



Testprotokoll - GreatGrade

Auftraggeber Daniel Brodbeck
Projektleiter Sara Roth
Autor Sara Roth
Klassifizierung Intern, vertraulich
Status In Arbeit, Genehmigt

Änderungsverzeichnis

Datum	Version	Änderung	Autor
28.08.2020	0.1	Dokument erstellt und initialisiert	Sara Roth
11.10.2020	0.2	Testfälle geschrieben	Sara Roth
17.10.2020	0.3	Tests durchgeführt und Ergebnis dokumentiert	Sara Roth
18.10.2020	1.0	Finale Version vom Testprotokoll	Sara Roth

Inhaltsverzeichnis

1	Einleitung	3
2	Testfälle – GreatGrade	4
2.1	Testfall-001, Usability mit sinnvollen Meldungen	4
2.2	Testfall-002, Client- und serverseitige Validierung	5
2.3	Testfall-003, Sessionhandling	6
2.4	Testfall-004, SQL-Injection, Script-Injection und Session-Hijacking werden verhindert	6
2.5	Testfall-005, Registrierung und Login	7
2.6	Testfall-006, Daten Erfassen Ändern und Löschen	8
2.7	Testfall-007, Sichere Speicherung von Daten	9
3	Testdurchführung und Testergebnisse	10
3.1	Testfall-001, Usability mit sinnvollen Meldungen	10
3.2	Testfall-002, Client- und serverseitige Validierung	10
3.3	Testfall-003, Sessionhandling	10
3.4	Testfall-004, SQL-Injection, Script-Injection und Session-Hijacking werden verhindert	10
3.5	Testfall-005, Registrierung und Login	10
3.6	Testfall-006, Daten Erfassen Ändern und Löschen	11
3.7	Testfall-007, Sichere Speicherung von Daten	11

1 Einleitung

Für die Projektarbeit wurde ein Kompetenzraster erstellt, das alle Funktionen aufgelistet hat, die erwartet werden. Um diese Kompetenzen an der Webapplikation testen zu können, wurde ein Testkonzept geschrieben.

Dabei wurde für jede technische Funktion, die das Projekt enthalten muss, einen Testfall geschrieben, um die vollständige Funktion überprüfen zu können.

Das Dokument wurde so aufgebaut, dass sich unter Kapitel zwei die Testfälle befinden, die im Projekt getestet wurden. Im Kapitel drei wurden all diese Testfälle ausgeführt und dazu das Ergebnis dokumentiert.

1.1 Testfall-001, Usability mit sinnvollen Meldungen

ID / Bezeichnung	T-001	Usability mit sinnvollen Meldungen
Beschreibung	Der Benutzer wird bei seinen Interaktionen mit dem Webaufttritt anhand von sinnvollen Meldungen informiert.	
Testvoraussetzung	Der Benutzer befindet sich auf der Login Maske.	
Testschritte	<ul style="list-style-type: none"> mit Username und Password anmelden <ul style="list-style-type: none"> Username: donald.duck Password: Password6% Meldung: «Password or username is incorrect.» mit Username und Password anmelden <ul style="list-style-type: none"> Username: donald.duck Password: Password5% Benutzer konnte sich im System anmelden In die Einstellungen wechseln (My Settings) Auf Change Password klicken <ul style="list-style-type: none"> 1. Input: Password6% 2. Input Password5% Meldung: «Could not change password.» Auf Change Password klicken <ul style="list-style-type: none"> 1. Input: Password6% 2. Input Password6% Meldung: «Password successfully changed.» 	
Erwartetes Ergebnis	Der Benutzer wird jeweils mit sinnvollen Meldungen über seine Interaktionen informiert.	

1.2 Testfall-002, Client- und serverseitige Validierung

ID / Bezeichnung	T-002	Client- und serverseitige Validierung
Beschreibung	Damit ein Admin beim Erstellen eines neuen Benutzers keine falschen Daten im Formular angeben kann, wurden alle Input-Felder client-, sowie serverseitig validiert.	
Testvoraussetzung	Ein Adminbenutzer ist in der Applikation eingeloggt und befindet sich in den Einstellungen (My Settings).	
Testschritte	<ul style="list-style-type: none">• In den Administrator Settings auf Create User klicken• Gebe als Firstname ein einfacher Leerschlag ein• Gebe als Lastname die Zahl 6 ein.• Nun wird man auf das korrekte Format hingewiesen• Den Lastname verbessern mit Tonic• Username: gin.tonic• Passwort: password• Hinweis auf richtiges Format• Passwort: Password5%• User Group: 3• Class: 1• Der Benutzer konnte nicht erstellt werden	
Erwartetes Ergebnis	Ein User kann nur im System registriert werden, wenn alle Angaben dabei mit dem richtigen Format eingegeben wurden.	

1.3 Testfall-003, Sessionhandling

ID / Bezeichnung	T-003	Sessionhandling
Beschreibung	Eine Session wird nach dem Login gestartet und kann jederzeit durch ein Login beendet werden.	
Testvoraussetzung	Korrekte Logindaten sind vorhanden.	
Testschritte	<ul style="list-style-type: none">• Seite ../src/public/index.php aufrufen• Error-Page erscheint• Login-Button klicken um auf Login Maske zu navigieren• korrekte Logindaten eingeben (BN: chrisp.bacon, PW: Password5%)• auf Logout-Button oben rechts klicken	
Erwartetes Ergebnis	Die eröffnete Session wurde beendet und zerstört. Man befindet sich wieder auf der Login Seite.	

1.4 Testfall-004, SQL-Injection, Script-Injection und Session-Hijacking werden verhindert

ID / Bezeichnung	T-004	SQL-Injection, Script-Injection und Session-Hijacking werden verhindert
Beschreibung	Alle Benutzereingaben, die zu Script- oder SQL-Injection führen könnten, werden vor dem Abschicken an den Server validiert, damit die manipulierte Eingabe nicht ausgeführt oder die gewünschte Ausgabe nicht verändert werden kann.	
Testvoraussetzung	Man befindet sich auf der Login Maske, um die Benutzerdaten einzugeben.	
Testschritte	<ul style="list-style-type: none">• Mit Benutzername und Passwort an der Applikation anmelden mit Java-Script Code.<ul style="list-style-type: none">○ BN: cesar.salad○ PW: <script>alert('You failed')</script>• Erneut anmelden :<ul style="list-style-type: none">○ BN: cesar.salad or 1=1○ PW: Password5%	
Erwartetes Ergebnis	Mit beiden Logindaten kann man sich nicht an der Webapplikation anmelden. Beim ersten Login erscheint auch keine Alert-Box.	

1.5 Testfall-005, Registrierung und Login

ID / Bezeichnung	T-005	Registrierung und Login
Beschreibung	Alle Benutzer, die in der Datenbank gespeichert sind, können sich mit dem Benutzername und dem Passwort auf der Webapplikation anmelden, um Zugriff auf die Notenverwaltung zu haben. Als Adminbenutzer kann man neue Benutzer im System registrieren.	
Testvoraussetzung	Man befindet sich auf der Login-Seite der Applikation ../src/public/login.php	
Testschritte	<ul style="list-style-type: none">• korrekter Benutzername eingeben (Admin-Rolle)• korrektes Passwort vom Benutzer eingeben• auf Login-Button klicken• auf Tab Settings• unter Administrator Settings auf Create User klicken• Vor-, Nachname, Benutzername Gruppe und Klasse ausfüllen• Button Create klicken um User im System zu speichern	
Erwartetes Ergebnis	Der neue Benutzer wurde erfolgreich gespeichert und man kann sich nun mit den Logindaten an der Applikation anmelden.	

1.6 Testfall-006, Daten Erfassen Ändern und Löschen

ID / Bezeichnung	T-006	Daten Erfassen Ändern und Löschen
Beschreibung	Mit einem Adminbenutzer kann man einen neuen Schüler im System aufnehmen, diesem in einem Schulfach eine Note eintragen und anschliessend kann dieser Benutzer im System auch wieder gelöscht werden.	
Testvoraussetzung	Ein Admin ist im System eingeloggt und befindet sich in den Einstellungen. (Settings)	
Testschritte	<ul style="list-style-type: none"> • Einen neuen User erstellen indem auf den Button Create User geklickt wird <ul style="list-style-type: none"> ○ Firstname: Tequilla ○ Lastname: Sunrise ○ Username: tequilla.sunrise ○ Password: Password5% ○ User Group: 3 ○ Class: 2 • klicke Button Create • In der Datenbank prüfen, ob einen Eintrag für den neuen User erstellt wurde • Wechsle auf Tab Overview • Wähle Fach English aus • Klicke auf View • Unter der Tabelle auf Button edit klicken • Bei User Tequilla Sunrise Note 4.5 eintragen • In der Datenbank überprüfen, ob die Note dem Schüler im Fach zugewiesen wurde • Wieder auf den Tab Settings wechseln • In Administrator Settings auf Delete User klicken • Im Dropdown User Tequilla Sunrise auswählen • Mit I [your username] agree bestätigen • Auf Delete klicken 	
Erwartetes Ergebnis	Der erstellte User Tequilla Sunrise existiert nicht mehr in der Datenbank.	

1.7 Testfall-007, Sichere Speicherung von Daten

ID / Bezeichnung	T-007	Sichere Speicherung von Daten
Beschreibung	Das Passwort wird als Hash-Wert mit Salt Zusatz in die Datenbank geschrieben. Der Datenbank User GGUser kann die Datenbank nicht löschen.	
Testvoraussetzung	Dieser Testfall wird über http://localhost/phpmyadmin oder mit der Konsole getestet.	
Testschritte	<ul style="list-style-type: none"> Mit GGUser in der Konsole anmelden <ul style="list-style-type: none"> <code>mysql – u GGUser -p</code> PW: <code>GGPassword</code> Befehl: <code>select password from tbl_users;</code> Tabelle mit Hash-Werten wird angezeigt und kann nicht identifiziert werden.  <ul style="list-style-type: none"> Befehl: <code>drop database db_greatgrade;</code> Zugriff wird verweigert 	
Erwartetes Ergebnis	Die Passwörter können in der Datenbank nicht herausgelesen werden und die Datenbank konnte nicht gelöscht werden.	

2 Testdurchführung und Testergebnisse

2.1 Testfall-001, Usability mit sinnvollen Meldungen

Tester	Sara Roth
Datum Testdurchführung	17.10.2020
Fehlerklasse (Testergebnis)	OK
Fehlerbeschreibung	keine

2.2 Testfall-002, Client- und serverseitige Validierung

Tester	Sara Roth
Datum Testdurchführung	17.10.2020
Fehlerklasse (Testergebnis)	OK
Fehlerbeschreibung	keine

2.3 Testfall-003, Sessionhandling

Tester	Sara Roth
Datum Testdurchführung	17.10.2020
Fehlerklasse (Testergebnis)	OK
Fehlerbeschreibung	keine

2.4 Testfall-004, SQL-Injection, Script-Injection und Session-Hijacking werden verhindert

Tester	Sara Roth
Datum Testdurchführung	19.10.2020
Fehlerklasse (Testergebnis)	OK
Fehlerbeschreibung	keine

2.5 Testfall-005, Registrierung und Login

Tester	Sara Roth
Datum Testdurchführung	17.10.2020
Fehlerklasse (Testergebnis)	OK
Fehlerbeschreibung	keine

2.6 Testfall-006, Daten Erfassen Ändern und Löschen

Tester	Sara Roth
Datum Testdurchführung	19.10.2020
Fehlerklasse (Testergebnis)	OK
Fehlerbeschreibung	keine

2.7 Testfall-007, Sichere Speicherung von Daten

Tester	Sara Roth
Datum Testdurchführung	17.10.2020
Fehlerklasse (Testergebnis)	OK
Fehlerbeschreibung	keine