

ISO4 – Testen

Opdracht 1

How To Break Software



Getests: NVU

Module: ISO4 Informatica Systeem Ontwikkeling 4 - Testen

Student: Herman van der Meulen

Studentnr.: s1013123

Docent: Eric van Wessel

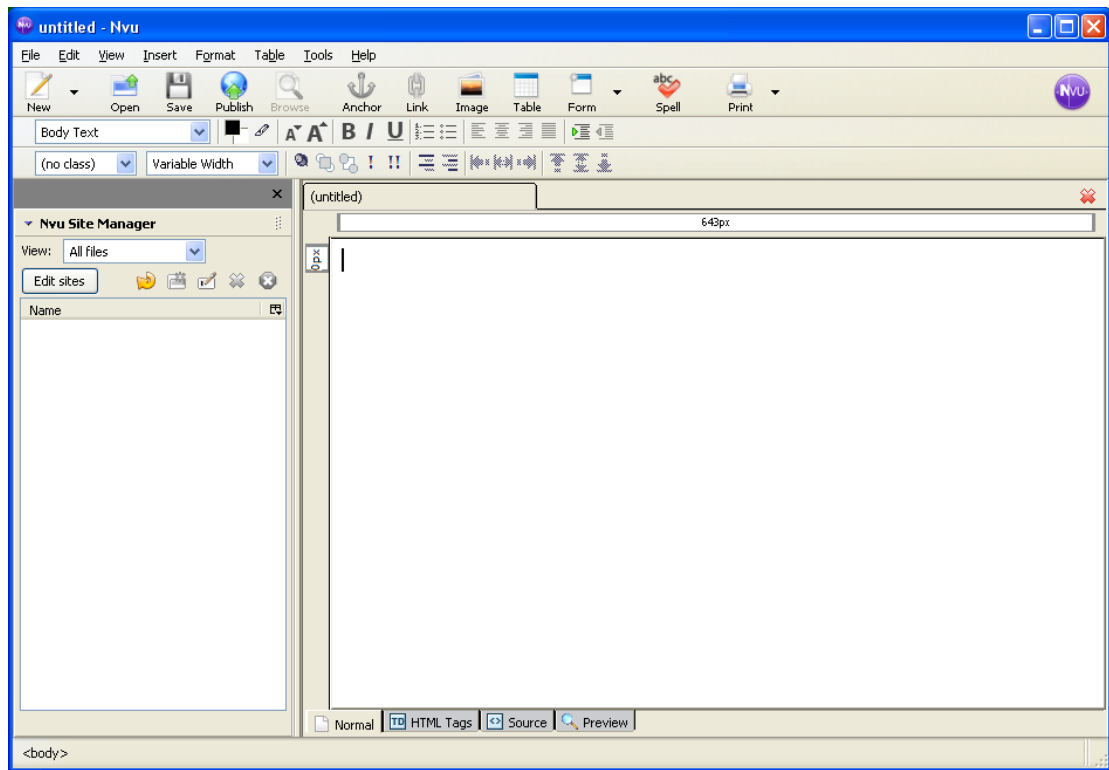
Inhoudsopgave

Geteste applicatie	3
User interface attacks	4
Attack 1 – Apply inputs that force all error messages to occur	4
Test 1.1: Afbeelding invoegen	4
Test 1.2: Afbeelding invoegen, met bepaalde grootte	5
Test 1.3: Tabel invoegen, groter dan 100%	7
Test 1.4: Formulier met ‘onzin’ action invoegen	9
Attack 2 – Apply inputs that force the software to establish default values	10
Test 2.1: Auteur voor nieuwe pagina, default testen	10
Attack 3 – Explore allowable character sets and data types	11
Test 3.1: Auteur voor nieuwe pagina, HTML code in de naam	11
Attack 4 – Overflow input buffers	12
Attack 5 – Find inputs that may interact and test combinations of their values	13
Test 5.1: Tabel invoegen met veel rijen en kolommen	13
Attack 6 – Repeat the same input or series of inputs numerous times	14
Test 6.1: Meerdere genaamde ankers met dezelfde naam	14
Attack 7 – Force different outputs to be generated for each input	16
Niet uit te voeren, uitgebreide documentatie nodig voor te verwachten outputs bij inputs ..	16
Attack 8 – Force invalid outputs to be generated	17
Test 8.1: Directe body tekst is niet valide (x)html	17
Attack 9 – Force properties of an output to change	18
Test 9.1: Achteraf veranderen van afbeelding	18
Attack 10 – Force the screen to refresh	19
Test 10.1: Controls voor aanpassen van de grootte van elementen	19
Attack 11 – Apply inputs using a variety of initial conditions	21
Test 11.1: Verplaatsen van elementen gebruikmakend van layers	21
Test 11.2: Element verslepen met muis eerst buiten de ‘viewport’	23
Attack 12 – Force a data structure to store too many or too few values	24
Test 12.1: Zeer grote textarea invoegen	24
Attack 13 – Investigate alternative ways to modify internal data constraints	25
Attack 14 – Experiment with invalid operand and operator combinations	26
Test 14.1: Invoegen van tabel, wisselen van ‘view’	26
Attack 15 – Force a function to call itself recursively	27
Test 16.1: Zeer grote marges bij paginainstellingen	28
Attack 17 – Find features that share data or interact poorly	31
Test 17.1: Tabel eigenschappen, breedte veranderen	31
System Interface Attacks	32
Attack 1 – Fill the file system to its capacity	32
Test 1.1: Opslaan bij volle disk	32
Attack 2 – Force the media to be busy or unavailable	33
Test 2.1: Nieuw bestand als onmogelijk door file system	33
Attack 3 – Damage the media	35
Test 3.1: Bestand laden van beschadigde CD	35
Attack 4 – Assign an invalid file name	37
Test 4.1: Tekstbestand openen in plaats van HTML	37
Attack 5 – Vary file access permissions	38
Test 5.1: Opslaan van een ‘alleen-lezen’ bestand	38
Attack 6 – Vary or corrupt file contents	40
Test 6.1: Corrupte afbeelding invoegen	40
Urenverantwoording	42

Geteste applicatie

De applicatie die getest zal worden heet 'NVU'

Wikipedia: *"Nvu (spreek uit: "N-view") is een WYSIWYG-webpagina-editor, gebaseerd op de Composer uit Mozilla. Het wordt soms gezien als de open source tegenhanger van gesloten software als Microsoft FrontPage en Macromedia Dreamweaver."*



screenshot van NVU startscherm

Met NVU kan op een visuele manier websites gemaakt worden.

User interface attacks

Attack 1 – Apply inputs that force all error messages to occur

Test 1.1: Afbeelding invoegen

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar.

Handelingen

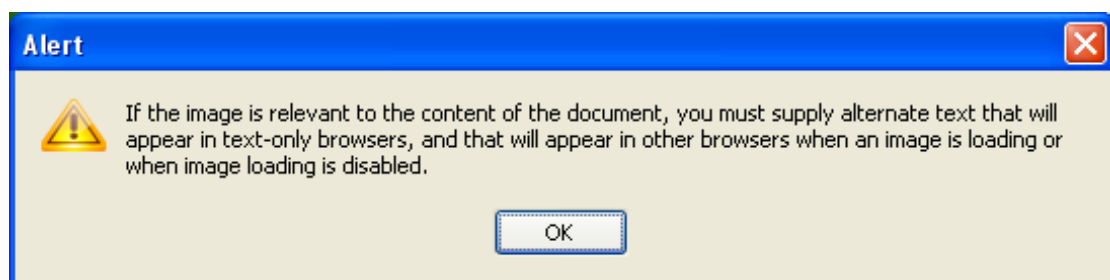
1. Klik op 'Insert', 'Image'
2. Vul een image location in
3. Vul GEEN ALT tekst in
4. Druk op 'OK'.

Verwachte gedrag

Ik verwacht dat de applicatie waarschuwt over de niet ingevulde ALT tekst.

Daadwerkelijke gedrag

De applicatie waarschuwt over de vergeten ALT tekst, zoals in onderstaande screenshot.



Conclusie

Er wordt goed gewaarschuwd voor de niet ingevulde ALT tekst. De gebruiker had trouwens ook kunnen kiezen voor het niet gebruiken van de ALT tekst. Dan komt de waarschuwing niet.

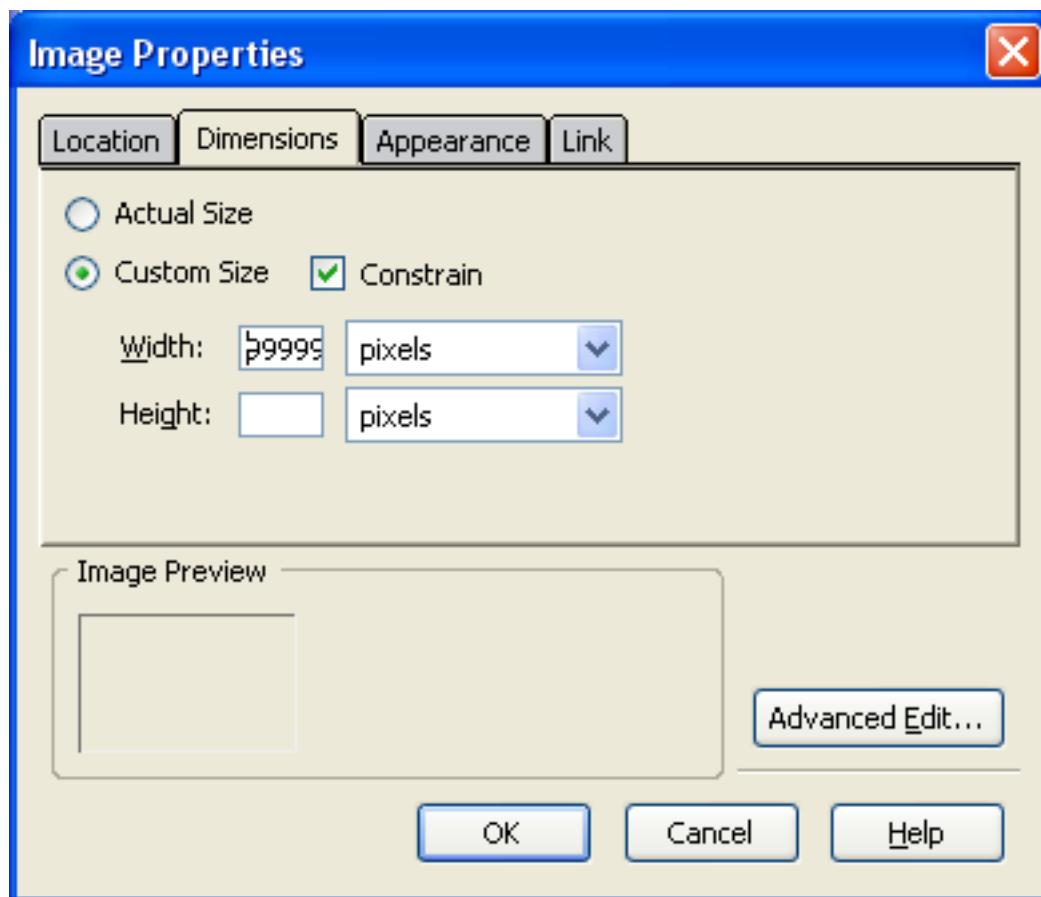
Test 1.2: Afbeelding invoegen, met bepaalde grootte

Uitgangssituatie

De applicatie is gestart, het beginscherf is zichtbaar.

Handelingen

1. Klik op 'Insert', 'Image'
2. Vul een image location in
3. Vul een ALT tekst in
4. Ga naar de tab 'Dimensions'
5. Kies 'Custom Size'
6. Kies voor de 'Width' de waarde: 999999

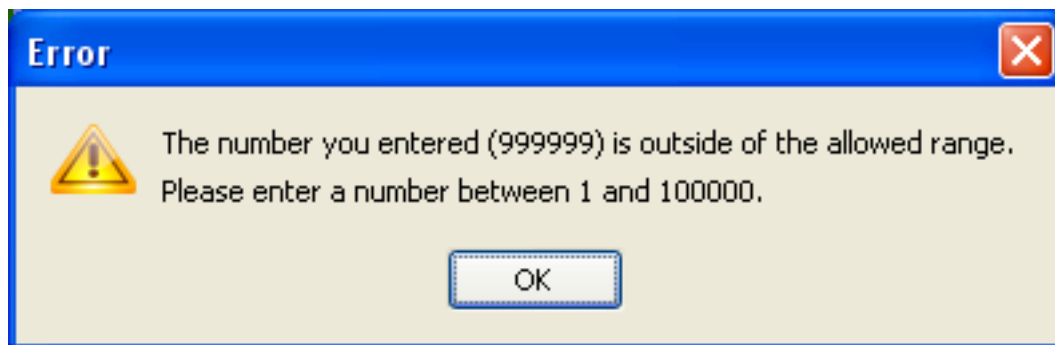


Verwachte gedrag

Ik verwacht dat de applicatie gewoon de afbeelding toevoegd met de 'width' attribuut op 999999px.

Daadwerkelijke gedrag

De applicatie heeft blijkbaar een maximum voor de dimensies van een afbeelding van 1 – 100000 pixels. Vreemd, want via andere wegen (direct wijzigen van de source) is dit wel te doen.



Conclusie

In de GUI zit een beperking van de breedte en hoogte van een afbeelding invoegen. Dit terwijl deze beperking er eigenlijk niet is. In de source kan een breedte en hoogte ingesteld worden tot maximaal 1000000.

Trouwens, alle velden van de applicatie waar een integer wordt gevraagd lijken beperkt tot een invoer tot maximaal 100000.

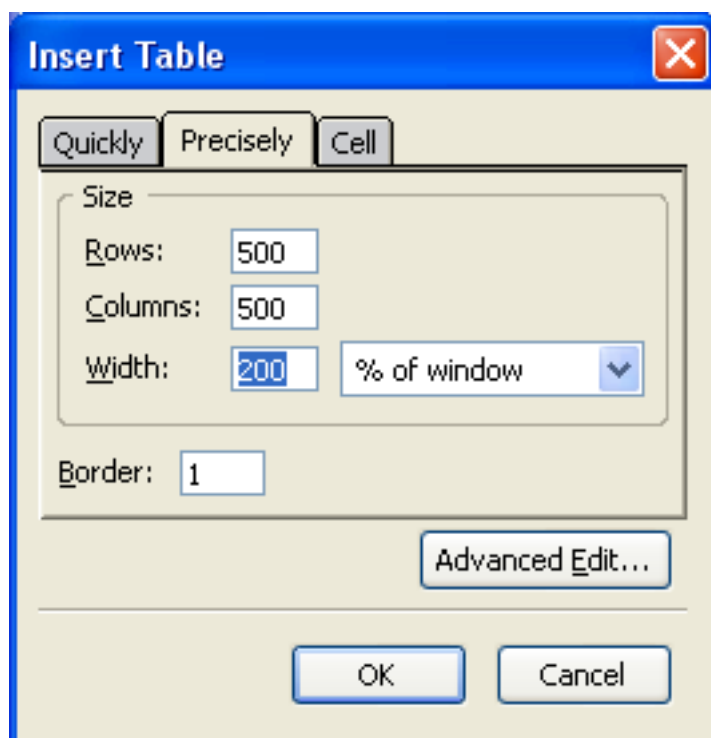
Test 1.3: Tabel invoegen, groter dan 100%

Uitgangssituatie

De applicatie is gestart, het beginscherf is zichtbaar.

Handelingen

1. Klik op 'Insert', 'Table'
2. Ga naar de tab 'Precisely'
3. Kies voor de 'Width' de waarde: 200
4. Klik op 'OK'

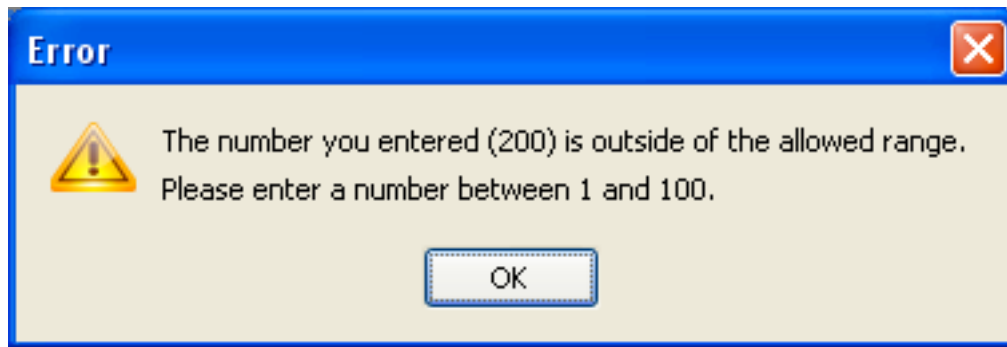


Verwachte gedrag

Ik verwacht dat de applicatie gewoon de tabel invoegd met een breedte van 200%.

Daadwerkelijke gedrag

De GUI van de applicatie heeft blijkbaar een maximum voor de dimensies van een tabel van 1 - 100 procent. Vreemd, want via andere wegen (direct wijzigen van de source) is dit wel te doen.



Conclusie

In de GUI zit een beperking van de breedte van een tabel invoegen, als er gekozen worden voor een percentage. Dit terwijl deze beperking er eigenlijk niet is. In de source kan een breedtepercentage ingesteld worden tot maximaal 10.000.000% (1^{e+7}%)

Test 1.4: Formulier met 'onzin' action invoegen

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar.

Handelingen

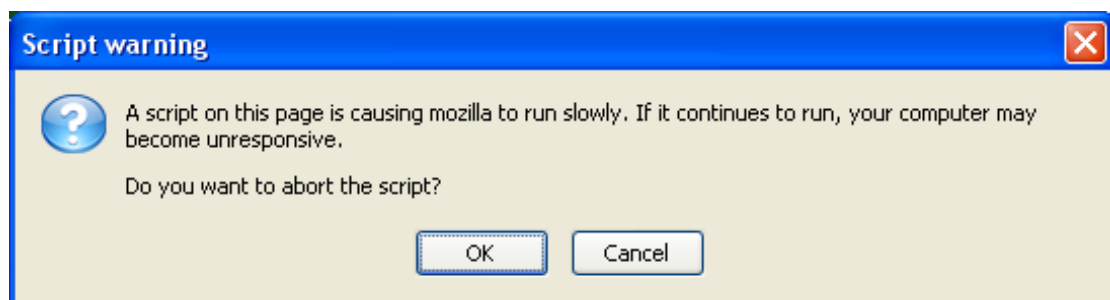
1. Klik op 'Insert', 'Form', 'Define Form'
2. Kies voor het veld 'Action URL' de waarde 'a'
3. Klik op 'OK'

Verwachte gedrag

Ik verwacht dat de applicatie gewoon het formulier toevoegd met de action attribuut met de waarde 'a'.

Daadwerkelijke gedrag

De applicatie lijkt te 'hangen'. Er wordt na 5-6 seconden van 100% cpu gebruikt gewaarschuwd dat er een script 'hangt'. Zie afbeelding hieronder.



Conclusie

Geen idee waarom, maar het invullen van een blijkbaar verkeerde 'action url' is in de GUI mogelijk, maar zorgt ervoor dat de applicatie 'hangt'.

Attack 2 – Apply inputs that force the software to establish default values

Test 2.1: Auteur voor nieuwe pagina, default testen

Uitgangssituatie

De applicatie is gestart, het beginscherf is zichtbaar.

Handelingen

1. Klik op 'Tools', 'Preferences'
2. Ga naar de tab 'New Page Settings'
3. Vul bij 'Author' in: 'Herman van der Meulen'
4. Klik op 'OK'
5. Sluit de huidige pagina, waardoor een nieuwe pagina wordt aangemaakt.
6. Bekijk de bron. Meta tag met author is aangemaakt met de juiste waarde
7. Herhaal bovenstaande stappen, maar bij stap 3, vul niks in.
8. Bekijk de bron. Meta tag met author wordt niet meer toegevoegd.

Verwachte gedrag

Ik verwacht dat de applicatie met de default (= leeg) gewoon geen metatag author weergeeft en als ik wel iets invul dan wel.

Daadwerkelijke gedrag

Zoals verwacht.

Conclusie

Op deze plek is het goed geïmplementeerd mbt "declare, assign en use" van de variabele. De default is gecodeerd als een lege string voor het preferences paneel, maar betekent het niet toevoegen van de meta tag in de pagina.

Attack 3 – Explore allowable character sets and data types

Test 3.1: Auteur voor nieuwe pagina, HTML code in de naam

Uitgangssituatie

De applicatie is gestart, het beginscherf is zichtbaar.

Handelingen

1. Klik op 'Tools', 'Preferences'
2. Ga naar de tab 'New Page Settings'
3. Vul bij 'Author' in: 'Herman</html>'
4. Klik op 'OK'
5. Sluit de huidige pagina, waardoor een nieuwe pagina wordt aangemaakt.
6. Bekijk de bron.

Verwachte gedrag

Ik verwacht dat de applicatie de HTML tekens vervangt door andere tekens om fouten in de gemaakte HTML pagina te voorkomen.

Daadwerkelijke gedrag

Zoals verwacht worden de HTML tekens in de string vertaald naar alt codes. De string wordt dan:

herman</html>

Conclusie

De applicatie vertaalt de HTML tekens goed, zodat de string gebruikt kan worden in de pagina. Hier is dus goed op gelet.

Attack 4 – Overflow input buffers

Al uitgevoerd, zie test 1.2

Attack 5 – Find inputs that may interact and test combinations of their values

Test 5.1: Tabel invoegen met veel rijen en kolommen

Uitgangssituatie

De applicatie is gestart, het beginscherf is zichtbaar.

Handelingen

1. Klik op 'Insert', 'Table'
2. Ga naar de tab 'Precisely'
3. Vul in bij rows en columns beide 299

Verwachte gedrag

Ik verwacht dat de applicatie gewoon een tabel aanmaakt van 299 bij 299 groot.

Daadwerkelijke gedrag

Zoals verwacht, maar het duurt wel heeeeel erg lang, een paar minuten in dit geval.

Conclusie

De applicatie kan omgaan met behoorlijk grote tabellen, maar wordt daardoor wel onbruikbaar langzaam. Het maximum aantal rijen en kolommen is hierdoor ook bijna niet te bepalen!

Attack 6 – Repeat the same input or series of inputs numerous times

Test 6.1: Meerdere genaamde ankers met dezelfde naam

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar.

Handelingen

1. Klik op 'Insert', 'Named Anchor'
2. Geef het anker de naam 'test'
3. Klik op 'Insert', 'Named Anchor'
4. Geef het anker de naam 'test2' (zelfde naam geeft waarschuwing/foutmelding)
5. Verander in de broncode van de pagina de string 'test2' naar 'test'
6. Klik op 'Insert', 'Named Anchor'
7. Geef het anker de naam 'test'

Verwachte gedrag

Ik verwacht dat de applicatie blijft waarschuwen dat er al een anker is met dezelfde naam.



Daadwerkelijke gedrag

Nadat 'test2' naar 'test' is gewijzigd in de bron van de pagina, mag er gewoon weer een 'test' anker aangemaakt worden via de GUI. Dit zou niet mogen.

```
1. <!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
2. <html>
3. <head>
4.   <meta
5.     content="text/html; charset=ISO-8859-1"
6.     http-equiv="content-type">
7.   <title></title>
8. </head>
9. <body>
10.  <a
11.    name="test"></a><a
12.    name="test"></a>
13. </body>
14. </html>
```

Conclusie

De applicatie controleert blijkbaar niet de broncode die net is aangepast. Daardoor mag er via de GUI gewoon een anker worden aangemaakt met een naam die dus al wel voor komt in de broncode van de pagina, maar nog niet is doorgevoerd naar de 'ontwerpview' van de pagina. De controle zou dus ook aan de hand van de broncode gedaan moeten worden.

Attack 7 – Force different outputs to be generated for each input

Niet uit te voeren, uitgebreide documentatie nodig voor te verwachten outputs bij inputs.

Test 6.1 geeft wel verschillende outputs bij dezelfde input. 6.1 zou dus ook onder deze attack kunnen staan.

Attack 8 – Force invalid outputs to be generated

Test 8.1: Directe body tekst is niet valide (x)html

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar.

Handelingen

1. Typ het een woord, bijvoorbeeld 'test' in de editor
2. Sla het document op, naam bijvoorbeeld test.html

Verwachte gedrag

Ik verwacht dat de applicatie netjes een nieuwe alinea aanmaakt voor het getypte woord, zodat het in een element binnen de body komt te staan.

Daadwerkelijke gedrag

De applicatie plaatst de getypte tekst direct in de 'body'.

Conclusie

De applicatie maakt dus heel gemakkelijk niet valide output.

Attack 9 – Force properties of an output to change

Test 9.1: Achteraf veranderen van afbeelding

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar.

Handelingen

1. Kies 'Insert', 'Image'
2. Kies een afbeelding met 'choose file'
3. Ga naar het tablad 'dimensions'
4. Selecteer 'custom size'
5. Kies voor breedte en hoogte beide het getal '100'
6. Klik 'OK'
7. Rechtermuisknop op de afbeelding
8. Kies 'Image properties'
9. Verander de afbeelding met 'choose file'
10. Klik 'OK'

Verwachte gedrag

Ik verwacht dat de applicatie gewoon de afbeelding vervangt en deze 100px bij 100px houdt

Daadwerkelijke gedrag

De applicatie past ook gelijk de afmetingen van de afbeelding aan.

Conclusie

De applicatie leest de afmetingen van de nieuwe afbeelding uit en zet die als de nieuwe afmetingen, dit terwijl alleen de afbeelding zelf vervangen is.

Attack 10 – Force the screen to refresh

Test 10.1: Controls voor aanpassen van de grootte van elementen

Uitgangssituatie

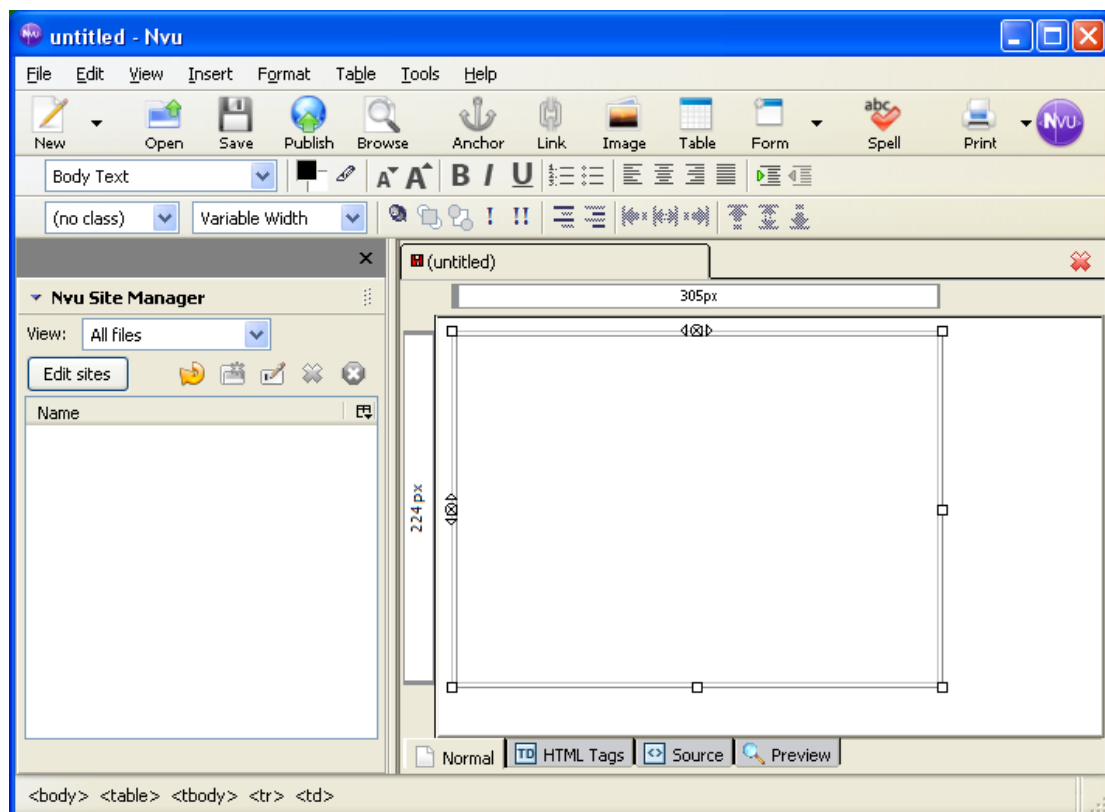
De applicatie is gestart, het beginscherm is zichtbaar.

Handelingen

1. Kies 'Insert', 'Table'
2. Kies een tabel van 1x1
3. Klik 'OK'
4. Vergroot de tabel meerdere keren zodat hij voor een deel buiten het getekende gedeelte valt

Verwachte gedrag

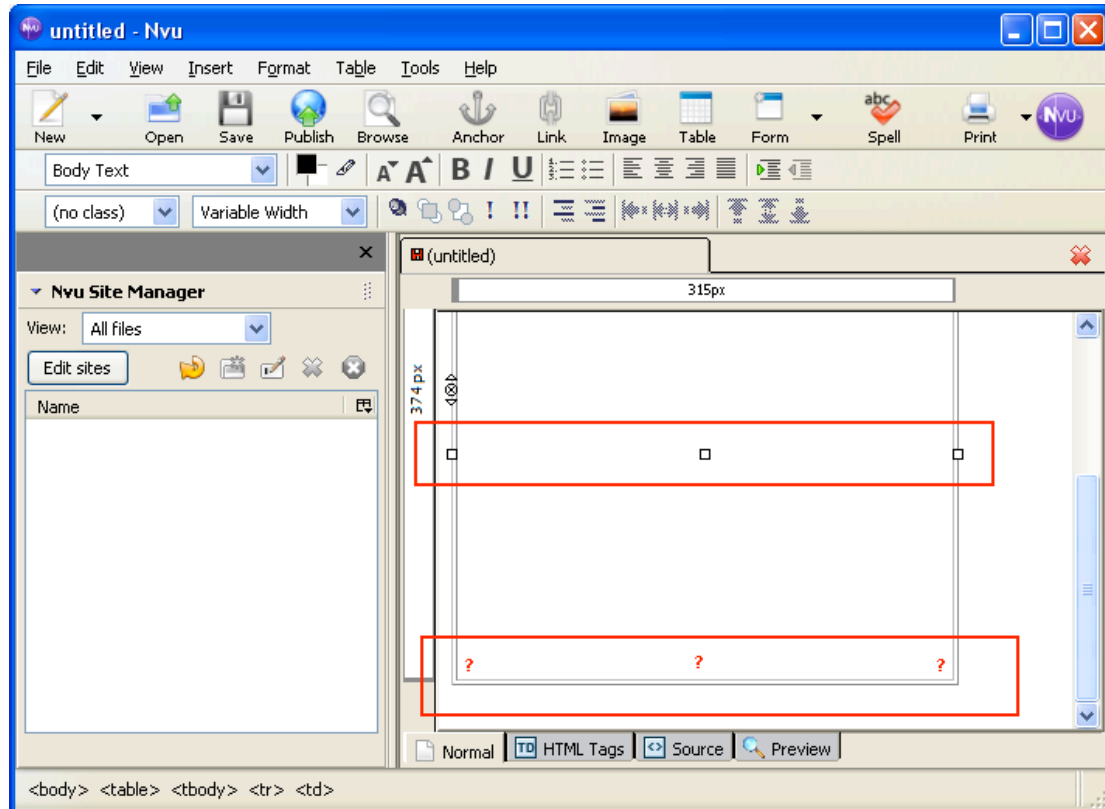
Ik verwacht dat de applicatie gewoon de controls voor het aanpassen op de hoekpunten van het element houdt



Daadwerkelijke gedrag

De applicatie plaatst de controls niet meer op de hoekpunten als het element niet in de 'viewport' past. Pas als het element weer klein genoeg is worden de controls weer op de hoekpunten gezet.

Dit effect treedt trouwens niet op als je volledig naar boven bent gescrolled.



Conclusie

De applicatie heeft grote moeite met elementen die groter zijn dan de huidige viewport.

Attack 11 – Apply inputs using a variety of initial conditions

Test 11.1: Verplaatsen van elementen gebruikmakend van layers

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar. De tekst 'test' is ingevoerd in het document.

Handelingen

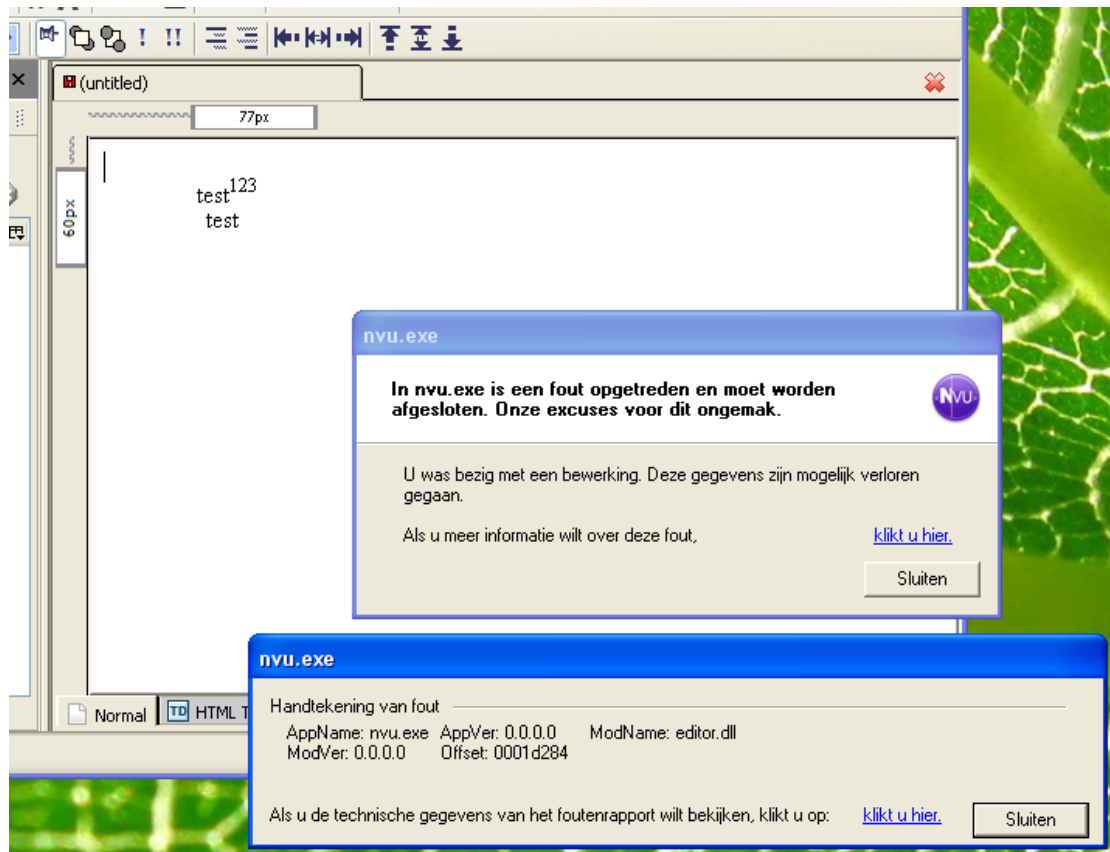
1. Selecteer de tekst
2. Maak van de tekst een layer met tekst ('Layer' knop)
3. Pak de layer vast bij de positioning control (kruis met punten)
4. Sleep met de muis naar boven, tot buiten de 'viewport'
5. Laat de muis los
6. Ga met de muis terug de 'viewport' in
7. Klik op een willekeurige positie in de 'viewport'

Verwachte gedrag

Ik verwacht dat de applicatie gewoon de layer plaatst waar bij punt 7 geklikt wordt.

Daadwerkelijke gedrag

De applicatie hangt na punt 7 direct! Op de Mac OS X versie blijft de applicatie in een oneindige loop.



Conclusie

Er zit blijkbaar een fout in het verslepen van elementen nadat de muis buiten de viewport is geweest. Zie ook de volgende test 11.2.

Test 11.2: Element verslepen met muis eerst buiten de 'viewport'

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar. Er is een afbeelding ingevoegd.

Handelingen

1. Klik op de afbeelding en houd de muis ingedrukt
2. Sleep de muis buiten de viewport
3. Sleep de muis terug in de viewport
4. Laat de muis los

Verwachte gedrag

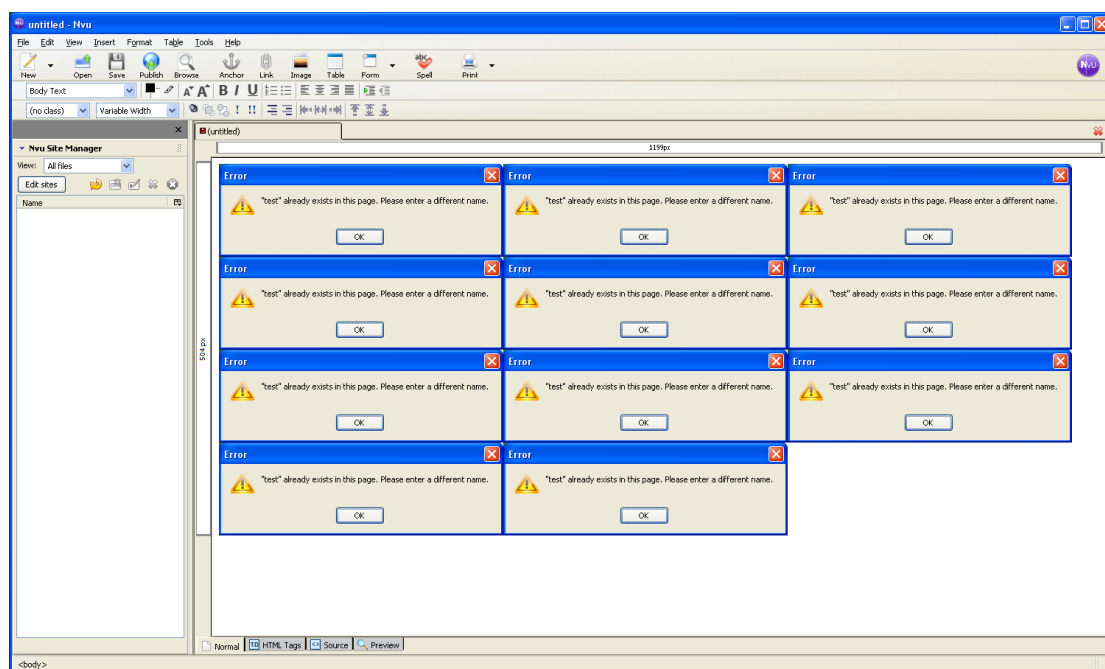
Ik verwacht dat de applicatie de afbeelding niet kan verplaatsen, dus gewoon laat staan

Daadwerkelijke gedrag

De applicatie plaatst een kopie van de afbeelding op de pagina. Heel vreemd, geen idee waarom.

Conclusie

De applicatie heeft, zoals ook bij 11.1 te zien was, grote moeite met acties deels buiten de 'viewport' om.



Attack 12 – Force a data structure to store too many or too few values

Test 12.1: Zeer grote textarea invoegen

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar.

Handelingen

1. Kies 'Insert', 'Form', 'Text area'
2. Kies een naam, bijvoorbeeld 'test'
3. Kies voor zowel breedte als hoogte 68000000 (68M)
4. Klik 'OK'

Verwachte gedrag

Ik verwacht dat de applicatie de textarea invoegd.

Daadwerkelijke gedrag

De applicatie plaatst de textarea, maar geeft hem breedte en hoogte van '0'.

Conclusie

De applicatie geeft een textarea weer een breedte en hoogte van '0' als deze groter dan 67 miljoen wordt opgegeven. De grens ligt ergens tussen de 67 en 68 miljoen.

Attack 13 – Investigate alternative ways to modify internal data constraints

Is al eerder aangevallen. Rest van alle invoer wordt goed beschermd met een duidelijke waarschuwing bij het overgaan van de limieten.

Attack 14 – Experiment with invalid operand and operator combinations

Niks kunnen vinden waar berekeningen worden gedaan waar de gebruiker invloed op uit kan oefenen. Daarom geen test in deze attack. Wel een andere test.

Test 14.1: Invoegen van tabel, wisselen van 'view'

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar.

Handelingen

1. Kies 'Insert', 'Table'
2. Kies voor een eenvoudige tabel invoegen, minimaal 1 cel
3. Klik 'OK'
4. Wijzig de 'view' naar 'source'
5. Mouseover de 'view' wisselaar

Verwachte gedrag

Ik verwacht dat de applicatie gewoon de view kan wijzigen.

Daadwerkelijke gedrag

De applicatie wijzigt de view nog goed, maar als er een tabel in de pagina zit, blijft er bij de view 'source' altijd een zandlopertje zichtbaar bij de muis. Dit gebeurt niet bij andere views of als er geen tabel in de pagina zit.

Conclusie

De applicatie heeft blijkbaar moeite met een tabel in de source, waardoor een zandloper zichtbaar blijft.

Attack 15 – Force a function to call itself recursively

Geen test kunnen uitvoeren waarin recursiviteit te triggeren was.

Test 5.1 blijft behoorlijk lang lopen, maar geeft uiteindelijk ook het gewenste resultaat. Dit zal waarschijnlijk geen recursiviteit zijn.

Attack 16 – Force computation results to be too large or too small

Test 16.1: Zeer grote marges bij paginainstellingen

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar. We zijn bij het scherm 'page setup', de tab 'Margins & Header/Footer'

Handelingen

1. Kies voor de top marge en bottom marge allebei 300 (is meer dan de helft)

Verwachte gedrag

Ik heb eigenlijk totaal geen verwachting. Ben wel benieuwd.

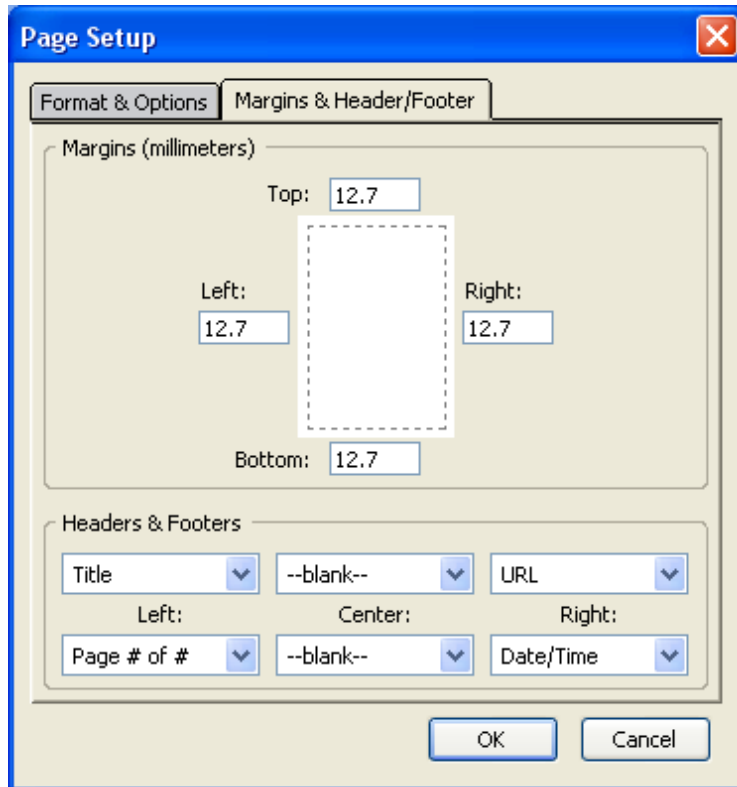
Daadwerkelijke gedrag

De applicatie vindt de ingevoerde waarden ok. De applicatie past zelfs de grootte van de preview van de pagina aan zodat het past. Het afdrukken van een dergelijke pagina resulteert in een lege pagina.

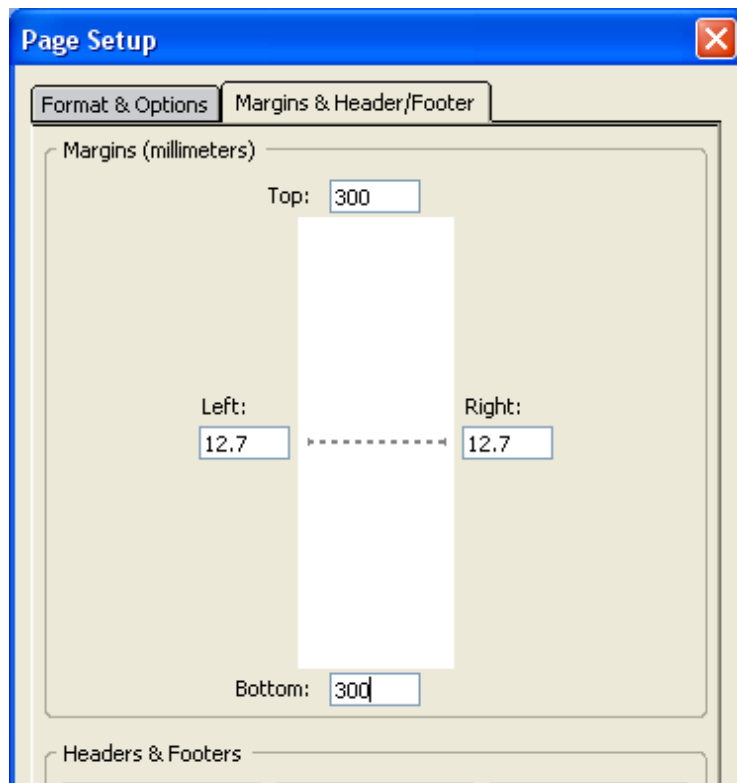
Conclusie

De applicatie heeft een behoorlijk hoge limiet voor de paginamarges, iets dat totaal niet realistisch is. Het maximum is niet te testen, want de grootte past hij gelijk toe in de preview, waardoor op een gegeven moment de invoervelden zelfs helemaal uit beeld verdwijnen!

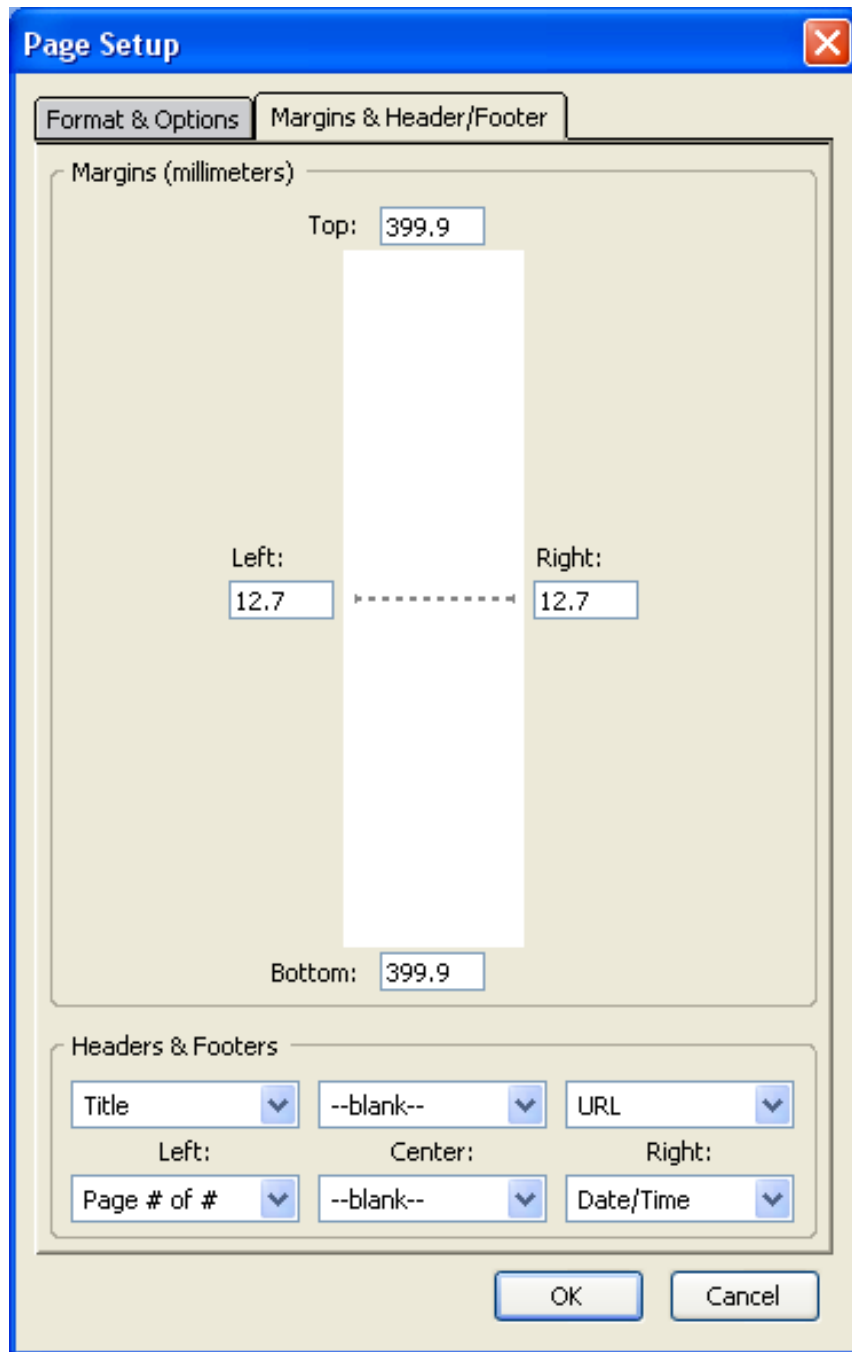
Deze test ging niet zozeer over interne berekeningen, maar wel over te grote resultaten ervan. Er zou een beperking ingebouwd moeten worden.



Normaal venster



Grotere marges, maakt grotere pagina???



En zelfs een groter frame?!

Attack 17 – Find features that share data or interact poorly

Test 17.1: Tabel eigenschappen, breedte veranderen

Uitgangssituatie

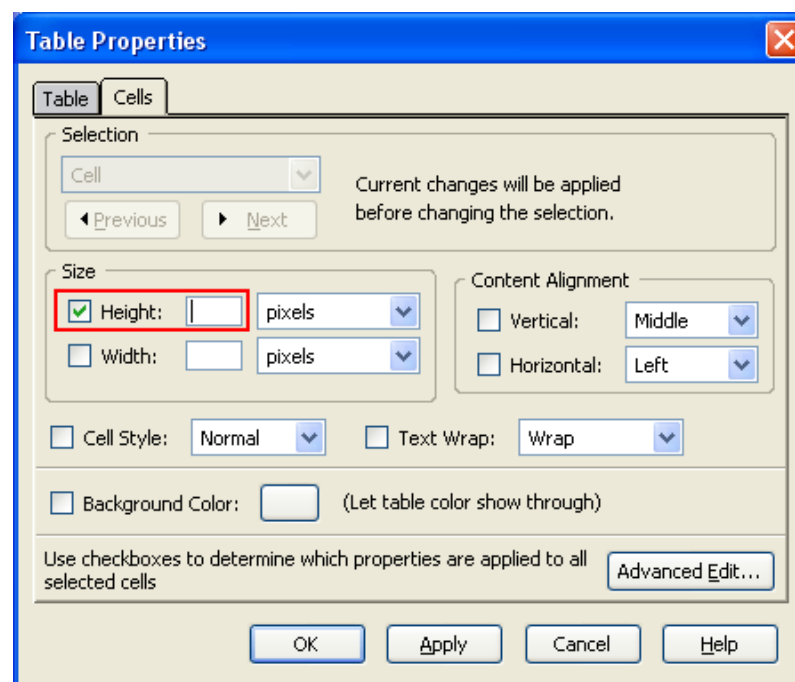
De applicatie is gestart, het beginscherm is zichtbaar. Er is een tabel ingevoegd op de pagina.

Handelingen

1. Rechtermuisknop op de tabel
2. Kies 'Table Cell Properties'
3. Voer bij 'breedte' het karakter 'a' in

Verwachte gedrag

Ik wist al dat de applicatie karakters weigert waar getallen horen, dus dat verwacht ik hier ook.



Daadwerkelijke gedrag

De applicatie weigert inderdaad het karakter, maar vinkt wel de checkbox ervoor aan dat er een waarde is ingevoerd. Dit klopt niet! Er is namelijk geen waarde ingevoerd, want de invoer heeft de applicatie zelf weer weggefilterd!

Conclusie

De applicatie heeft een goede oplossing om te voorkomen dat er andere tekens dan getallen ergens ingevoerd worden. Hij haalt die meteen weg. Deze functionaliteit werkt alleen niet goed samen met de functionaliteit die weergeeft of een waarde is ingevoerd in een veld!

System Interface Attacks

Attack 1 – Fill the file system to its capacity

Test 1.1: Opslaan bij volle disk

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar.

Handelingen

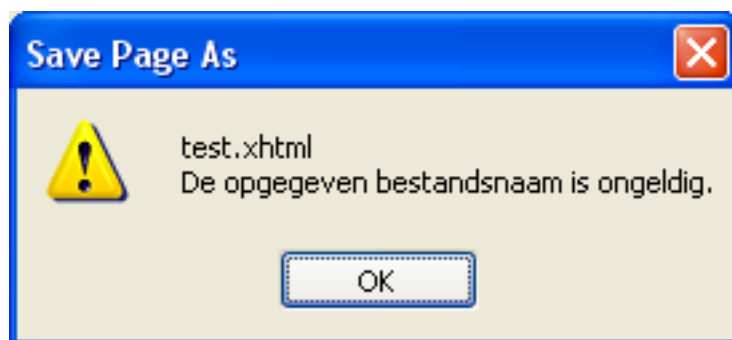
1. Kies 'File', 'Save as'
2. Vul een naam in
3. Kies 'OK'

Verwachte gedrag

Ik verwacht dat de applicatie een melding geeft dat er geen schijfruimte meer is.

Daadwerkelijke gedrag

De applicatie geeft gelijk een melding, maar die heeft niks te maken met dat er geen schijfruimte meer is. Er wordt gemeld dat de bestandsnaam niet geldig is. Er kunnen verschillende namen getest worden, niks is geldig.



Conclusie

De applicatie heeft op tijd door dat het bestand niet kan worden weggeschreven. Er wordt alleen de verkeerde conclusie uit getrokken.

Attack 2 – Force the media to be busy or unavailable

Test 2.1: Nieuw bestand als onmogelijk door file system

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar.

Handelingen

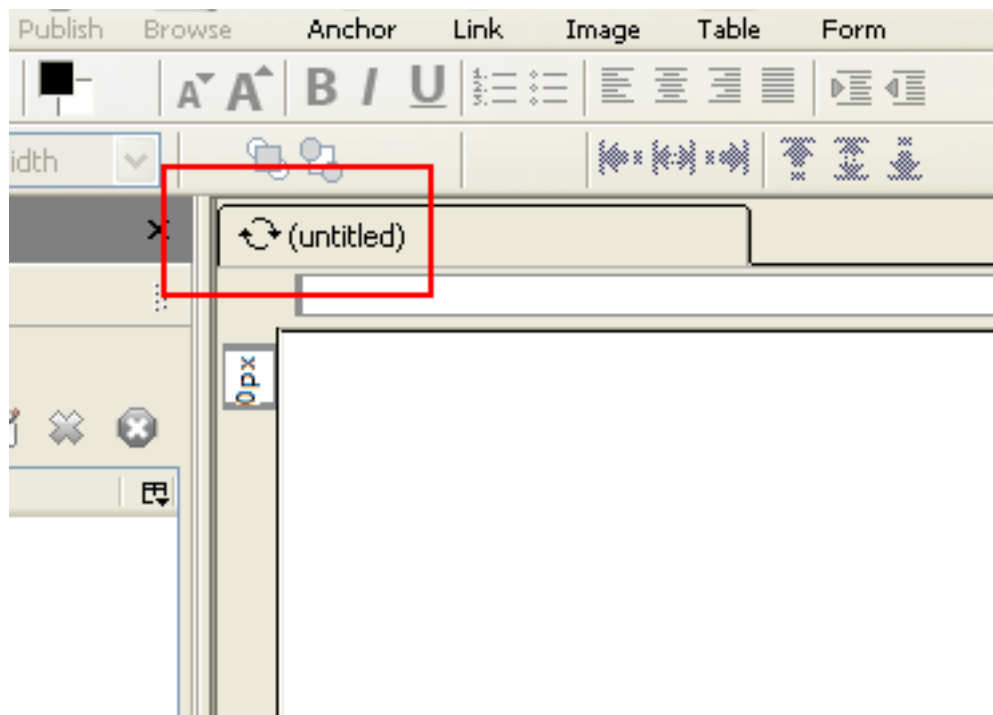
1. Klik op het 'sluiten' kruisje van het document (hierdoor wordt het document gesloten en vanzelf een nieuwe aangemaakt)

Verwachte gedrag

Ik verwacht dat de applicatie een melding geeft dat er geen nieuw bestand meer aangemaakt mag worden van het file system.

Daadwerkelijke gedrag

De applicatie lijkt het document te sluiten en wil een nieuwe aanmaken. Dit lukt niet. Er wordt een soort 'wachtcloon' zichtbaar, dat aangeeft dat de applicatie bezig is, maar er gebeurt niks.



Conclusie

De applicatie heeft geen idee van het probleem. Er wordt geen waarschuwing gegeven. De applicatie loopt gewoon vast op dit probleem.

Als op de 'normale' manier een nieuw bestand wordt aangemaakt ('File', 'New') wordt alleen een windowframe zichtbaar waar je niks mee kan. Zie onderstaande afbeelding.

Attack 3 – Damage the media

Test 3.1: Bestand laden van beschadigde CD

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar. Er is een bestand op CD gebrand.

Handelingen

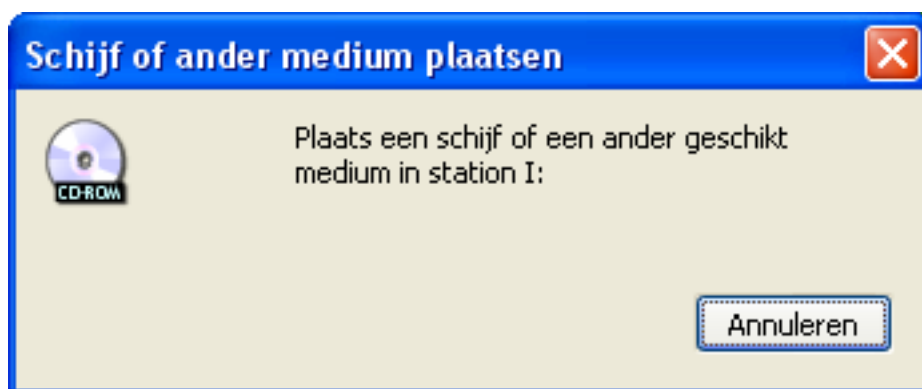
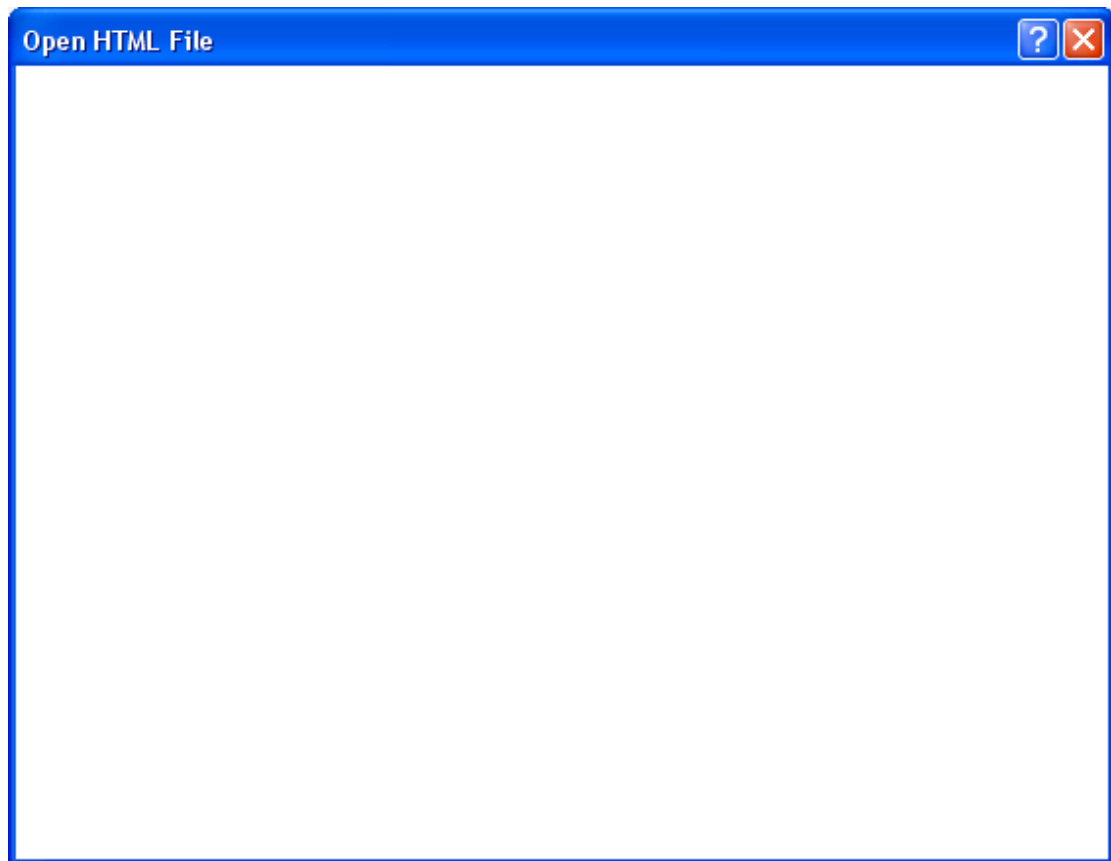
1. Beschadig de CD door er met een scherp object krassen op te maken
2. Stop de CD in de computer
3. Open de applicatie NVU
4. Kies 'File', 'Open'
5. Browse naar de CD
6. Open het bestand

Verwachte gedrag

Ik verwacht dat de applicatie een melding geeft dat óf de CD er niet is, óf het bestand niet gevonden is.

Daadwerkelijke gedrag

De applicatie probeert de CD drive te openen, maar faalt daarbij. Het 'openen' scherm wordt volledig wit en 'hangt'. Het OS geeft daarna nog een melding dat er een andere schijf geplaatst moet worden.



Conclusie

De applicatie heeft niet door wat er aan de hand is met de kapotte media. Het blijft eindeloos proberen de CD te lezen, wat de applicatie zelf onbruikbaar maakt.

Attack 4 – Assign an invalid file name

Test 4.1: Tekstbestand openen in plaats van HTML

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar. Er is een HTML bestand (nvu.html) en hetzelfde bestand waar alleen de extensie van is veranderd (nvu.txt).

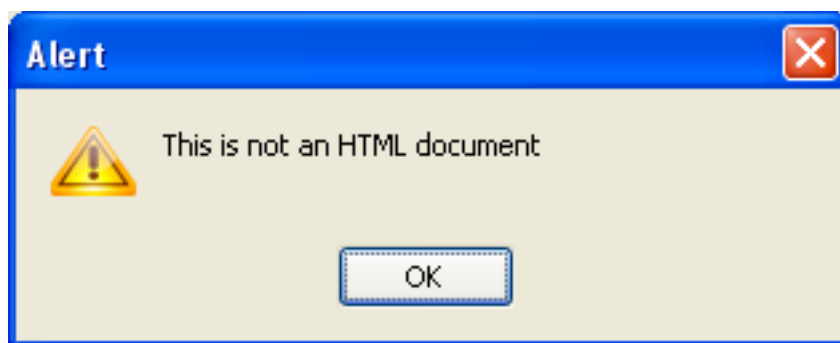


Handelingen

1. Kies 'File', 'Open'
2. Kies het bestand 'nvu.txt'
3. Kies 'Open'

Verwachte gedrag

Ik verwacht dat de applicatie een melding geeft dat het geen HTML bestand betreft, maar met de keuze of ik het wel wil proberen te openen.



Daadwerkelijke gedrag

De applicatie geeft gelijk een melding dat het geen HTML bestand betreft. De applicatie geeft geen mogelijkheid op het bestand te openen.

Conclusie

De applicatie controleert heel strict op de extensie. Er wordt dus bij het openen niet ook naar de inhoud gekeken. Een verkeerde extensie betekent gelijk een verkeerd bestand.

Attack 5 – Vary file access permissions

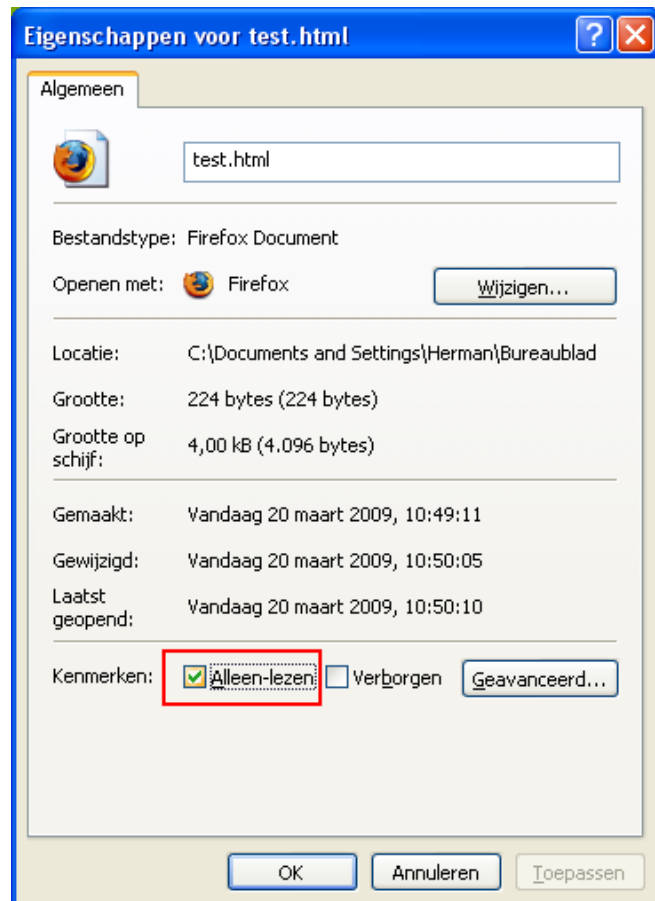
Test 5.1: Opslaan van een 'alleen-lezen' bestand

Uitgangssituatie

De applicatie is gestart, het beginscherm is zichtbaar. Er is een HTML bestand, gemaakt door NVU gewijzigd naar de 'alleen-lezen' permissie van Windows XP.

Handelingen

1. Kies 'File', 'Open'
2. Kies het 'alleen-lezen' bestand
3. Kies 'Open'
4. Verander de pagina
5. Kies 'File', 'Save'

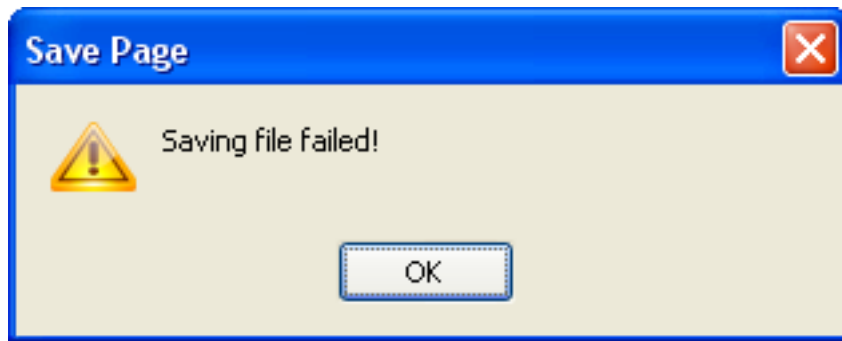


Verwachte gedrag

Ik verwacht dat de applicatie een melding geeft dat het bestand niet opgeslagen kan worden, omdat het een alleen-lezen bestand betreft.

Daadwerkelijke gedrag

De applicatie geeft gelijk een melding, maar die heeft niks te maken met dat het een alleen-lezen bestand betreft. Er komt alleen een melding dat het opslaan is mislukt.



Conclusie

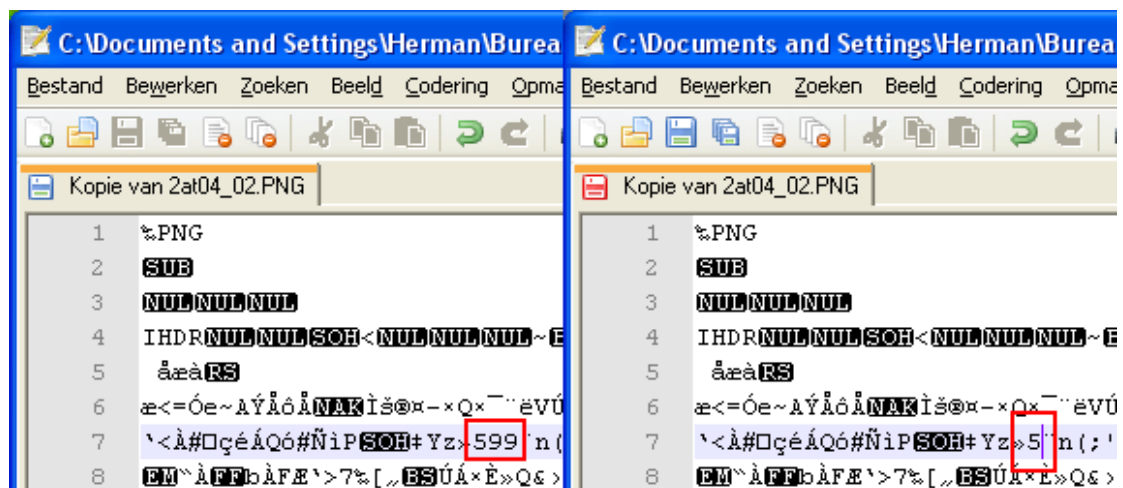
De applicatie krijgt waarschijnlijk van het OS door dat het bestand niet opgeslagen mag worden, alleen weet de applicatie niet waardoor dit komt.

Attack 6 – Vary or corrupt file contents

Test 6.1: Corrupte afbeelding invoegen

Uitgangssituatie

Pas een PNG afbeelding aan in een teksteditor, verander één of twee numerieke karakters. Hieronder mijn aanpassing, met het gevolg als het aangepaste bestand wordt geopend met een willekeurig afbeeldingen bekijk programma.



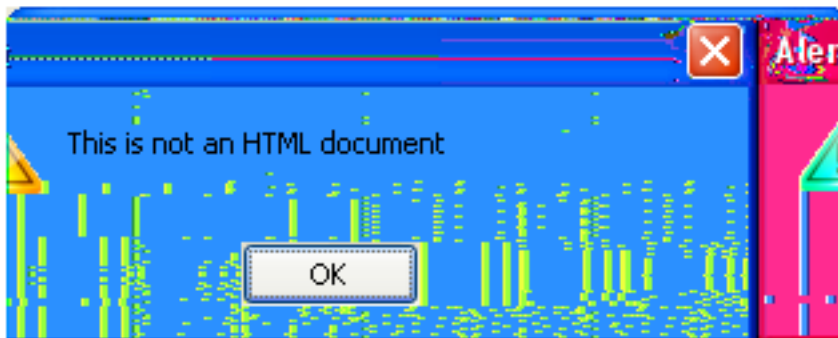
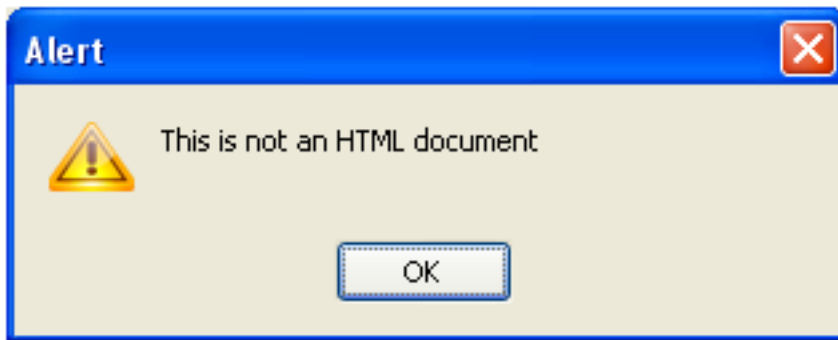
De applicatie is gestart, het beginscherm is zichtbaar.

Handelingen

1. Kies 'Insert', 'Image'
2. Kies het veranderde corrupte bestand
3. Kies 'OK'

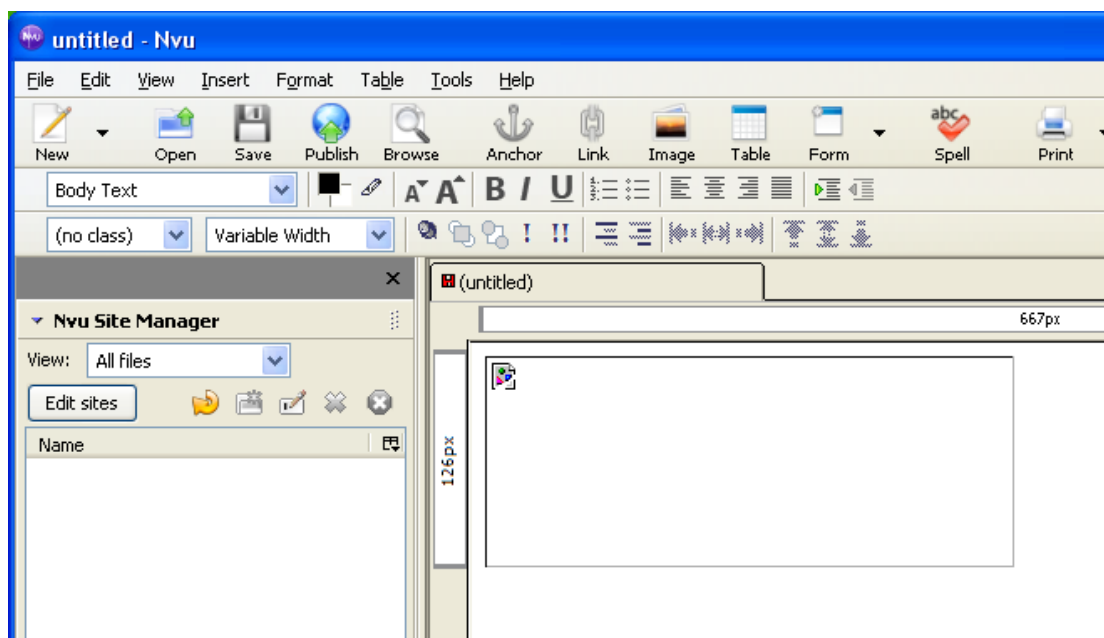
Verwachte gedrag

Ik verwacht dat de applicatie gewoon de afbeelding invoegt en dat het gewoon eruit ziet als in de afbeelding bekijk programma's.



Daadwerkelijke gedrag

De applicatie voegt de afbeelding in met de juiste grootte, maar de afbeelding is niet zichtbaar. Zie hieronder.



Conclusie

De applicatie kan nog wel de afmetingen van de afbeelding herkennen, maar kan geen bitmap meer opbouwen uit het bestand. Dat kunnen andere applicaties wel degelijk. Blijkbaar is het bestand toch te corrupt geraakt door de twee karakters extra.

Urenverantwoording

Hieronder een grove dagenplanning van de activiteiten voor dit werkstuk/verslag. In totaal is er zo'n 22 tot 26 uur gaan zitten in het totaal van deze activiteiten. Natuurlijk zat de meeste tijd in het voorbereiden/verzinnen van de attacks en het uitvoeren daarvan. Daarnaast is veel tijd gaan zitten in het maken en plaatsen van de juiste schermafbeeldingen bij de attacks.

Ik hoop dat de inhoud van het werkstuk juist is en dat de tijd goed besteed is. Ik vond het zelf in ieder geval heel interessant. Hoe langer je een applicatie test, hoe meer fouten je vindt!

