Secure Software Development – SSD

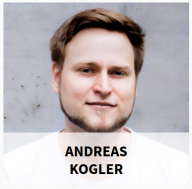
Organizational + Warmup Assignment

Kogler, Schrammel, Bachmann, Hennerbichler, Schumm

05.10.2022

Winter 2022/23, www.iaik.tugraz.at/ssd

- Lecturers:



- Teaching Assistants:

Ferdinand Bachmann, Lorenz Schumm, Tobias Hennerbichler

In this course you will learn ...

- This course is not about web security
- You learn about memory safety vulnerabilities
- You learn basic security techniques
- You need to deeply understand attacks in order to defend

- This course is not about web security
- You learn about memory safety vulnerabilities
- You learn basic security techniques
- You need to deeply understand attacks in order to defend

- This course is not about web security
- You learn about memory safety vulnerabilities
- You learn basic security techniques
- You need to deeply understand attacks in order to defend

- This course is not about web security
- You learn about memory safety vulnerabilities
- You learn basic security techniques
- You need to deeply understand attacks in order to defend


WHEN YOUR SECURITY GATE
IS A LADDER
imgflip.com

… how to defend

- You won't learn how to configure your webserver properly
- This course is (almost) not about crypto
- You learn defensive coding principles
- Our target is native code (e.g., C, C++)
- Why not Java, C#, Python??
  - Tons of legacy code written in C
  - Performance

… how to defend

- You won't learn how to configure your webserver properly
- This course is (almost) not about crypto
- You learn defensive coding principles
- Our target is native code (e.g., C, C++)
- Why not Java, C#, Python??
  - Tons of legacy code written in C
  - Performance

… how to defend

- You won't learn how to configure your webserver properly
- This course is (almost) not about crypto
- You learn defensive coding principles
- Our target is native code (e.g., C, C++)
- Why not Java, C#, Python??
  - Tons of legacy code written in C
  - Performance

- You won't learn how to configure your webserver properly
- This course is (almost) not about crypto
- You learn defensive coding principles
- Our target is native code (e.g., C, C++)
- Why not Java, C#, Python??
  - Tons of legacy code written in C
  - Performance

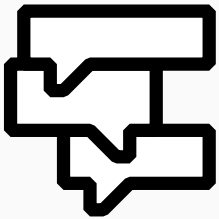
… how to defend

- You won't learn how to configure your webserver properly
- This course is (almost) not about crypto
- You learn defensive coding principles
- Our target is native code (e.g., C, C++)
- Why not Java, C#, Python??
  - Tons of legacy code written in C
  - Performance

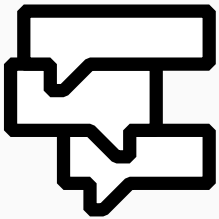
- You won't learn how to configure your webserver properly
- This course is (almost) not about crypto
- You learn defensive coding principles
- Our target is native code (e.g., C, C++)
- Why not Java, C#, Python??
  - Tons of legacy code written in C
  - Performance

- You won't learn how to configure your webserver properly
- This course is (almost) not about crypto
- You learn defensive coding principles
- Our target is native code (e.g., C, C++)
- Why not Java, C#, Python??
  - Tons of legacy code written in C
  - Performance

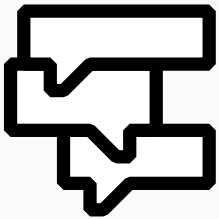
Organizational



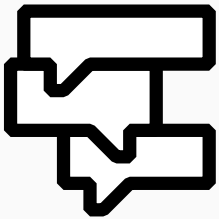
- Website: `https://www.iaik.tugraz.at/ssd`
- Discord: `https://discord.gg/cmPzndy6Xd`
  - Announcements and possible clarifications
  - Reading is mandatory!
  - Ask your own questions, especially if relevant for other students
  - Do not post any solutions!
- Email: `ssd@iaik.tugraz.at`



- Website: `https://www.iaik.tugraz.at/ssd`
- Discord: `https://discord.gg/cmPzndy6Xd`
  - Announcements and possible clarifications
  - Reading is mandatory!
  - Ask your own questions, especially if relevant for other students
  - Do not post any solutions!
- Email: `ssd@iaik.tugraz.at`



- Website: `https://www.iaik.tugraz.at/ssd`
- Discord: `https://discord.gg/cmPzndy6Xd`
  - Announcements and possible clarifications
  - Reading is mandatory!
  - Ask your own questions, especially if relevant for other students
  - Do not post any solutions!
- Email: `ssd@iaik.tugraz.at`



- Website: `https://www.iaik.tugraz.at/ssd`
- Discord: `https://discord.gg/cmPzndy6Xd`
  - Announcements and possible clarifications
  - Reading is mandatory!
  - Ask your own questions, especially if relevant for other students
  - Do not post any solutions!
- Email: `ssd@iaik.tugraz.at`

- Practical **assignments**
  - Group size = 1
  - Multiple weeks per assignment
- **tutorium** session / question hours
  - Not mandatory but highly recommended
- **Discord** channel for Q&A
  - Mandatory to read (announcements, clarifications ...)
- Final **oral exam**
  - Mandatory

- Practical **assignments**
  - Group size = 1
  - Multiple weeks per assignment
- **tutorium** session / question hours
  - Not mandatory but highly recommended
- **Discord** channel for Q&A
  - Mandatory to read (announcements, clarifications ...)
- Final **oral exam**
  - Mandatory

- Practical **assignments**
  - Group size = 1
  - Multiple weeks per assignment
- **tutorium** session / question hours
  - Not mandatory but highly recommended
- **Discord** channel for Q&A
  - Mandatory to read (announcements, clarifications ...)
- Final **oral exam**
  - Mandatory

- Practical **assignments**
  - Group size = 1
  - Multiple weeks per assignment
- **tutorium** session / question hours
  - Not mandatory but highly recommended
- **Discord** channel for Q&A
  - Mandatory to read (announcements, clarifications ...)
- Final **oral exam**
  - Mandatory

- Practical **assignments**
  - Group size = 1
  - Multiple weeks per assignment
- **tutorium** session / question hours
  - Not mandatory but highly recommended
- **Discord** channel for Q&A
  - Mandatory to read (announcements, clarifications ...)
- Final **oral exam**
  - Mandatory

- Practical **assignments**
  - Group size = 1
  - Multiple weeks per assignment
- **tutorium** session / question hours
  - Not mandatory but highly recommended
- **Discord** channel for Q&A
  - Mandatory to read (announcements, clarifications ...)
- Final **oral exam**
  - Mandatory

- Practical **assignments**
  - Group size = 1
  - Multiple weeks per assignment
- **tutorium** session / question hours
  - Not mandatory but highly recommended
- **Discord** channel for Q&A
  - Mandatory to read (announcements, clarifications ...)
- Final **oral exam**
  - Mandatory

- Practical **assignments**
  - Group size = 1
  - Multiple weeks per assignment
- **tutorium** session / question hours
  - Not mandatory but highly recommended
- **Discord** channel for Q&A
  - Mandatory to read (announcements, clarifications ...)
- Final **oral exam**
  - Mandatory

- Practical **assignments**
  - Group size = 1
  - Multiple weeks per assignment
- **tutorium** session / question hours
  - Not mandatory but highly recommended
- **Discord** channel for Q&A
  - Mandatory to read (announcements, clarifications ...)
- Final **oral exam**
  - Mandatory

How to get a grade?

- Solve first warmup assignment (mandatory)
- Solve other assignments to collect points
- Take the oral exam
- Your final mark consists of:
  - Points for each assignment
  - Optional bonus points (only count if you passed the course)
  - Oral exam (OE) in January
- Overall $Grade = sum(assignment + bonus) \cdot percentage(OE)$

How to get a grade?

- Solve first warmup assignment (mandatory)
- Solve other assignments to collect points
- Take the oral exam
- Your final mark consists of:
  - Points for each assignment
  - Optional bonus points (only count if you passed the course)
  - Oral exam (OE) in January
- Overall $Grade = sum(assignment + bonus) \cdot percentage(OE)$

How to get a grade?

- Solve first warmup assignment (mandatory)
- Solve other assignments to collect points
- Take the oral exam
- Your final mark consists of:
  - Points for each assignment
  - Optional bonus points (only count if you passed the course)
  - Oral exam (OE) in January
- Overall $Grade = sum(assignment + bonus) \cdot percentage(OE)$

How to get a grade?

- Solve first warmup assignment (mandatory)
- Solve other assignments to collect points
- Take the oral exam
- Your final mark consists of:
  - Points for each assignment
  - Optional bonus points (only count if you passed the course)
  - Oral exam (OE) in January
- Overall $Grade = sum(assignment + bonus) \cdot percentage(OE)$

How to get a grade?

- Solve first warmup assignment (mandatory)
- Solve other assignments to collect points
- Take the oral exam
- Your final mark consists of:
  - Points for each assignment
  - Optional bonus points (only count if you passed the course)
  - Oral exam (OE) in January
- Overall $Grade = sum(assignment + bonus) \cdot percentage(OE)$

How to get a grade?

- Solve first warmup assignment (mandatory)
- Solve other assignments to collect points
- Take the oral exam
- Your final mark consists of:
  - Points for each assignment
  - Optional bonus points (only count if you passed the course)
  - Oral exam (OE) in January
- Overall $Grade = sum(assignment + bonus) \cdot percentage(OE)$

How to get a grade?

- Solve first warmup assignment (mandatory)
- Solve other assignments to collect points
- Take the oral exam
- Your final mark consists of:
  - Points for each assignment
  - Optional bonus points (only count if you passed the course)
  - Oral exam (OE) in January
- Overall $Grade = sum(assignment + bonus) \cdot percentage(OE)$

How to get a grade?

- Solve first warmup assignment (mandatory)
- Solve other assignments to collect points
- Take the oral exam
- Your final mark consists of:
  - Points for each assignment
  - Optional bonus points (only count if you passed the course)
  - Oral exam (OE) in January
- Overall $Grade = sum(assignment + bonus) \cdot percentage(OE)$

$> 90\%$:	Sehr gut | Excellent (1)
78.5% - 90%:	Gut | Good (2)
67.5% - 78.49%:	Befriedigend | Average (3)
50% - 67.49%:	Genügend | Fair (4)
$< 50\%$:	Nicht Genügend | Poor (5)

Assignments

- Defenselets
  - Warmup: no points, but mandatory
  - Defenselets: 39%
- Defensive Programming
  - Defensive 1: 30%
  - Defensive 2: 31%

Assignments

- Defenselets
  - Warmup: no points, but mandatory
  - Defenselets: 39%
- Defensive Programming
  - Defensive 1: 30%
  - Defensive 2: 31%

Assignments

- Defenselets
  - Warmup: no points, but mandatory
  - Defenselets: 39%
- Defensive Programming
  - Defensive 1: 30%
  - Defensive 2: 31%

- Defenselets
  - Warmup: no points, but mandatory
  - Defenselets: 39%
- Defensive Programming
  - Defensive 1: 30%
  - Defensive 2: 31%

- Defenselets
  - Warmup: no points, but mandatory
  - Defenselets: 39%
- Defensive Programming
  - Defensive 1: 30%
  - Defensive 2: 31%

- Defenselets
  - Warmup: no points, but mandatory
  - Defenselets: 39%
- Defensive Programming
  - Defensive 1: 30%
  - Defensive 2: 31%

Oral exam

- Mandatory
- After all deadlines in January
- There will be multiple time slots
- You need to be able to:
  - Answer questions to each assignment and the tasks you fulfilled
  - Insufficient answers will yield to point deduction
  - Too few can even yield to a negative grade
  - More information will be given with each assignment

Oral exam

- Mandatory
- After all deadlines in January
- There will be multiple time slots
- You need to be able to:
  - Answer questions to each assignment and the tasks you fulfilled
  - Insufficient answers will yield to point deduction
  - Bad and non-existing answers will yield to a negative grade
  - More information will be given with each assignment

Oral exam

- Mandatory
- After all deadlines in January
- There will be multiple time slots
- You need to be able to:
  - Answer questions to each assignment and the tasks you fulfilled
  - Insufficient answers will yield to point deduction
  - Lack of knowledge will yield to a negative grade
  - More information will be given with each assignment

Oral exam

- Mandatory
- After all deadlines in January
- There will be multiple time slots
- You need to be able to:
  - Answer questions to each assignment and the tasks you fulfilled
  - Insufficient answers will yield to point deduction
    - and can even yield to a negative grade
  - More information will be given with each assignment

Oral exam

- Mandatory
- After all deadlines in January
- There will be multiple time slots
- You need to be able to:
  - Answer questions to each assignment and the tasks you fulfilled
  - Insufficient answers will yield to point deduction
    - and can even yield to a negative grade
  - More information will be given with each assignment

- Mandatory
- After all deadlines in January
- There will be multiple time slots
- You need to be able to:
  - Answer questions to each assignment and the tasks you fulfilled
  - Insufficient answers will yield to point deduction
    - and can even yield to a negative grade
  - More information will be given with each assignment

- Mandatory
- After all deadlines in January
- There will be multiple time slots
- You need to be able to:
  - Answer questions to each assignment and the tasks you fulfilled
  - Insufficient answers will yield to point deduction
    - and can even yield to a negative grade
  - More information will be given with each assignment

- Mandatory
- After all deadlines in January
- There will be multiple time slots
- You need to be able to:
  - Answer questions to each assignment and the tasks you fulfilled
  - Insufficient answers will yield to point deduction
    - and can even yield to a negative grade
  - More information will be given with each assignment

- No plagiarism will be tolerated!
- We check for plagiarism!
  - If we suspect plagiarism, affected students are questioned
  - All students involved in plagiarism will receive 0 points
  - At least one student: `Ungültig/Täuschung` with all its consequences

Plagiarism

- No plagiarism will be tolerated!
- We check for plagiarism!
  - If we suspect plagiarism, affected students are questioned
  - All students involved in plagiarism will receive 0 points
  - At least one student: `Ungültig/Täuschung` with all its consequences

Plagiarism

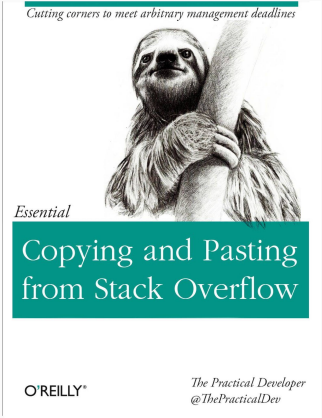
- No plagiarism will be tolerated!
- We check for plagiarism!
  - If we suspect plagiarism, affected students are questioned
  - All students involved in plagiarism will receive 0 points
  - At least one student: `Ungültig/Täuschung` with all its consequences

Plagiarism

- No plagiarism will be tolerated!
- We check for plagiarism!
  - If we suspect plagiarism, affected students are questioned
  - All students involved in plagiarism will receive 0 points
  - At least one student: `Ungültig/Täuschung` with all its consequences

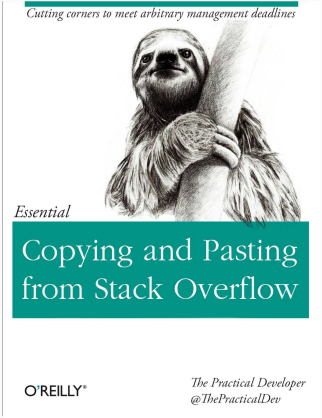
- No plagiarism will be tolerated!
- We check for plagiarism!
  - If we suspect plagiarism, affected students are questioned
  - All students involved in plagiarism will receive 0 points
  - At least one student: `Ungültig/Täuschung` with all its consequences

Plagiarism



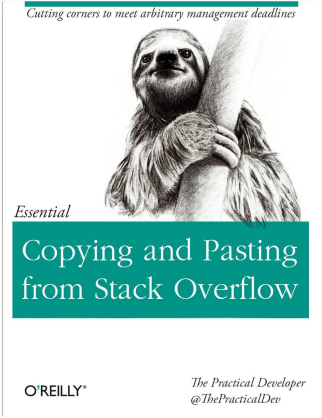
- No copying from the internet or other sources
- No sharing of source code / solutions with other students
- Protect your results from unintended access of others
- Discussions with other students are highly appreciated
- Exchange ideas, hints, pitfalls but no code snippets, solutions, etc.
- We want everyone to learn and understand for themselves

Plagiarism



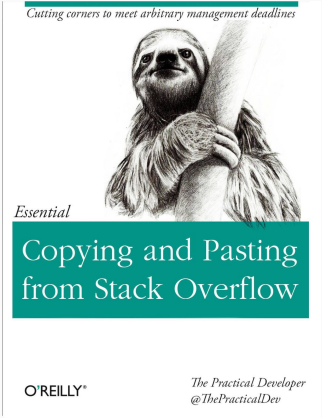
- No copying from the internet or other sources
- No sharing of source code / solutions with other students
- Protect your results from unintended access of others
- Discussions with other students are highly appreciated
- Exchange ideas, hints, pitfalls but no code snippets, solutions, etc.
- We want everyone to learn and understand for themselves

Plagiarism

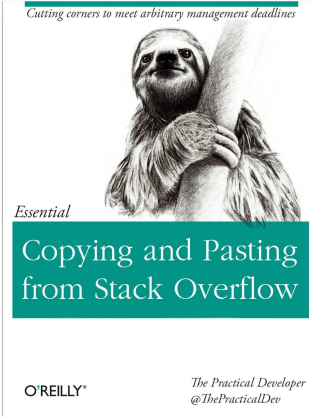


- No copying from the internet or other sources
- No sharing of source code / solutions with other students
- Protect your results from unintended access of others
- Discussions with other students are highly appreciated
- Exchange ideas, hints, pitfalls but no code snippets, solutions, etc.
- We want everyone to learn and understand for themselves

Plagiarism

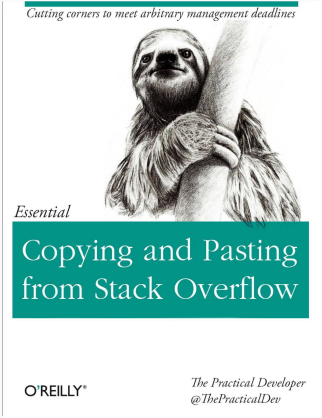


- No copying from the internet or other sources
- No sharing of source code / solutions with other students
- Protect your results from unintended access of others
- Discussions with other students are highly appreciated
- Exchange ideas, hints, pitfalls but no code snippets, solutions, etc.
- We want everyone to learn and understand for themselves



- No copying from the internet or other sources
- No sharing of source code / solutions with other students
- Protect your results from unintended access of others
- Discussions with other students are highly appreciated
- Exchange ideas, hints, pitfalls but no code snippets, solutions, etc.
- We want everyone to learn and understand for themselves

Plagiarism



- No copying from the internet or other sources
- No sharing of source code / solutions with other students
- Protect your results from unintended access of others
- Discussions with other students are highly appreciated
- Exchange ideas, hints, pitfalls but no code snippets, solutions, etc.
- We want everyone to learn and understand for themselves

Assignments

- Defenselets
  - Warmup: getting started (today)
  - Find, and fix (security) bugs
  - Prerequisites: x86 assembler basics; C/C++

Assignments

- Defenselets
  - Warmup: getting started (today)
  - Find, and fix (security) bugs
  - Prerequisites: x86 assembler basics; C/C++

Assignments

- Defenselets
  - Warmup: getting started (today)
  - Find, and fix (security) bugs
  - Prerequisites: x86 assembler basics; C/C++

- Defenselets
  - Warmup: getting started (today)
  - Find, and fix (security) bugs
  - Prerequisites: x86 assembler basics; C/C++

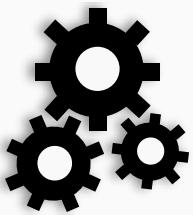
- Defensive Programming
  - Develop a secure application
  - Learn to avoid mistakes and code defensively
  - More details when the exercise is handed out

- Defensive Programming
  - Develop a secure application
  - Learn to avoid mistakes and code defensively
  - More details when the exercise is handed out

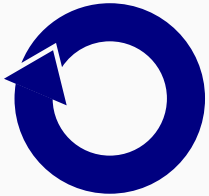
- Defensive Programming
  - Develop a secure application
  - Learn to avoid mistakes and code defensively
  - More details when the exercise is handed out

- Defensive Programming
  - Develop a secure application
  - Learn to avoid mistakes and code defensively
  - More details when the exercise is handed out

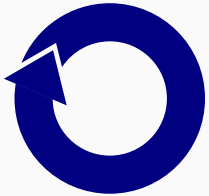
Tooling



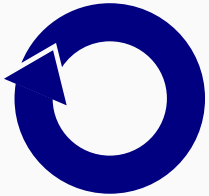
- Git repository
- Docker image
- Test system with scoreboard



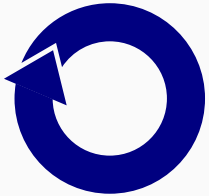
- Every student gets access to a personal git repository
  - An e-mail will be sent out the next days
- Git Upstream Repository
  - Necessary files (defenselets, source code, etc.) for every assignment will be published here
  - Including patches, fixes or other updates
  - You need to pull those changes into your repository
  - `https://extgit.iaik.tugraz.at/sase/practicals/2022/exercise2022-upstream.git`



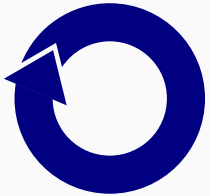
- Every student gets access to a personal git repository
  - An e-mail will be sent out the next days
- Git Upstream Repository
  - Necessary files (defenselets, source code, etc.) for every assignment will be published here
  - Including patches, fixes or other updates
  - You need to pull those changes into your repository
  - `https://extgit.iaik.tugraz.at/sase/practicals/2022/exercise2022-upstream.git`



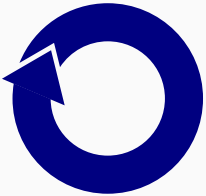
- Every student gets access to a personal git repository
  - An e-mail will be sent out the next days
- Git Upstream Repository
  - Necessary files (defenselets, source code, etc.) for every assignment will be published here
  - Including patches, fixes or other updates
  - You need to pull those changes into your repository
  - `https://extgit.iaik.tugraz.at/sase/practicals/2022/exercise2022-upstream.git`



- Every student gets access to a personal git repository
  - An e-mail will be sent out the next days
- Git Upstream Repository
  - Necessary files (defenselets, source code, etc.) for every assignment will be published here
  - Including patches, fixes or other updates
  - You need to pull those changes into your repository
  - `https://extgit.iaik.tugraz.at/sase/practicals/2022/exercise2022-upstream.git`

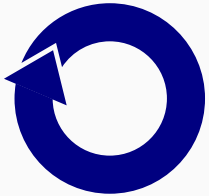


- Every student gets access to a personal git repository
  - An e-mail will be sent out the next days
- Git Upstream Repository
  - Necessary files (defenselets, source code, etc.) for every assignment will be published here
  - Including patches, fixes or other updates
  - You need to pull those changes into your repository
  - `https://extgit.iaik.tugraz.at/sase/practicals/2022/exercise2022-upstream.git`



- Every student gets access to a personal git repository
  - An e-mail will be sent out the next days
- Git Upstream Repository
  - Necessary files (defenselets, source code, etc.) for every assignment will be published here
  - Including patches, fixes or other updates
  - You need to pull those changes into your repository
  - `https://extgit.iaik.tugraz.at/sase/practicals/2022/exercise2022-upstream.git`

Git Upstream



- Every student gets access to a personal git repository
  - An e-mail will be sent out the next days
- Git Upstream Repository
  - Necessary files (defenselets, source code, etc.) for every assignment will be published here
  - Including patches, fixes or other updates
  - You need to pull those changes into your repository
  - `https://extgit.iaik.tugraz.at/sase/practicals/2022/exercise2022-upstream.git`

- Final submission for each assignment must be git-tagged
  - Missing or incorrect tag results in 0 points for the assignment
- The tag label starts with the assignment name, followed by a dash and a number, e.g., `warmup-1`, `defenselets-17`, `defensive1-42`, `defensive2-123`
- You can always update your final submission by increasing the number
- The tag with the highest number before the deadline counts

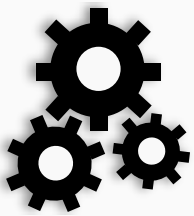
Git Tags

- Final submission for each assignment must be git-tagged
  - Missing or incorrect tag results in 0 points for the assignment
- The tag label starts with the assignment name, followed by a dash and a number, e.g., `warmup-1`, `defenselets-17`, `defensive1-42`, `defensive2-123`
- You can always update your final submission by increasing the number
- The tag with the highest number before the deadline counts

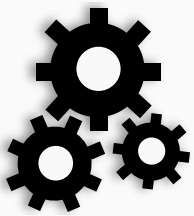
- Final submission for each assignment must be git-tagged
  - Missing or incorrect tag results in 0 points for the assignment
- The tag label starts with the assignment name, followed by a dash and a number, e.g., `warmup-1`, `defenselets-17`, `defensive1-42`, `defensive2-123`
- You can always update your final submission by increasing the number
- The tag with the highest number before the deadline counts

- Final submission for each assignment must be git-tagged
  - Missing or incorrect tag results in 0 points for the assignment
- The tag label starts with the assignment name, followed by a dash and a number, e.g., `warmup-1`, `defenselets-17`, `defensive1-42`, `defensive2-123`
- You can always update your final submission by increasing the number
- The tag with the highest number before the deadline counts

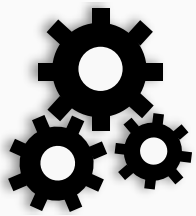
- Final submission for each assignment must be git-tagged
  - Missing or incorrect tag results in 0 points for the assignment
- The tag label starts with the assignment name, followed by a dash and a number, e.g., `warmup-1`, `defenselets-17`, `defensive1-42`, `defensive2-123`
- You can always update your final submission by increasing the number
- The tag with the highest number before the deadline counts



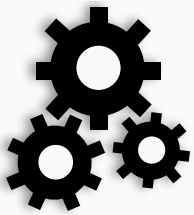
- We prepared a Docker image
  - Based on Ubuntu
  - Pre-installed tools, compilers
  - Script will be added to the git upstream repository
- Technically, you don't need to use it, but your submission will be tested on it.



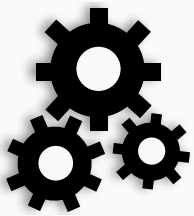
- We prepared a Docker image
  - Based on Ubuntu
  - Pre-installed tools, compilers
  - Script will be added to the git upstream repository
- Technically, you don't need to use it, but your submission will be tested on it.



- We prepared a Docker image
  - Based on Ubuntu
  - Pre-installed tools, compilers
  - Script will be added to the git upstream repository
- Technically, you don't need to use it, but your submission will be tested on it.



- We prepared a Docker image
  - Based on Ubuntu
  - Pre-installed tools, compilers
  - Script will be added to the git upstream repository
- Technically, you don't need to use it, but your submission will be tested on it.



- We prepared a Docker image
  - Based on Ubuntu
  - Pre-installed tools, compilers
  - Script will be added to the git upstream repository
- Technically, you don't need to use it, but your submission will be tested on it.

Test system

- All your submissions will be tested with our test system
  - Thus, you need to respect and meet file naming constraints of the assignments
    - Don't worry, it's not much.
- You will receive binary feedback for each task group that you submit
  - If you solve the defenselet
  - If your project compiles
  - If your implementation behaves correctly
- You won't get any output log.

- All your submissions will be tested with our test system
  - Thus, you need to respect and meet file naming constraints of the assignments
    - Don't worry, it's not much.
- You will receive binary feedback for each task group that you submit
  - If you solve the defenselet
  - If your project compiles
  - If your implementation behaves correctly
- You won't get any output log.

- All your submissions will be tested with our test system
  - Thus, you need to respect and meet file naming constraints of the assignments
    - Don't worry, it's not much.
- You will receive binary feedback for each task group that you submit
  - If you solve the defenselet
  - If your project compiles
  - If your implementation behaves correctly
- You won't get any output log.

- All your submissions will be tested with our test system
  - Thus, you need to respect and meet file naming constraints of the assignments
    - Don't worry, it's not much.
- You will receive binary feedback for each task group that you submit
  - If you solve the defenselet
  - If your project compiles
  - If your implementation behaves correctly
- You won't get any output log.

- All your submissions will be tested with our test system
  - Thus, you need to respect and meet file naming constraints of the assignments
    - Don't worry, it's not much.
- You will receive binary feedback for each task group that you submit
  - If you solve the defenselet
  - If your project compiles
  - If your implementation behaves correctly
- You won't get any output log.

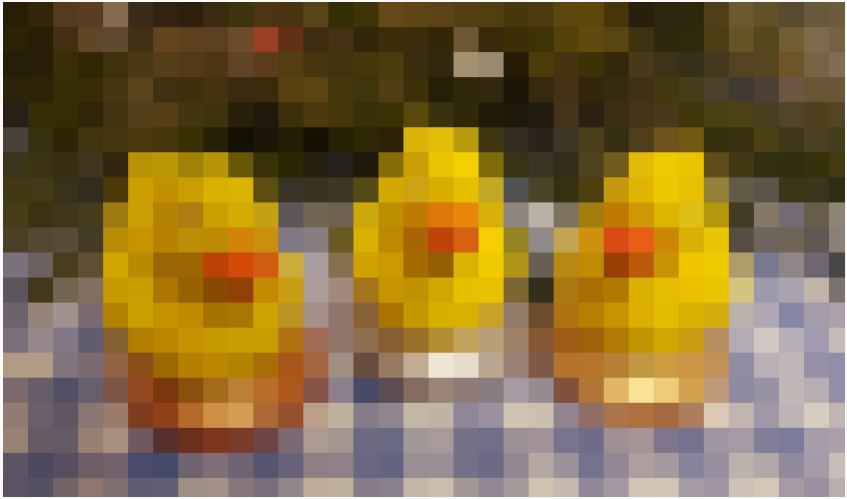
- All your submissions will be tested with our test system
  - Thus, you need to respect and meet file naming constraints of the assignments
    - Don’t worry, it’s not much.
- You will receive binary feedback for each task group that you submit
  - If you solve the defenselet
  - If your project compiles
  - If your implementation behaves correctly
- You won’t get any output log.

- All your submissions will be tested with our test system
  - Thus, you need to respect and meet file naming constraints of the assignments
    - Don’t worry, it’s not much.
- You will receive binary feedback for each task group that you submit
  - If you solve the defenselet
  - If your project compiles
  - If your implementation behaves correctly
- You won’t get any output log.

- All your submissions will be tested with our test system
  - Thus, you need to respect and meet file naming constraints of the assignments
    - Don’t worry, it’s not much.
- You will receive binary feedback for each task group that you submit
  - If you solve the defenselet
  - If your project compiles
  - If your implementation behaves correctly
- You won’t get any output log.

Rank	Group	Angr Management	Calculator	Callcenter	Card game	Combined	EchoService	Guess a Number	Heap Magic	My first ROP chain	PinGen	PredictMe	Reveal the secret	cmacro	cryptomaster	fast_math	nice_sequences	pgnuinverter	pluginsystem	rust	terminator	turing_completeness	Score	Date	Commit
1	group11	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	113.64%	2019-11-18 09:02:23 UTC+0000	894735f1013a2fad091ba164058f1588a267e7fb
2	group24	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	113.64%	2019-11-18 09:41:45 UTC+0000	3b57f8f5e72ecba469db742d2a27ca1e99096585
3	group63	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	113.64%	2019-11-18 08:08:01 UTC+0000	685d44b58416f22b785fc57d62456b109c09c659
4	group07	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	104.55%	2019-11-18 08:49:45 UTC+0000	27d591a6210747340 3ecedf6661f61231b78caac
5	group20	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	104.55%	2019-11-18 09:30:28 UTC+0000	be8a62615dceabce9b89bc85366b51d55a84f789
6	group23	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	104.55%	2019-11-18 09:37:52 UTC+0000	4ac448f71c2854937bdf9b19e6eb55fb4cc8d2a7
7	group26	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	104.55%	2019-11-18 09:47:20 UTC+0000	1c938337db5dfb3efc02cd6f8b53dbf3a878bf72
8	group69	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	104.55%	2019-11-18 08:24:49 UTC+0000	bcd923cd330d78d82e31eb761f2284004a07f7f6
9	group02	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 08:36:26 UTC+0000	c9f31f9c8c260c879a67bddf78ab8968d27f15a6
10	group08	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 08:51:39 UTC+0000	2ffe16ce753faa882460ab01198a781f270963c8
11	group14	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 09:04:21 UTC+0000	396038c0e7486384fceeef2789f007fa64f05f77
12	group15	✔	✔	✔	✔	✔	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 09:09:24 UTC+0000	b223b6a8885a61cdfee3ad68c075278a10c5a95d
13	group18	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 09:29:38 UTC+0000	8604e5cdcfef8b794770041895805da7bc36b287
14	group22	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 09:34:15 UTC+0000	b293b8a7b49b654be7ca49bbaf8f233ae5f86e1a
15	group29	✔	✔	✔	✔	✔	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 09:55:50 UTC+0000	0ed2ee85bb64d9283d39b28a7bda07e85a016fe1
16	group36	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 10:15:10 UTC+0000	f4d5e574536937693f04dc3e07058fe7bd423b29
17	group37	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 10:16:48 UTC+0000	f126157d2420bc0c62fb8c2fb31d92d46af9613c
18	group42	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 09:20:04 UTC+0000	9392ff556a97c99c53db39d07194083b594ab6cc
19	group49	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 10:46:06 UTC+0000	f140390cec993d31cd30f312537d2e260e6f68cb
20	group50	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 10:50:03 UTC+0000	0c2f8f1b01451ab17627c8eb44b729f57fd909f0
21	group52	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 10:51:40 UTC+0000	d155686983985829c3f358f17bd01472db6c5d5e
22	group53	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 10:52:53 UTC+0000	2539f629ab544b789bb1adc1172cd434bc7ca2a4
23	group71	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	100.00%	2019-11-18 08:28:41 UTC+0000	e23a008cc6dc3b7defb54907aa71c21675c1c2cf
24	group09	✘	✔	✔	✔	✔	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	95.45%	2019-11-18 08:54:22 UTC+0000	50d7bb4cbfba44ca2f8bb82d4009c37f3913c99e
25	group27	✘	✔	✔	✔	✔	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	95.45%	2019-11-18 09:47:12 UTC+0000	6e1e2fa6237a1601e3a0b3b6f94e575d1ab0230b
26	group30	✘	✔	✔	✔	✔	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	95.45%	2019-11-18 09:56:11 UTC+0000	ea6f82901aec52ee3fd1ef74dffd89c573c21c50

Awards



Warmup

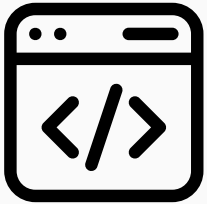
Assignment 0

- We prepared a warmup defenselet for you to explore and exploit
  - A defenselet contains one or multiple bugs
  - Find the bugs and fix them
  - In some cases: provide the input that triggered the bug

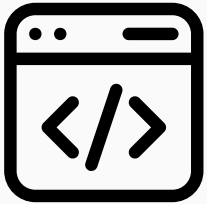
- We prepared a warmup defenselet for you to explore and exploit
  - A defenselet contains one or multiple bugs
  - Find the bugs and fix them
  - In some cases: provide the input that triggered the bug

- We prepared a warmup defenselet for you to explore and exploit
  - A defenselet contains one or multiple bugs
  - Find the bugs and fix them
  - In some cases: provide the input that triggered the bug

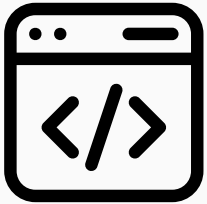
- We prepared a warmup defenselet for you to explore and exploit
  - A defenselet contains one or multiple bugs
  - Find the bugs and fix them
  - In some cases: provide the input that triggered the bug



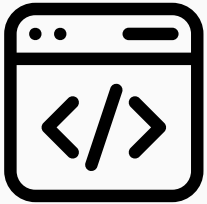
- Analyze the source code (if available) and find the bug
- You can use tools to make the bug search easier (see tutorials)
- However, your fixed defenselet must be supported by the reference image
- Many tools and libraries are pre-installed



- Analyze the source code (if available) and find the bug
- You can use tools to make the bug search easier (see tutorials)
- However, your fixed defenselet must be supported by the reference image
- Many tools and libraries are pre-installed



- Analyze the source code (if available) and find the bug
- You can use tools to make the bug search easier (see tutorials)
- However, your fixed defenselet must be supported by the reference image
- Many tools and libraries are pre-installed



- Analyze the source code (if available) and find the bug
- You can use tools to make the bug search easier (see tutorials)
- However, your fixed defenselet must be supported by the reference image
- Many tools and libraries are pre-installed

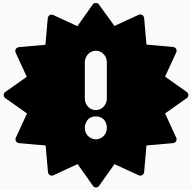
- Our test system will automatically test your defenselet
- It will parse the output and the additional tooling information
  - Success, if the bug is fixed
  - Failure, otherwise

- Our test system will automatically test your defenselet
- It will parse the output and the additional tooling information
  - Success, if the bug is fixed
  - Failure, otherwise

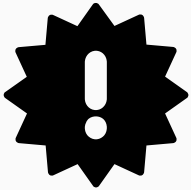
- Our test system will automatically test your defenselet
- It will parse the output and the additional tooling information
  - Success, if the bug is fixed
  - Failure, otherwise

- Our test system will automatically test your defenselet
- It will parse the output and the additional tooling information
  - Success, if the bug is fixed
  - Failure, otherwise

Deadlines



- Warmup:
  - **Deadline:** 19th of October 23:59 (19.10.2022)
  - **Tag:** `warmup`
- Defenselets:
  - **Deadline:** tba at handout
  - **Tag:** `defenselets`
- Defensive Programming 1:
  - **Deadline:** tba at handout
  - **Tag:** `defensive1`
- Defensive Programming 2:
  - **Deadline:** tba at handout
  - **Tag:** `defensive2`



- Warmup:

  Deadline: 19th of October 23:59 (19.10.2022)

  Tag: `warmup`

- Defenselets:

  Deadline: tba at handout

  Tag: `defenselets`

- Defensive Programming 1:

  Deadline: tba at handout

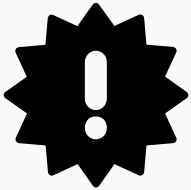
  Tag: `defensive1`

- Defensive Programming 2:

  Deadline: tba at handout

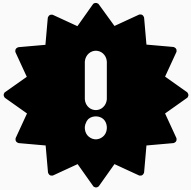
  Tag: `defensive2`

Deadlines



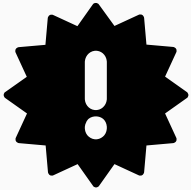
- Warmup:
  - **Deadline:** 19th of October 23:59 (19.10.2022)
  - **Tag:** `warmup`
- Defenselets:
  - **Deadline:** tba at handout
  - **Tag:** `defenselets`
- Defensive Programming 1:
  - **Deadline:** tba at handout
  - **Tag:** `defensive1`
- Defensive Programming 2:
  - **Deadline:** tba at handout
  - **Tag:** `defensive2`

Deadlines



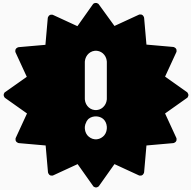
- Warmup:
  - **Deadline:** 19th of October 23:59 (19.10.2022)
  - **Tag:** `warmup`
- Defenselets:
  - **Deadline:** tba at handout
  - **Tag:** `defenselets`
- Defensive Programming 1:
  - **Deadline:** tba at handout
  - **Tag:** `defensive1`
- Defensive Programming 2:
  - **Deadline:** tba at handout
  - **Tag:** `defensive2`

Deadlines

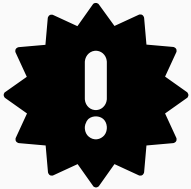


- Warmup:
  - **Deadline:** 19th of October 23:59 (19.10.2022)
  - **Tag:** `warmup`
- Defenselets:
  - **Deadline:** tba at handout
  - **Tag:** `defenselets`
- Defensive Programming 1:
  - **Deadline:** tba at handout
  - **Tag:** `defensive1`
- Defensive Programming 2:
  - **Deadline:** tba at handout
  - **Tag:** `defensive2`

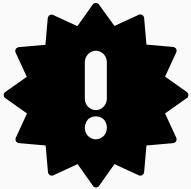
Deadlines



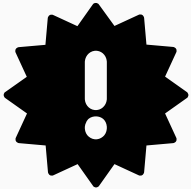
- Warmup:
  - **Deadline:** 19th of October 23:59 (19.10.2022)
  - **Tag:** `warmup`
- Defenselets:
  - **Deadline:** tba at handout
  - **Tag:** `defenselets`
- Defensive Programming 1:
  - **Deadline:** tba at handout
  - **Tag:** `defensive1`
- Defensive Programming 2:
  - **Deadline:** tba at handout
  - **Tag:** `defensive2`



- Warmup:
  - **Deadline:** 19th of October 23:59 (19.10.2022)
  - **Tag:** `warmup`
- Defenselets:
  - **Deadline:** tba at handout
  - **Tag:** `defenselets`
- Defensive Programming 1:
  - **Deadline:** tba at handout
  - **Tag:** `defensive1`
- Defensive Programming 2:
  - **Deadline:** tba at handout
  - **Tag:** `defensive2`

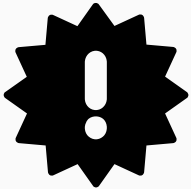


- Warmup:
  - **Deadline:** 19th of October 23:59 (19.10.2022)
  - **Tag:** `warmup`
- Defenselets:
  - **Deadline:** tba at handout
  - **Tag:** `defenselets`
- Defensive Programming 1:
  - **Deadline:** tba at handout
  - **Tag:** `defensive1`
- Defensive Programming 2:
  - **Deadline:** tba at handout
  - **Tag:** `defensive2`

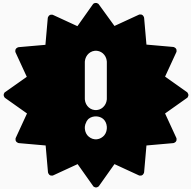


- Warmup:
  - **Deadline:** 19th of October 23:59 (19.10.2022)
  - **Tag:** `warmup`
- Defenselets:
  - **Deadline:** tba at handout
  - **Tag:** `defenselets`
- Defensive Programming 1:
  - **Deadline:** tba at handout
  - **Tag:** `defensive1`
- Defensive Programming 2:
  - **Deadline:** tba at handout
  - **Tag:** `defensive2`

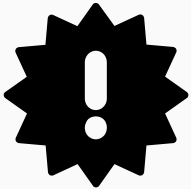
Deadlines



- Warmup:
  - **Deadline:** 19th of October 23:59 (19.10.2022)
  - **Tag:** `warmup`
- Defenselets:
  - **Deadline:** tba at handout
  - **Tag:** `defenselets`
- Defensive Programming 1:
  - **Deadline:** tba at handout
  - **Tag:** `defensive1`
- Defensive Programming 2:
  - **Deadline:** tba at handout
  - **Tag:** `defensive2`

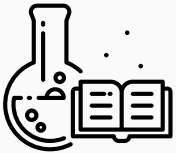


- Warmup:
  - **Deadline:** 19th of October 23:59 (19.10.2022)
  - **Tag:** `warmup`
- Defenselets:
  - **Deadline:** tba at handout
  - **Tag:** `defenselets`
- Defensive Programming 1:
  - **Deadline:** tba at handout
  - **Tag:** `defensive1`
- Defensive Programming 2:
  - **Deadline:** tba at handout
  - **Tag:** `defensive2`

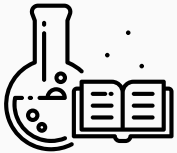


- Warmup:
  - **Deadline:** 19th of October 23:59 (19.10.2022)
  - **Tag:** `warmup`
- Defenselets:
  - **Deadline:** tba at handout
  - **Tag:** `defenselets`
- Defensive Programming 1:
  - **Deadline:** tba at handout
  - **Tag:** `defensive1`
- Defensive Programming 2:
  - **Deadline:** tba at handout
  - **Tag:** `defensive2`

Demo



- The demos will be available at:
- `https://extgit.iaik.tugraz.at/sase/practicals/2022/exercise2022-demos.git`



- The demos will be available at:
- `https://extgit.iaik.tugraz.at/sase/practicals/2022/exercise2022-demos.git`

Expectations

- Time management
- x86 assembler basics, C/C++ skills
- Basic debugging knowledge
- Basic scripting knowledge
- Willingness to try and learn
- More importantly: Be creative and have fun!

Help! I feel already overwhelmed...

- Start early and play around
- Visit the lecture
- Visit the tutorial sessions
- Ask your questions in the tutorials / Discord
- Check the internet
- Read, try, fail, try again, read more, fail, try again, succeed

- Start early and play around
- Visit the lecture
- Visit the tutorial sessions
- Ask your questions in the tutorials / Discord
- Check the internet
- Read, try, fail, try again, read more, fail, try again, succeed

- Start early and play around
- Visit the lecture
- Visit the tutorial sessions
- Ask your questions in the tutorials / Discord
- Check the internet
- Read, try, fail, try again, read more, fail, try again, succeed

- Start early and play around
- Visit the lecture
- Visit the tutorial sessions
- Ask your questions in the tutorials / Discord
- Check the internet
- Read, try, fail, try again, read more, fail, try again, succeed

- Start early and play around
- Visit the lecture
- Visit the tutorial sessions
- Ask your questions in the tutorials / Discord
- Check the internet
- Read, try, fail, try again, read more, fail, try again, succeed

- Start early and play around
- Visit the lecture
- Visit the tutorial sessions
- Ask your questions in the tutorials / Discord
- Check the internet
- Read, try, fail, try again, read more, fail, try again, succeed

Any Questions?