Web Application Security - Cyber Skills Aotearoa

Haumarutanga Taupānga Tukutuku – Pūkenga ā-Ipurangi Aotearoa

Kaiako guide

grok academy

Cyber Skills Aotearoa

Tātai Aho Rau CORE EDUCATION

Cyber Skills Aotearoa

A guide to supporting ākonga engagement

Supported by:

ASB aws bnz certnz N4L Te Kāwanatanga o Aotearoa New Zealand Government NCSC

Ngā Ihirangi | Table of Contents

He aha te Grok Academy? What is Grok Academy?

Grok Academy provides resources, online courses and competitions, teacher workshops, curriculum guidance and online cyber security advice for all future focused kaiako.

Our Mission

At Grok Academy, our mission is to educate all learners in transformative computing skills, knowledge and dispositions, empowering them to meet the challenges and seize the opportunities of the future.

To us, computing encompasses basic digital literacy through to advanced computer science and related disciplines, and the application of these skills across all disciplines.

Our Goal

We believe that a solid computer science understanding is vital whether you want to fight climate change, make the next blockbuster movie or unlock the secrets of the universe.

We've taught thousands of ākonga to program in classrooms, lecture halls and online, and are now bringing top-notch STEM education into classrooms and homes around the world.

Partner Acknowledgements

Cyber Skills Aotearoa has been developed by Grok Academy in partnership with Tātai Aho Rau | CORE Education, AWS, ASB, BNZ, CERT NZ, Netsafe, The National Cyber Security Centre (NCSC), and te Kāwanatanga o Aotearoa | the New Zealand Government.

Nau mai, haere mai | Welcome

This guide supports kaiako to create an effective learning programme based on the Cyber Skills Aotearoa Yr 9-13 Web Application Security Challenge.

We hope this guide will build your confidence as you support your ākonga to get the most out of the challenge, and that their motivation and engagement grows alongside their understanding of cybersecurity.

If you have any feedback or questions about Cyber Skills Aotearoa, please email us at help@grokacademy.org.

This Challenge introduces ākonga to web application security – the branch of cyber security concerned with securing web applications.

Our lives are lived both online and offline. Every day, ākonga interact with websites that remember who they are, show them content tailored to their interests, and allow them to submit assignments, order food or talk to friends. There are frequent news reports about popular web applications that have been hacked. This course helps ākonga to understand how hacks and breaches occur.

Ākonga work through problems to develop their understanding of how web applications work, the code that creates them, and how information can be accessed or revealed unintentionally. The challenge includes an introduction to HTML and a small amount of coding.

Ākonga explore security vulnerabilities on four fictitious websites created for this Challenge. This allows them to explore authentic, real-life web application security concepts and techniques from within the Grok Academy's hosted platform.

The Challenge includes notes, guided investigative problems, some programming activities using HTML and multi-choice problems to test understanding and skills.

The Challenge also emphasises the ethical component of cyber security. Ākonga are introduced to scenarios where they may be able to access unauthorised information. They are asked to consider when it is acceptable to exploit security vulnerabilities in web applications. Through a series of videos, they hear from cyber security professionals who discuss their careers, how they started in cyber security, and caution about using cyber skills unethically.

Everyone featured in the videos is an employee of the organisation they represent, and they work in a variety of roles.

The challenge is designed to be completed over 6-8 hours, but may take longer depending on time spent on off-line activities and classroom discussions.

How the Challenge relates to The New Zealand Curriculum

The Challenge has close ties to the Technology learning area. The Technology learning area is about the interrelationship between people, technology, and the environment, and understanding 'intervention by design'.

> With its focus on design thinking, technology education supports students to be innovative, reflective and critical in designing new models, products, software, systems and tools to benefit people while taking account of their impact on cultural, ethical, environmental and economic conditions.
>
> The aim is for students to develop broad technological knowledge, practices and dispositions that will equip them to participate in society as informed citizens and provide a platform for technology-related careers. Technology in the New Zealand Curriculum (2017)

Key areas that the Technology learning area addresses

Digital Technologies (NZC)

- Computational Thinking for Digital Technologies and Designing and Developing Digital Outcomes focus on developing students' capability to create unique digital outcomes for specific needs and purposes. These Technological areas significantly contribute to developing the knowledge and skills students need as digital citizens and as users of digital technologies across the curriculum. They also provide opportunities to further develop their key competencies:
  - Thinking
  - Using language, symbols, and texts
  - Managing self
  - Relating to others
  - Participating and contributing

- Computational Thinking for Digital Technologies (CTDT) – ākonga will develop an understanding of computer science principles that underlie all digital technologies. They'll learn core programming concepts so that they can become creators of digital technology, not just users.

- Designing and Developing Digital Outcomes (DDDO) – ākonga will develop an understanding that digital applications and systems are created for humans by humans, with a focus on designing and producing quality, fit-for-purpose, digital outcomes. They develop their understanding of the technologies people need in order to locate, analyse, evaluate and present digital information efficiently, effectively and ethically.

In particular, the web apps challenge is related to:

NZC Technology/Digital Technologies
Designing and Developing Digital Technologies Progress Outcome 3 (DDDO PO3)

> In authentic contexts, students follow a defined process to design, develop, store, test and **evaluate digital content to address given contexts or issues, taking into account immediate social, ethical and end-user considerations**. They identify the key features of selected software and choose the most appropriate software and file types to develop and combine digital content.
>
> Ākonga understand the role of operating systems in managing digital devices, security, and application software and are able to apply file management conventions using a range of storage devices. **They understand that with storing data comes responsibility for ensuring security and privacy**.

NZC Technology/Digital Technologies
Computational Thinking for Digital Technologies Progress Outcome 7 (CTDT PO7)

> In authentic contexts and taking account of end-users, students analyse concepts in digital technologies (for example, information systems, encryption, computer security, error control, complexity and tractability, autonomous control) by explaining the relevant mechanisms that underpin them, how they are used in real world applications, and the key problems or issues related to them.
>
> *Assessment specifications Level 2 Digital Technologies and Hangarau Matihiko 2023 DCAT*
>
> For computer security, questions may cover: **spam emails, two-factor authentication**, reCAPTCHA, **common issues, steps individuals should take to protect their data, data privacy, ways to protect individual computers** and computers managed by an organisation, policies or practices of a multi-national technology corporation. Assessment Specifications » NZQA
>
> DDDO progress outcome 3 covers learning up to approximately Year 10. CTDT progress outcome 7 covers learning up to approximately Year 12. The elements in bold are covered in this challenge.

While there isn't any specific programming content within the Cyber Skills Aotearoa Yr 9-13 Web Application Security Challenge, students do learn some basic HTML/CSS content and how web applications use cookies, sessions and tokens. The content in the Challenge supports programmes of learning that focus on web design or web application development. In addition, the challenge supports the development of testing and debugging skills that are part of both DDDO and CT progress outcomes.

Nature of Technology (NZC)

There are also many connections to the Nature of Technology strand and the learning outcomes that explore the relationship between humans and technology at each year level.

> *The nature of technology strand guides teachers to develop learning activities that support students to question why the world around them is the way it is. They develop perspectives and become aware of the relationship between people as users and designers/creators of technology and how that technology in turn impacts on more people, the environment, and on culture.*
>
> *They learn to critique the impact of technology on societies and the environment and to explore how developments and outcomes are valued by different peoples in different times.*
> *Students have opportunities to increase their understanding of the complex moral and ethical aspects that surround technology and technological developments. They ask big questions such as "if it can be done, should it be done?" TKI - Nature of technology*
>
> In Characteristics of Technology (CoT) technology is defined as "purposeful intervention by design", and technological practice as the activity through which technological outcomes are created and have impact in the world. Technological outcomes are designed to enhance the capabilities of people and expand human possibilities. They change the made world in ways that have positive and/or negative impacts on the social and natural world. TKI - Characteristics of technology
>
> CoT encourages teachers to guide students to:
>
> - Determine the impacts different technologies have had on society and/or the environment over time (Level 3)
> - Understand that "expanding human possibilities" can result in positive and negative impacts on societies and natural environments and may be experienced differently by particular groups of people (Level 4)
> - Analyse a range of examples of technologies to examine how people's perceptions and/or level of acceptance has influenced the practices and decisions underpinning their development and implementation (Level 5)

The Challenge supports future focused capabilities and 21st century skills

Te Marautanga o Aotearoa and NZC support ākonga to develop future focused capabilities. The mātāpono whānui | overarching principles of both curricula serve as the first foundations on which educators, communities, and ākonga can begin to co-design their future focused and sustainable vision for learning.

> Your students will develop their digital fluency through a range of authentic curriculum opportunities. Your local curriculum should emphasise the capabilities, principles, and literacies that students are expected to develop as they become more innovative, creative, and discerning in their use of a range of technologies. elearning.tki.org.nz/Teaching/Digital-fluency

Hōtaka ako | Learning programme

Learning intentions

After completing the Challenge, ākonga will be able to:

- Explain what a web application is
- Navigate around a web application using the address bar
- Use HTML to make simple edits to a web page
- Use developer tools within Grok's hosted platform to explore visible and hidden components of a web application
- Explain different types of hackers (ethical vs malicious, offensive vs defensive)
- Understand the circumstances when it is acceptable to explore vulnerabilities in web applications
- Explain authorisation, and common ways web applications authorise users
- Explain authentication, and the types of rights the users of web applications might have

Module outline

The Web Application Security Challenge consists of four modules:

1. Introduction to web applications

    Ākonga explore what a web application is. They learn how to use URLs to navigate between pages in an app to find information on other pages that isn't otherwise viewable. They investigate how information is sent from a server to a client and learn how information can be sent to the server through the URL.

    Ākonga are introduced to scenarios where they may be able to access unauthorised information. They are asked to consider when it is acceptable to exploit security vulnerabilities in web applications and encouraged to use their skills ethically: only testing with the app owner's permission, reporting vulnerabilities, and not exploiting them for their own gain.

2. Web application security

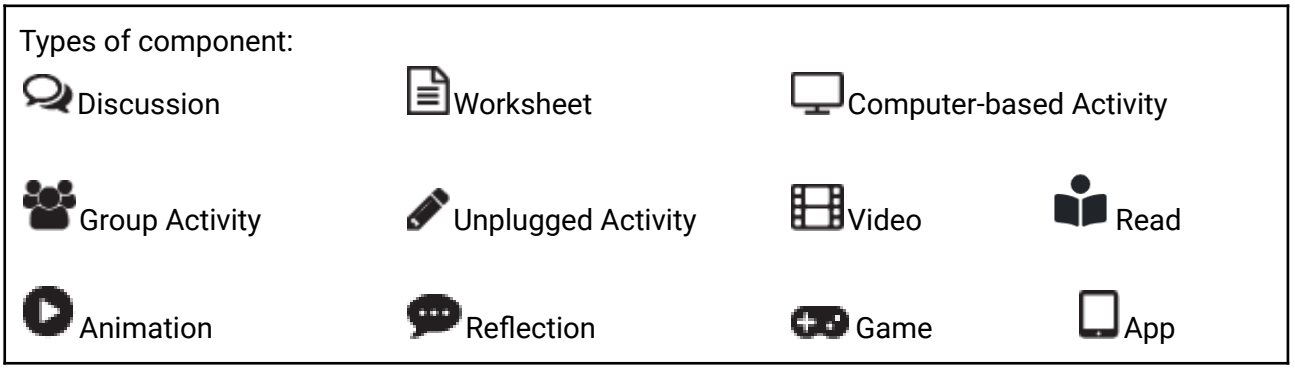
    Ākonga edit HTML and see how web applications are built using HTML. They investigate and edit web forms, and see how web forms are used to send information from a device to a server.

3. Authentication

    Ākonga investigate how users prove their identity when using web applications. In the module ākonga investigate password fields in forms, cookies and tokens. Security vulnerabilities associated with each of these authentication methods are discussed and explored.

4. Authorisation

   Ākonga investigate how different users have different rights to access information and perform actions within a web application. They explore how authorisation can be changed and how this may be exploited. They look at all of the data that is sent to a device by the server including information which may not be displayed.



Challenge Introduction for Ākonga — why study web application security?

Let's start with a definition: cyber security is a fancy name for a collection of tools and methods that people or companies use to protect themselves, their networks, systems or programs from attack. Attackers are usually trying to get access to electronically stored sensitive information, or to steal money.

So understanding these tools and methods is a pretty good way to learn how to keep yourself safe online. But not just that – cyber security is a great source of future jobs. There is a significant shortage of people with the skills to help protect companies and other people.

To learn about cyber security in this Challenge we're going to explore web application security – how developers make web applications like Netflix or YouTube secure for users.

Cyber attacks are happening all the time. Visit https://cybermap.kaspersky.com/ to see a representation of current cyber attacks.

Key Vocabulary

Authentication: Proof of the identity of a user logging onto a network.

Authorisation: The function of specifying access rights/privileges to resources, which is related to information security and computer security in general and to access control in particular.

Bug: A glitch or imperfection in a computer program.

Cookies: Data or text files that websites store on a user's computer to identify, track, and monitor the user's activity and preferences.

Decomposition: Breaking down data, processes, or problems into smaller parts.

Debugging: Finding mistakes in a program and correcting them.

Ethics: The study of principles relating to right and wrong conduct. The standards that govern the conduct of a person, especially a member of a profession.

Hackers:

> **Malicious Hackers**: These hackers engage in unauthorised and malicious activities. They break into computer systems or networks with the intention of causing harm, stealing information, or committing illegal activities.
>
> **Ethical Hackers**: These individuals use their hacking skills for good. They are hired by organisations to identify vulnerabilities in computer systems, networks, or software and help improve security. Their goal is to protect systems from malicious attacks.

It's important to note that hacking itself is neutral and can be used for both ethical and unethical purposes. The distinction lies in the intentions and actions of the hackers.

Pattern Recognition & Generalisation: Looking for patterns, similarities and trends in data.

Sequencing: Putting instructions one after another.

Source Code: The set of instructions and statements that is written by a programmer using a human-readable programming language.

Token-based authorisation: An authorization token is like a special pass or ticket that allows you to enter certain areas or do specific things in a computer system or app. It's kind of like a digital ID card that proves you have permission to access certain information or perform certain actions. This token is used to keep things secure and make sure only the right people can do certain things online. It's like having a key to a locked door that lets you in, but only if you're authorised to be there.

Variables: A value that can change, depending on conditions or information passed to the program.

Web application: A software application that is accessed via a web browser often over a network but sometimes offline.

Web form: A web form (or HTML form) is a place where users enter data or personal information that’s then sent to a server for processing.

Kōwae 1: Ngā Taupānga Tukutuku | Module 1: Introduction to Web Applications

Preparation and timing

No prior knowledge is required for this activity. This module should take approximately 1-2 lessons to complete depending upon use of suggested classroom activities.

Learning Overview

- What a web application is
- How to navigate between pages in the app using the address bar
- How to find information on other pages that isn't otherwise viewable
- How information can be sent to the server through the URL
- How to edit the information which is sent to the server by modifying an URL
- Differences between white hat and black hat hackers
- Red teams and blue teams in cybersecurity
- Using skills ethically: only testing with the app owner's permission, reporting vulnerabilities, and not exploiting them for your own gain

Suggested Implementation

Activity 1

 Group activity

What is a web application? (Suggested time: 20-30 minutes)
In groups of three or four, ākonga discuss the five websites / web applications that they use most frequently. Combine these individual lists into one group list and:

- record how many times each web application appeared in the groups individual list
- discuss whether the web app requires a sign in to use it
- discuss what information is the same for every user
- discuss what information is different for each user
- discuss what information the web application might know about you, to be able to adjust the content to be specific to the user.

Web app name	Sign in required?	What's the same?	What's different?	What does it know about you?
Spotify	Yes	Appearance, layout	Recommendations, playlists	Name Location Profile picture Age? Listening history? Friends?

Online Module 1: Web applications

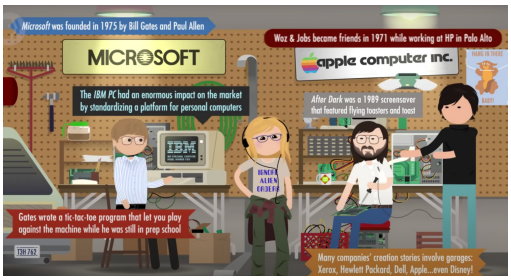
Computer-based Activity : Web Application Security

Complete Online Module 1: Web Applications:

Activity 2

Video:

Watch the video: As an extra activity, you could show ākonga the Crash Course Computer Science episode relating to the world wide web:



There is a lot of information packed into this fast paced episode – pause where necessary and revisit as you work through this challenge.

End of Module Activity

Reflection Group Activity

Discuss in small groups:

- How much information about you is stored on web applications? How does this make you feel?
- What are the benefits of web applications being tailored to your needs? What are the drawbacks?
- What information do applications on your device know about you?
- What would happen if your device is lost or stolen? What security do you have on your device to prevent others from accessing your data?

Kōwae 2: Te Whakahaumarutanga Taupānga Tukutuku | Module 2: Web Application Security

Preparation and timing

Ākonga should first complete Web Application Security Module 1. This module should take approximately 1-2 lessons to complete depending upon use of suggested classroom activities.

Learning Overview

- What HTML is and how tags are used to control what is displayed on your screen
- How style tags can be used to change the way information is displayed
- How a lot of web applications use forms to collect and send information to servers
- How forms can be edited, and how this can expose security vulnerabilities
- How to ethically report vulnerabilities in web applications

Suggested Implementation

Activity 1

Computer based activity (suggested time: 10 minutes)

We use Web apps so frequently – it's time to take a closer look at the coding behind them. Ākonga visit a simple website or webapp – we suggest your own school's website.

Ask ākonga to hover over some text or an image on the page, and right click. You can select a command to view (or, 'Inspect') the code which creates the element you are hovering over:

Ākonga will be using HTML later in this course. For now ākonga should:

- Explore the source code – is there anything recognisable here? (For example, can they see the headings or text from the page in the HTML?)
- If hovering over an image, what information can you find out about that image? (Image size? File name?)
- Edit a heading to change the text displayed on the screen.
- Discuss: if ākonga have edited a heading, has that changed the web app? Or just what is displayed on their computer? (A video later in this module answers this question.)

Online Module 2: Web application security

Computer-based Activity: Web Application Security

Complete Online Module 2: Web Application Security

Extension Activity

Video Read

In this module ākonga learn about the difference between GET and POST methods for sending information to a server. There are various other methods such as PUT and DELETE that ākonga can explore as an extension activity.

Here is a brief overview of of the four methods:

GET: The GET method is used to retrieve or fetch data from a specified resource. It is primarily used for reading information without modifying or altering the resource. When you visit a webpage or click on a link, your web browser typically sends a GET request to the server to retrieve the HTML content of that page. Since GET requests are included in the URL itself, the data is visible in the browser's address bar and server logs. Therefore, it is recommended not to use GET for sensitive data or operations that modify server state.

POST: The POST method is used to submit data to be processed by the resource identified by the URL. It is commonly used for creating new resources or submitting form data. When you fill out a web form and click "Submit," the data is typically sent to the server using a POST request. Unlike GET requests, POST requests send data in the request body, making it more secure for transmitting sensitive information. POST requests are not cached by default and do not appear in the browser's address bar, offering an additional layer of security.

PUT: The PUT method is used to update or replace an existing resource with new data. It sends the entire representation of the resource to the server. PUT is commonly used in RESTful APIs to update or overwrite an existing resource. Similar to POST, the data is sent in the request body, ensuring confidentiality. It is important to note that some web frameworks or APIs may have different conventions or restrictions when it comes to using PUT.

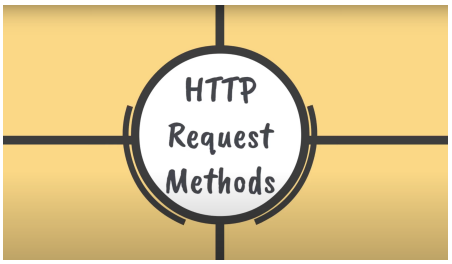
DELETE: The DELETE method is used to remove or delete a specified resource. It instructs the server to delete the resource identified by the URL. When you delete a file or unsubscribe from a service, a DELETE request is typically sent to the server to delete the corresponding resource. Similar to GET requests, DELETE requests include data in the URL itself. However, since the purpose is to delete a resource rather than retrieve data, the security concerns are often different.

In terms of security differences between GET and POST, GET requests are less secure for transmitting sensitive information because the data is visible in the URL and can be logged. On the other hand, POST requests are more secure since the data is sent in the request body and not visible in the address bar or server logs. Therefore, when transmitting sensitive data, such as passwords or personal information, it is recommended to use POST instead of GET to ensure confidentiality.

It's worth noting that while POST requests provide better security for transmitting sensitive data, other security measures, such as encryption (HTTPS), server-side validation, and authentication, should also be implemented to ensure overall security in web applications.

This W3Schools article provides further details about the difference between GET and POST.

This video provides an explanation of GET POST PUT and DELETE methods.



End of Module Activity

Reflection Group Activity

Where's the line?

In the computer based activity above ākonga have explored the HTML used to create web apps. The HTML for any web app can be revealed using the 'inspect' or 'inspect element' feature. Discuss as a group where the line is between curiosity and potentially risky or illegal behaviour, with these examples:

- Inspecting HTML
- Inspecting the HTML of a nice looking graphic to see if you can reuse it on a website you are creating
- Inspecting the HTML on a website to see if there are non-visible elements
- Changing HTML on your computer to change the colour of a heading
- Changing the HTML on your computer to change the contents of a form on a webpage to send unexpected information to a server

Information:
The examples above range from innocuous to clearly inappropriate, but it's hard to be really precise about where the line is. There are many factors to consider – legal implications, ethical behaviour, and intellectual property considerations. We want ākonga to think about the different aspects of cyber security, and also appreciate that curiosity without reflection can have serious consequences.

Kōwae 3: Motuhēhēnga | Module 3: Authentication

Preparation and timing

Ākonga should first complete Web Application Security Modules 1 and 2. This module should take approximately 1-2 lessons to complete depending upon use of suggested classroom activities.

Overview

- How users prove their identity when using web applications
- Different types of fields in forms
- How websites use cookies to customise and improve users' experiences
- The difference between first and third party cookies
- Potential security vulnerabilities in forms and cookies
- The use of hashing algorithms and tokens to improve security
- The trade-offs within web application security known as the CIA triad

Suggested Implementation

Activity 1

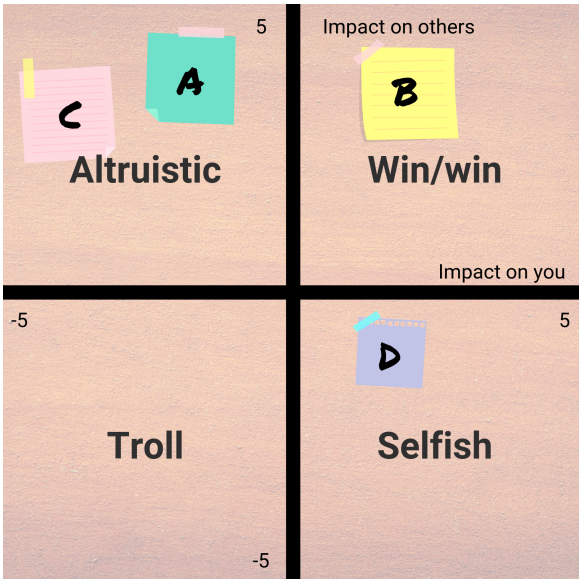
Unplugged Activity Group Activity

Scenarios and their impacts (suggested time: 45 minutes)
In this activity ākonga are challenged to consider behaviour both online and offline which raises ethical questions:

- Ākonga examine online and offline scenarios to consider the impact of those scenarios would have on others and on themselves
- Ākonga create a scattergram showing their responses to scenarios
- Ākonga learn about authentication – how you prove your identity online

This activity can be completed either unplugged or online. For the unplugged version, ākonga can work either individually or in groups. You will need post-it notes, and a large plus sign on the wall or floor to divide a surface into four quadrants, as illustrated below (it's not necessary to include the captions Win/win, selfish, etc.)

Alternatively, individual ākonga could complete the activity with individual sheets of paper, simply writing the letters on the page in the positions they choose.



Select all or some of the scenarios below, and ask ākonga to briefly consider the impact of this action on others, and on themselves. Write the letter of the relevant scenario on a post it, and place the post it in position based on the impact of others (from -5, that is, strongly negative, to +5, strongly positive on the x-axis) and likewise the impact on self on the y-axis. When thinking about the impact on themselves, ākonga should assume that they have been noticed/detected, and that any positive or negative consequences would be experienced in full(e.g, a cash reward, detention, or a prison sentence).

Scenarios – feel free to add your own or ask ākonga to generate additional scenarios

A	Accessing a maths test online a week before anyone else can.
B	Working out how to get new skins in an online game without paying for them.
C	Creating your own discount code at your favourite online store and using it to buy discounted goods.
D	Using another person's session token to get early access to ticket sales for your favourite band.
E	Using another persons' account details to access music streaming when you'd normally have to pay a subscription.
F	Staying logged in as another user on a school computer and looking at the other person's results.
G	Staying logged in as another user on a shared computer and purchasing 100 bags of Doritos for them as a joke.
H	Altering an address field in a form on a website so all the pizzas are delivered to your home.
I	Staying logged in as another user on a messaging website and sending a message pretending to be them.
J	Using a friend's library card to borrow books.

K	Getting an IOU from the tuck shop for a lunch order, and giving a friend's name instead of your own.
L	Phoning a pizza shop and ordering a pizza for delivery to friends house which they have to pay for when it arrives, as a joke.
M	Picking up next week's maths test from the photocopier, when you realise your teacher left it there by accident.
N	Stealing a set of your favourite collectible cards from the dairy.
O	Asking for the student discount at the local cinema, when you know the discount is only for ākonga from the local high school and you're visiting from out of town.
P	Using your student bus pass to travel to a friend's house during the holidays.
Q	Phoning the doctor and pretending to be your older brother so you can find out if his whooping cough blood test came back positive.
R	Signing in to your school website with your friend's permission to find out when their next assignment is due.
S	Going to the school library and seeing your friend is signed in to a computer, so signing them out.
T	Finding a set of keys on the street, handing them in, and getting a reward in return.
U	Finding a set of keys on the street, and going out of your way to take them to a police station, for no reward.
V	Hearing at school that all your friends are accessing a VIP discount on a website that they shouldn't be able to access, and alerting the website owner so they can fix the bug.
W	Buying an item in a store when you know it has been incorrectly priced (it's selling for $0.99 when it should be $9.99)
Y	Entering a bug bounty online, and exploring a test website to find vulnerabilities, with prizes for the top competitors.
Z	Arriving at a movie screening night, and when the usher asks 'did you buy the VIP tickets or the general tickets' answering 'VIP', even though you purchased the general tickets.

Information:
These situations are intentionally a little ambiguous, and are designed to generate discussion. We suggest ākonga place post-it notes quickly, based on their initial impressions, and then have a discussion once all post-it notes have been placed on the wall.

It's desirable for the results to spread across the four quadrants:

- win/win – a positive impact for others and yourself
- altruistic – a positive for others, and a negative impact for yourself
- selfish – a positive for yourself, a negative for others
- troll – a negative for both yourself and others.

You may wish to start as a group with these four scenarios, which cover the four quadrants: Y (win/win), U (altruistic), W (selfish – it's hard to see any real negative consequence for you as it's clear there's an error but you've not done anything with a legal consequence), G (troll, when you consider the consequence for yourself of using another person's account without being authorised.)

Discussion questions:

- Are there any scenarios that different ākonga have categorised very differently?
- Once you have seen others' responses, does anyone want to change their answer? Is this because of a misunderstanding in the question, or because seeing everyone else's answers, you've reconsidered your initial judgement?
- When we refer to 'impact on others' – who is the other? Can one question have multiple others? What do you do if there is a positive impact for one user and a negative for another?
- Is there any noticeable difference in how ākonga respond to real life scenarios, compared with online scenarios?

If you prefer to do this activity online, you can copy this document: https://docs.google.com/spreadsheets/d/1Vw4ZpHNDYKW4HB9HZbsyCt04kn9wYBYFLPER8JRuLAg/edit?usp=sharing which contains the scenarios and includes a scattergram to plot results. It will plot one result per scenario. You could adapt this to plot multiple responses to each scenario.

Online Module 3: Authentication

 Computer-based Activity
Complete Online Module 3: Authentication

Activity 2

 Reflection  Group Activity

Shared computers

In the computer-based activity you have seen one example of how your password can be exposed. This is a particular risk when you are using a shared computer (such as one in your library or school computer laboratory). As a group, make a list of three things to remember when using a shared computer.

Extension Activities

 Read  Computer-based Activity

Kaiako and ākonga may wish to explore cookies, hashing algorithms and authorisation tokens in more depth.

There are different types of cookies as explained below:

1. **Session Cookies**: Imagine you're attending a school event. When you enter, the organisers give you a temporary ID sticker to wear. This sticker helps them identify you during the

event. Similarly, session cookies are like temporary stickers that websites give your web browser when you visit them. These cookies are used to remember your actions and preferences during your visit. They are stored temporarily in your browser's memory and are deleted once you close the browser or leave the website.

2. **Persistent Cookies**: If you have a library card, you know that your library keeps track of your borrowing history. Persistent cookies are similar. They are stored on your computer for a longer period, even after you close your browser. These cookies help websites remember you and your preferences when you visit them again in the future. For example, they can remember your username, language preference, or customised settings.

3. **Secure Cookies**: Imagine you have a diary with a lock and key. Only you have the key to unlock it and read your secrets. Secure cookies work similarly. They are used for secure websites that require encryption, such as online banking or shopping websites. Secure cookies ensure that your sensitive information, such as your login details or financial data, is encrypted and protected from unauthorised access.

4. **Third-Party Cookies**: Sometimes, when you attend a school event, a different organisation sets up a booth to collect information about attendees. Similarly, third-party cookies are created by websites other than the one you are currently visiting. They are often used by advertisers or analytics companies to track your online behaviour across multiple websites. These cookies can help personalise ads or gather statistics about website usage.

It's important to note that cookies are just small text files and do not contain viruses or malware. They are used to enhance your browsing experience and provide convenience. However, it's always a good practice to manage your cookie settings in your browser and be cautious about sharing personal information online.

Remember, cookies are like little helpers that make your web browsing more personalised and convenient, but it's essential to be aware of how they work and make informed choices about your privacy and security online.

- This article, All you need to know about third-party cookies, describes third-party cookies in more detail and shows how to check the cookies stored in your browser.
- The Computer Science Field Guide has a chapter with activities that provides more detail on hashing algorithms.
- This article, More cybercriminals stealing auth tokens to bypass MFA, also provides more details about cyber security threats to access tokens.

Kōwae 4: Whakaaetanga | Module 4: Authorisation

Preparation and timing

Ākonga should first complete Web Application Security Modules 1-3 . This module should take approximately 1-2 lessons to complete depending upon use of suggested classroom activities.

Overview

- Information and powers should be limited to people with the proper authority or permission is called authorisation
- Certain users might need access to some information that other users do not
- Certain users, such as administrators, have special privileges that allow them to perform actions that regular users cannot
- Technologies and techniques web developers use to add authorisation to their web applications
- Authorisation bugs that can leave web applications vulnerable to hackers

Suggested Implementation

Activity 1

 Group activity  Unplugged Activity

Physical vs web application authorisation (Suggested time: 60 minutes)

In this activity ākonga consider how authorisation is managed in the physical world through a school building management scenario, and draw parallels to how web applications manage authorisation for different types of users.

This activity is best completed offline in small groups, but can be done individually. Each group will need a copy of a table similar to the one shown below, adjusted to take into account the organisation/scenario chosen by the kaiako.

The implementation below is based on ākonga working through a school-based scenario. This has been chosen because it is a context ākonga are generally familiar with. You can perform exactly the same process for any type of organisation, depending on how challenging you'd like it to be for your ākonga.

> Your school is implementing a swipe card system to control access to your school grounds, buildings and rooms/areas in response to a recent intruder alert. Your group has been tasked to come up with a design of the access control system. For each area in the school, you are required to:
>
> - Identify which group of people can have access to the area

- Specify any restrictions that may be placed on that access (e.g. specific hours, dates etc)
- Provide reasons for your decisions

The table below can be used as a starting point. It identifies some of the main locations in the school and some of the user types that need to be considered. Since all ākonga, kaiako, staff members and visitors to the school will be provided with an access card, you can break the users up into any number of groups you like to manage access.

Location	Users (and restrictions)							Explanation
	Visitors	Ākonga	Kaiako	Cleaners	Caretaker	Fire Dept	Principal	
Front office	Yes – school hours only	Yes – school hours only	Yes	Yes	Yes	Yes	Yes	Access is required by all groups, but some only when school is on. Cleaners do their work outside school hours and should be treated as visitors during school hours.
Principal's office	No	No	No	Yes	Yes	Yes	Yes	Cleaners and the caretaker require access to do their work, but the Principal should have separate lockable storage to store sensitive information that cannot be accessed by others.
Plant room								
Store rooms								
Cleaning cupboards								
Classrooms								
Staff common room								
Staff rooms								
Canteen								
Workshops								
Food room								

The above table is intentionally incomplete. You may choose to provide ākonga with more example information, change the number of groups/locations, or otherwise alter it to suit your ākonga.

Produce a table similar to the above using landscape orientation, and give ākonga additional user columns so they can add extra users as they are identified.

 Discussion:

Questions

- How many different types of access are required for your solution?
- Are there any groups of people who could have their access combined into a single category to simplify the table a bit?
- What kinds of date/time restrictions make sense for a school? How flexible do these need to be to suit the needs for all of the users of a given type?
- How do you balance the practicalities of the design with the specific needs? For example, does it make sense to have separate controls for every single classroom or storage area? How do you decide when a room needs its own access rules?
- What are some of the important factors that you consider when deciding the access rules for a particular area?
- How does your answer compare to those of other ākonga? Why is your design different?

Ākonga proceed to online module 4 on authorisation. Draw their attention to the “School of Grok / Te Kura o Grok” web application – the reflection activity asks them to consider parallels between that web app and the access control activity they’ve just completed.

Online Module 4: Authorisation

 Computer-based Activity
Complete Online Module 4: Authorisation

End of Module Activity

 Reflection  Group Activity

Now that you’ve completed the Authorisation module, how could the School of Grok / Te Kura o Grok be improved to better meet the needs of individual users? Consider how your school’s Learning Management System works and the features it has. What different types of users should School of Grok / Te Kura o Grok implement? What access should each of those users have? What additional features should be prioritised?