LIST OF ATTACHMENTS

APPENDIX A

Table 8 Classification of factors for probability[15]

Likelihood factors							
Threat Agent Factors (TAF)				**Vulnerability Factors (VF)**			
Skills required (SL)	**Motive (M)**	**Opportunity (O)**	**Population Size (S)**	**Easy of Discovery (ED)**	**Ease of Exploit (EE)**	**Awareness (A)**	**Intrusion Detection (IDE)**
Not Applicable [0]	Not Applicable [0]	Full access or expensive resources required [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]
No technical skills [1]	Low or no reward [1]	Special access or resources required [4]	System Administrators [2]	Practically impossible [1]	Theoretical [1]	Unknown [1]	Active detection in application [1]
Some technical skills [3]	Possible reward [4]	Some access or resources required [7]	Intranet Users [4]	Difficult [3]	Difficult [3]	Hidden [4]	Logged and reviewed [3]
Advanced computer user [5]	High reward [9]	No access or resources required [9]	Partners [5]	Easy [7]	Easy [5]	Obvious [6]	Logged without review [8]
Network and programming skills [6]			Authenticated users [6]	Automated tools available [9]	Automated tools available [9]	Public knowledge [9]	Not logged [9]
Security penetration skills [9]			Anonymous Internet users [9]				

[15] https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Table 9 Classification of impact factors[16]

Impact factors							
Technical Impact Factors (TIF)				**Business Impact Factors (BIF)**			
Loss of confidentiality (LC)	**Loss of Integrity (LI)**	**Loss of Availability (LAV)**	**Loss of Accountability (LAC)**	**Financial damage (FD)**	**Reputation damage (RD)**	**Non-Compliance (NC)**	**Privacy violation (PV)**
Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]
Minimal non-sensitive data disclosed [2]	Minimal slightly corrupt data [1]	Minimal secondary services interrupted [1]	Attack fully traceable to individual [1]	Damage costs less than to fix the issue [1]	Minimal damage [1]	Minor violation [2]	One individual [3]
Extensive non-sensitive data disclosed [6]	Minimal seriously corrupt data [3]	Minimal primary services interrupted [5]	Attack possibly traceable to individual [7]	Minor effect on annual profit [3]	Loss of major accounts [4]	Clear violation [5]	Hundreds of people [5]
Extensive critical data disclosed [7]	Extensive slightly corrupt data [5]	Extensive primary services interrupted [7]	Attack completely anonymous [9]	Significant effect on annual profit [7]	Loss of goodwill [5]	High profile violation [7]	Thousands of people [7]
All data disclosed [9]	Extensive seriously corrupt data [7]	All services completely lost [9]		Backruptcy [9]	Brand damage [9]		Millions of people [9]

[16] https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

APPENDIX B

Table 10 Description of STRIDE threats and mitigations[17]

Type	Description	Security Control
Spoofing	Threat action aimed at accessing and use of another user's credentials, such as username and password.	Authentication
Tampering	Threat action intending to maliciously change or modify persistent data, such as records in a database, and the alteration of data in transit between two computers over an open network, such as the Internet.	Integrity
Repudiation	Threat action aimed at performing prohibited operations in a system that lacks the ability to trace the operations.	Non-Repudiation
Information disclosure	Threat action intending to read a file that one was not granted access to, or to read data in transit.	Confidentiality
Denial of service	Threat action attempting to deny access to valid users, such as by making a web server temporarily unavailable or unusable.	Availability
Elevation of privilege	Threat action intending to gain privileged access to resources in order to gain unauthorized access to information or to compromise a system.	Authorization

[17] https://owasp.org/www-community/Threat_Modeling_Process#stride

APPENDIX C

Table 11 Protocol template for threat modelling

Application decomposition	Protocol name		
	Description of the use case		
	Document owner		
	Participating		
	Checked by		
	Category data classification		
	Architecture		
	Network location		
	Authentication factors		
	Digital signing		
	Encryption		
	Account Privileges		
Threat modeling and risk analysis	STRIDE THREATS	Spoofing	
		Tampering	
		Repudiation	
		Information disclosure	
		Denial of service	
		Elevation of privilege	
	DREAD vekcor		
	Likelihook		
	Impact		
	Risk score		
Mitigations	STRIDE mitigations	Spoofing	
		Tampering	
		Repudiation	
		Information disclosure	
		Denial of service	
		Elevation of privilege	

APPENDIX D

Table 12 List of aspects and factors allocated.

Aspects							
Dataclass (DC)	**Architecture (ARCH)**	**Network location (NL)**	**Authentication factors (AF)**	**Signing (SIG)**	**Encryption (ENC)**	**User Priviliges (UP)**	**Authentication protocols (AP)**
Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Not Applicable [0]	Anonymous web User [0]	RSA Key based (certificate) [2]
Public [1]	More than 3-tier [4]	No inspection [1]	Multi factor authentication [1]	RSA Asymmetric Signature [1]	RSA, ECC, GPG, PGP, Hybrid [2]	User with valid credentials [2]	SAML, OAuth2, OIDC [3]
Internal [4]	3-tier [5]	1 inspection node [3]	3 factor authentication [2]	HMAC symmetric signature [2]	AES, TLS [4]	DB server Administrator [4]	Kerberos ticket [4]
Confidential [6]	2-tier [7]	2 inspection nodes [4]	2 factor authentication [3]	Event based token [5]	3DES [6]	Service provider Administrator [5]	NTLM [5]
Strictly confidential, unknown data classification [9]	1-tier, Unknown architecture [9]	3 inspection nodes [5]	1 factor authentication [5]	Time based token [6]	DES [7]	Service provider user process [7]	LDAP, RADIUS [6]
		4 inspection nodes [7]	User identification only [7]	Timestamp [7]	ENCODE [8]	Service provider root/administrator process [9]	OTP, CAPTCHA [7]
		More than 4, Unknown Location [9]	No authentication [9]	HASH [8]	None, Unknown encryption [9]		APIKEY, BASE64, ClearText, Cookies [8]
				None, Unknown signing [9]			None, Unknown authentication mechanism [9]

APPENDIX E

Table 13 Measured DREAD factor values for all aspect values.

Aspects / Threats	Aspect Value	Likelihood factors								Impact factors							
		Threat Agent Factors (TAF)				Vulnerability Factors (VF)				Technical Impact Factors (TIF)				Business Impact Factors (BIF)			
		SL	M	O	S	ED	EE	A	IDE	LC	LI	LAV	LAC	FD	RD	NC	PV
		1,3,5,6,9	1,4,9	4,7,9	2,4,5,6,9	1,3,7,9	1,3,5,9	1,4,6,9	1,3,8,9	2,6,7,9	1,3,5,7	1,5,7,9	1,7,9,	1,3,7,9	1,4,5,9	2,5,7	3,5,7,9
dataclass (0,1,5,6,9)	1		1							2				1	1	2	3
dataclass (0,1,5,6,9)	4		4							6				7	4	5	5
dataclass (0,1,5,6,9)	6		9							6				7	9	7	7
dataclass (0,1,5,6,9)	9		9							9				9	9	7	9
architect(0,1,4,7,9)	1	1	1	4	2	1	1	1	1	2	1	1	1	1	1	2	3
architect(0,1,4,7,9)	4	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5
architect(0,1,4,7,9)	7	9	9	7	9	7	9	9	8	7	7	7	7	7	9	7	7
architect(0,1,4,7,9)	9	9	9	9	9	9	9	9	9	9	7	9	9	9	9	7	9
netloc(0,1,3,4,5,7,9,)	1	1	1	4	2	1	1	1	1	2	1	1	1	1	1	2	3
netloc(0,1,3,4,5,7,9,)	3	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3
netloc(0,1,3,4,5,7,9,)	4	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5
netloc(0,1,3,4,5,7,9,)	5	5	9	7	5	7	5	6	8	6	5	5	7	7	5	5	5
netloc(0,1,3,4,5,7,9,)	7	9	9	7	9	7	9	9	8	7	7	7	7	7	9	7	7
netloc(0,1,3,4,5,7,9,)	9	9	9	9	9	9	9	9	9	9	7	9	9	9	9	7	9
sign(1,2,5,6,7,8,9)	1	1	1	4	2	1	1	1	1	2	1		1	1	1	2	3
sign(1,2,5,6,7,8,9)	2	3	4	4	2	3	3	4	3	2	3		7	3	4	2	3
sign(1,2,5,6,7,8,9)	5	5	9	7	5	7	5	6	8	6	5		7	7	5	5	5

sign(1,2,5,6,7,8,9)	6	6	9	7	6	7	9	6	8	6	7		7	7	9	7	7
sign(1,2,5,6,7,8,9)	7	9	9	7	9	7	9	9	8	7	7		7	7	9	7	7
sign(1,2,5,6,7,8,9)	8	9	9	9	9	9	9	9	8	9	7		9	9	9	7	9
sign(1,2,5,6,7,8,9)	9	9	9	9	9	9	9	9	9	9	7		9	9	9	7	9
enc(2,4,6,7,8,9)	2	3	4	4	2	3	3	4	3	2	3			3	4	2	3
enc(2,4,6,7,8,9)	4	5	4	4	4	7	5	4	8	6	5			7	4	5	5
enc(2,4,6,7,8,9)	6	6	9	7	6	7	9	6	8	6	7			7	9	7	7
enc(2,4,6,7,8,9)	7	9	9	7	9	7	9	9	8	7	7			7	9	7	7
enc(2,4,6,7,8,9)	8	9	9	9	9	9	9	9	8	9	7			9	9	7	9
enc(2,4,6,7,8,9)	9	9	9	9	9	9	9	9	9	9	7			9	9	7	9
up(2,4,5,7,9)	2	3	4	4	2	3	3	4		2				3	4	2	3
up(2,4,5,7,9)	4	5	4	4	4	7	5	4		6				7	4	5	5
up(2,4,5,7,9)	5	5	9	7	5	7	5	6		6				7	5	5	5
up(2,4,5,7,9)	7	9	9	7	9	7	9	9		7				7	9	7	7
up(2,4,5,7,9)	9	9	9	9	9	9	9	9		9				9	9	7	9

APPENDIX F

Table 14 List of authentication protocols by observed aspects.

Authentication protocols	Aspects	Likelihood factors								Impact factors							
		Threat Agent Factors (TAF)				Vulnerability Factors (VF)				Technical Impact Factors (TIF)				Business Impact Factors (BIF)			
		SL	M	O	S	ED	EE	A	IDE	LC	LI	LAV	LAC	FD	RD	NC	PV
	dc, arch, nl, af, sig, enc, up	1,3,5,6,9	1,4,9	4,7,9	2,4,5,6,9	1,3,7,9	1,3,5,9	1,4,6,9	1,3,8,9	2,6,7,9	1,3,5,7	1,5,7,9	1,7,9,	1,3,7,9	1,4,5,9	2,5,7	3,5,7,9
mTLS	9,7,**3**,3,9,2,**2**	3	4	4	2	3	3	4	3	2	3	5	7	3	4	2	3
SAML	9,**5**,**4**,5,1,9,**2**	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3
OAuth2	9,**5**,**4**,5,1,9,**2**	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3
OIDC	9,4,**5**,5,1,9,**2**	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3
Kerberos/SPNEGO	9,4,**4**,5,6,4,**5**	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5
NTLM	9,4,**3**,5,8,9,**5**	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3
Digest access authentication	9,4,**3**,5,8,9,**5**	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3
LDAP	9,**7**,**3**,5,**8**,9,7	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3
RADIUS	9,**7**,**3**,5,**7**,9,7	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3
OTP	9,**5**,**4**,7,**9**,9,9	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5
CAPTCHA	9,**7**,**4**,7,5,9,9	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5
APIKEY	9,**7**,9,7,9,9,9	9	9	7	9	7	9	9	8	7	7	7	7	7	9	7	7
HTTP Basic	9,**7**,9,5,9,**8**,9	5	9	7	5	7	5	6	8	6	5	7	7	7	5	5	5
ClearText	9,9,9,7,9,9,9	9	9	7	9	9	9	9	8	9	7	7	7	7	9	7	7
Cookies	9,**4**,**3**,5,9,9,9	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3
Unknown	9,9,9,9,9,9,9	9	9	9	9	9	9	9	9	9	7	9	9	9	9	7	9
None	9,9,9,9,9,9,9	9	9	9	9	9	9	9	9	9		9	9	9	9	7	9

APPENDIX G

Table 15 TMP0 values for authentication protocols used in calculations.

		Likelihood factors								Impact factors												
TMP (0)	dc, arch, nl, af, sig, enc, up	Threat Agent Factors (TAF)				Vulnerability Factors (VF)				Technical Impact Factors (TIF)				Business Impact Factors (BIF)				**risklevel**	**liklevel**	**likvalue**	**implevel**	**impvalue**
		SL	M	O	S	ED	EE	A	IDE	LC	LI	LAV	LAC	FD	RD	NC	PV					
Certificate	9,7,**3**,3,9,2,**2**	3	4	4	2	3	3	4	3	2	3	5	7	3	4	2	3	MEDIUM	MEDIUM	3,250	MEDIUM	3,625
SAML	9,**5**,**4**,5,1,9,**2**	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3	INFO	LOW	1,500	LOW	2,000
OAuth2	9,**5**,**4**,5,1,9,**2**	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3	INFO	LOW	1,500	LOW	2,000
OIDC	9,4,**5**,5,1,9,**2**	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3	INFO	LOW	1,500	LOW	2,000
Kerberos/SPNEGO	9,4,**4**,5,6,4,**5**	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5	MEDIUM	MEDIUM	5,125	MEDIUM	5,500
NTLM	9,4,**3**,5,8,9,**5**	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	MEDIUM	3,500	MEDIUM	4,500
Password based mTLS	9,4,**3**,5,8,9,**5**	3	4	4	2	3	3	4	8	2	5	5	7	3	4	2	3	MEDIUM	MEDIUM	3,875	MEDIUM	3,875
Digest access authentication	9,4,**3**,5,8,9,**5**	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	MEDIUM	3,500	MEDIUM	4,500
LDAP	9,**7**,**3**,5,**8**,9,7	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	MEDIUM	3,500	MEDIUM	4,500
RADIUS	9,**7**,**3**,5,**7**,9,7	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	MEDIUM	3,500	MEDIUM	4,500

OTP	9,**5**,**4**,7,**9**,9,9	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5	MEDIUM	MEDIUM	5,125	MEDIUM	5,500
CAPTCHA	9,**7**,**4**,7,5,9,9	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5	MEDIUM	MEDIUM	5,125	MEDIUM	5,500
APIKEY	9,**7**,4,7,9,9,9	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5	MEDIUM	MEDIUM	5,125	MEDIUM	5,500
BASE64	9,**7**,9,5,9,**8**,9	5	9	7	5	7	5	6	8	7	7	5	7	7	5	5	5	CRITICAL	HIGH	6,500	HIGH	6,000
ClearText	9,9,9,7,9,9,9	9	9	7	9	9	9	9	8	9	7	7	7	7	9	7	7	CRITICAL	HIGH	8,625	HIGH	7,500
Cookies	9,**4**,**3**,5,9,9,9	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	MEDIUM	3,500	MEDIUM	4,500
Unknown	9,9,9,9,9,9,9	9	9	9	9	9	9	9	9	9	7	9	9	9	9	7	9	CRITICAL	HIGH	9,000	HIGH	8,500
None	9,9,9,9,9,9,9	9	9	9	9	9	9	9	9	9	7	9	9	9	9	7	9	CRITICAL	HIGH	9,000	HIGH	8,500

APPENDIX H

BADI

- Models
- Aspects
- Threats
- Users

Aspects

Data classification level

New

#	Name	Value	Description
1	Not Applicable [0]	0	Not Applicable [0]
2	Public [1]	1	Public [1]
3	Internal [4]	4	Internal [4]
4	Confidential [6]	6	Confidential [6]
5	Strictly confidential, unknown data classification [9]	9	Strictly confidential, unknown data classification [9]

Architecture

New

#	Name	Value	Description
6	Not Applicable [0]	0	Not Applicable [0]
7	More than 3-tier [4]	4	More than 3-tier [4]
8	3-tier [5]	5	3-tier [5]
9	2-tier [7]	7	2-tier [7]
10	1-tier, Unknown architecture [9]	9	1-tier, Unknown architecture [9]

Authentication protocol

New

#	Name	Value	Description
46	Certificate		Certificate
47	SAML		SAML
48	OAuth2		OAuth2
49	OIDC		OIDC
50	Kerberos/SPNEGO		Kerberos/SPNEGO
51	NTLM		NTLM
52	Digest access authentication		Digest access authentication
53	LDAP		LDAP
54	RADIUS		RADIUS
55	OTP		OTP
56	CAPTCHA		CAPTCHA
57	APIKEY		APIKEY
58	BASE64		BASE64

Figure 18 Application screen for editing aspects

BADI

- Models
- Aspects
- Threats
- Users

Threats

Threat list

New

#	Name	Desc.	Auth	DataClass	Arch.	Location	Auth fact.	Sign	Enc	Priv.	Risk	Lik.	Lik. value	Imp.	Imp. value	Timestamp
50	tmp0	Worst case scenario	APIKEY	Strictly confidential, unknown data classification [9]	2-tier [7]	More than 4, Unknown Location [9]	User identification only [7]	None, Unknown signing [9]	None, Unknown encryption [9]	Service provider root/administrator process [9]	CRITICAL	HIGH	8.375	HIGH	7.25	2022-03-31 16:29:13
51	tmp0	Worst case scenario	BASE64	Strictly confidential, unknown data classification [9]	2-tier [7]	More than 4, Unknown Location [9]	1 factor authentication [5]	None, Unknown signing [9]	ENCODE [8]	Service provider root/administrator process [9]	CRITICAL	HIGH	6.5	HIGH	6	2022-03-31 16:27:54
3	dc(6)	Data classification (6)		Confidential [6]							LOW	LOW	1.125	MEDIUM	4.5	2022-03-31 16:06:16
2	dc(4)	Data classification (4)		Internal [4]							LOW	LOW	0.5	MEDIUM	3.375	2022-03-31 16:05:10
4	dc(9)	Data classification (9)		Strictly confidential, unknown data classification [9]							LOW	LOW	1.125	MEDIUM	5.375	2022-03-31 16:04:41
1	dc(1)	Data classification (1)	0	Public [1]	0	0	0	0	0	0	INFO	LOW	0.125	LOW	1.125	2022-03-31 15:57:42
31	enc(7)	Encryption type (7)							DES [7]		HIGH	HIGH	8.375	MEDIUM	5.5	2022-03-24 17:18:04
30	enc(6)	Encryption type (6)							3DES [6]		HIGH	HIGH	7.25	MEDIUM	5.375	2022-03-23 17:18:04
29	enc(4)	Encryption type (4)							AES [4]		MEDIUM	MEDIUM	5.125	MEDIUM	4	2022-03-22 17:18:04
28	enc(2)	Encryption type (2)							RSA, ECC, GPG, PGP, Hybrid [2]		LOW	MEDIUM	3.25	LOW	2.125	2022-03-21 17:18:04
27	sign(9)	Signature (9)						None, Unknown signing [9]			CRITICAL	HIGH	9	HIGH	7.375	2022-03-20 17:18:04
26	sign(8)	Signature (8)						HASH [8]			CRITICAL	HIGH	8.875	HIGH	7.375	2022-03-19 17:18:04
25	sign(7)	Signature (7)						Timestamp [7]			CRITICAL	HIGH	8.375	HIGH	6.375	2022-03-18 17:18:04
24	sign(6)	Signature (6)						Time based token [6]			CRITICAL	HIGH	7.25	HIGH	6.25	2022-03-17 17:18:04
54	tmp0	Worst case scenario	Unknown	Strictly confidential, unknown data classification [9]	1-tier, Unknown architecture [9]	More than 4, Unknown Location [9]	No authentication [9]	None, Unknown signing [9]	None, Unknown encryption [9]	Service provider root/administrator process [9]	CRITICAL	HIGH	9	HIGH	8.5	2022-03-17 17:18:04

Figure 19 Threat screen

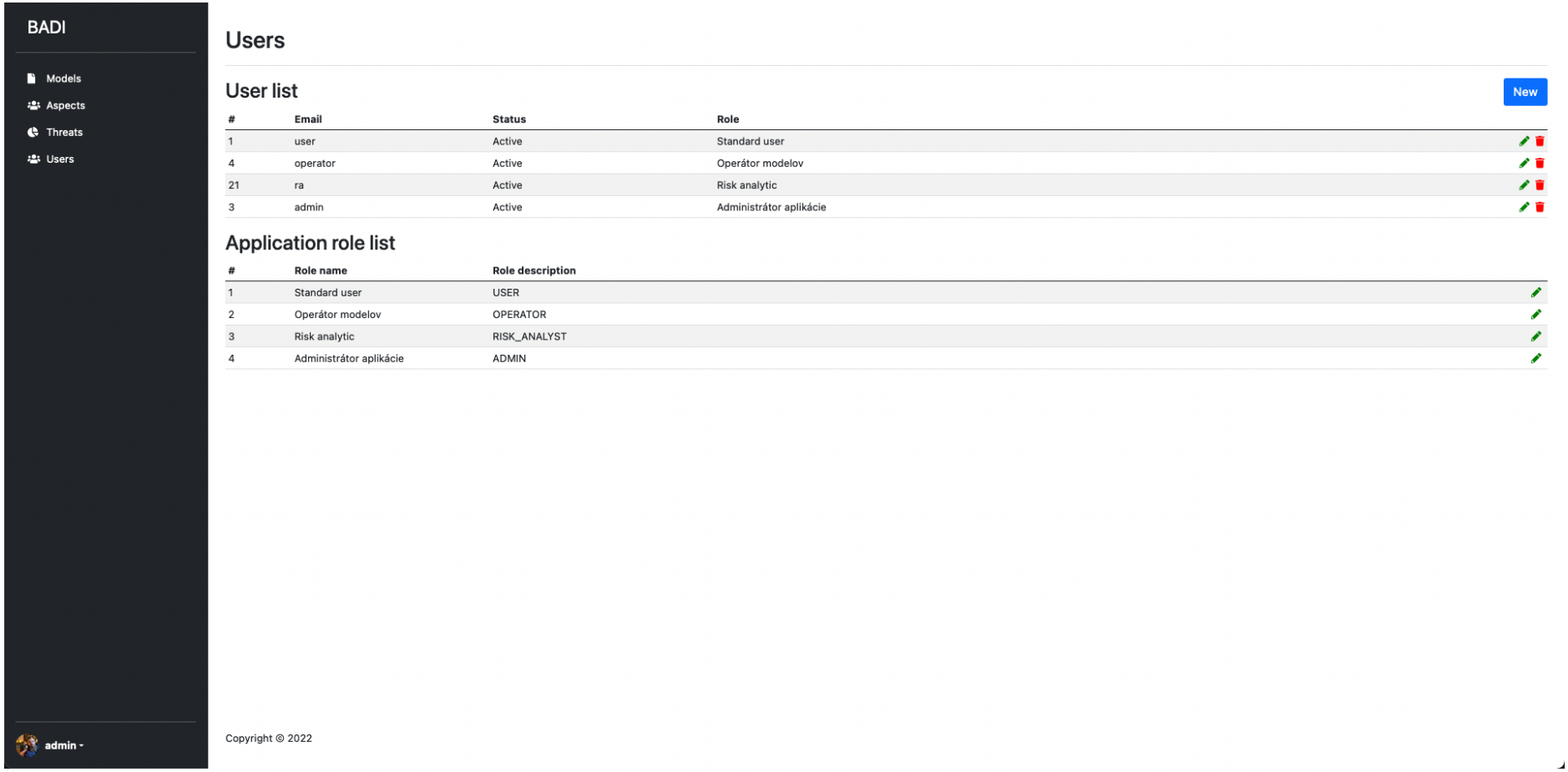

Figure 20 User Management Screen

submit Cancel

DREAD faktorizácia

model_name	Authprot	SL	M	O	S	ED	EE	A	IDE	LC	LI	LAV	LAC	FD	RD	NC	PV	Risklevel	Likvalue	Liklevel	Impvalue	Implevel	Action
	0																	INFO	0	LOW	0	LOW	save
	APIKEY	5	4	4	4	7	5	4	8	5	5	5	7	7	4	5	5	MEDIUM	5.125	MEDIUM	5.375	MEDIUM	save
	BASE64	5	9	7	5	7	5	6	8	7	7	5	7	7	5	5	5	CRITICAL	6.5	HIGH	6	HIGH	save
	CAPTCHA	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5	MEDIUM	5.125	MEDIUM	5.5	MEDIUM	save
	Certificate	3	4	4	2	3	3	4	3	2	3	5	7	3	4	2	3	MEDIUM	3.25	MEDIUM	3.625	MEDIUM	save
	ClearText	9	9	7	9	9	9	9	8	9	7	7	7	7	9	7	7	CRITICAL	8.625	HIGH	7.5	HIGH	save
	Cookies	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	3.5	MEDIUM	4.5	MEDIUM	save
	Digest access authentication	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	3.5	MEDIUM	4.5	MEDIUM	save
	Kerberos/SPNEGO	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5	MEDIUM	5.125	MEDIUM	5.5	MEDIUM	save
	LDAP	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	3.5	MEDIUM	4.5	MEDIUM	save
	None	9	9	9	9	9	9	9	9	9	7	9	9	9	9	7	9	CRITICAL	9	HIGH	8.5	HIGH	save
	NTLM	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	3.5	MEDIUM	4.5	MEDIUM	save
	OAuth2	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3	INFO	1.5	LOW	2	LOW	save
	OIDC	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3	INFO	1.5	LOW	2	LOW	save
	OTP	5	4	4	4	7	5	4	8	6	5	5	7	7	4	5	5	MEDIUM	5.125	MEDIUM	5.5	MEDIUM	save
	RADIUS	3	4	4	4	3	3	4	3	6	3	5	7	3	4	5	3	MEDIUM	3.5	MEDIUM	4.5	MEDIUM	save
	SAML	1	1	4	2	1	1	1	1	2	1	5	1	1	1	2	3	INFO	1.5	LOW	2	LOW	save
	Unknown	9	9	9	9	9	9	9	9	9	7	9	9	9	9	7	9	CRITICAL	9	HIGH	8.5	HIGH	save

Figure 21 Preview screen for suggested protocols

APPENDIX I

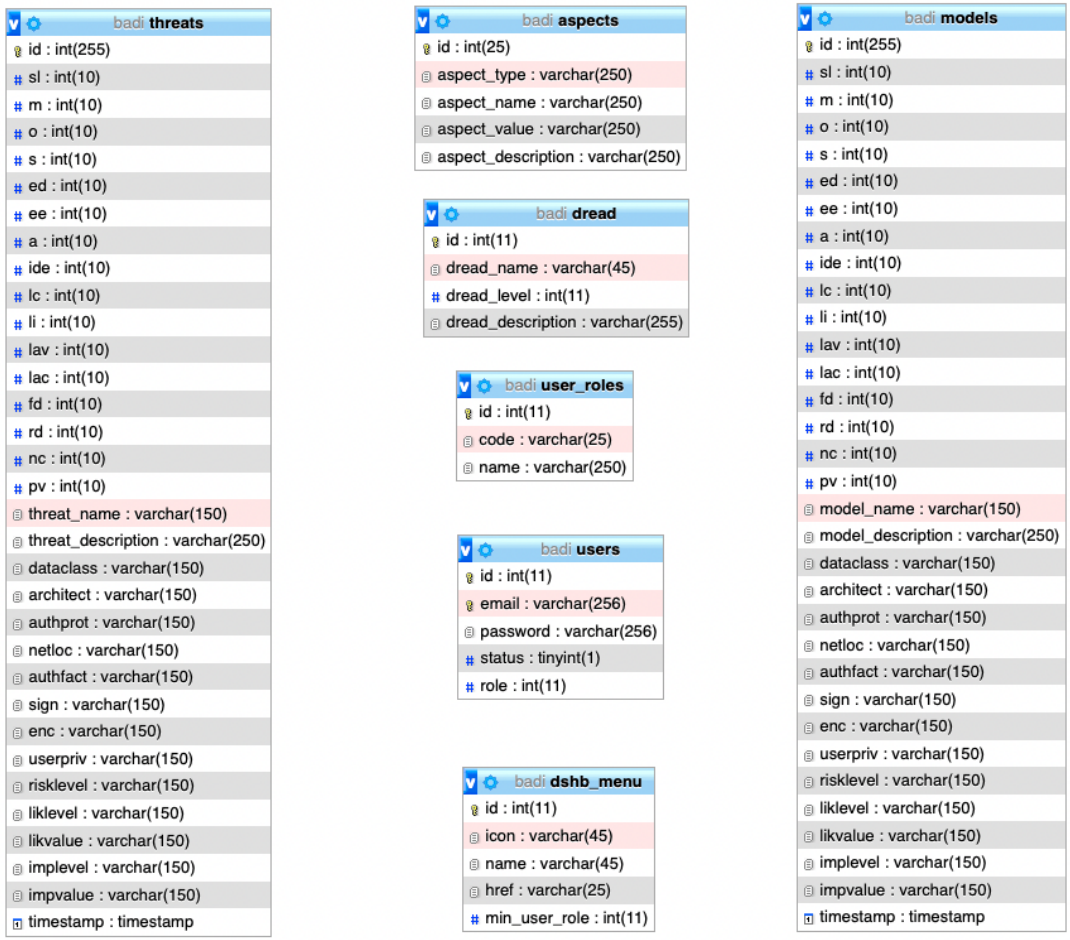

Figure 22 List of tables in a database

APPENDIX J

The source codes are located on GITHUB: https://github.com/MarekHrabcak/bad