av1_data_trans

device package	comment
Activ8rLives Body Analyser com.activ8rlives.mobile	executing attacks on traffic to reveal that most of the messages are not authenticated at all; also passwords are transmitted in clear text registered and collected data; measurement captured aggregated from teststeps
FitBit aria com.fitbit.FitbitMobile	captured data and viewed in dashboard; single measurement only aggregated from teststeps
HAPI Connected Scale com.hapiconnect	replay tampering and injection tested test run to collect data from app only; registered, paired and executed measurements; on device firewall was limitting data collection to app only aggregated from teststeps
iChoice S1 com.medm.medmwt.diary	ran some attacks against the data in transmission dawith firewall activated registered, paired and collected data aggregated from teststeps
Thomson TBS705 com.stabxtom.thomson	tried to tamper with traffic by manipulating requests and stealing the session to use it to inject further measurements; however data couldnt be synchroniyed back into the application (even after deleting all app data the app doesnt intially download all dataa from server; previous measurements are simply lost collected data with firewall on device activated aggregated from teststeps
Withings WS-30 com.withings.wiscale2	recorded registration and measurements with active firewall aggregated from teststeps tampered with data and executed some replay attacks; data is not validated and can cause server errors if weight to high
iChoice S1 com.medm.ichoice.diary	created data and inspected traffic

av1_data_trans

test step	rating	desc	Activ8rLives Body Analyser com.activ8rlives.mobile	FitBit aria com.fitbit.FitbitMobile	HAPI Connected Scale com.hapiconnect	iChoice S1 com.medm.medmwt.diary	Thomson TBS705 com.stabxtom.thomson	Withings WS-30 com.withings.wiscale2	iChoice S1 com.medm.ichoice.diary
av1_inject	vulnerable: 1 / not vulnerable: 0	inject new data to the stream	1 requests with new measurements are not authenticated and measurements are mapped by userid; so as soon as one finds out a user ID measurements can be happily inserted	1 possible based on reverse engineering the transfer protocol	1 injection is possible with reconstructing the signature value.. all required values can be read from the communication stream	1 injection is only possible as long as the user provides an authenticated session	1 injection is possible	1 possible as long as scale has session and this can be used	1 possible since records just come with UUID and the auth token seems to be valid for quite some time
av1_replay	vulnerable: 1 / not vulnerable: 0	finding some way to replay information to the server	1 replaying of messages is easliy possible but will replace the existing record for a day as only one record per day can exist	1 replay possible and will create new entries on online platform; entry time is based on time when measurement got sent to the server	0 simple replay is not possible due to client side generated signatures	0 replay is not possible as every record comes with a separate uuid	1 replay attacks are perfectly possible even with stolen session ID.. however the generated data seems to be unaccessible to the user	1 replay attacks are possible within the same session session is requested based on a once which is used to generate a hash the server is able to use that hash to identify the user and sends user information including a valid session key	0 no; UUID defeats a simple replay attack
av1_ssl	not using SSL: 1 / using SSL: 0	is using SSL	0 using SSL	0 using ssl	1 no SSL	0 using SSL	1 no SSL	0 using SSL	0 yes

av1_ssl_forg	vulnerable: 1 / not vulnerable: 0	secure and correct implementation of communication encryption	1 working - username and password in message body clear text	0 not working	1 no SSL usage	0 not working	1 working - username in clear text, mobile id and password somehow encrypted or obfuscated	0 not working	1 yes, trustmanager issue
av1_ssl_forg_ca	vulnerable: 1 / not vulnerable: 0	in addition to data_com_ssl_forg the trusted CA certificate is installed	1 working as without CA certificate	1 working	1 NO SSL - username in cleartext and password somehow encrypted or obfuscated	0 not working	1 NO SSL	1 working	1 vulnerable as for other
av1_tamper	not vulnerable: 0 / upper limit e.g. weight: 1 / no limit or validation: 2	tampering the data before it can reach the server defeating input validation	2 tampering with the weight data is possible a weight up to 99999999 kg can be entered; beyond that the server will respond with an error	1 no limit possible but crc16 error detection code has to be recalculated for the full message; see python script which will allow to forge some messages	2 possible at any point in time	1 records can be changed but still the max weight is validated and limited to 300kg	2 data can be easily changed and is happily accepted by the server	2 data can be changed and apparently the server is not validating the data so that unplausible data can be entered tried to change the user ID so that the data would be inserted into a different account -> that however was not successful	1 changes possible within the limits of up to 300 kg
			6.0	4.0	6.0	2.0	7.0	5.0	4.0

av2_mobile_device

device package	comment
Activ8rLives Body Analyser **com.activ8rlives.mobile**	used some basic app functions to generate data
FitBit aria **com.fitbit.FitbitMobile**	investigating application data
HAPI Connected Scale **com.hapiconnect**	investigating the device
iChoice S1 **com.medm.medmwt.diary**	looking for data leakage
Thomson TBS705 **com.stabxtom.thomson**	found way too much information in the device logs
Withings WS-30 **com.withings.wiscale2**	run the app to synchronize and export app data to disk for further investigation
iChoice S1 **com.medm.ichoice.diary**	using app for a while

av2_mobile_device

test step	rating	desc	Activ8rLives Body Analyser com.activ8rlives.mobile	FitBit aria com.fitbit.FitbitMobile	HAPI Connected Scale com.hapiconnect	iChoice S1 com.medm.medmwt.diary	Thomson TBS705 com.stabxtom.thomson	Withings WS-30 com.withings.wiscale2	iChoice S1 com.medm.ichoice.diary
av2_export_backup	data not encrypted: 2 / data in backup encrypted: 1 / no data stored: 0	data is being backed up using the android backup command	0 no data in backup found	2 database not encrypted and shared prefs in clear text	2 database unencrypted, password in clear text in shared prefs,	1 sqlite databases not encrypted; shared preferences are obscured and encrypted	2 backup contains unencrypted database which includes all information from measurements to device information / information on session and any credentials can be picked up from the shared prefs folder	2 database is available and data can be read in clear text	2 data in caches but unencrypted
av2_export_logging	information available: 1 / no information: 0	investigate the Android log for unencrypted information	0 no suspicious data in logging information	0 no information in log file	1 logging contains detailed information on every single request send to the server	0 no information leaked in logcat	1 logcat shows detailed logs with even some information on the recorded data and partly http traces bluetooth connection management is shown in full including MAC addresses which are logged and saved	0 no information written to logcat	0 no additional logging information
			0.0	2.0	3.0	1.0	3.0	2.0	2.0

av3_mobile_app

device package	comment
Activ8rLives Body Analyser com.activ8rlives.mobile	setting up user account and checking password policies
FitBit aria com.fitbit.FitbitMobile	registered although web page failed; registration was redirected to web browser; no registration from within mobile application possible paired scale again and configured wifi ; this time better timing with phone packet capture while it is connected to the scale investigating the app and collecting data
HAPI Connected Scale com.hapiconnect	registered user and setup app change passwords and analysed traffic
iChoice S1 com.medm.medmwt.diary	registered user and provided some basic data
Thomson TBS705 com.stabxtom.thomson	ran regestration test steps paired the scale with the app tried some input validations, injection, tampering by manually adding data check the password change process and turns out that an attacker can change the victims password at any point in time after the victim opened the app and the attacker was listening to the traffic and hence able to steal the current password hash password change via email link on not secure website
Withings WS-30 com.withings.wiscale2	setting up the withings scale and saw some weird input validations (details in test cases) some manual entry added and uploaded to withings server aggregated from teststeps password change and export tests
iChoice S1 com.medm.ichoice.diary	registered user and investigated app collected data

av3_mobile_app

Activ8rLives Body	HAPI Connected

test step	rating	desc	Analyser com.activ8rlives.mobile	FitBit aria com.fitbit.FitbitMobile	Scale com.hapiconnect	iChoice S1 com.medm.medmwt.diary	Thomson TBS705 com.stabxtom.thomson	Withings WS-30 com.withings.wiscale2	iChoice S1 com.medm.ichoice.diary
av3_code_comment	informational	any comment on the code	app crashing with Android 6.0.1 so reverting back to Android 6 also App is Xamarin based and running in Monodroid VM on Android which is some C style based implementation	tbd tbd	passwords are just hased with MD5 no salt; after re login signature looks suspicious as no password is transmitted - seems to be generated based on current time, previous access token and some generat random number; but all this information is available to an attacker	code is somewhat supprisingly just a few lines and decompiled code doesn't show all the information hence something must have been applied to the code also certificate pinning is implemented and had to be removed in order to run further tests	code shows many different frameworks and addons integrated with the solution (also see addons table) the app itself shows less possibilities to make actually use of these frameworks and addons the password seems to be MD5 hashed but since the communication is not encrypted and the hash is not randomiyed that is pointless, simply use the hash value to execute anything	tbd	java coding with native dependencies
av3_data_coll	informational	data collected and send by the mobile app	normal data collection of pictures and other details on the phone	weight can be entered and other fitness data	not possible to enter data manually	manual input only and photo capture to set profile picture	as mentioned app collecteds weight data but also sends phone identifier to china	added entry manually to be uploaded to server API with server seems to be different from the scales API query parameters instead of body but everything is SSL encrypted some input validation inside the mobile application is done; manual entries are possible; no othe seems to be transmitted	weight can be entered manually and is limited to 300
av3_data_leakage	no data leaked: 0 / complies with privacy policy: 1 / data leaked beyond privacy policy: 2	identifiable for the user or the phone that is being collected	2 xamarin framework is sending the android device id home and is tracking different events such as network change from wifi to lte, application startup and a full device fingerprint including attributes such aus screensize, resolution, network, model, memroy, cpu count, android version, client version, app installed	0 device fingerprinting and application usage tracking but without any personal data ; all data is being send to mixpanel.com	2 no SSL implemented so data can easily be read; in addition passwords are just MD5 hased without salts what makes them vulnerable to rainbow table lookups; full personal information including email address, password, date of birth, weight and height can be read	1 as far as captured no data was being leaked	2 !! advertising librariy Umeng detected.. library is sending a full device fingerprint including IMEI and MAC (where it cant retrieve the MAC because of Android 6 changes) /n password (encrypted) and email send over unencrypted network; password seems to be some kind of 16byte hash.. tried a few tools to get the pattern and repoduce it but so far without success reveals full details during pairing as serial numbers, device hardware version, software version and some specific password are sent unencryted	1 none	0 no leakage identified
av3_data_wipe	unsecure feature: 1 / secure feature: 0	can data be wiped from the mobile application	1 no possibility to wipe data from inside the app	1 no feature	1 not possible from within the app	1 no data wipe option	1 no data wipe from within the app only be using the system settings; also no possibility to delete data from the server and hard to contact them as there is no email received or any information inside the app	1 no possibility to wipe data from app or from device, no way to delete account	1 no option

ID	Scoring	Description							
av3_export_cloud	unsecure feature: 1 / secure feature: 0	data being exported somewhere into the cloud (dropbox et al)	n/a n/a	n/a no export possible	n/a screenshots can be exported which show some graph with weight overview	n/a n/a	n/a no possibility	n/a no export option in app	n/a n/a
av3_export_sdcard	unsecure feature: 1 / secure feature: 0	can data be exported to SD card or other locations on device and is that data encrypted	n/a n/a	n/a no export possible	n/a n/a	n/a n/a	n/a no option	n/a no export option	n/a n/a
av3_export_social	unsecure feature: 1 / secure feature: 0	export variants to social media and data encryption while exporting	n/a n/a	0 connection to facebook possible but for information only	0 screenshot of the graph can be shared with any 3rd party app	n/a n/a	0 twitter, facebook and email but none of them worked	n/a sharing is just inviting and as such possible to gmail, drive, bluetooth and android beam	n/a n/a
av3_pwd_change_freq	no period or frequency: 2 / either one: 1 / both: 0	password change period (must) and frequency (can)	n/a can't change password from within the app	n/a	2 nothing enforced	n/a	2 no password change policy or frequency enforced	2 n/a	n/a
av3_pwd_change_policy	no policy: 0 / min characters: 1 / mixed charsets: 2	password policy enforced on password change	n/a n/a	n/a	1 min 6 characters	n/a	1 password policy is just 6 characters only and nothing else	n/a	n/a
av3_pwd_change_reuse	yes, unlimited: 0 / no, but history can be bypassed (see change freq): 1 / no without limitation: 2	can a password be reused and how much difference is required	n/a n/a	n/a	1 last password can't be reused	n/a	2 passwords can be reused at any point in time how often ever the user wants to	n/a	n/a
av3_reg_acc_verif	none: 2 / email account verification: 1 / two factor authentication 0	email account verification or two factor authentication	2 received no email on account verification / registration	n/a	2 not at all	2 no - but received email with pointers to privacy statements and similar stuff	2 no verification email received	2 there is no trace of account verification not even a single email was received assumption that this might be solution dependent as the withings watch caused a lot of spam in the inbox	2 received registration confirmation email
av3_reg_data_input	informational	Specifies the data fields and types which are required as inputs	weight, height, waistline, birthdate and bio data, fitness goal and setps towards the goal basic validation on weight, height and waistline	n/a n/a	username, email, weight and height, and password	only email address and password mandatory; name, birth date and height can be entered later from within the app	email, password, name, gender, name, birthday, height, weight, waistline, picture	select scale n email and password n firstname, lastname, birthdate, height, weight	name, email, gender optionally later weight, height and profile picture
		Comments on							

av3_reg_data_validation	data not validated: 1 / data is validated: 0	data validation during user registration: weight, heitght, email...	0 basic validation on weight, height and waistline	n/a n/a	0 weight and height only	0 height and weight are limited; no other validation	0 limited values for weight, height, waistline, age	0 email adress is validated n password provided A n very high weights are not allowed 600lb but weird error message n height is accepted at 3m	1 limited to 300 height and weight
av3_reg_pripol_link	no link or information: 1 / link available: 0	link to privacy policy or any kind of information on such topic	0 link to terms and conditions plus acceptance of terms and conditions is required to use the app	n/a n/a	1 no explicit link visible	1 not visible during registration but linked from within the app	1 no link to privacy policy apparent	0 link to privacy policy is provided http://www.withings.com/uk/en/legal also terms and conditions but both links are pointing to the same webpage1	1 no link visible
av3_reg_pwd_policy	no policy: 2 / min characters: 1 / mixed charsets: 0	is a password policy enforced	2 no password policy as registration with a simple A was possible	n/a n/a	1 min 6 characters	1 min 6 character	1 6-16 characters	2 no hint to any kind of password policy could be found	1 min 6 characters
			7.0	1.0	11.0	6.0	12.0	8.0	6.0

av4_third_party

device package	comment
Activ8rLives Body Analyser **com.activ8rlives.mobile**	leakage of data to xamarin
FitBit aria **com.fitbit.FitbitMobile**	no data being leaked
HAPI Connected Scale **com.hapiconnect**	investigating data leakage
iChoice S1 **com.medm.medmwt.diary**	no data leakage found
Thomson TBS705 **com.stabxtom.thomson**	data leakage to third party investigated
Withings WS-30 **com.withings.wiscale2**	data leakage
iChoice S1 **com.medm.ichoice.diary**	no leakage observed

av4_third_party

test step	rating	desc	Activ8rLives Body Analyser com.activ8rlives.mobile	FitBit aria com.fitbit.FitbitMobile	HAPI Connected Scale com.hapiconnect	iChoice S1 com.medm.medmwt.diary	Thomson TBS705 com.stabxtom.thomson	Withings WS-30 com.withings.wiscale2	iChoice S1 com.medm.ichoice.diary
			1	0	1	0	1	0	0
av4_data_leakage	no data leaked: 0 / complies with privacy policy: 1 / data leaked beyond privacy policy: 2	data leakage to third party services	detailled data on the device is leaked to xamarin servers; this data can be used for fingerprinting and shouldn't be collected; there are other device identifiers that can be used /n pictures taken are uploaded to an image service and not to their own servers	no data being leaked so far	no data leakage apparent	no data leakage to third party on recor d	data is being leaked to advertising companies; data includes phone identifier information	no data being leaked	no leakage observed
			1.0	0.0	1.0	0.0	1.0	0.0	0.0

av5_sensor_device

device package	comment
Activ8rLives Body Analyser com.activ8rlives.mobile	connected scale and did some measurements
FitBit aria com.fitbit.FitbitMobile	some measurements with the scale captured firmware being send to the scale measurements with increasing weight from 75.9, 76.0 to 76.1
HAPI Connected Scale com.hapiconnect	paired scale but the app ended up in some loop sending the same request infintely running pairing and data collection test cases
iChoice S1 com.medm.medmwt.diary	paired device and did some measurements
Thomson TBS705 com.stabxtom.thomson	collected some data by weighting and sending data to web server
Withings WS-30 com.withings.wiscale2	first tried to setup scale using bluetooth but didnt work; then tried via wifi and would work; traffic from scale to withings webserver is http only; possibly can be exploited for replay attacks as well; maybe firmware update will defeat the http vulnerability as the scale partly communicates via https collected data from scale and successfully uploaded to withings; added a new user within the same account, but withings offers as well to associate the same scale with different accounts; replay attacks are likely to be successful manipulated request for firmware and got link to update.. firmware can be downloaded
iChoice S1 com.medm.ichoice.diary	collected data from scale

av5_sensor_device

test step	rating	desc	Activ8rLives Body Analyser com.activ8rlives.mobile	FitBit aria com.fitbit.FitbitMobile	HAPI Connected Scale com.hapiconnect	iChoice S1 com.medm.medmwt.diary	Thomson TBS705 com.stabxtom.thomson	Withings WS-30 com.withings.wiscale2	iChoice S1 com.medm.ichoice.diary
av5_data_coll	informational	characteristics of data collected by the sensor	collecting data from scale and transferring it immediately without any user interact the webservice	data is being collected as weight and bodyfat; data can be assigned to a user immediatley after that user has been synchronised to the scale	weight is collected and uploaded; as far as seen no other data is added	collects data from scale as expected and save's on device; after some time it will be synchronized to the server	collecting weight information just as expected	data is being transmitted via http only scale is able to display the weather of the day other then that it just collects a measurements with a UNIX timestamp and the weight in g this a JSON document being posted to the server also location information is send to the scale and used by it; this communication is encrypted	measurement just as expected; can be tampered and injection possible as long as auth token is valid
av5_pairing_process	informational	pairing process between sensor and phone	no pairing process as such as the scale doesn't authenticate itself with the app but communicates anonymously	pairing is initiated from the web page where the user has to login to a account; after obtaining a registration credentials for the scale, the scale is started to expose a wifi hotspot and then one has to connect to the scales hotspot to configure it; this is done by selecting a wifi network it should connect to and providing relevant login credentials; however these credentials are transmitted in clear text and hence leaked during the login process; the scale is then linked to the users account and can send data to that account	pairing process is without real device pairing using a passcode or something	pairing comes again without real bluetooth pairing.. interestingly the device asks for location access rather than bluetooth access permission	no real pairing	pairing is possible via bluetooth to the phone; it requires an authentication and is persisted; thereafter the scale is able to communicate via wifi or bluetooth with the server	no real pairing process
av5_swfw_update	vulnerable: 1 / not vulnerable: 0	update cycle related issues	1 app to server communication doesn't show any hint regarding a firmware version for the scale	0 firmware is queried from scale after uploading new measurements; firmware can be updated on a regular basis	1 communication between app and server doesn't show any hint of information on possible firmware updates	1 no version information exchanged between app and server	1 scale sends its version on registration to the server but doesn't expect any updates	0 scale asks server if any firmware update is available and provides the currently installed version intercepting this request and changing the firmware yields a link to an update send by server	1 no software or firmware update cycle
			1.0	0.0	1.0	1.0	1.0	0.0	1.0

av6_web_application

device package	comment
Activ8rLives Body Analyser com.activ8rlives.mobile	basic ellaboration of the web page user registration via web page
FitBit aria com.fitbit.FitbitMobile	gathered data on web page; attention: wlan SSID is mentioned on web page
HAPI Connected Scale com.hapiconnect	data input tests and testing manipulation investigated web page
iChoice S1 com.medm.medmwt.diary	explored web access tested for csrf vulnerability
Thomson TBS705 com.stabxtom.thomson	no web page found which would come with the solution
Withings WS-30 com.withings.wiscale2	investigate if account can be delete with spoofed information --> account can't be deleted with stolen session id from unencrypted sensor device communication
iChoice S1 com.medm.ichoice.diary	registered and researched web interface

av6_web_application

test step	rating	desc	Activ8rLives Body Analyser com.activ8rlives.mobile	FitBit aria com.fitbit.FitbitMobile	HAPI Connected Scale com.hapiconnect	iChoice S1 com.medm.medmwt.diary	Thomson TBS705 com.stabxtom.thomson	Withings WS-30 com.withings.wiscale2	iChoice S1 com.medm.ichoice.diary
av6_csrf	vulnerable: 1 / not vulnerable: 0	basic CSRF attack	1 — csrf token are not renewed after request so that if an attacker manages to steal one of them he is able to send requests for the duration of the session; csrf token is correctly bound to the session	0 — ouath and csrf tokens protect	0 — tested on password change and found that websites protects against CSRF	0 — not vulnerable.. is using authenticity tokens for requests	n/a — n/a	0 — protected	
av6_data_input	data not validated: 1 / data is validated: 0	data input via web UI and validation	0 — data is limited to max 300kg	0 — weight data and other measurement data can be entered on web page	1 — data is not validated since unreasonably high measurements can be entered	1 — data is not validated but sanitized	n/a — n/a	0 — limited	
av6_data_wipe	insecure feature: 1 / secure feature: 0	wipe and delete data from the web account	1 — data wipe is not available from the web page; the policy mentions two mail addresses one for deactivation and one for deletion of which none worked; email send to again another mail address and waiting for response -> even worse managed to send an email from a different email account to delete another account	0 — no feature implemented but possible per email request; sender email has to be the account email	0 — no option	0 — account deletion possible	n/a — n/a	0 — account can be deleted but has 7 days period before they claim that data will actually be removed from their systems	

Field	Scoring	Description						
av6_export_cloud	insecure feature: 1 / secure feature: 0	data being exported somewhere into the cloud (dropbox et al)	n/a; no export options	n/a; n/a	n/a; n/a	n/a; n/a	n/a; n/a	n/a; n/a
av6_export_disk	insecure feature: 1 / secure feature: 0	can data be exported to SD card or other locations on device and is that data encrypted	0; excel document can be exported and data within that document is unencrypted	0; your data belongs to you - comment and download via htt	n/a; n/a	0; download as csv or html page	n/a	0; only after account deletion data can be downloaded
av6_export_social	insecure feature: 1 / secure feature: 0	export variants to social media and data encryption while exporting	n/a; no social sharing other than the web platforms own sharing is implemented; carer can be invited and also practitioners and clinics can get access; however that feature was not working	0; social sharing possible but with detailled privacy settings	0; facebook, twitter	n/a; only within the same platform	n/a	n/a; no hint that data can be shared online
av6_pri_pol	no link or information: 1 / link available: 0	pirvacy poclicy linked and available	0; the privacy policy is linked from the web page	0; accessible from the page footer area where it is linked	0; link in footer but not very visible	0; linked on web page	n/a	0; visibly linked from web interface
av6_pwd_change_freq	no period or frequency: 2 / either one: 1 / both: 0	password change period (must) and frequency (can)	2; not implemented	2; no frequency defined	2; none	2; none	n/a	2; no frequency enforced
av6_pwd_change_policy	no policy: 2 / min characters: 1 / mixed charsets: 0	password policy enforced on password change	2; none	1; min 8 characters	1; 6 characters	1; min 6 characters	n/a	1; min 6 char; any char no type enforcement
av6_pwd_change_reuse	yes, unlimited: 0 / no, but history can be bypassed (see change freq): 1 / no without limitation: 2	can a password be reused and how much difference is required	2; none	2; unlimited reuse	2; unlimited	2; not limited	n/a	2; unlimited reuse
av6_reg_acc_verif	none: 2 / email account verification: 1 / two factor authentication 0	email account verification or two factor authentication	2; none	1; account verification per email send but not enforced	2; no	1; no.. just email with confirmation that account has been created	n/a	2; no verification
av6_reg_data_input	informational	Specifies the data fields and types which are required as inputs	same as app	mail, name, dob, weight (limited), height (limited)	name, email, date of birth, goals	same as app	n/a; n/a	same as mobile app
av6_reg_data_validation	data not validated: 1 / data is validated: 0	Comments on data validation during user registration: weight, heitght,	0; same as app: only medical data	0; sanitized and validated	1; no	0; same as app	n/a	0; some data validation for height and weight

		email...						
av6_reg_pripol_link	no link or information: 1 / link available: 0	link to privacy policy or any kind of information on such topic	1 not visible but very hidden in footer	0 privacy policy link is available and has to be acknowledged; in addition hint that data is transferred to the US	1 not visible but very hidden in footer	0 visible in registration form	n/a n/a	0 yes
av6_reg_pwd_policy	no policy: 2 / min characters: 1 / mixed charsets: 0	is a password policy enforced	2 no	1 min 8 character	1 min 6 characters	1 min 6 characters	n/a n/a	1 min 6 char
av6_sql_injection	vulnerable: 1 / not vulnerable: 0	inject sql queries to learn information from the server	0 protects against basic sql injection	0 not possible	0 no	0 not possible	n/a	