



**Getting Serious About Security**

# Serious Games



- Enjoyable way to learn as a group
- Practice with instant feedback (or produce real work)
- Build trust/collaboration within the team
- Social permission for exploration / disagreement

# Agile App Security Game

## Pick a password

Don't reuse your bank password, we didn't spend a lot on security for this app.

At least 6 characters

Continue

**Purpose** Education/Practice

**Setup** <1 hour

**Runtime** 1-1.5 hours

**Group Size** 2-6 per team

**Fun** – ☆ ☆ ☆ ☆ ☆

**Creator** Charles Weir





You play a member of the agile dev team working on the “MoneyZoom” money management app.

The pilot version just went viral but because you’re so agile, all the security features were MVP (i.e. nonexistent).

You need to prioritize and implement security enhancements in the best order to minimize threats to you and your users.

- Over 4 rounds (aka 2 week sprints), you are given a set of story cards for security features you can implement for different costs, fitting within a fixed budget per sprint.
- For each sprint, the team discusses and agrees which stories to implement.
- At the end of each sprint, the teams get feedback on what hack attempts have occurred and which have been mitigated by features implemented.

# Setup & Tips

Download: <https://www.securedevelopment.org/resources/>

## Print & Cut Up:

- For each team -> 1 x Instructions, 1 x Playing Card Set

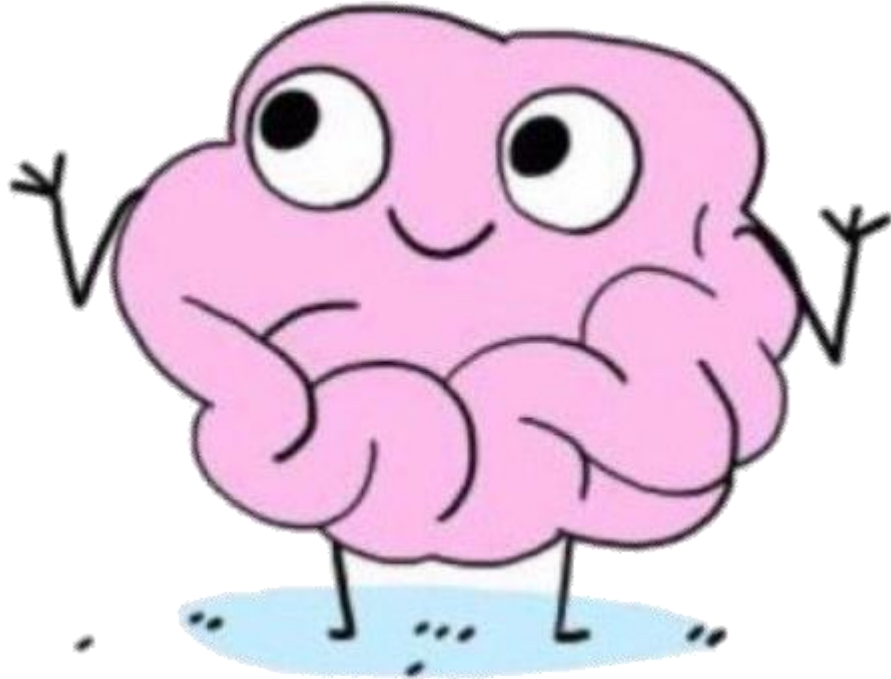
## Tips:

- Read both the leaders and players instructions thoroughly so you can facilitate smoothly, but also be willing to wing it
- The discussion is the main point, so allow extra time for discussion if required, and do a team debrief afterwards

# Social Engineering Game

**Hacker:** You owe the ATO  
\$500 in iTunes gift cards

**Brain:** Seems legit



**Purpose** Education/Awareness

**Setup** <1 hour

**Runtime** 1-1.5 hours

**Group Size** 2-12\*

**Fun** ☆ ☆ ☆ ☆

**Creator** Nixu Cybersecurity


The Social Engineering Game was created by Nixu Cybersecurity for practicing social engineering scenarios to help people to be more resistant and aware of social engineering attacks.



- The group splits up into pairs, then takes turns playing attacker and victim.
- The victim picks a random occupation and personality, then creates a fake social footprint of publicly available information about the imaginary victim.
- The attacker chooses an attacker role and mission, “investigates” the victim's social footprint, then they run through a simulated encounter.

Your role as a victim will be:

**CXO Assistant**



**nixu**

**Victim**


hACME 2.0



**nixu** 20

**Personality Trait: Ambitious**


- Bigger salary, new position, new job.
- Focus is on anything that would result in more power or money.
- "I always aim high"



**nixu**

**Personality Trait: Suspicious**

- Strangers can be malicious.
- Will reveal only the minimum necessary.
- Everyone is a stranger!
- "I don't know you"



**nixu**

**Personality Trait**

hACME 2.0



**nixu** 28

# Social Footprint – hACME 2.0

**(Do not reveal this to the attacker)**

Victim's role: \_\_\_\_\_

Victim's personalities: \_\_\_\_\_

1. Write down what kind of information can the attacker find about your character and your personalities collected.

LinkedIn: (for example: years of experience, current and previous positions, companies worked, voluntary work, courses, etc.)

---



---



---

Facebook: (for example: is there a family, popularity, expensive or cheap vacation trips, lifestyle, embarrassments, adventures, obsessions, etc.)

---



---



---

Your trash can contains: (for example: ready made food, ingredients, bills, pictures, fliers, etc.)

---



---



---

If you are followed for 24hs: (for example: your routine, early or late at work, what did you do after work, how late at home, etc.)

---



---




---

2. When the attacker is learning about the victim, you are not acting, just answer to his/her questions as if you are a browser or a camera.

3. When the attacker is ready to perform his/her attack, you start acting!

**Alias: "The Charismatic"**

Can make almost any story believable. Impossible not to like this person.



**nixu**

**Attacker**


hACME 2.0



**nixu** 11

**Your mission is:**

Collect information about a relevant client of hACME such as name of the client, contact person and other potentially valuable details.



**nixu**

**Attacker Mission**

hACME 2.0



**nixu** 06



# Social Engineering Game Setup & Tips

Download: <https://www.nixu.com/blog/free-social-engineering-playing-cards>

## Print & Cut Up:

- For each pair -> 1 x Instructions, 2 x Victim Sheets, 2 x Attacker Sheet
- For the group -> 1x Playing Card Set

## Tips:

- Read the instructions thoroughly so you can explain the game well.
- Acting / full on roleplaying is optional. Just roll with whatever people are comfortable with.

# Elevation of Privilege



**Purpose** Threat Modelling

**Setup** <1 hour

**Runtime** 1-2 hours

**Group Size** 3-6\*

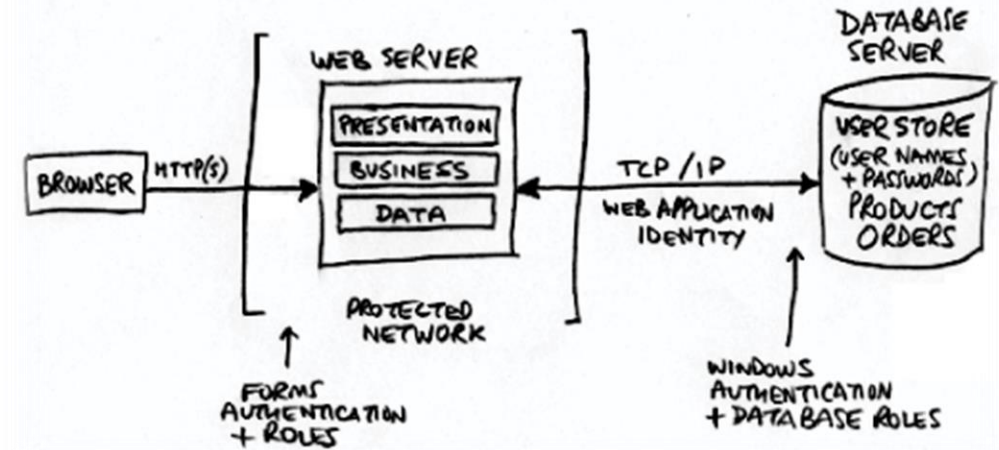
**Fun** ☆ ☆ ☆ ☆

**Creator** Adam Shostack

Threat	Desired Property
<b>Spoofing</b> - Impersonating something or someone else	Authenticity
<b>Tampering</b> - Modifying data or code	Integrity
<b>Repudiation</b> - Claiming not to have performed an action	Non-repudiability
<b>Information disclosure</b> - Exposing information to someone not authorized to see it	Confidentiality
<b>Denial of Service</b> - Denying or degrading service to users	Availability
<b>Elevation of Privilege</b> - Gain capabilities without proper authorization.	Authorization

+ Privacy

1. Draw a diagram of the system



2. Play:

- Deal out all the cards
- Play hands (once around the table)
- Connect the threat on a card to the diagram (if you can)
- Play in the same suit if you can, high card wins the hand
- Play once through the deck

# Elevation of Privilege Setup & Tips

Download: <https://github.com/adamshostack/eop/>

Buy: <https://agilestationery.co.uk/products/elevation-of-privilege-game>

Play Online: <https://www.google.com/search?q=play+elevation+of+privilege+online>

See Also: <https://martinfowler.com/articles/agile-threat-modelling.html>

## Tips:

- Ensure you have a clear, up to date diagram before starting
- Pre-filter the deck for cards that are totally irrelevant to your system (or don't)
- Record the best threats and add to your backlog (if you will actually fix them)
- Aces are for threats not listed on the cards, not a “win everything” card



# OWASP Juice Shop



**Purpose** Education/Practice

**Setup** 0-2 hours

**Runtime** 4+ hours

**Group Size** Unlimited

**Fun** – ☆ ☆ ☆ ☆ ☆

**Creator** Björn Kimminich

# Running on Docker

1. Install Docker
2. Run `docker pull bkimminich/juice-shop`
3. Run `docker run --rm -p 3000:3000 bkimminich/juice-shop`
4. Browse to `http://localhost:3000`

# Running on Heroku



Deploy to Heroku

# Running a “CTF” Competition

<https://pwning.owasp-juice.shop/part1/ctf.html>

<https://docs.ctfd.io/docs/deployment/>

```
npm install -g juice-shop-ctf-cli  
juice-shop-ctf
```

```
docker pull ctfd/ctfd:2.1.2
```

```
docker run --rm -p 8000:8000 ctfd/ctfd:2.1.2
```

```
# Browse to http://localhost:8000 and enter setup details
```

```
# Go to the section Admin > Config > Backup and Import from the zip generated earlier
```

```
docker run -d -e "CTF_KEY=xxx" -e "NODE_ENV=ctf" -p 3000:3000 bkimminich/juice-shop
```

# OWASP Juice Shop Links & Tips

Github: <https://github.com/bkimminich/juice-shop>

Manual: <https://bkimminich.gitbooks.io/pwning-owasp-juice-shop/content/>

See Also: <https://owasp.org/www-project-vulnerable-web-applications-directory/>

## Tips:

- Fun is directly correlated with hacking success, so ensure appropriate support/training so people don't totally flounder.
- Use a CTF server to make it a competition
- Deploy to Kubernetes if you have an existing cluster



# Incident Response Test



**Purpose** Test your processes

**Setup** 1+ hours

**Runtime** 1+ hours

**Group Size** Unlimited

**Fun** ☆ ☆ ☆ ☆ ☆



**Creator** You

```

class Program
{
    0 references
    static void Main(string[] args)
    {
        var random = new Random();

        while (true)
        {
            Console.WriteLine("Connecting to master host");
            Thread.Sleep((int)Math.Floor(500 + 1000 * random.NextDouble()));
            Console.WriteLine("Downloading instructions");
            Thread.Sleep((int)Math.Floor(500 + 1000 * random.NextDouble()));
            Console.WriteLine("Executing instructions:");
            var iterations = random.Next(2, 5);
            for(int i = 0; i < iterations; i++)
            {
                Thread.Sleep((int)Math.Floor(1000 + 5000 * random.NextDouble()));
                Console.WriteLine("$$$$$$");
            }
            Console.WriteLine("Wiping up");
            Thread.Sleep((int)Math.Floor(1000 + 5000 * random.NextDouble()));
            Console.WriteLine("Lurking for 30 seconds");
            Thread.Sleep(30000);
        }
    }
}

```

<input type="checkbox"/> Name ^	Date modified	Type	Size
 Bit.exe	5/02/2021 11:10 AM	Application	5 KB
 bit.log	9/03/2021 6:27 PM	Text Document	1 KB

```

bit.log - Notepad
File Edit Format View Help
Connecting to master host
Downloading instructions
Executing instructions:
$$$$$$
$$$$$$
$$$$$$
$$$$$$
Wiping up
Lurking for 30 seconds
Connecting to master host
Downloading instructions
Executing instructions:
$$$$$$

```


There is an instance of an executable called Bit.exe running on the test server.  
 File Path: C:\temp\Bit.exe (includes a bit.log file with it)  
 It seems to be doing some dodgy stuff.

# Incident Response Test Setup & Tips

## Setup:

- Review the surface area of your system and plan an “attack”, then just do it.

## Tips:

- Let your boss know before you do this! 
- Debrief afterwards and update (or create) incident response documentation
- Trade off **plausibility**, **impact** and **discoverability**. e.g. crypto-locking a prod system might be plausible but probably too much impact. But fake malware might not actually be discovered unless it has some impact.

**ANY QUESTIONS?**





CENTRAL  
COAST  
CODERS