



Webtechnologies for AI_INF - Evaluatie Technisch Rapport, Database en Code (2021)

Questions Responses 1

Section 1 of 7

Webtechnieken voor KI/INF - Evaluatieformulier Technisch Rapport, Database en Code

Gebruik dit formulier om het technisch rapport, de database en de source code te beoordelen van een groep.

Er volgen drie reeksen vragen en/of stellingen:

1. over het technisch rapport,
2. over de database, en
3. over de source code.

Beoordeel alle vragen op een schaal van 1 (waardeloos) tot en met 10 (uitstekend). Wees niet bang om een 1 uit te delen als in het geheel niet is voldaan aan de vraag, of om een 10 uit te delen als volledig is voldaan aan de vraag. Als je het niet zeker weet, maak dan een schatting en geef dit aan in de Opmerkingen aan het eind van elke reeks vragen.

After section 1 Continue to next section

Section 2 of 7

Untitled section

Group

Groupnumber *



Short-answer text

.....

Link *

Waarschijnlijk <http://agileXYZ.science.uva.nl/> met 'XYZ' het nummer van de server van de groep.

Short-answer text

.....

TA *

1. Yuri Demchenko
2. Wessel de Jong
3. Brandsen, Jurre
4. Dijkstra, Riemer
5. Greven, Jip
6. Khawalid, Alex
7. Kirkeng, Mathias
8. Kombrink, Meike
9. Kortman, Jacco
10. Lely, Miles van der
11. Monkau, Denise
12. Muller, Tim
13. Portma, Ranno



Rosmalen, Yochem van

15. Verhaar, Mitchel

16. Verweij, Julian

17. Wacanno, Robin

18. Westerveld, Bryan

19. Wolf, Ivan de

20. Koen van Elsen

After section 2 Continue to next section ▼

Section 3 of 7

Technisch rapport



Beoordeel hier het technisch rapport. Sectie 3.3 van de handleiding beschrijft de regels waar dit rapport aan moet voldoen. Tijdens PAV is ook aandacht besteed aan rapporteren, dus (kleine) afwijkingen kunnen voorkomen.

Er volgen nu eerst drie algemene beoordelvragen over het rapport.

Voor de beoordelvragen die daarna volgen kan het rapport als leidraad gebruikt worden, maar let op dat de werkelijkheid anders kan zijn dan wat in het rapport staat beschreven! Controleer dus altijd in de source code of wat is beschreven ook werkelijk is geïmplementeerd.

Indeling *

Het rapport heeft een goede indeling, bv: inleiding, probleem-/onderwerpomschrijving, ontwerp, resultaten, conclusies. De preciese indeling mag hiervan afwijken, als die maar zinnig is.

1 2 3 4 5 6 7 8 9 10



Verzorging *

De opmaak is netjes, er is niets op spelling en grammatica aan te merken, het rapport heeft een titel, de naam van de groep en de namen van de groepsleden+studentnummers zijn vermeld.

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

Inhoudelijke kwaliteit *

Alle beschrijvingen zijn duidelijk en volledig (alles dat in de opdrachtomschrijving staat beschreven staat erin) en functioneel (er is geen sprake van "gezwam").

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

Opmerkingen m.b.t. het verslag (optioneel)

Indien nodig

Long-answer text

After section 3 Continue to next section



Section 4 of 7

Database



De volgende vragen hebben betrekking op het ontwerp van het datamodel. Dit moet in het rapport als een schema zijn opgenomen, waarschijnlijk als screenshot van Designer in phpMyAdmin.



Het datamodel bestaat uit 5 of meer tabellen met niet-triviale relaties. *

Een 1:1 relatie is triviaal (tabellen kunnen dan net zo goed bijeen genomen worden), tabellen met slechts 2 kolommen zijn vaak overbodig *tenzij* het tussentabellen zijn voor n:m relaties.

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

De tabellen en de kolommen in elke tabel hebben goed gekozen namen. *

Fout: Tabel1, Tabel2, etc. Goed: Klanten(_tabel), Producten(_tabel) etc.

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

Elke kolom is van een verstandig gekozen type *

I.e.: INT voor gehele getallen (is UNSIGNED aangegeven indien ≥ 0 ? Is AUTO_INCREMENT aangegeven indien gebruikt als primary index?), FLOAT of DECIMAL voor reële getallen, (VAR)CHAR voor strings, etc. Bij een VARCHAR: is die groot genoeg? (let daar vooral op bij encrypted passwords! Die moet minimaal 60 zijn, 255 is beter), datum in DATE/DATETIME/TIMESTAMP (en niet VARCHAR)?

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

Het datamodel past bij de opdrachtomschrijving *

Geeft het datamodel een goede afspiegeling van de gevraagde toepassing? Zijn de entiteiten en de relaties tussen entiteiten op een zinnige manier opgedeeld in verschillende tabellen? Zie eventueel de opdrachtomschrijving in de

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend



Eerste normaalvorm: de volgorde van rijen en kolommen in de tabellen heeft geen betekenis, *
elke cel bevat één data item, alle kolommen bevatten wezenlijk verschillende data

Fout: tabel met bv. "telnr1", "telnr2" kolommen, geen primary key (elk record (:elke rij) moet gegarandeerd uniek zijn).

Discutabel: adres, huisnummer, postcode en plaats in één kolom.

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

Tweede normaalvorm: entiteiten die niet bij elkaar horen, zitten in verschillende tabellen (cq. *
entiteiten die wél bij elkaar horen, zitten in dezelfde tabel)

Een fout ontwerp is vaak te herkennen doordat in de tabellen een subset van een record herhaaldelijk terugkeert in andere records.

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

Derde normaalvorm: er bestaan geen transitieve afhankelijkheden *

Fout: er bestaat een kolom die "berekenbaar" is uit andere entiteiten (bv. "excl BTW" en "incl BTW" in één tabel is fout).

Discutabel: "postcode" en "woonplaats" in dezelfde tabel (want een woonplaats is af te leiden uit een postcode, echter zo'n tabel kost geld). In de laatste week is wel een postcodetabel beschikbaar gemaakt, maar de groepen hebben waarschijnlijk geen tijd gehad om die te integreren.

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

Opmerkingen over de database (optioneel)

Indien nodig

Long-answer text



After section 4 Continue to next section ▼

Section 5 of 7

Source code



De volgende vragen hebben betrekking op de ingeleverde code: PHP, Javascript, HTML/CSS en de SQL queries.

Raadpleeg de code zoals die is ingeleverd via Blackboard.

De vragen over de code zijn opgedeeld in de volgende subsecties:

- Structurering van het backend (de PHP code),
- Vormgeving, HTML en CSS,
- Navigatie en gebruikersinteractie (inclusief Javascript code),
- Beveiliging van de website tegen "schadelijke" gebruikersinvoer.

Structuur

Description (optional)

De PHP code is logisch gestructureerd *

De code is op zinnige wijze opgedeeld in verschillende files. Er is geen herhaling van dezelfde code in verschillende files. Ontwerp van eigen Classes is niet verplicht maar als daar toch gebruik van is gemaakt en ze zijn zinnig gestructureerd, dan mag daar best een bonus voor gegeven worden.

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

De layout van de PHP code is consistent en duidelijk *

A.u.b. geen "heilige huisjes" toepassen als "indentatie moet x spaties zijn". Wees objectief.

1	2	3	4	5	6	7	8	9	10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐



De PHP code is voorzien van voldoende commentaar *

Niet triviale code wordt verklaard met kort commentaar, overbodig of te veel commentaar is ook niet goed.

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

De PHP code is voorzien van voldoende foutafhandling *

Er mogen nooit PHP foutmeldingen zichtbaar zijn in de browser: die moeten netjes worden afgevangen. Het negeren van fouten is ook niet goed.

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

De code is portable *

Installatie op andere hosts zou mogelijk moeten zijn zonder noemenswaardige wijzigingen in de code. Fout: harde pathnames

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

"Geleende" PHP code wordt voldoende credited *

Gebruik van code die niet zelf is geschreven is toegestaan, maar alléén als dat duidelijk is aangegeven en de bron is vermeld. Let op: de bron mag ook in de ingeleverde README.txt vermeld worden. Als de geleende code bestaat uit minder dan 10 regels, dan hoeft de bron niet vermeld te worden. Code die als voorbeeldcode is getoond tijdens het college mag zonder bronverwijzing worden gebruikt.

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend



Opmerkingen over structuur (optioneel)

Indien nodig.

Long-answer text

Vormgeving, HTML en CSS

Description (optional)

De website is overzichtelijk vormgegeven *

Goed gebruik van fonts en kleurcombinaties, passend bij de opdracht.

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

De vormgeving past zich goed aan bij resizen van de browser *

Is gebruik gemaakt van een "Responsive" ontwerp, oftewel: maakt de site effectief gebruik van de grootte van het window? Is de site ook nog bruikbaar in een klein window (op een tablet of smartphone)?

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

Er is goed gebruik gemaakt van CSS *

Er zijn minstens 5 style rules. Er zijn geen "hacks" gebruikt om de verkregen layout te bereiken (fout: herhaalde "
" tags om witruimte te maken of "<h1>" om ergens accent op te leggen). Er mag géén gebruik gemaakt zijn van Bootstrap of andere externe stylesheets: de layout moet zélf geïmplementeerd zijn!

	1	2	3	4	5	6	7	8	9	10	
--	---	---	---	---	---	---	---	---	---	----	--



Alle pagina's bevatten W3C compliant (X)HTML en CSS *

Studenten zijn gevraagd HTML5 compliant pagina's te maken. Neem een steekproef: copy-paste de HTML source van een paar pagina's ("View Source" in je browser) naar de HTML5 validator website: <https://validator.w3.org/>

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

Dynamische content wordt gegenereerd op basis van data uit de database *

Fout: hardcoded opties in selection boxes waar die uit de database verkregen hadden moeten worden. Algemeen: het moet niet nodig zijn voor de beheerder van de website om HTML pagina's of PHP code te editen als een nieuw item aan de database wordt toegevoegd.

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

Opmerkingen over vormgeving, HTML en CSS (optioneel)

Indien nodig.

Long-answer text

Navigatie en gebruikersinteractie

Description (optional)

De navigatie zit logisch in elkaar *

Werken alle menus en "links" van de site zoals verwacht mag worden? Zijn de belangrijkste functies op een makkelijke, intuïtieve manier te vinden?



Waardeloos



Uitstekend

Er is een duidelijk en functioneel onderscheid in de afhandeling van niet-ingelogde gebruikers, ingelogde gebruikers en de admin-interface *

Niet-ingelogde gebruikers mogen minder dan ingelogde gebruikers die weer minder mogen dan admins.

1

2

3

4

5

6

7

8

9

10

Waardeloos



Uitstekend

In- en uitloggen werkt correct *

Wordt er correct gebruik gemaakt van sessions? Zijn afgeschermd pagina's daadwerkelijk onbereikbaar als men niet is ingelogd? Probeer eens dit: log in als admin en ga naar een pagina die alleen admin mag zien; copy de URL, log uit, paste de URL. Is de admin pagina toch bereikbaar: fout!

1

2

3

4

5

6

7

8

9

10

Waardeloos



Uitstekend

Formulieren zijn duidelijk en worden gebruiksvriendelijk afgehandeld *

Zijn formulieren kort, bondig en wordt om zinnige invoer gevraagd? Zijn verplichte velden als zodanig aangegeven? Wordt in de browser (i.e. met Javascript) het volgende gedaan: checks op lege velden als die verplicht zijn, op geldig email address, verificatie van password, check op password sterkte?

1

2

3

4

5

6

7

8

9

10

Waardeloos



Uitstekend

Fouten in form input worden vriendelijk afgehandeld *

Fout: een form weer helemaal opnieuw in moeten vullen als ergens een foutje is gemaakt. Fout: javascript "alert" (: een pop-up window) bij foute invoer. Goed: cursor focus naar veld waar input verkeerd was, form velden pre-populeren met voorbeelden.



	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

De functionaliteit om data toe te voegen aan de database werkt correct *

Controleer ook correct gebruik van de SQL query in de PHP code.

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

De functionaliteit om data te updaten in de database werkt correct *

Controleer ook correct gebruik van de SQL query in de PHP code. Is er bijvoorbeeld bescherming tegen abusievelijk "te veel" updaten d.m.v. een "LIMIT 1"?

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

De functionaliteit om data te verwijderen uit de database werkt correct *

Controleer ook correct gebruik van de SQL query in de PHP code. Is er bijvoorbeeld bescherming tegen abusievelijk "te veel" verwijderen d.m.v. een "LIMIT 1"?

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

Overige functionaliteit doet wat ervan verwacht mag worden *

Vangt de site exceptionele invoer correct af? Probeer bij een webshop eens nul of een negatief aantal producten te bestellen, type eens karakters waar een getal gevraagd wordt, gaat de site goed om met verwijzingen naar items die



Waardeloos



Uitstekend

De site geeft adequate feedback op gebruikersinteractie *

Is er goede, functionele feedback op interactie? Er mag nooit een gevoel van onzekerheid ontstaan of wel gebeurd is wat moet gebeuren.

1

2

3

4

5

6

7

8

9

10

Waardeloos



Uitstekend

De site maakt op functionele wijze gebruik van AJAX *

Bv. live search results, suggesties bij form input, in-place query-results.

1

2

3

4

5

6

7

8

9

10

Waardeloos



Uitstekend

Opmerkingen over Navigatie en gebruikersinteractie (optioneel)

Indien nodig.

Long-answer text

Beveiliging

Description (optional)

Alle user input is "sanitized" server-side *

Alleen client-side sanitizen (i.e. in Javascript) is niet voldoende: input via GET of POST moet ook sanitized worden! Let op gevaarlijke constructies als "include(\$_GET['url'])". Studenten kennen htmlspecialchars() en strip_tags() om gevaarlijke input



1 2 3 4 5 6 7 8 9 10

Waardeloos ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ Uitstekend

Er is voorzien in een afdoende bescherming tegen SQL injection *

Studenten is opgedragen gebruik te maken van PDO. Als gebruik wordt gemaakt van het oude mysql(i), met prepared statements, dan is dat pas nét voldoende als er mysql_real_escape_string() is gebruikt om SQL injection te voorkomen (maar afgeraden op college): anders onvoldoende. Bonus voor een eigen SQL Class waarin de beveiliging correct

1 2 3 4 5 6 7 8 9 10

Waardeloos ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ Uitstekend

MySQL inlog-gegevens zijn effectief afgeschermd van de buitenwereld *

De MySQL username/password is op geen enkele wijze door een browser te bemachtigen en staan ook niet letterlijk in een PHP file. Goed: de inlog-gegevens staan in een config file buiten de document-root (bv. /var of /var/www, maar niet onder /var/www/html).

1 2 3 4 5 6 7 8 9 10

Waardeloos ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ Uitstekend

Pagina's met gevoelige content zijn SSL beveiligd *

Bv: als een password moet worden ingetypt, dan is de verbinding encrypted (httpS in de addressbar). Studenten is geleerd hoe ze automatisch moeten redirecten naar HTTPS. Probeer ook eens of een gevoelige pagina alsnog leesbaar is door "https" te veranderen in "http": dat zou niet mogen kunnen.

1 2 3 4 5 6 7 8 9 10

Waardeloos ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ Uitstekend

Passwords zijn nergens "clear text" leesbaar *



Fout: passwords die leesbaar voorkomen in de database, configuratie files of source code. Studenten is verteld dat ze encrypted passwords moeten opslaan gebruik makend van de PHP functies password_hash() en password_verify(). Gebruik van MD5 en SHA1 als encryptie methode is alleen voldoende als er gebruik is gemaakt van een "salt" (die dan wel onbereikbaar moet zijn voor de browser).

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

Opmerkingen over Beveiliging (optioneel)

Indien nodig.

Long-answer text

Privacy and cookie consent

Description (optional)

Cookie consent is asked explicitly *

Fully handled: Cookie consent is asked and stored, cookie sent checked, only technological cookie used, not usage statistics collected, appropriate text is provided in the report explaining cookie implementation

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

Statement and policy about handling personal data *

Statement and policy about handling personal data is provided and user agreement asked

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend



Opmerkingen over Privacy en cookie (optioneel)

Indien nodig.

Long-answer text

After section 5 Continue to next section



Section 6 of 7

Web API and use of external data



Students had to make/use an API in this course. The process of using data of other websites to automatically fill the database, is also allowed (data-dumps/webscraping). Things like a log-in with Facebook, or just showing someone's location on a google maps interface, is not sufficient.

How well has the API been applied? Is the data they harvested useful? Or is all their DB input perhaps harvested from other websites automatically by a script? And if they wrote their own API, how well can it provide data produced by their web service to be useful for external services?

1 2 3 4 5 6 7 8 9 10

Waardeloos

☐☐☐☐☐☐☐☐☐☐

Uitstekend

How well is the API integrated? Does it stick out like a "sore-thumb", or does it feel like it is part of the website? Does it get raw JSON on the screen, or is it nicely post-processed? If they wrote their own: Does it follow the RESTful (or similar) standard? Does the provided API URL make sense? Is there any documentation on provided API?

1 2 3 4 5 6 7 8 9 10

Waardeloos

☐☐☐☐☐☐☐☐☐☐

Uitstekend



Is the code for the API's somewhat safe/efficient? Could keys be accessed by others? Is the output properly processed? (there are some standard methods to process XML/CSV/JSON, don't have them re-invent the wheel). In case of their own API, the emphasis is on efficiency of getting their mysql data into a standard format like PHP/CSV. Can you break it easily?

	1	2	3	4	5	6	7	8	9	10	
Waardeloos	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Uitstekend

Algemene opmerkingen over deze uitwerking

Long-answer text

After section 6 Continue to next section



Section 7 of 7

Tenslotte



Description (optional)

Algemene opmerkingen over deze uitwerking

Long-answer text

