Beurteilungsraster Projekt Modul 183

Application stirrt nicht ab, Funktionen Anforderungen aus druktioneren wie gewinscht gem. Applikation stirrt nicht ab, Funktionen Anforderungen aus druktioneren wie gewinscht gem. Projektantrag (ohne nur bestimmte enter der Benutzer das Recht nicht hat: Wenn der Beeutzer Absentzerguppen ausführen dirfen, sind sawohl im Prontend wie auch im Backenb der berücksichtigt und durcht nacht berücksichtigt und durcht nacht der berücksichtigt und durcht nacht sicht berücksichtigt und durcht nacht sicht berücksichtigt und durcht nacht nacht sicht sicht ber an der Server aufrufbar ausgeliefert. Der Login-Mechanismus ist sicher implementeitert, Passwörter sind gehabed und gesalen gespeichert Der Login-Mechanismus ist sicher implementeitert, Passwörter sind gehabed und gesalen gespeichert Der Login-Mechanismus ist sicher implementeitert, Passwörter sind gehabed und gesalen gespeichert Der Login-Mechanismus ist sicher implementeitert, Passwörter sind gehabed und gesalen gespeichert Der Login-Mechanismus wird servenden gernachte das reichte sicher erachteiter habeit und gehaben der Session-Tavation wurde in der Losung berücksichtigt und abgesichert Der Login-Mechanismus und verwendet. Das Problem der Session-Tavation wurde in der Losung berücksichtigt und abgesichert Das Problem der Session-Tavation wurde in der Losung der Session zum in der Losung berücksichtigt und abgesichert Das Problem der Session-Tavation wurde in der Losung Session zum wurden aus der alten Session zum wurden aus der Allen Session zum wurden aus der Allen Session zum einer Session zum wurden aus der Allen Session zum einer Session zum wurden aus werden Session zum einer Session zum einer Session zum wurden aus werden Session zum einer Session	Kriterium	Doku-Eintrag zwingend	Indikatoren	Belegende Feststellungen	-	0	+
Die gemäss Projektantrag definierten Anforderungen sind funktionsfähig implementiert	Allgemein	doppelt gewichtet (0.4)					
Funktionen, welche nur bestimmte Benutzer (a Brutzergruppen ausführen dürfen, sind sowohl im Frontend wie auch im Backend berücksichtigt und funktionieren Der Login-Mechanismus ist sicher implementiert, Passwörter sind gehashed und gesalzen gespeichert Das Problem der Session-Fixation wurde in der Lösung berücksichtigt und abgesichert Das Problem der Session-Fixation wurde in der Lösung berücksichtigt und abgesichert Das Problem der Gegenmassnahmen Wie wurde das realisier? In weiche Massnahmen wurden an welchen Stelle Wie wurde das realisier? Absicherung Standardangriffe migletions werden durch entsprechende Gegenmassnahmen werhindert Wiche Massnahmen werhindert Wie wurde das realisier? Absicherung Standardangriffe migletions werden durch entsprechende Gegenmassnahmen werhindert Wie wurde werden durch entsprechende Gegenmassnahmen Wie wurde werden durch entsprechende Gegenmassnahmen Werther das verden daren Werther das	Die gemäss Projektantrag definierten Anforderungen sind funktionsfähig	-	funktionieren wie gewünscht gem. Projektantrag (ohne				
Funktionen, welche nur bestimmte Benutzer / Benutzer gruppen ausführen dürfen, sind sowohl im Frontend wie auch im Backend berücksichtigt und funktionieren Der Login-Mechanismus ist sicher implementiert, Passwörter sind gehashed und gesalzen gespeichert Ober Dos Problem der Session-Fixation wurde in der Lösung berücksichtigt und abgesichert Das Problem der Session-Fixation wurde in der Lösung berücksichtigt und abgesichert Absicherung Standardangriffe migletions werden durch entsprechende Gegenmassnahmen verhindert Wie wurde das realisiert? Absicherung Standardangriffe migletions werden durch entsprechende Gegenmassnahmen wurden an welchen Stellen wurden an welchen Stellen Prepared Statements, Named Queries mit Parametern, Wurden inputvalidierung (Client-Server), Rechtebeschränkung DB-User inputvalidierung (Client-Server) Uptub Excaping Der Benutzer erhölt keine rehlermediungen, welche auf Applikationismerna schliessen lässen. Dies erfordert ein adäquates Errorhandling, Logging Der Benutzer erhölt keine rehlermediungen, welche auf Applikationismerna schliessen lässen. Dies erfordert ein adäquates Errorhandling und Logging Der Benutzer erhölt keine rehlermediungen, welche auf Applikationismerna schliessen lässen. Dies erfordert ein adäquates Errorhandling und Logging Der Benutzer erhölt keine rehlermediungen, welche auf Applikationismerna schliessen lässen. Dies erfordert ein adäquates Errorhandling und Logging Der Benutzer erhölt keine rehlermediungen, welche auf Applikationismerna schliessen lässen. Dies erfordert ein adäquates Errorhandling und Logging Der Benutzer erhölt keine rehlermediungen, welche auf Applikationismerna schliessen lässen. Dies erfordert ein adäquates Errorhandling und Logging Der Benutzer erhölt keine rehlermediungen geneme rehlermediungen erhölterten schliessen lässen. Dies erfordert ein adäquates Errorhandling und Logging Der Benutzer erhölter erhö	sicharas Sassionhandling	I	Γ				
implementiert, Passwörter sind gehashed und gesalzen gespeichert Wie wurde das realisiert? Das Problem der Session-Fixation wurde in der Lösung berücksichtigt und abgesichert Wie wurde das realisiert? Ja Wie wurde das realisiert? Wie wurde as degingenter zeitpunkt. Alifällige Wie warde attente. Named Queries mit Parametern, Imputalidierung (Client-Server), Wie wurde liert-Server) Output Escaping welche Massnahmen wurden an welchen Stellen getroffen Wie wurde stellentierung (Client-Server) Output Escaping welche Massnahmen werken durch en wurden an welchen Stellen getroffen Session/Sessioncookie (Content Security Policy >- evt. als Schwerpunkt wählbar) Errorhandling, Logging Errorhandling, Logging Errorhandling und Logging Egene Fehlerseiten für HTTP Stati 403, 404 und 500 auch über Unterschied dev/prod Umgebung möglich Fehler/Ereignisse werden intern adäquats geloggt Eigenes Kriterium mit eigenem Fokusthema doppelt gewichtet (0.4) Eigene Skriterium geines Tokens wie wurde es gerenzung der Sessiondauer entsprechende Gegenmassnahmen implementiert, Formulare per POST übertragen	Funktionen, welche nur bestimmte Benutzer / Benutzergruppen ausführen dürfen, sind sowohl im Frontend wie auch im Backend berücksichtigt und	-	hat: * Funktion nicht sichtbar * Funktion nicht manuell mit Tools auf dem Server aufrufbar * allfällige Formulare werden gar nicht				
in der Lösung berücksichtigt und abgesichert Wie wurde das realisiert? Wie wurde das realisiert? Absicherung Standardangriffe Injections werden durch entsprechende Gegenmassnahmen verhindert Welche Massnahmen wurden an welchen Stellen getroffen in junyvalidierung (Client-Server), Rechtebeschränkung DB-User Merchebeschränkung DB-User Welche Massnahmen werhindert Welche Massnahmen werhindert werden an welchen Stellen getroffen Welche Massnahmen werhindert werden an welchen Stellen getroffen Welche Massnahmen werhindert werden werden an welchen Stellen getroffen Welche Massnahmen werhindert werden seesion/Sessioncookie (Content Security Policy > evt. als Schwerpunkt wählbar) Errorhandling, Logging Errorhandling, Logging Der Benutzer erhält keine Fehler werden durch ein addquates Eigene Fehlerseiten für HTTP Stati 403, Umgebung möglich Fehler/Freignisse werden intern adäquat geloggt Eigenes Kriterium mit eigenem Fokusthema doppelt gewichtet (0.4) Eigenes Kriterium mit eigenem Fokusthema doppelt gewichtet (0.4) Eigenes Kriterium mit eigenem Fokusthema doppelt gewichtet (0.4)	implementiert, Passwörter sind	•	Passwörter mit Salt und Hash in der DB, aktuell als offiziell sicher erachteter				
injections werden durch entsprechende Gegenmassnahmen verhindert welche Massnahmen wurden an welchen Stellen getroffen XSS-Angriffe werden durch entsprechende Gegenmassnahmen verhindert XSS-Angriffe werden durch entsprechende Gegenmassnahmen verhindert welche Massnahmen wurden an welchen Stellen getroffen Session/Sessioncookie (Content Security Policy -> evt. als Schwerpunkt wählbar) Errorhandling, Logging Der Benutzer erhält keine Fehlermeldungen, welche auf Applikationsinterna schliessen lassen. Dies erfordert ein adäquates Errorhandling und Logging Telgene Fehlerseiten für HTTP Stati 403, 404 und 500 -> auch über Unterschied dev/prod Umgebung möglich Fehler/Ereignisse werden intern adäquat geloggt Eigenes Kriterium mit eigenem Fokusthema doppelt gewichtet (0.4) Beispiel: CSRF Angriffe werden durch entsprechende Gegenmassnahmen ja Berücksichtigung eines Tokens wie wurde es Begrenzung der Sessiondauer entsprechende Gegenmassnahmen inplementiert, Formulare per POST übertragen	in der Lösung berücksichtigt und	•	geeigneten Zeitpunkt. Allfällige Übernahme von Daten aus der alten				
injections werden durch entsprechende Gegenmassnahmen verhindert welche Massnahmen wurden an welchen Stellen getroffen XSS-Angriffe werden durch entsprechende Gegenmassnahmen verhindert XSS-Angriffe werden durch entsprechende Gegenmassnahmen verhindert welche Massnahmen wurden an welchen Stellen getroffen Session/Sessioncookie (Content Security Policy -> evt. als Schwerpunkt wählbar) Errorhandling, Logging Der Benutzer erhält keine Fehlermeldungen, welche auf Applikationsinterna schliessen lassen. Dies erfordert ein adäquates Errorhandling und Logging Telgene Fehlerseiten für HTTP Stati 403, 404 und 500 -> auch über Unterschied dev/prod Umgebung möglich Fehler/Ereignisse werden intern adäquat geloggt Eigenes Kriterium mit eigenem Fokusthema doppelt gewichtet (0.4) Beispiel: CSRF Angriffe werden durch entsprechende Gegenmassnahmen ja Berücksichtigung eines Tokens wie wurde es Begrenzung der Sessiondauer entsprechende Gegenmassnahmen inplementiert, Formulare per POST übertragen		1		ı	F	F	1
XSS-Angriffe werden durch entsprechende Gegenmassnahmen verhindert welche Massnahmen wurden an welchen Stellen getroffen welche Massnahmen wurden an welchen Stellen getroffen Welche Massnahmen wurden an welchen Stellen getroffen Errorhandling, Logging Der Benutzer erhält keine Fehlermeldungen, welche auf Applikationsinterna schliessen lassen. Dies erfordert ein adäquates Errorhandling und Logging Errorhandling und Logging Der Benutzer erhält keine Fehlermeldungen, welche auf Applikationsinterna schliessen lassen. Dies erfordert ein adäquates Errorhandling und Logging Der Benutzer erhält keine Fehlerseiten für HTTP Stati 403, 404 und 500 -> auch über Unterschied dev/prod Umgebung möglich Fehler/Ereignisse werden intern adäquat geloggt Eigenes Kriterium mit eigenem Fokusthema doppelt gewichtet (0.4) Beispiel: Session/Sessioncookie (Content Security Policy -> evt. als Schwerpunkt wählbar) Keine Exceptions gelangen bis zum Client Eigene Fehlerseiten für HTTP Stati 403, 404 und 500 -> auch über Unterschied dev/prod Umgebung möglich Fehler/Ereignisse werden intern adäquat geloggt Eigenes Kriterium mit eigenem Fokusthema doppelt gewichtet (0.4) Beispiel: Session/Sessioncookie (Content Security Policy -> evt. als Schwerpunkt wählbar)	Injections werden durch entsprechende	welche Massnahmen wurden an welchen Stellen	Named Queries mit Parametern, Inputvalidierung (Client+Server),				
entsprechende Gegenmassnahmen verhindert welche Massnahmen wurden an welchen Stellen getroffen welche Massnahmen wurden an welchen Stellen getroffen Errorhandling, Logging Der Benutzer erhält keine Fehlermeldungen, welche auf Applikationsinterna schliessen lassen. Dies erfordert ein adäquates Errorhandling und Logging Errorhandling und Logging Der Benutzer erhält keine Fehlermeldungen, welche auf Applikationsinterna schliessen lassen. Dies erfordert ein adäquates Errorhandling und Logging Der Benutzer erhält keine Fehlermeldungen, welche auf Applikationsinterna schliessen lassen. Dies erfordert ein adäquates Errorhandling und Logging Der Benutzer erhält keine Fehlermeldungen, welche auf Applikationsinterna schliessen lassen. Dies erfordert ein adäquates Errorhandling und Logging Der Benutzer erhält keine Eigene Fehlerseiten für HTTP Stati 403, 404 und 500 Umgebung möglich Fehler/Ereignisse werden intern adäquat geloggt Eigenes Kriterium mit eigenem Fokusthema doppelt gewichtet (0.4) Beispiel: CSRF Angriffe werden durch wie wurde es implementiert, Formulare per POST übertragen	XSS-Angriffe werden durch	getrorien					
Der Benutzer erhält keine Fehlermeldungen, welche auf Applikationsinterna schliessen lassen. Dies erfordert ein adäquates Errorhandling und Logging Errorhandling und Logging Eigenes Kriterium mit eigenem Fokusthema doppelt gewichtet (0.4) Beispiel: CSRF Angriffe werden durch entsprechende Gegenmassnahmen Keine Exceptions gelangen bis zum Client Eigene Fehlerseiten für HTTP Stati 403, 404 und 500 -> auch über Unterschied dev/prod Umgebung möglich Fehler/Ereignisse werden intern adäquat geloggt doppelt gewichtet (0.4) Berücksichtigung eines Tokens Begrenzung der Sessiondauer Formulare per POST übertragen		welche Massnahmen wurden an welchen Stellen	Output Escaping sichere Konfiguration der Session/Sessioncookie (Content Security Policy -> evt. als				
Der Benutzer erhält keine Fehlermeldungen, welche auf Applikationsinterna schliessen lassen. Dies erfordert ein adäquates Errorhandling und Logging Errorhandling und Logging Eigenes Kriterium mit eigenem Fokusthema doppelt gewichtet (0.4) Beispiel: CSRF Angriffe werden durch entsprechende Gegenmassnahmen Keine Exceptions gelangen bis zum Client Eigene Fehlerseiten für HTTP Stati 403, 404 und 500 -> auch über Unterschied dev/prod Umgebung möglich Fehler/Ereignisse werden intern adäquat geloggt doppelt gewichtet (0.4) Berücksichtigung eines Tokens Begrenzung der Sessiondauer Formulare per POST übertragen	English Was Land	I	T		1	1	1
Fokusthema doppelt gewichtet (0.4) Beispiel: CSRF Angriffe werden durch entsprechende Gegenmassnahmen doppelt gewichtet (0.4) ja Berücksichtigung eines Tokens Begrenzung der Sessiondauer Formulare per POST übertragen	Der Benutzer erhält keine Fehlermeldungen, welche auf Applikationsinterna schliessen lassen. Dies erfordert ein adäquates	-	Client Eigene Fehlerseiten für HTTP Stati 403, 404 und 500 -> auch über Unterschied dev/prod Umgebung möglich Fehler/Ereignisse werden intern				
CSRF Angriffe werden durch wie wurde es Begrenzung der Sessiondauer entsprechende Gegenmassnahmen implementiert, Formulare per POST übertragen		doppelt gewichtet (0.4)					
0 0 0	CSRF Angriffe werden durch entsprechende Gegenmassnahmen	wie wurde es implementiert,	Begrenzung der Sessiondauer Formulare per POST übertragen				
					0	0	0

Startnote:		
Starthote.	4	
Bewertungsschritt:	0.2	
Note:	4	
Bedeutung Bewertungsstufe		
- Kriterium nicht ersichtlich / nicht er	füllt, Doku fehlt oder ist sehr lücke	enhaft und knapp
0 Kriterium teilweise erfüllt / Doku vo	orhanden und Kernaussagen korre	ekt dokumentiert
+ Kriterium erfüllt / Doku ausführlich	und stimmig	