WM243| Human Behaviour In Cyber Systems
Student IDs: 2032869, 2143478, 2147214, 2152233, 2139422, 2101239
CW2: Fixing The Prototype

Link to website: http://10.10.3.228/

Introduction

Usability refers to how easily a user interacts with a website and is a key element of interaction design. Considering how the product is used, who is using it and the activities to be supported when in use are vital to establishing the functionality and usability of the website in order to create usability goals. The user experience should include usability goals where the product is interactive, safe to use, efficient, easy to learn and has engaging, positive connotations.

Design principles cover: visibility, feedback, constraints, mapping, consistency and affordances. When all of these principles are fulfilled, the usability of the website increases for all users, whether novice or experienced.

Our website, named ‘Movie Rentals’, allows users to select a movie to rent, determine how long they would like to rent it for and purchase it online using a credit/debit card. How easily these goals can be achieved then indicates how usable our website is.

Schniderman (1998) says usability can be measured through the time it takes to learn how to use the product, the speed of the performance, the rate or errors by users, retention over time and subjective satisfaction. Alternatively, Nielsen (1993) measures usability through its learnability, efficiency, memorability, errors and satisfaction rate. By evaluating how usable the website is, the developers can check if the design is acceptable and applicable for the wider user population. Measuring usability can occur through quantitative assessments with task-performance measurements, analytical evaluations examining the interactivity and through system centred or interaction centred evaluations. System-centred evaluations use heuristics, which are explored in section 3, whilst interaction centred evaluations follow a cognitive walkthrough where a user explains their thought process and actions whilst using the website.

Usability Requirements

Usability Problems Found In the Initial Prototype

The severity of usability problems depends on:

1. The frequency the problem occurs
    a. How often does the problem affect users? Is it common for errors to occur?
2. The impact of the problem
    a. Does the impact affect usability? Can you continue to use the website if the problem persists? Can a user overcome the issue on their own?
3. The persistence of the problem
    a. Are users impacted several times by the problem? Does the problem repeatedly impact the user experience?
4. The market impact
    a. Does the problem impact sales and/or popularity of the website?

We used a 1-5 rating scale as well as a Heuristic Evaluation to determine the immediate changes needed and the higher priority tasks:

1: There are no usability problems

2: Only cosmetic problems persist

3: Minor usability problems exist with low priority

4: Major usability problems exist with high priority

5: Usability catastrophe which is imperative to fix.

We identified and fixed 23 issues with the prototype. More details on these issues can be found in the table below.

Problem	**Usability Scale Rating**	**Heuristic Evaluation**
No navigation bar on the website between web pages	5	Nielsen's 3rd principle is broken as web pages cannot be identified or navigated through clearly as there is no navigation bar.
No error messages or error handling when erroneous data entered or incorrect values clicked.	4	Nielsen's 5th principle focuses on error prevention from the outset, and no error handling messages have been coded into the webpages, therefore users can enter invalid information when selecting film renting duration, at the log-in page and during the payment process which impacts usability as the user could be unable to purchase the film.
No user feedback when a user adds items to their basket to confirm it was added	4	Nielsen's 1st principle is about keeping users informed with feedback, and currently the user is unaware if their actions did anything as there are no prompts or pop-ups to confirm this.
No movie images visible	2	Nielsen's 8th principle is broken, with no images giving poor visibility, potentially deterring customers from purchasing films as the webpage looks incomplete and a user is unable to compare/confirm the movie poster to one they are familiar with.
Movie images are different sizes and not correctly aligned	2	Nielsen's 8th principle is broken, with no image consistency, giving poor visibility, potentially

		deterring customers from purchasing films as the webpage looks incomplete and messy.
Invalid descriptions of films	2	Nielsen's 8th principle isn't adhered to, with incorrect information active that diminishes visibility and could confuse the user. For example, 'Demonic' features a default plaintext description, with no actual information on the film.
Poor format & layout of website	4	Nielsen's 8th principle covers website design being minimal and aesthetic, although the current webpage is incomplete with alignment issues.
Poor colour scheme of website	4	Nielsen's 8th principle covers website design being minimal and aesthetic, although the current webpage is incomplete with poor colour scheming.
Website basket has no validation	4	Nielsen's 5th principle is broken as validation is a form of error prevention to prevent security vulnerabilities as well as impacting the user experience if a user tries to enter card details which are invalid or in the wrong boxes.
Signup page for users to login - users need to be able to create accounts. Currently, you can sign up with incorrect values entered.	3	Nielsen's 4th principle focuses on consistency and standards, in which a log-in page on a website you make purchases is very common to keep track of purchases and user information; this

		needs to be implemented.
No accessibility features	3	Nielsen's 6th principle focuses on recognition, where the website should be accessible, consistent and information should be retrievable. The website does not account for this currently, lacking text to inform the user on how to navigate the site.
No help page for users	4	Nielsen's 10th principle requires help documentation for the user so they don't have to rely on memory and can have an error mitigating section; the website currently does not have this feature.
The invoice page does not print the inventory of purchased items	3	Nielsen's 1st principle is broken through a lack of feedback on whether the purchase went through and the correct film was purchased which negatively impacts the user experience.
No input validation for any of the checkout fields	4	Nielsen's 9th principle is broken as users won't be able to checkout if entry fields are left blank/contain invalid data which prevents full functionality; this needs to be implemented.
Lack of consistency in web page design	3	Nielsen's 4th principle focuses on consistency and standards, however the sample page lacks differentiation between headers and text, as well as a lack of brand recognition and consistency across

		platforms
Poor input methods	3	Nielsen's 3rd principle is user navigation and control, the sample page had users input their card number by incrementing the value by 1 until they reached their card number - this process is slow and outdated and does not give the user control
The title <HTML> element is the same for all the pages, preventing the user from identifying a page's content by its tab bar.	3	The tag that show up on the tabs when you're on the website stay the same for all webages, saying 'Movie Rentals' instead of their respective titles 'Basket, 'Movie', 'Contact Us' etc. This contradicts Nielsen's 3rd principle of Navigation as these tags are incorrect and represent the wrong information, potentially negatively effecting the user experience. Furthemore, Nielsen's 6th principle is compromised as the webpages are not recognisable.
No search bar to search movies.	4	This breaks Nielsen's 3rd principle, making Navigation throughout the website harder. A search bar would mean a user can search for the film without scrolling through them all. Furthermore, a search bar would apply to Nielsen's 7th principle, acting as a user shortcut for more experienced users on the website to quickly locate the information they want.
No placeholders used to	3	The website has no

imply what should go in the input fields.		placeholders, meaning the user is not prompted what to enter, not in lines with Nielsen's 1st principle as the user is not informed about what to enter or the actions to be completed. Additionally, the 4th principle of consistency and standards is broken, as most websites use prompts such as 'Search..' within the text boxes to the user has clarity.
The hyperlinks don't work.	5	The hyperlinks on the movie selection page which say 'View Movie' did not work, breaking Nielsen's 6th Heuristic as actions are not accessible and retrievable. This means the user cannot read further information about the film, and won't be as entitled to purchase it.
View basket and empty basket are right next to each other, so the user may accidentally click empty basket when they meant to view it.	3	Nielsen's 5th principle focuses on error prevention which is not avoided having contrasting terms next to each other which counteract each other's actions. A solution would be to change them into buttons to create some distance.
Not clear what the 'exit' link does.	3	On the previous website, there was a hyperlink labelled 'exit' (which did not work). This goes against Nielsen's principle of user navigation and control, as users cannot 'exit' using this link, affecting usability and navigation.

No affordances or mapping used.	4	The lack of affordances are not in line with Nielsen's second principle because it doesn't use familiar concepts to indicate the user to perform appropriate actions into the website. For example, there is no iconography or text to suggest the user performs an action.
Data fields can be submitted when empty (login)	3	This contradicts Nielsen's 5th principle of Error Prevention, for example, users would be able to enter blank fields, and therefore an incomplete login - therefore creating an error. This goes against principles of error prevention.
Redundant sign-up button (login)	3	Not being able to create an account definitely interferes with usability.
Invalid email addresses can be used to sign up	3	Conflicts with Nielsen's 5th principle - and would allow erroneous data to be submitted

Nielsen's Heuristics

Nielsen (2005) explores ten general principles for user interface design. Heuristics are a mental shortcut people use to simplify problems and avoid cognitive overload, basing decisions on previous experiences. The first principle is the 'visibility of system status', in which the system should always keep users informed about what is going on, through feedback on the user interface within reasonable time. To implement this into our website, user feedback is given through 'pop ups' which prompt the user about their actions when they click around the webpage. Additionally, when you hover over a button, the colour gradient changes to indicate the mouse is active on that location - therefore, the user is receiving feedback they are navigating correctly and that the site is interactive.

Nielsen’s second principle is the ability to ‘match between system and the real world’, where the system should use real world phrases and concepts familiar to the real world, rather than system specific terms. In order to make information appear in a natural and logical way we used a scroll menu to display the movies. We avoided the use of jargon, so any button or feature the user must interact with is in simple English. In addition, the ‘Contact Us’ page uses accordions so text appears logical rather than cluttering the page with long, technical terms.

User navigation and control is the third principle, where users need to be able to navigate the website easily with everything marked clearly – including the ability to undo actions and exit the site. To ensure smooth navigation, we implemented a navigation bar at the top of the website that includes hyperlinks to the webpages ‘Movies’, ‘View Basket’, ‘Contact us’, and ‘Log Out’. There is also an animated search bar for users who are looking for a specific movie. Furthermore, the navigation bar is retractable when scrolling, therefore is not in the way of the usability of the site, but reappears when the user begins to scroll up.

The next principle is guaranteed consistency and standards – conventions used should be familiar and the same across platforms, where actions are the same as seen on other websites. For example, we took inspiration from other successful movie streaming websites which use dark mode and displays the movies in a scroll carousel menu. Our website uses familiar conventions such as the navigation bar with the company logo in the top corner and website content being centralised. Everything on the site which is accessible is clickable, using listeners and buttons which appear bolder and change colour when a mouse hovers over them.

Error Prevention is a key principle, preventing errors from happening from the initial design. Errors are a focus usability target taking up 30% of interaction time. They should offer simple error handling with step by step instructions and permit easy reversal of actions. They need to be: explicit, visible, human-readable, precise and constructive. An example of how we minimise errors is through 'pop up' messages, which prompt the user that an error has occurred. For example, when entering banking details, the CVC must be in the correct format, and if it is entered incorrectly a pop up message telling the user the format it needs to be entered in comes up, therefore they are informative as well as preventing the user from repetitive mistakes.

Nielsen's sixth principle focuses on recognition, where the user should not have to remember any information from one part of the website to another and all actions should be accessible, visible and retrievable whenever they are needed. Users of our website experience continuity through the navigation bar which hyperlinks to the corresponding page so users don't have to remember previously viewed pages. The navigation bar features a search bar which allows users to retrieve information about the films, even if they are spelt incorrectly.

Both novice and experienced users should have efficient use of the website, where it caters to both. Therefore, users should be able to tailor their experience specific to their abilities. To allow users to have a flexible experience we have implemented user shortcuts within the movies page, where users can navigate the movies using the arrows left and right as well as key binding to the keyboard arrows, therefore users with different technical abilities and familiarities can operate the website. Furthermore, the implementation of the search bar creates a user shortcut for those familiar with the webpage to quickly navigate to the film they want.

The design of the website should be minimal and aesthetic, compliant to Nielsen's eighth principle. The website should not appear cluttered or contain irrelevant information that may diminish visibility, adhering to the principles of contrast, repetition, alignment and proximity. Focusing on the design of our website, we used a very dark grey background contrasting to salmon pink and white text which was consistently used across all pages. The format throughout the website stayed centralised and the layout is clear featuring 1 main film at a time, fading the background movies to not appear cluttered. A white shadow is prevalent behind the movies, with a glowing animation which moves with the navigation of the site further creating contrast - this is repeated for every single movie adhering to the principle of recognition and repetition. The alignment of the movies is landscape, displaying one movie at a time across the row - reducing clutter.

Recovery is a principle in which users can understand error messages in plain language and be able to recognise, diagnose and recover from the error. These error messages should contain a solution in order to be constructive. Our website error messages come up through pop-ups which contain information on how to resolve the error, for example on the payment processing page when you enter numbers that don’t meet the validation requirements, an error message states the correct layout to enter it in. Furthermore, a ‘404 Page Not found’ error page has been created which follows the page’s layout and tells the user how to fix the problem and navigate back to the main website.

Including a help and documentation page on the website which is easy to access and focused on user tasks in a readable, simple format. To apply this principle to our website we created a ‘Contact Us’ page which displays terms and conditions, our cookie policy, customer help-line and a FAQ section to answer user enquiries. The help section covers how to complete user tasks such as purchasing and paying for a film, whilst addressing concerns users may have, such as getting refunds if there was an issue with the movie and who to contact about this.

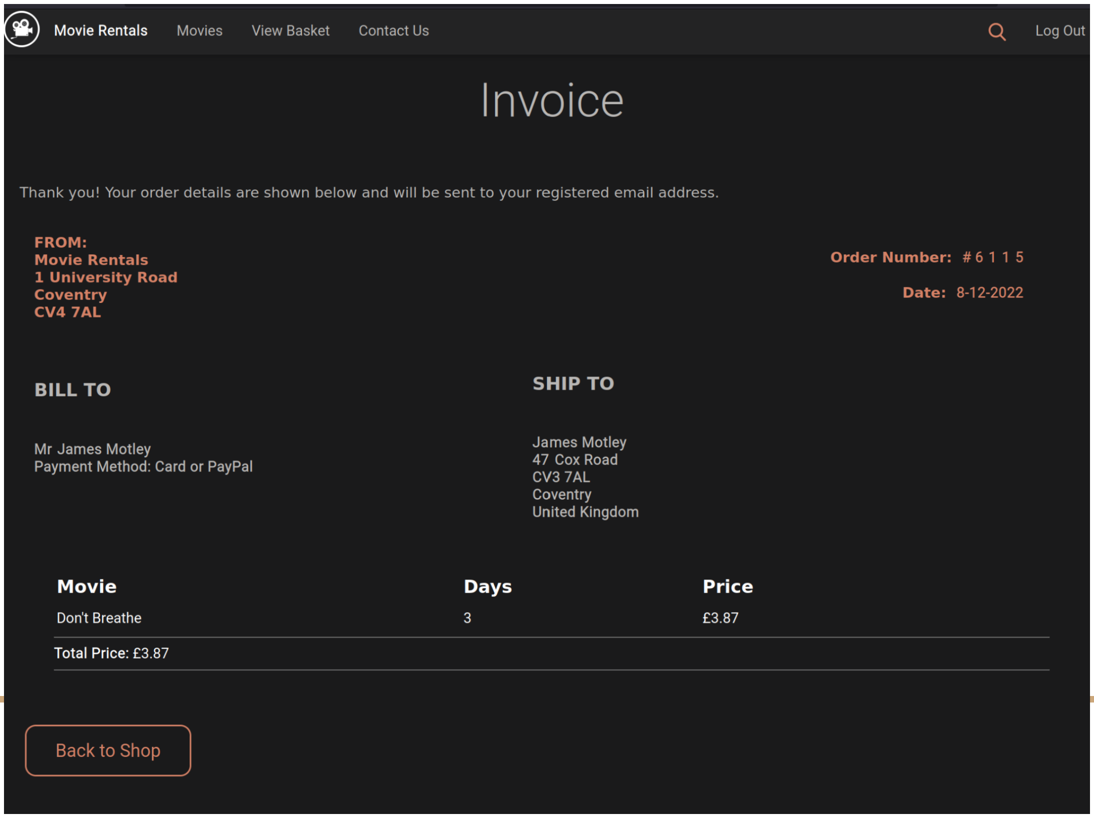
Nielsen’s principles have advantages and disadvantages, in which evaluators can focus on specific issues to work on whilst pinpointing faults with individual elements early on in the project to determine their impact on the user experience. Testing is easier against these principles, where users are not required. This reduces legal and ethical implications as well speeding up the process. In addition, this can be combined with usability testing to ensure the testing process is thorough. However, evaluators can view problems differently, resulting in subjectivity when determining the severity of problems and how quickly they need to be fixed.

Our Redesigned Prototype

Abigail

Invoice.html was redesigned to show the customer's order details. This allows them to check their order details and ensure there are no mistakes. They will also receive a copy of the invoice in their email inbox in case they have an issue with their order and need to retrieve an order number when communicating with customer service. The user can then click 'Back to Shop' if they wish to continue browsing movies.

As this is only a prototype, no email is sent. Alternatively, if the user wants to keep a paper copy of their invoice, they can press ctrl+p and they will be redirected to print their invoice off. However, if they are careless with the paper copy this could be a security implication as the invoice contains personal information such as their home address and order number.



Invoice

Thank you! Your order details are shown below and will be sent to your registered email address.

FROM:
Movie Rentals
1 University Road
Coventry
CV4 7AL

Order Number: #6115

Date: 8-12-2022

BILL TO

Mr James Motley
Payment Method: Card or PayPal

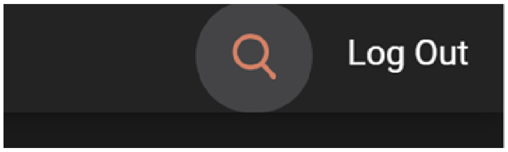
SHIP TO

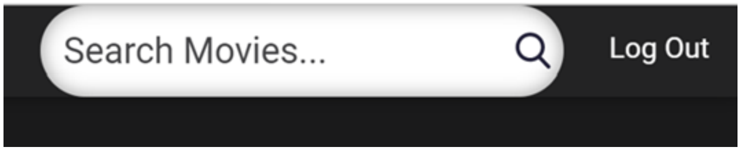
James Motley
47 Cox Road
CV3 7AL
Coventry
United Kingdom

Movie	Days	Price
Don't Breathe	3	£3.87

Total Price: £3.87

I implemented an animated search bar to improve website navigation for the user. The magnifying glass is an affordance, as it informs the user of a search tool. Affordances make the user's life easier as they support successful interactions with the world of physical things and virtual objects. There is also a placeholder that says "Search Movies" which gives the user more information about the function of the search bar.

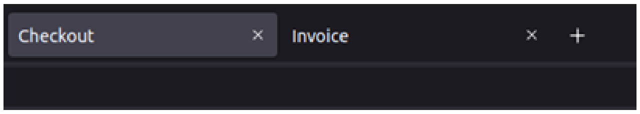


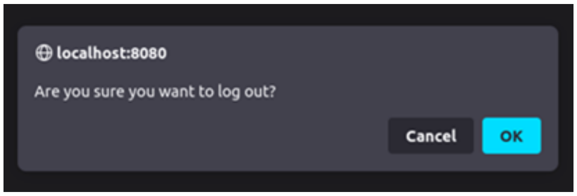


The search bar is animated because when the user clicks the magnifying glass, the search bar stretches out and a placeholder inviting the user to search for their desired movie becomes visible. This compacted search bar is ideal for all screen sizes including mobile phones as it doesn't take up much space when not in use. This follows the flexibility and efficiency heuristic and the minimalist design heuristic. Lastly, the search bar has a successful contingency design. This means that even if the user misspells the name of the movie, our search engine can still find it. For example, typing in 'paw patrool' still retrieves the movie 'Paw Patrol'.

I used a HTML form to collect the user's search input, send it to a web server and transfer the user to the web page that corresponds with the movie they searched. This is done using a GET request. However, browsers usually cache GET requests so if searching for sensitive information the GET request is not ideal as past searches will come up the next time the search bar is used. This can be avoided by using a POST request instead. Also, the user's input is sent to the web server in plaintext, but installing an SSL certificate to encrypt SSL traffic can secure the data being sent from HTML forms.

Some other contributions I made include looking around the website for issues I could fix. This included changing the HTML title element from movie rentals to a name which reflected the page, so the user could identify a page amongst several tabs which links to Nielsen’s 7th Heuristic of flexibility and efficiency of use. I also added a confirmation message that pops up when the user clicks ‘Log Out’ to prevent them accidentally logging out. This follows Nielsen’s 5th Heuristic which focuses on error prevention. I styled the buttons using css to make them more interactive for the user. The buttons look the same across the website which links to Nielsen’s 4th Heuristic on consistency and standards.





Are you sure you want to log out?

In line with Nielsen’s 8th Heuristic, I researched aesthetically pleasing websites and studied them to understand what makes a good design. As a result I decided a scroll carousel menu would be the best way to display the movies on our website.

Joel

Login.html, login.css, login.js

We identified many issues with the original login page, and it was not working in accordance with some of Nielsen's 10 principles. Firstly, there was no error prevention, and the login form allowed invalid data to be inputted. The login form would submit even if the fields contained no data. This is not good practice, as a customer may be unaware that they have entered incorrect information at login, and consequently may not be able to redeem a purchased movie.

To fix this I created several functions in JavaScript to monitor the input fields (using event listeners), that would display the appropriate error message and prevent the form from being submitted. This would happen if:

- Fields were left empty
- Invalid email address was entered
- Passwords do not match
- Username less than 4 characters

The error messages make it easy for the user to identify where they have entered incorrect information, and adhere to Nielsen's 5th principle.

The original login screen used ugly colours that made the site look dated and boring, and the layout didn't appear to be user friendly nor welcoming. This contradicts Nielsens 8th principle about aesthetics. The design also seemed unprofessional, and may give users the impression that the website is not legitimate and possibly untrustworthy.

I remedied these issues primarily with css. I reshaped and resized the boxes so to fill up more of the screen, which made the page much more pleasing to the eye. I also changed the colours, to make it appear much more vibrant and friendly whilst maintaining good readability. These colours match the rest of our website's pages, and this consistency makes the site appear professional.

I also created a separate screen for users without an existing account to create one. I believe this makes it much more straightforward to use, as this is the format that I most frequently encounter on other sites. This structure will be more familiar to the user.

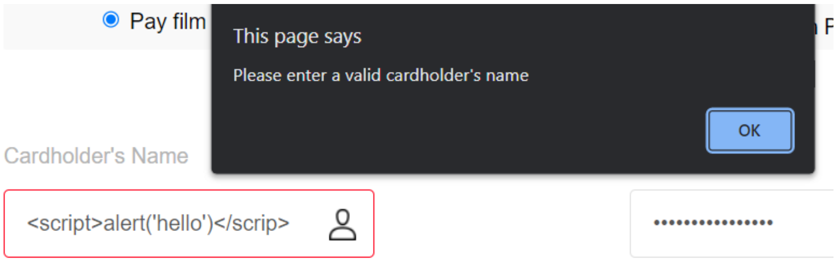
On the original, the sign-up button was redundant, and did not actually perform any action. I added additional features such as allowing users to choose a username, and also requiring the password to be entered twice during account creation to ensure that the user typed what they intended.

As for security, there should be a lot of consideration here as the login page deals with user credentials, which if leaked, could have huge consequences. There is the potential that users will have saved sensitive information such as credit card details to their account, and the leaking of this data would be a breach of the UK GDPR. However, storing account details of users was beyond the scope of this task, so there is currently no risk of any account details being leaked. However, if this feature was implemented in a future build, we would have to ensure that the passwords associated with usernames are properly hashed, and stored in a secure database. It would also be crucial to ensure that proper input sanitisation takes place in all input fields. This would be to prevent an SQL injection attack.

Niall

order.html, order.css, order.js, 404.html

No field validation/input sanitisation can lead to several types of web application based attacks, specified by the OWASP top 10, such as cross site scripting (XSS), SQL injections etc. which in turn can lead to user data exposure thus, violating UK GDPR. As can be seen in Figure 1, a mock XSS attack is rendered useless as the cardholder's name only accepts letters not characters; however without this the likelihood of experiencing one of these issues is significantly higher due to a lack of input sanitisation. To adhere to Nielsen's 5th principle, I implemented error messages which are informative and tell the user how to resolve the issue. For example, when a user enters the cardholder's name incorrectly, the error message relays "Please enter a valid cardholders name" which informs the user where the error occurred and how to remedy it. Additionally, I redesigned the input boxes allowing for dropdown menus for expiry date and country fields which also functions as a form of input sanitisation, meaning the user can only select valid input options and reduces the chances of an SQL injection into the field.



This page says

Please enter a valid cardholder's name

Cardholder's Name

<script>alert('hello')</scrip>

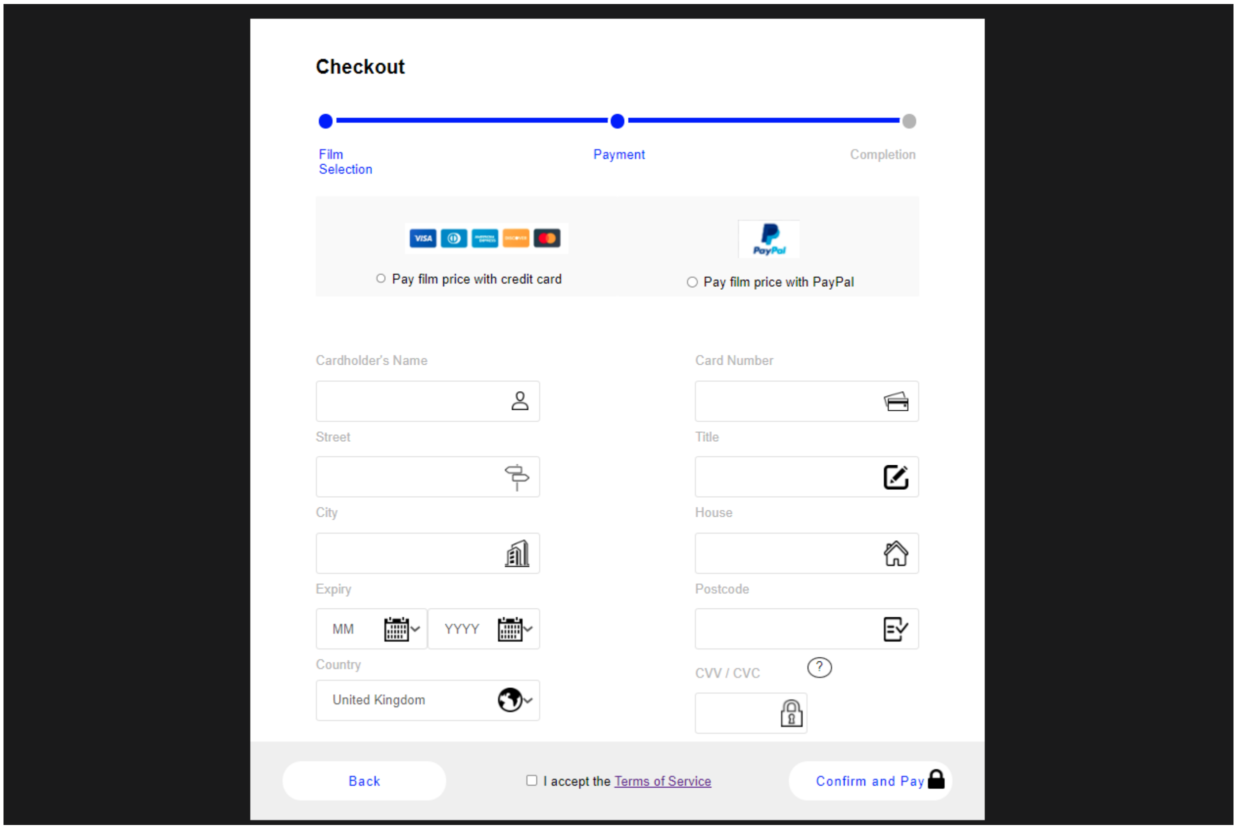
••••••••••••••••

Figure 1.

Further error handling was managed via a redesigned 404 error page, implementing the colour scheme through CSS to create consistency between pages. The page features a gif to create a user friendly experience and informative information on the error, as opposed to plaintext which doesn't explain the issue the user has encountered. Therefore, this applies to Nielsen's 5th Heuristic principle where suitable actions are explained to mitigate the error and provide explanatory solutions to the user.

The Issues featured on the former webpage feature:

- Lack of current system status which violates Nielsen's 1st usability characteristic
- No iconography which makes the user experience
- Lack of dropdown menus leading to no input sanitisation
- No visual icons for payment methods
- Lack of CSS animations for buttons which inform user's current cursor position
- Lack of aesthetics for the page (all entry fields are clumped together) this can alienate and confuse the user as there's no clear distinctions between different fields
- Font choice is not suited to the type of page, It looks unprofessional and the font is not as concise as other styles
- The page is unscalable meaning it is unable to be loaded on other platforms for example mobile devices and smaller computer screen resolutions

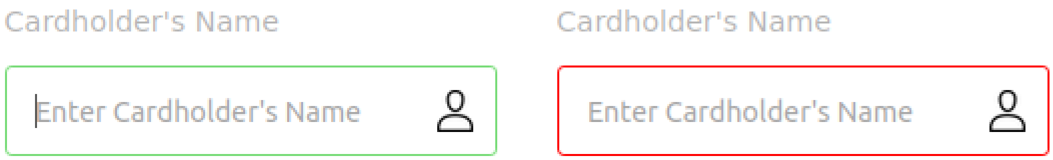


Country: United Kingdom

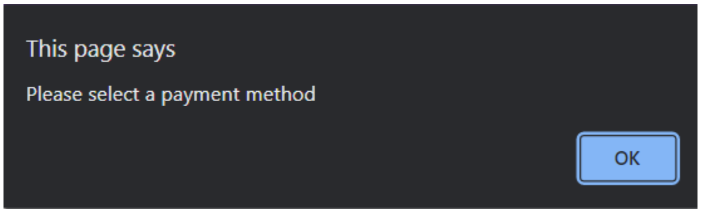
To counteract this, I redesigned the checkout.html webpage, as seen above, to adhere to Nielsen's 8th principle, redesigning the webpage to a cleaner more efficient user interface allowing for icons alongside every field. Using Neilsen's 1st usability principle the system status, not previously apparent on the webpage, has now been implemented at the top of the page allowing for users to understand where they are in the movie rental process. To represent what stage in the process the user is at, I implemented a graphical bar with the headers "film selection", "payment" and "complete" adhering to Neilsen's first principle, where system status is readily available to the user.

To adhere to Neilsen's 8th principle, I redesigned the webpage's aesthetics to appear more minimal and coherent through CSS, changing the input style of the text boxes and adding graphic icons to make the user interface appear more friendly, summarising the information a user should input, further reinforcing the content to be entered into the field. The payment process graphics were also altered, allowing the user to select between card payment types and PayPal, using their proprietary icons.

The user's current position is now reflected by highlighting the input fields in green and when the data is invalid these fields are highlighted in red as seen below this following Nielsen's 5th Heuristic which informs the user about their errors.



The user also is provided with appropriate popup messages dependant on their error, seen below, also following Neilsens 5th Heuristic. These pop ups were not originally present on the original site.

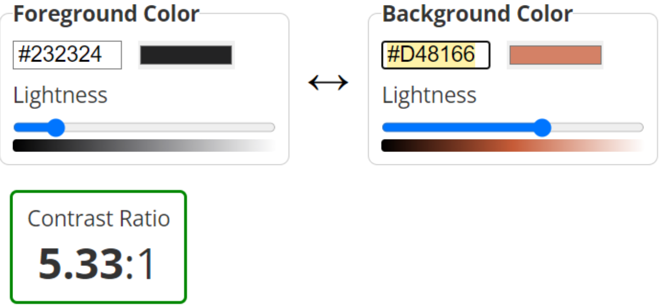

This page says

Please select a payment method

Rosie

The entire webpage needed to be redesigned in correspondence with Nielsen's Third Principle - user navigation and control. In order to do this, I implemented a top navigation bar which allowed for easier navigation of the website - this includes moving to and from: movies.html, basket.html, shop.html, login.html & about.html. This improves user experience and makes the webpage generally easier to understand and navigate, as dictated by Nielsen. As well as this, the navigation bar features highlighted sections for the web page the user is currently on, as well as highlighting areas when they are hovered over with a mouse pointer - this further helps to coincide with principles of user navigation and control.

Furthermore, Nielsen’s Fourth principle dictates websites should have guaranteed consistency and standards. I helped to follow this by including a company logo in the top corner of the navigation bar, which is consistent with other similar websites, ie. Netflix. Furthermore, as a group we agreed on and implemented a ‘dark mode’ theme for our website, this again is consistent with other similar pages like Netflix and Amazon Prime - this makes it more familiar to users and therefore more usable.



Foreground Color #232324

Background Color #D48166

Contrast Ratio 5.33:1

I also considered other accessibility needs, for example, the colour scheme chosen also allows for greater accessibility - for example, all colours chosen follow a ‘3:1’ ratio (WebAIM (2019)), meaning they are clear for users who may have difficulty distinguishing colours or are hard of sight. In our project, the Salmon Accent/Text colours have a ratio of 5.33:1, meaning it greatly exceeds the necessary minimum of ‘3:1’.

Furthermore, it follows WGAC AA for normal text, graphical objects and user interface components, as well as WGAC AA & WGAC AAA for large text. WGAC “covers a wide range of recommendations for making Web content more accessible. Following these guidelines will make content accessible to a wider range of people with disabilities, including blindness and low vision, deafness and hearing loss, learning disabilities, cognitive limitations, limited movement, speech disabilities, photosensitivity and combinations of these" (Caldwell et al., 2008)

The font chosen was Geneva, I chose this on account of its accessibility for those with dyslexia - this is mainly due to its clear shapes and spacing (making it easier to read). Furthermore, Geneva is the chosen font for websites such as Facebook.com, this is because it allows for internal white space, differentiation of letter forms and greater legibility. This therefore improves the accessibility of our website to those who may struggle with reading or those who have issues with vision.

Finally, I created about.html, which allows users to find contact details for the web page as well as a terms of service and cookies policy. Despite the fact that the website does not currently use cookies, it felt necessary to emulate other similar websites. Furthermore, a terms of service allows for greater overall security, as it means the allowed terms are listed clearly for users and actions can be taken if these were to be broken, ie. account termination.

Sarah

The 'Contact Us' page has been re-designed to feature 4 'accordions', which are retractable text boxes with a bold header, and information which is concealed until the user clicks on it. These are titled 'Terms and Conditions', 'Cookie Policy', 'FAQ and Help Page' and 'Contact Us'. These were created using Javascript, HTML and CSS.

The introduction of 'Terms and Conditions' and 'Cookie Policy' create a more informative experience for the user, outlining the legal implications of using our website, which is common for a user to see when browsing and purchasing online, these contain technical jargon which a novice user would be unfamiliar with. Therefore, putting this information into an accordion fulfils Nielsen's 2nd principle to make information appear in a logical way, using concepts and phrases familiar to the real world. This is reinforced when using terms such as 'FAQ' where the user will associate the acronym with 'Frequently Asked Questions' and know where to locate help. The data used within these conditions was collected by Rosie, who initially did research and designed the page before it was updated to fit design principles.

Nielsen’s third principle is adhered too with this, where they can navigate the accordion with the ‘+’ to expand the box and ‘-’ to reduce the size of it, therefore not cluttering the page with excess information the user does not need to see, also complying to design principles about remaining minimalistic and aesthetic. To further observe the design principles, the boxes are rounded with clear sans-serif font and headers are in a bolder, larger text to be distinct.

Furthemore, the ‘FAQ and Help Page’ complies to Nielsen’s 10th principle which is to include a help page which is easy to find and focuses on questions a user may have when visiting our website, such as how to complete tasks like selecting a film or how to purchase a film, this then creates an accessible experience for users of different difficulty levels.

The movie page was edited on ‘movies.js’ where I added HTML and JavaScript to edit the descriptions of the film, which were either invalid (contained filler information irrelevant to the film) or information which was not detailed enough to give the user a good understanding of the film. The descriptions are now updated to be relevant, and I added a class in JavaScript to update the age certification of the film onto the webpage which is visible when a user clicks ‘View Movie’ to adhere to Nielsen’s 8th principle.

Seb

Outside of usability contributions, I established an initial web service infrastructure on which we could host our site. *Lighttpd* was chosen as a web server due to its lightweight nature,

- Setup lighttpd webserver.
- Setup SSH for all users.
- Created automated website-updater script (*update-website*).

1. **Within basket.html**:
    1.1. Update broken hyperlink "Continue Shopping" to navigate to "shop.html".
    1.2. Improve style for readability and consistency with the rest of the website.
    1.3. "Clear Basket" refreshes page for visual feedback.

    1.4. Rounding errors solved and appropriate units added to field values.
    1.5. Alert generated if user attempts to pay for nothing.
    1.6. Padded prices with 0s where required.

2. **Within shop.html** (renamed to shopRevamp.html):
    2.1. Movie list generation is now dynamic and based on the *movies* object, allowing new movies to be easily added to the catalogue.
    2.2. Developed interactive, lateral view of movies similar to those found in games consoles.
    2.3. Positioned movie details directly under each movie.
    2.4. Padded movie prices with 0s where required.
    2.5. Added keyboard shortcuts for advanced users.
    2.6. Added overlay for selection of days to rent.
    2.7. Added errors for too many days requested, or an invalid number.
    2.8. Added constraints to the ‘days to rent’ to prevent invalid values.
3. **Within about.html**:
    3.1. Tweaked visuals of accordion menus to be more user-friendly.
4. **Additions to the search bar**:
    4.1. Visual tweaks to animations.
    4.2. Rely on movies object so that new movies can easily be added
    4.3. Search predictions displayed as user types.
    4.4. Search results navigate to the shop.
5. **Additions to the navigation bar**:
    5.1. Improve visual feedback on hover.
    5.2. Add indication of current page.
    5.3. Made the navbar hide while scrolling down the page.

I will now discuss how my contributions relate to the Nielsen usability heuristics.

Section 2: Within shop.html

Nielsen’s fourth principle of consistency and standards is enforced by the CSS style sheet being applied to all webpages, with the movie details being moved into an accordion below the film using the same colour scheme and similar drop down menus as used within the Contact Us page, consistent across the website.

Nielsen’s second principle is adhered to with the implementation of the scroll menu to display the movies in a landscape row, using arrows which are key-binded to the arrow keys on the user keyboard to navigate through the films. This means the movies are in a logical, natural order reminiscent of common user interfaces found in games consoles, for example. The seventh usability principle is enforced via the keyboard shortcuts, such as the arrow keys and enter key to view movie details, included in this page, allowing frequent users to learn how to make efficient use of the site.

This also adheres to Nielsen’s third principle of navigation, where a user can navigate through the site using two different means, and navigation is marked clearly through the large arrows on either side - acting as an affordance.

Contribution 2.6 removes clutter from the interface by transferring rental options to a popup overlay, improving the site’s conformance to Nielsen’s 8th principle which encourages minimalism.

Examples of Nielsen’s 5th and 9th principles arise from contribution 2.7 and 2.8, since this prevents errors and provides possible solutions.

Section 4: Additions to the Search Bar

The introduction of a search bar by Abigail helped to fulfil Nielsen’s 3rd Principle of User Navigation and Control. I further contributed to this by adding search predictions displayed as the user types, as well as search results navigating to the shop. These help to increase the usability of the site by fulfilling this principle of user navigation and control, for example search predictions help users to not only find the movies they are looking for, but also see what is available (and so therefore helping to fulfil the idea of error prevention, as users will not search for movies which are not provided). Furthermore, this follows the conventions of other similar websites such as Netflix and Amazon (and so therefore the 4th Principle of guaranteed consistency and standards), therefore further increasing usability.

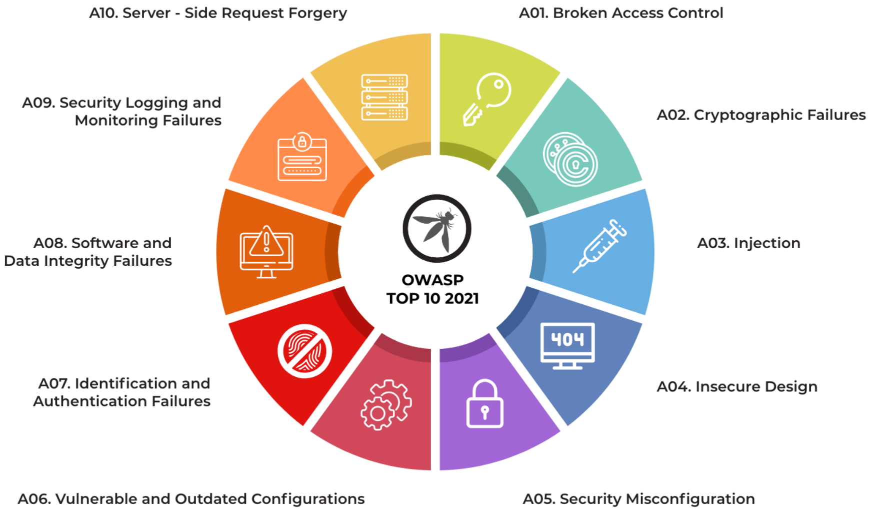
Furthermore, search results navigating to the shop page allows users to easily navigate the website, fulfilling Nielsen's 3rd principle of User Navigation and Control.

Section 5: Additions to Navigation Bar

The navigation bar has been changed, which is now retractable when the user scrolls down the webpages, adhering to Nielsen's third principle therefore not affecting usability of the website or cluttering the top of the webpage when you scroll through the contact page. To adhere to Nielsen's 8th and 1st principle, when a user hovers over the hyperlinked webpage they wish to navigate to the colour of the text change, consistent with the colour scheme across the site whilst increasing visibility of the system status as the user knows where their mouse is on the page and the page they will navigate towards next.

Recommendations On Security Requirements

The following table shows the OWASP top ten security risks facing web applications for the year 2021. By analysing each threat, specific security recommendations for our movie rental website can be made with the assumption that it would in future operate in a production environment.


A10. Server - Side Request Forgery
A01. Broken Access Control
A09. Security Logging and Monitoring Failures
A02. Cryptographic Failures
A08. Software and Data Integrity Failures
OWASP TOP 10 2021
A03. Injection
404
A07. Identification and Authentication Failures
A04. Insecure Design
A06. Vulnerable and Outdated Configurations
A05. Security Misconfiguration

(OWASP, 2021)

OWASP Ranking	Description
1. Broken Access Control (A01:2021).	A weakness that allows an attacker to gain access to user accounts - The attacker in this context can function as a user or as an administrator in the system.
2. Cryptographic Failures (A02:2021).	Cryptographic failures occur when important stored or transmitted data (such as a social security number) is compromised.
3. Injection (A03:2021).	A code injection occurs when invalid data is sent by an attacker into a web application in order to make the application do something it was not designed to do.
4. Insecure Design (A04:2021).	Focuses on risks related to design flaws. As organisations continue to “shift left,” threat modelling, secure design patterns and principles, and reference architectures are not enough.
5. Security Misconfiguration (A05:2021).	Security misconfigurations are design or configuration weaknesses that result from a configuration error or shortcoming.
6. Vulnerable and Outdated Components (A06:2021).	Related to components that pose both known and potential security risks, rather than just the former. Components with known vulnerabilities, such as CVEs, should be identified and patched, whereas stale or malicious components should be evaluated for viability and the risk they may introduce.
7. Identification and Authentication Failures (A07:2021).	Includes CWEs related to identification failures. Specifically, functions related to authentication and session management, when implemented incorrectly, allow attackers to compromise passwords, keywords, and sessions, which can lead to stolen user identity and more.
8. Software and Data Integrity Failures (A08:2021).	Focuses on software updates, critical data, and CI/CD pipelines used without verifying integrity. Also now included in this entry, insecure deserialization is a deserialization flaw that allows an attacker to remotely

	execute code in the system.
9. Security Logging and Monitoring Failures (A09:2021).	Logging and monitoring are activities that should be performed on a website frequently—failure to do so leaves a site vulnerable to more severe compromising activities.
10. Server-Side Request Forgery (A10:2021).	A new category this year, a server-side request forgery (SSRF) can happen when a web application fetches a remote resource without validating the user-supplied URL. This allows an attacker to make the application send a crafted request to an unexpected destination, even when the system is protected by a firewall, VPN, or additional network access control list. The severity and incidence of SSRF attacks are increasing due to cloud services and the increased complexity of architectures.

(OWASP, 2021)

Security misconfigurations can be avoided by coding securely and using best practices to ensure no vulnerabilities stem from the source code. Cross site scripting (XSS) raises security risks for web applications, therefore secure coding practises for all languages should be adopted, before testing the product and releasing it. With JavaScript, you can achieve more secure code by validating and sanitising inputs to ensure only acceptable characters can be input into the webpage that cannot launch XSS attacks.Furthermore, using the 'innerText' property within the DOM to return the content without CSS style elements and any scripts protects the program from DOM-based XSS attacks, in which the OWASP classifies this attack to have moderate potential consequences (Hollander, 2020). To ensure HTML security, HTML encryption can be incorporated alongside the use of digital certificates to validate our domain.

To mitigate SQL injections, input validation is also vital whilst using parameterized queries and prepared statements instead of concatenations. Prepared statements ensure an attacker cannot change the intent of the query, although this can harm performance. Our website needs to take user input to complete purchases, therefore where limiting validation to list-only input would reduce attack likelihood, this is not practical. However, it can be used for some elements such as selecting dates or numerical values.

Insecure design is prevented from following design principles and having all developers follow the same rules and best practices when working on the web application. Following heuristics not only increases usability, but prompts users to act accordingly on the website - navigating through common conventions rather than clicking around and accidentally exploiting unknown vulnerabilities.

References

Caldwell, B., Cooper, M., Guarino Reid, L. and Vanderheiden, G. (2008). Web Content Accessibility Guidelines (WCAG) 2.0. *WGAC*. [online] Available at: https://www.w3.org/TR/WCAG20/ [Accessed 4 Dec. 2022].

Hollander,M. (2020). Most Common Security Vulnerabilities Using JavaScript. [online] SecureCoding. Available at: https://www.securecoding.com/blog/most-common-security-vulnerabilities-using-javascript/ [Accessed 30 Nov. 2022].

Nielsen, J., 1995. How to conduct a heuristic evaluation. Nielsen Norman Group, 1(1), p.8.

OWASP (2021). OWASP Top Ten. [online] Owasp.org. Available at: https://owasp.org/www-project-top-ten/. [Accessed 30 Nov. 2022].

Shneiderman, B. (1998). Designing the user interface: Strategies for effective human (3rd ed.). Boston, MA: Addison Wesley Longman, Inc.

WebAIM (2019). *WebAIM: Contrast Checker*. [online] Webaim.org. Available at: https://webaim.org/resources/contrastchecker/.