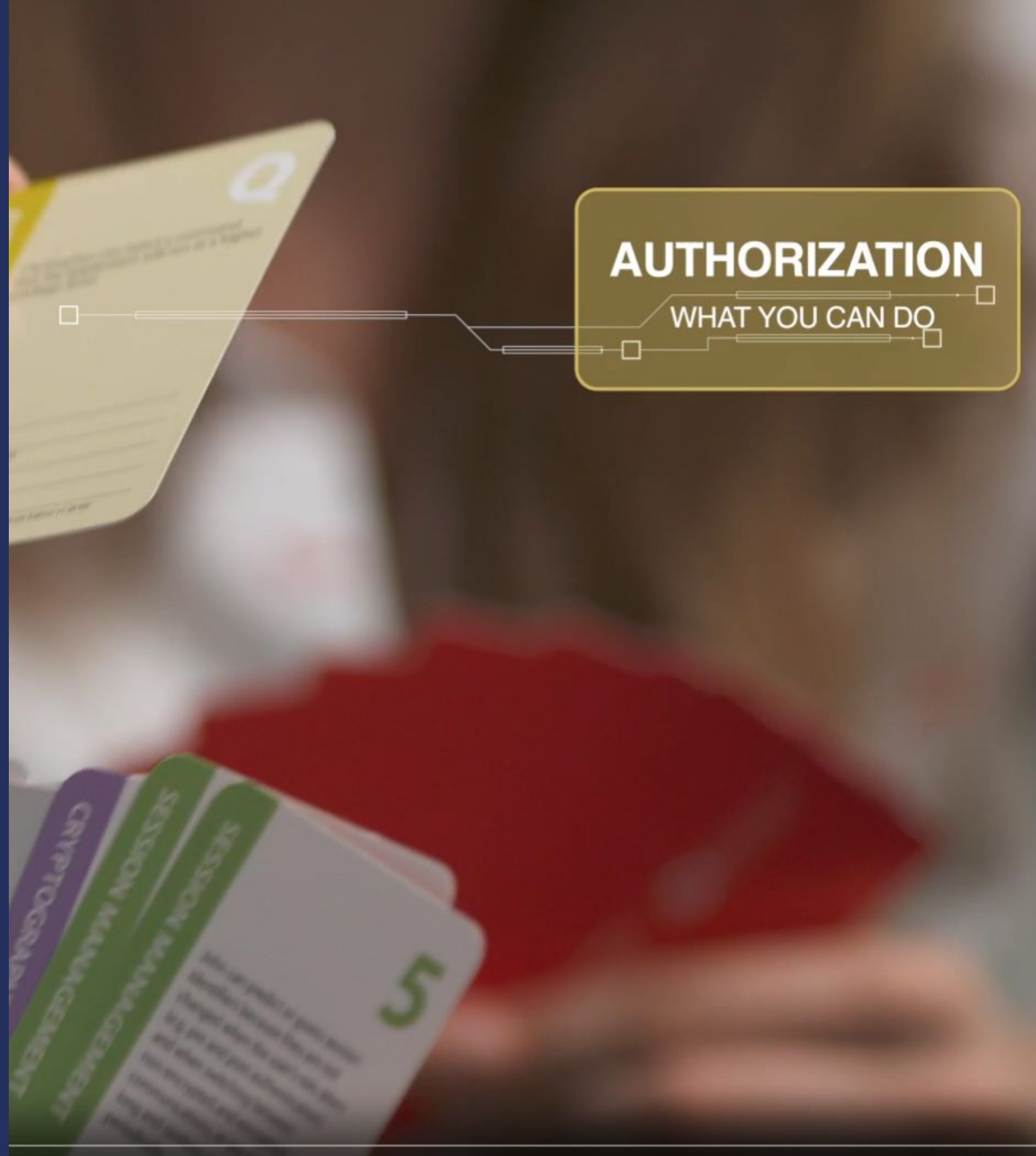


Authentication

(Identity)

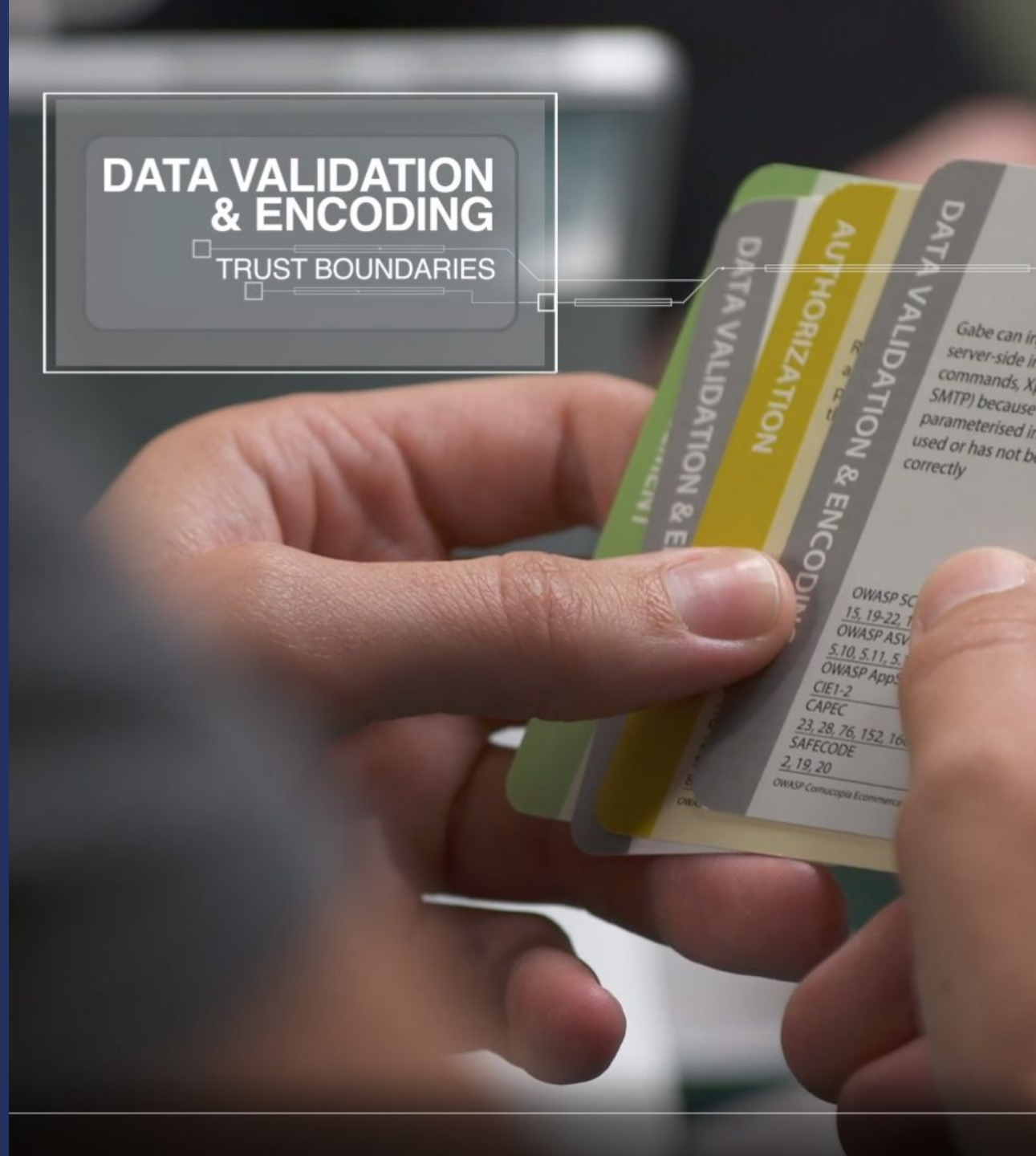
Authorisation

(Access Control)



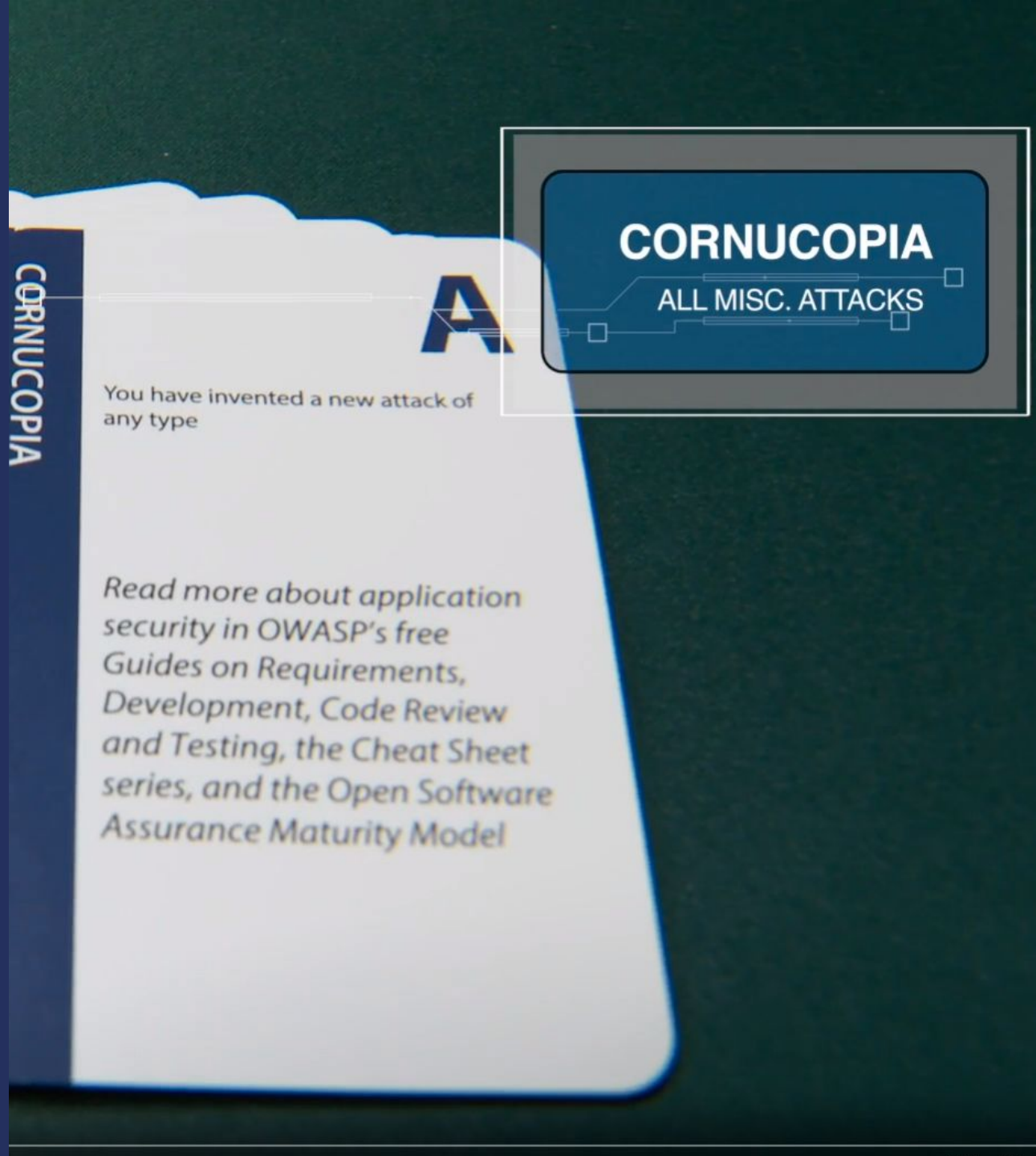
Session Management

Data Validation and Encoding



Cryptography

Cornucopia


CORNUCOPIA
ALL MISC. ATTACKS
CORNUCOPIA
A
You have invented a new attack of any type
Read more about application security in OWASP's free Guides on Requirements, Development, Code Review and Testing, the Cheat Sheet series, and the Open Software Assurance Maturity Model

How to play Cornucopia

The game is a simple one to play. Each of the suites consists of cards with faces from the standard deck: 2 through ten and Jack, Queen, King and Ace. Aces are high and each card describes an attack.

1

PRE-SORT

Sometimes you only want some cards from the deck

2

DEAL

All the cards, to all the players equally

3

PLAY

Look at the app, look at your hand. Select a card

4

DESCRIBE

Using the tools Cornucopia provides, describe the attack

5

CONVINCE

Your fellow players may not be convinced by your play

6

SCORE

1 point for a valid attack, 1 for the highest valid card played

7

FOLLOW SUIT

The next player follows the suit played originally

8

AWARD

Winner has the most points, there should be a prize

9

FOLLOW UP

Each valid item should be noted and added to the backlog

Video

Play-through

Where Has This Been Done?

RBI (Reed Business Information) is a division of RELX (Reed, Elsevier, Lexisnexis, and Reed eXhibitions) which is a FTSE #10 company who have customers in more than 198 countries and offices in about 50 cities, and employs over 15,000 people.

SCALE

15,000

Employees and 1,500 developers. Building products for 7 markets

COMPLEX

HARD PROBLEMS

Massive data sets, hugely time sensitive, critical in nature and requiring complex calculations.

REGULATED

FS-ISAC

Building software for banking puts RBI in the domain of the FS-ISAC (Financial Services Information Sharing and Analysis Center).

AGILE

rbi reed business information

MOVING FAST

Building software to meet the customer's ever growing requirements.

“… Cornucopia empowers … (engineers) to move fast more securely”

Jeff Jenkins
(CISO at Reed Business Information)

How Do You Make it Work?

Use the decks

Physical decks are awesome, table-top gaming is great when it is real. Not always doable but there are options.

Change up the game

Not all features hit all the five (six) areas. Use the parts that make sense for the features you are building. Not all features need you to work them through this. Not all features need threat modelling...

Use the systems you have available

We live in a world where gaming together may not be a thing for a while. It can still work.

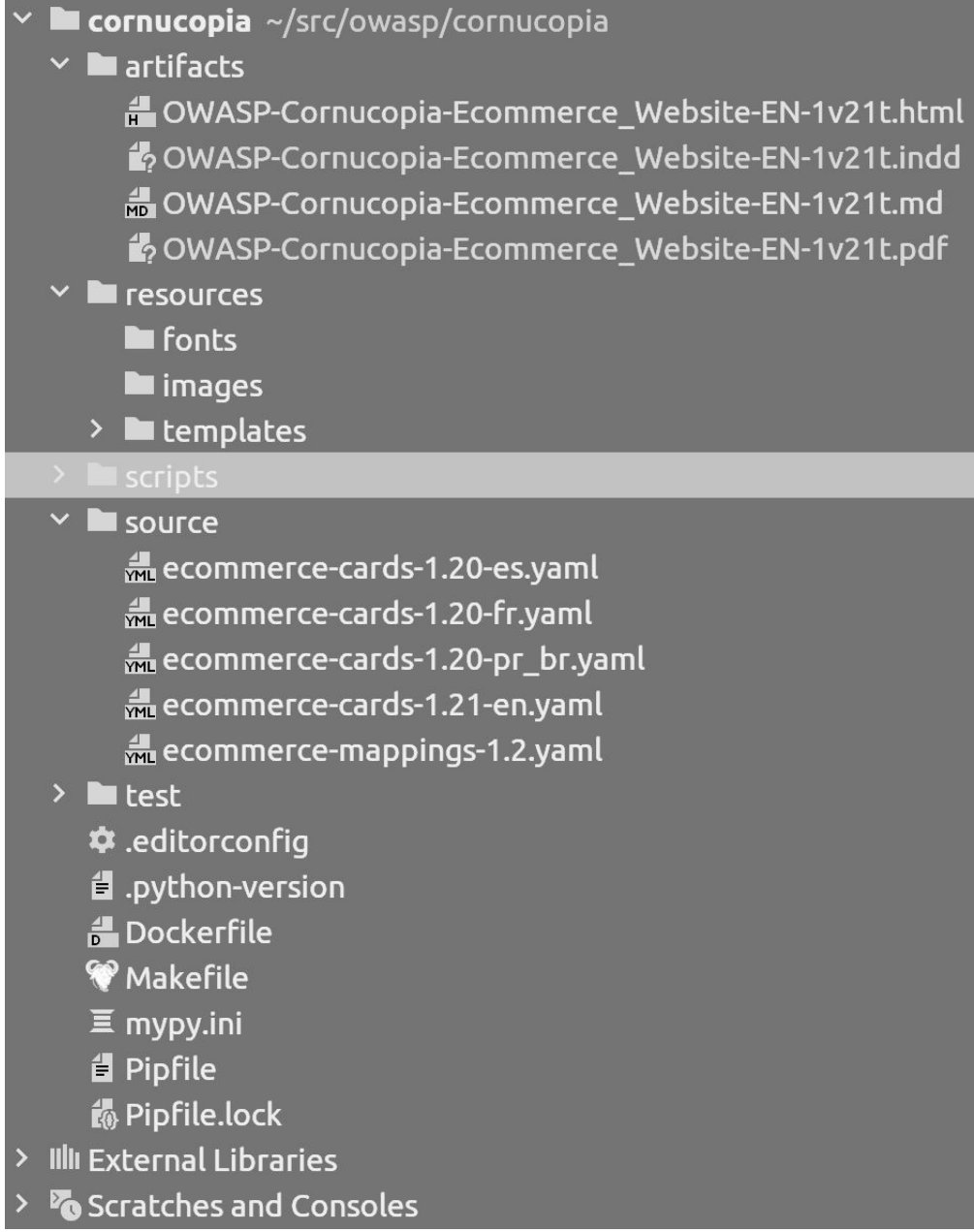
Project Milestones

Automated builds

We've moved from Microsoft Word to YAML and Python for building HTML and INDD (and Word)

Made an App

Physical table-top is awesome! But, we are distributed teams and need do this remotely

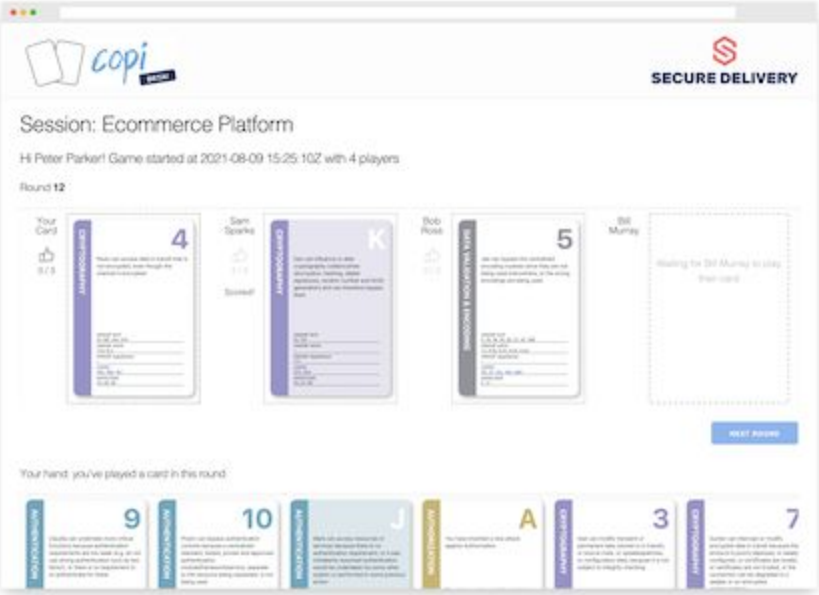


Project Next Steps

Improved content

More languages, updated mappings for things like ASVS, Logging Benchmark, etc.

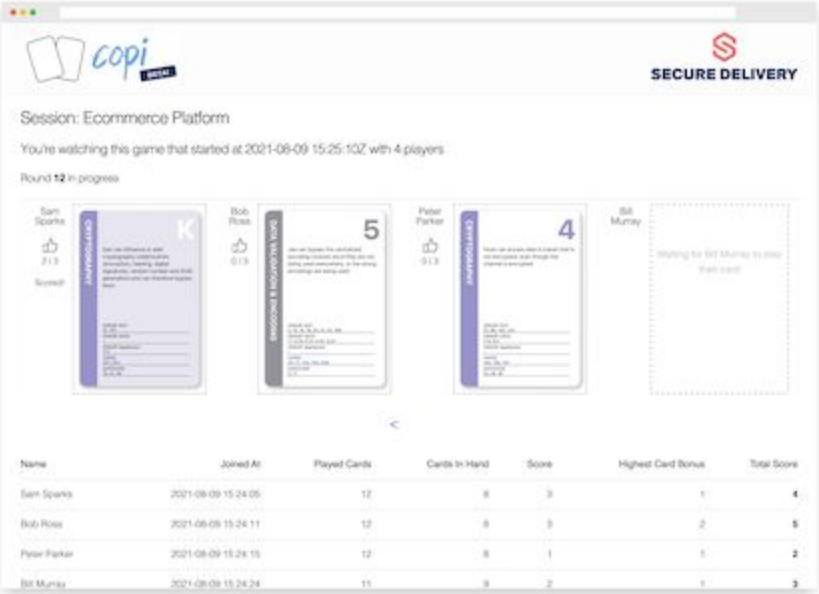
Project: https://owasp.org/www-project-cornucopia/
Repository: https://github.com/OWASP/cornucopia



Use Copi

Copi is free to use and completely tracker-free. It is beta however so use it and report anything you find to us.

Play: https://copi.securedelivery.io/
Issues: copi-support@securedelivery.io



SECURE DELIVERY

enquiries@securedelivery.io

Links

Executive Order 14028:
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standard-vendor-or-developer

OWASP Top 10 (2021):

https://owasp.org/Top10/A04_2021-Insecure_Design/

Threat Modelling in a Minute:

https://www.youtube.com/playlist?list=PLS_NHNPMyDedUq4CbnyaeoZFBYfoOxy3t

Video Playthrough: https://youtu.be/BZVoQurTEMc