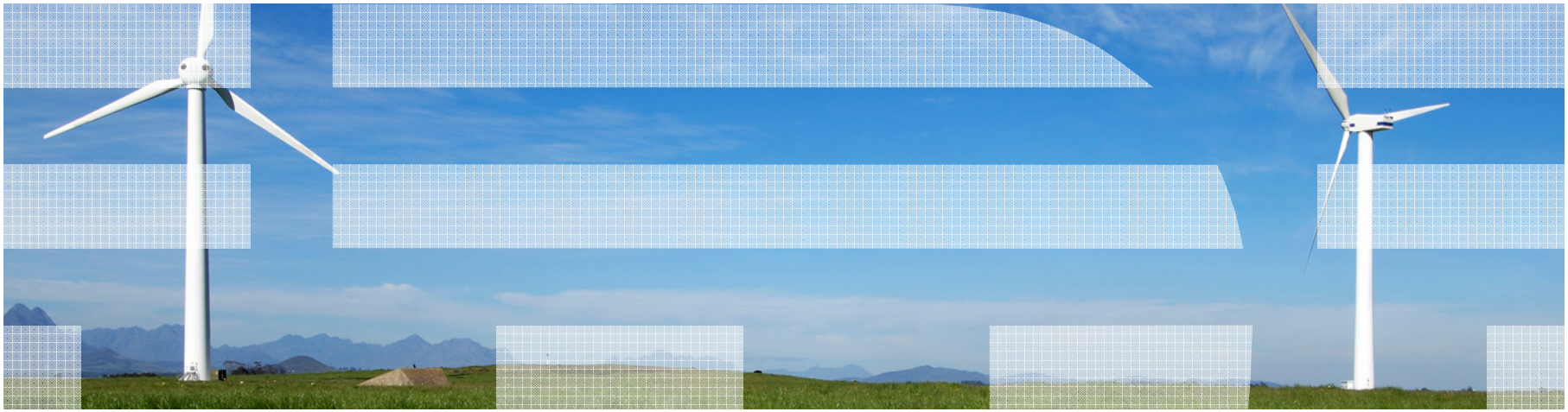
Secure Engineering and Design in an IT Project context



Bernard Van Acker

Agenda

- Selecting the security measures
- Implementing the security measures
- Testing the security measures

Slides with real life examples are modified to preserve confidentiality

Input for selection

- Security Policies
- Threat models

Input needed from business stakeholders

Threat	Origin	Impact	Exposure
Intercept and disclose unwanted information in transit			
Intercept and corrupt information in transit	Internal		
Enter data under false identity	Internal External		
Sudden increase in volume, causing the system to stop functioning	External		
Repudiation of information sent by clients	Internal External		
Misuse of information coming from the infrastructure through hacking	External		

A mailinglist from a competitor contains the same typo as data from our company.

How bad is bad? Using a technique from the public sector.

Score impact	Financial losses, in Euros	Juridical consequences	Image	Social and human
0	No significant losses	No consequences	No consequences	No consequences
1	<10 000	Internal sanctions	Occasional complaints	Slight irritation of staff
2	10 000-100 000	Juridial claims	Occasional criticism in the media	Temporary dissatisfaction of staff or customers
3	100 000 - 10 000 000	Juridical sanctions	Serious criticism in the media	Serious dissatisfaction of staff or customers
4	>10 000 000	Heavy juridical sanctions	Irreparably damaged image	Loss of human life; permanent loss of customers

Basis: HUET, A., STAQUET, A., "Business Risk Management: FEDICT Quick-Win-methode", 2006 V1.0, p4

… applied in the private sector

Confidentiality/Integrity	Financial losses, in Euros	Juridical consequences	Image	Social and human
Unauthorized reading of data by staff	0	0	0	0
Unauthorized reading of data by external people	1	0	0	0
Intentional corruption of data by staff	2	1	0	1
Intentional corruption of data by external people	2	1	0	2

Question on security baseline, for determining the risk occurrence

- When assessing the risk in the context of a project, should we take as a baseline:

A: A hypothetical situation **without** security measures
…. where existing security measures are identified after risk assessment

B: the current situation **with** the security measures in place
where the occurrence of the risk takes into account the security measures in place

Selection table security measures: importance of risk and effecitveness of security measure

Risk description	Importance of the risk (impact x frequency)				Effectiveness of the countermeasure																			
					Electronic Signature (PKI non rep)				Access control (strong authentication)				Logging + audit				Encrgption in transit		Input filtering		Backup	Version control	Security patch mgnt	Encrgption at rest
	Intern IT	Intern niet-IT	Extern departement	Extern	IT	Intern niet-IT	Extern departement	Extern internet	IT	Intern niet-IT	Extern departement	Extern internet	IT	Intern niet-IT	Extern departement	Extern internet	(i)	(e)	(i)	(e)				
Intercept and disclose unwanted information in transit	4	4	4	4	0	0	0	0	2	3	3	3	2	2	2	2	1	1	2	2	0	0	2	0
Intercept and corrupt information in transit	1	1	0	4	0	0	0	0	0	0	0	0	0	0	0	0	3	3	0	0	0	0	0	0
Enter data under false identity	3	3	3	6	3	3	3	3	2	2	2	3	1	1	1	1	0	0	1	1	1	0	2	0
Sudden increase in volume, causing the system to stop functioning	3	3	3	6	0	0	0	0	0	1	1	3	2	2	2	2	0	0	2	2	3	0	3	0
Repudiation of information sent by clients	6	6	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	2	2	1	2	0	2
Misuse of information coming from the infrastructure through hacking	0	0	2	2	0	0	0	0	1	1	1	1	1	1	1	1	0	0	1	1	0	0	1	1
Other unavailability	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0	2

Selection table security measures: selection based on added value, cost and implementation risk.

Risico-categorie:	Added value of the security countern																			
	Electronic Signature (PKI non rep)				Access control (strong authentication)				Logging + audit				Encryption in transit		Input filtering		Backup	Version contro	Securit g patch mgnt	Encrypt tion at rest
	IT	Intern niet-IT	Extern depart ement	Extern interne t	IT	Intern niet-IT	Extern depart ement	Extern interne t	IT	Intern niet-IT	Extern depart ement	Extern interne t	(i)	(e)	(i)	(e)				
Intercept and disclose unwanted information in transit	0	0	0	0	8	12	12	12	8	8	8	8	4	4	8	8	0	0	8	0
Intercept and corrupt information in transit	0	0	0	0	0	0	0	0	0	0	0	0	3	12	0	0	0	0	0	0
Enter data under false identity	9	9	9	18	6	6	6	18	3	3	3	6	0	0	3	6	6	0	12	0
Sudden increase in volume, causing the system to stop functioning	0	0	0	0	0	3	3	18	6	6	6	12	0	0	6	12	18	0	18	0
Repudiation of information sent by clients	0	0	0	0	0	6	0	0	0	0	0	0	0	0	12	0	6	12	0	12
Misuse of information coming from the infrastructure through hacking	0	0	0	0	0	0	2	2	0	0	2	2	0	0	0	2	0	0	2	2
Other unavailability	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	4	0	4
Toegevoegde waarde index	9	9	9	18	14	27	23	50	17	17	19	28	7	16	29	28	34	16	40	18
Kost (L/M/H)	M	M	M	M	H	H	H	H	M	M	M	M	M	M	M	H	H	L	M	M
Risico(L/M/H)	M	M	M	M	H	H	H	H	M	M	M	M	M	L	L	M	L	L	M	L
Voorgesteld (X) of niet (N)	N	N	N	N	X	X	X	X	X	X	X	X	N	X	X	N	X	X	X	X

=> double-check whether the set of selected measures mitigate adequately

Selection table security measures: double-check

Risk description	Importance of the risk (impact x frequency)				Effectiveness of the countermeasure																			
					Electronic Signature (PKI non rep)				Access control (strong authentication)				Logging + audit				Encryption in transit		Input filtering		Backup	Version control	Security patch mgnt	Encryption at rest
	Intern IT	Intern niet-IT	Extern department	Extern	IT	Intern niet-IT	Extern department	Extern internet	IT	Intern niet-IT	Extern department	Extern internet	IT	Intern niet-IT	Extern department	Extern internet	(i)	(e)	(i)	(e)				
Intercept and disclose unwanted information in transit	4	4	4	4	0	0	0	0	2	3	3	3	2	2	2	2	1	1	2	2	0	0	2	0
Intercept and corrupt information in transit	1	1	0	4	0	0	0	0	0	0	0	0	0	0	0	0	3	3	0	0	0	0	0	0
Enter data under false identity	3	3	3	6	3	3	3	3	2	2	2	3	1	1	1	1	0	0	1	1	1	0	2	0
Sudden increase in volume, causing the system to stop functioning	3	3	3	6	0	0	0	0	0	1	1	3	2	2	2	2	0	0	2	2	3	0	3	0
Repudiation of information sent by clients	6	6	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	2	2	1	2	0	2
Misuse of information coming from the infrastructure through hacking	0	0	2	2	0	0	0	0	1	1	1	1	1	1	1	1	0	0	1	1	0	0	1	1
Other unavailability	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0	2

=> Here we see the added value of the security policy

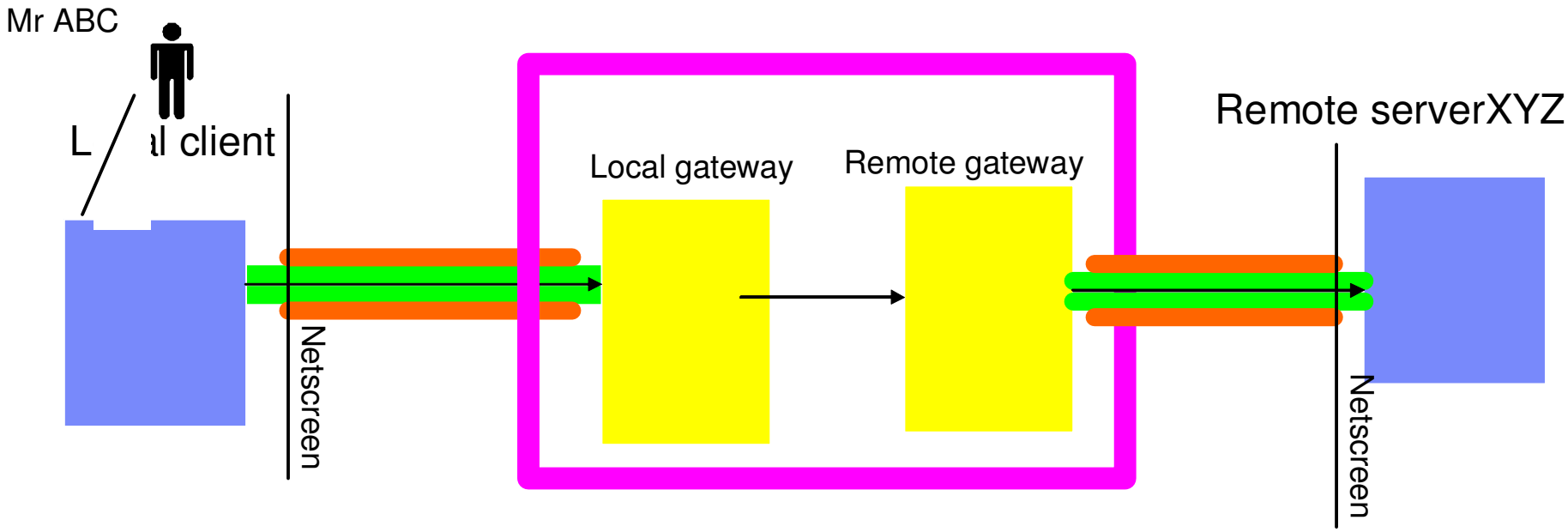
Agenda

- Selecting the security measures
- Implementing the security measures
- Testing the security measures

First measure: watch the security skills of your team

Example: Advanced Web Attacks and Countermeasures

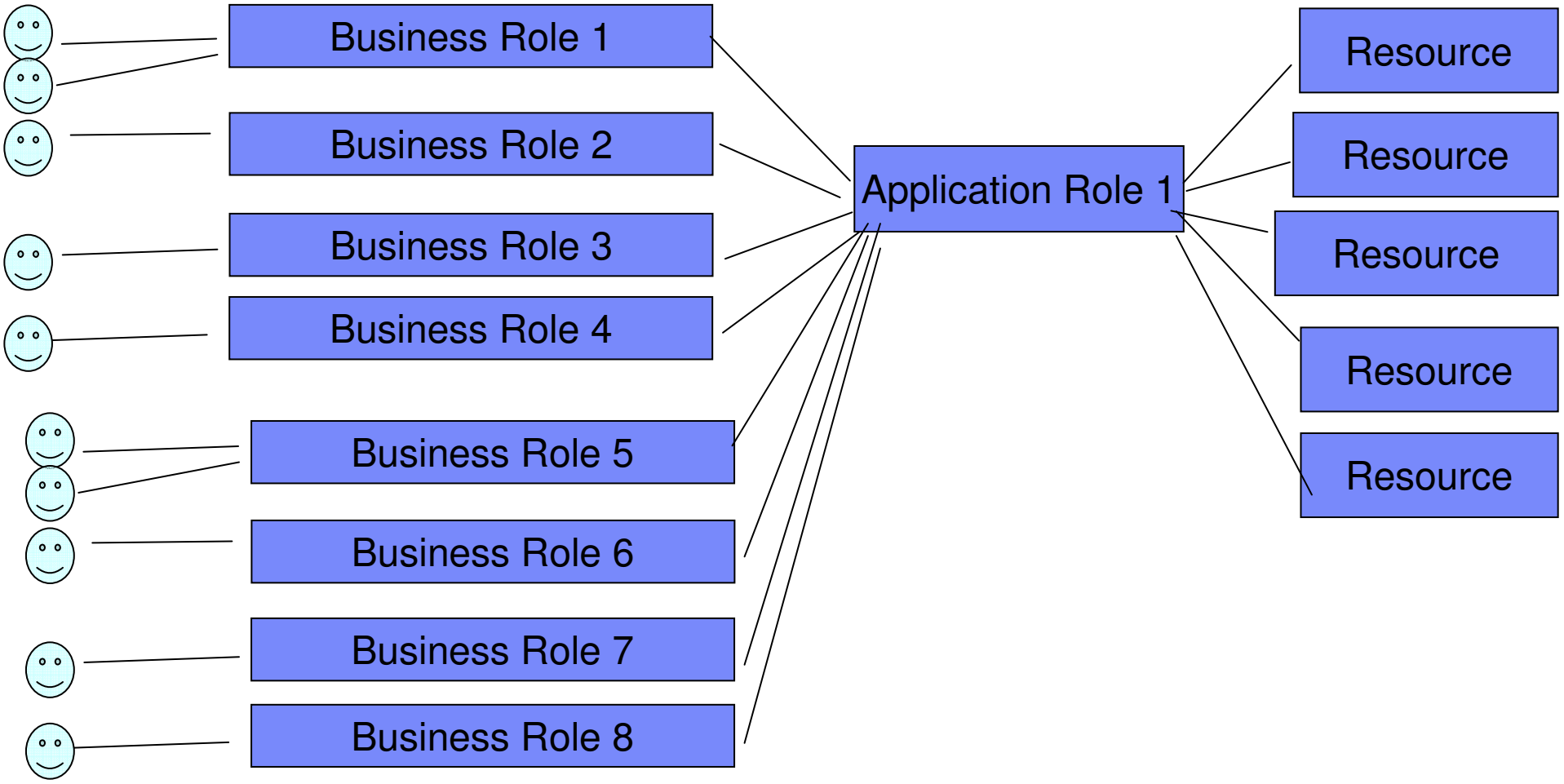
Keep the overview



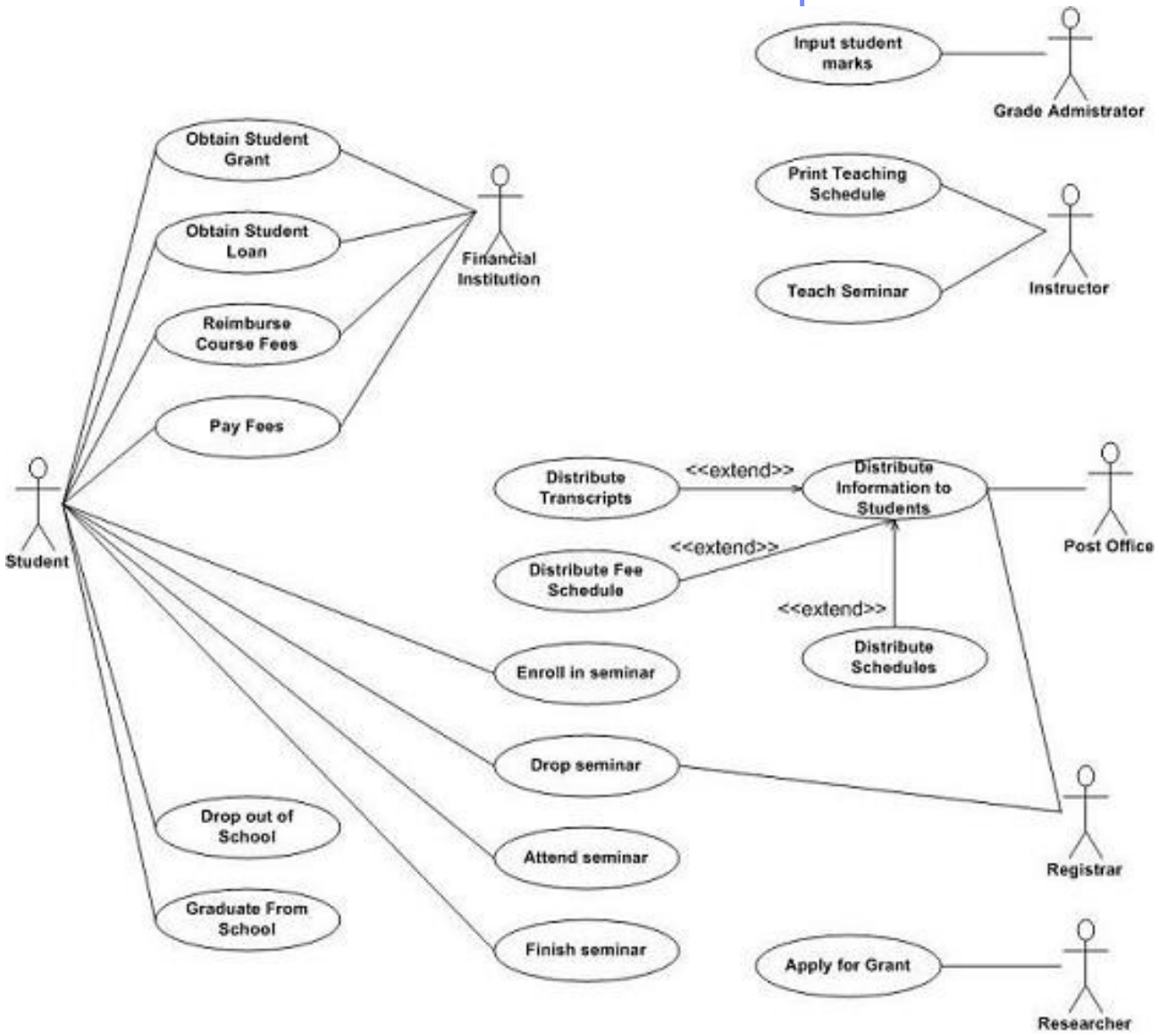
Legend:

- IPSec AES 256 bit
- Zone with mainly physical security.
- SSL/TLS

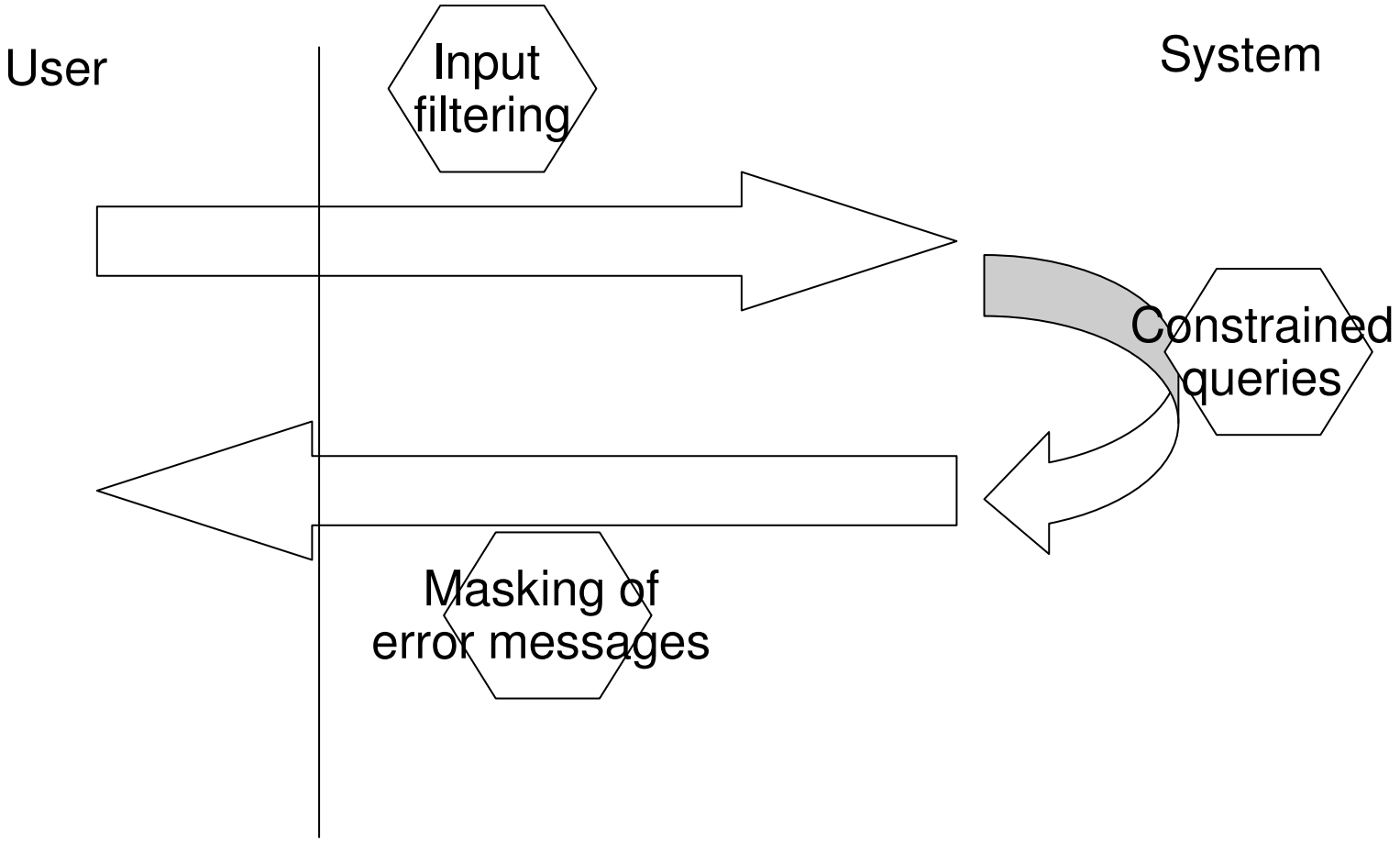
Risks related to over-enineering in access control design



Access control and actor- use case relationship



Places to counter for SQL injections & cross site scripting



Question on input filter to counter cross site scripting

- public static boolean isValidString(String value)
- {
- boolean isValid = (!isNotEmpty(value) || (isNotEmpty(value) && isValidRegEx(value, "^[0-9a-zA-Z ,;:%!\\Q//'\"?@.-()\\E‘ÄÇÖÜßàâäçèéêëîïôöùûü]*$")));
- return isValid;
- }

Concatenated SQL

```
String queryString = "select e from Facturen e «  + "where e.BTWNummer = '" + BTWNummer
   + "'";
list = find(queryString, ...)
```

=> better: parameterized queries: constraints on queries executed

Example of error screen with too much information

- eu.SlagerijJanssens.exceptions.SLAGERIJJANSSENSPersistenceException: <openjpa-1.1.1-SNAPSHOT-r422266:739055 nonfatal general error> org.apache.openjpa.persistence.PersistenceException: DB2 SQL error: SQLCODE: -302, SQLSTATE: 22001, SQLERRMC: null {prepstmnt 715350 SELECT t0.CD801A_ID, t4.HEADER_ID, t4.CORRELATION_IDENTIFIER, t4.DATE_OF_PREPARATION, t4.VLEESLEVERING_IDENTIFIER, t4.VLEESLEVERING_RECIPIENT, t4.VLEESLEVERING_SENDER, t4.TIME_OF_PREPARATION, t5.VLEESLEVERING_ID, t5.VLEESLEVERING_STATUS, t6.VLEESLEVERING_TYPE_ID, t6.VLEESLEVERING_TYPE_DESCRIPTION, t1.AAD_CONTAINER_ID, t7.VRACHTWAGEN_TRADER_ID, t7.AAD_CONTAINER_FK, t7.ACC_OR_REJ_ROR_FK, t7.CITY, t8.LANG_CODE_ID, t8.LANGUAGE_CODE, t7.POST_CODE, t7.STREET_NAME, t7.STREET_NUMBER, t7.SUBMITTED_DRAFT_OF_JOURNAALPOST_FK, t7.TRADER_ID, t7.TRADER_NAME, t9.KOELSYSTEEM_TRADER_ID, t9.AAD_CONTAINER_FK, t9.CITY, t10.LANG_CODE_ID, t10.LANGUAGE_CODE, t9.POST_CODE, t9.STREET_NAME, t9.STREET_NUMBER, t9.SUBMITTED_DRAFT_OF_JOURNAALPOST_FK, t9.TRADER_EXCISE_NUMBER, t9.TRADER_NAME, t11.DELIVERY_PLACE_TRADER_ID, t11.AAD_CONTAINER_FK, t11.ACC_OR_REJ_ROR_FK, t11.CHANGED_DESTINATION_FK, t11.CITY, t12.LANG_CODE_ID, t12.LANGUAGE_CODE, t11.POST_CODE, t11.STREET_NAME, t11.STREET_NUMBER, t11.SUBMITTED_DRAFT_OF_JOURNAALPOST_FK, t11.TRADER_ID, t11.TRADER_NAME, t2.EXCISE_MOVEMENT_BESTELBON_ID, t2.AAD_CONTAINER_FK, t2.AAD_REFERENCE_CODE, t2.ACC_OR_REJ_ROR_FK, t2.DATE_OF_VALIDATION_OF_BESTELBON, t2.SEQUENCE_NUMBER, t1.CD801A_FK, t13.PLACE_OF_DISP_TRADER_ID, t13.AAD_CONTAINER_FK, t13.CITY, t14.LANG_CODE_ID, t14.LANGUAGE_CODE, t13.POST_CODE, t13.REFERENCE_OF_TAX_WAREHOUSE, t13.STREET_NAME, t13.STREET_NUMBER, t13.SUBMITTED_DRAFT_OF_BESTELBON_FK, t13.TRADER_NAME FROM T_CD801A t0 INNER JOIN T_AAD_CONTAINER t1 ON t0.CD801A_ID = t1.CD801A_FK LEFT OUTER JOIN T_HEADER t4 ON t0.HEADER_FK = t4.HEADER_ID LEFT OUTER JOIN T_VLEESLEVERING t5 ON t0.VLEESLEVERING_FK = t5.VLEESLEVERING_ID INNER JOIN T_EXCISE_MOVEMENT_BESTELBON t2 ON t1.AAD_CONTAINER_ID = t2.AAD_CONTAINER_FK INNER JOIN T_HEADER_BESTELBON t3 ON t1.AAD_CONTAINER_ID = t3.AAD_CONTAINER_FK LEFT OUTER JOIN T_VRACHTWAGEN_TRADER t7 ON t1.AAD_CONTAINER_ID = t7.AAD_CONTAINER_FK LEFT OUTER JOIN T_KOELSYSTEEM_TRADER t9 ON t1.AAD_CONTAINER_ID = t9.AAD_CONTAINER_FK LEFT OUTER JOIN T_DELIVERY_PLACE_TRADER t11 ON t1.AAD_CONTAINER_ID = t11.AAD_CONTAINER_FK LEFT OUTER JOIN T_PLACE_OF_DISPATCH_TRADER t13 ON t1.AAD_CONTAINER_ID = t13.AAD_CONTAINER_FK LEFT OUTER JOIN TRD_VLEESLEVERING_TYPE t6 ON t5.VLEESLEVERING_TYPE_FK = t6.VLEESLEVERING_TYPE_ID LEFT OUTER JOIN TRD_LANG_CODE t8 ON t7.LANG_CODE_FK = t8.LANG_CODE_ID LEFT OUTER JOIN TRD_LANG_CODE t10 ON t9.LANG_CODE_FK = t10.LANG_CODE_ID LEFT OUTER JOIN TRD_LANG_CODE t12 ON t11.LANG_CODE_FK = t12.LANG_CODE_ID LEFT OUTER JOIN TRD_LANG_CODE t14 ON t13.LANG_CODE_FK = t14.LANG_CODE_ID WHERE (t2.AAD_REFERENCE_CODE = ? AND t3.SEQUENCE_NUMBER = ?) FETCH FIRST 1 ROWS ONLY [params=(String) 11BEGWQ3NIN20009KXEQ1", (String) 1]} [code=-302, state=22001]SQLCA OUTPUT[Errp=SQLRI5A9, Errd=-2146041770, 86, 0, 0, -3998, 0]at eu.emcs.orm.bridge.jpa.JPAMapper.execute(JPAMapper.java:515)

Conclusion: no single measure solves all your security problems

- Correct attitude: healthy alertness

=> Advice: document the residual risk

Agenda

- Selecting the security measures
- Implementing the security measures
- Testing the security measures

The types of security tests

- Testing for physical & administrative security measures: not always in scope of an AD project
- Security at application level: blurring distinction between manual and automated security tests

<table>
<tr><th></th><th>Manual</th><th>Automatic</th></tr>
<tr><td>White Hat</td><td colspan="2">Combination of tools & judgement</td></tr>
<tr><td>Black Hat:
- Ethical hacking
- Test for malware</td><td colspan="2">Combination of tools & judgement</td></tr>
</table>

The more focused & independent the testing team, the better.

The ‘scary’ authentication bypass

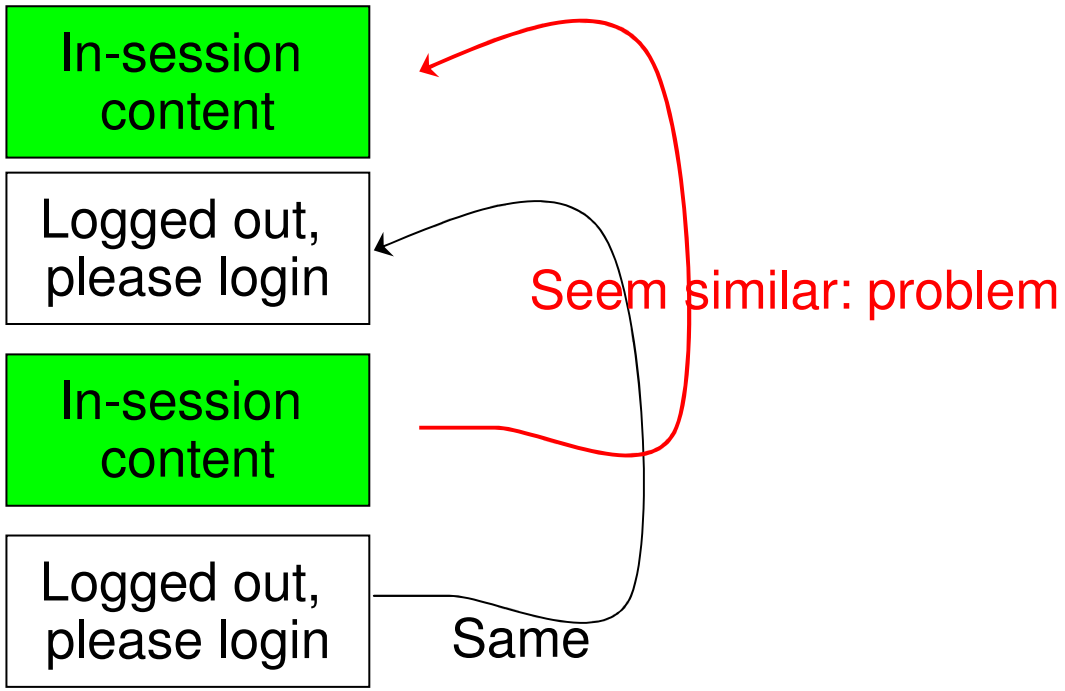
- **Description:** Authentication Bypass Using SQL Injection: HEX(29) -- (right parenthesis SQL comment) variant

- **Difference:**
- The following changes were applied to the original request:
- Removed cookie '**JSESSIONID**'
- Set parameter '**tempDataDTO.streetName**'s value to '**4ppSc4n**'
- Set parameter '**tempDataDTO.traderName**'s value to '**4ppSc4n**'
- Set parameter '**generalDataDTO.authStartdate**'s value to '**4ppSc4n**'
- Set parameter '**generalDataDTO.authActivationDate**'s value to '**4ppSc4n**'
- Set parameter '**tempDataDTO.streetName**'s value to '**weeeeeeeeeeee%27%29+--+**'
- Set parameter '**generalDataDTO.authStartdate**'s value to '**s3ct3amy**'
- Set parameter '**generalDataDTO.authActivationDate**'s value to '**s3ct3amy**'

- **Reasoning:**
- The test result seems to indicate a vulnerability because when four types of request were sent - a valid login, an invalid login, an SQL attack, and another invalid login - the responses to the two invalid logins were the same, while the response to the SQL attack seems similar the response to the valid login.

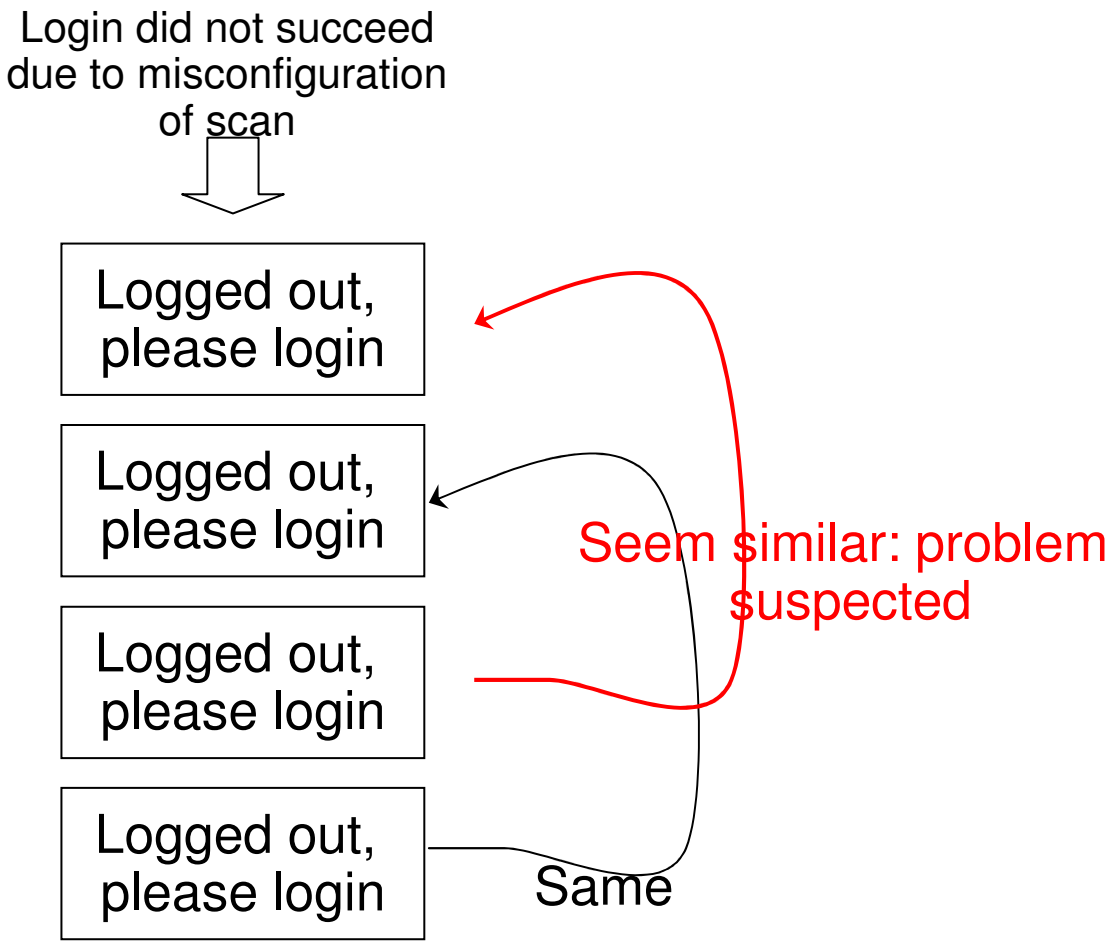
Reasoning applied by Appscan

- Valid login
  - Expected: login
- Invalid login
  - Expected: logout
- SQL attack
  - Expected: no access
- Invalid login
  - Expected: logout,



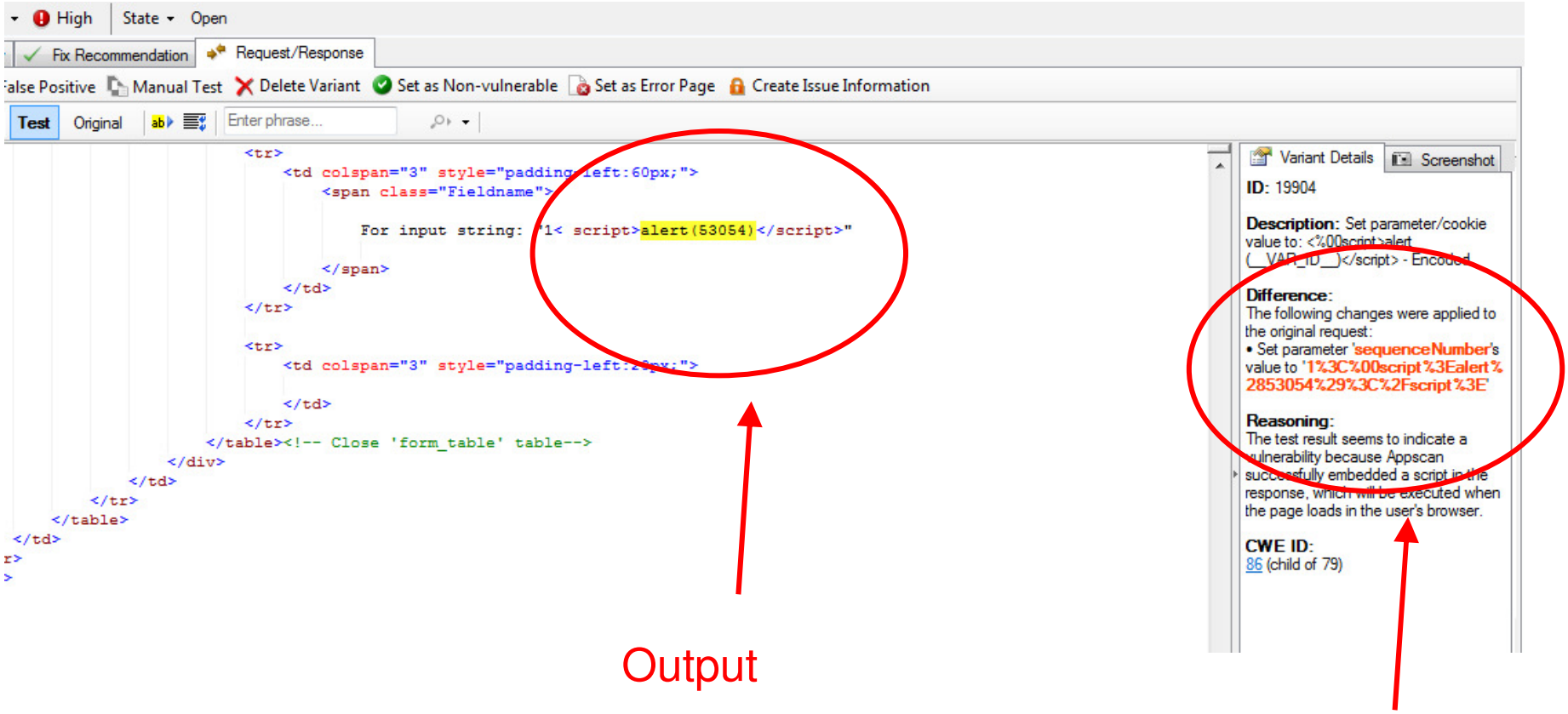
What really happened was a misconfiguration of the scan

- Valid login
  - Expected: login
- Invalid login
  - Expected: logout
- SQL attack
  - Expected: no access
- Invalid login
  - Expected: logout,



=> Fixing the login misconfiguration in the scan resolved the issue

The « correctly noticed » cross site scripting error



But…. how to explain this to non-technical people?

Cross-site scripting explained

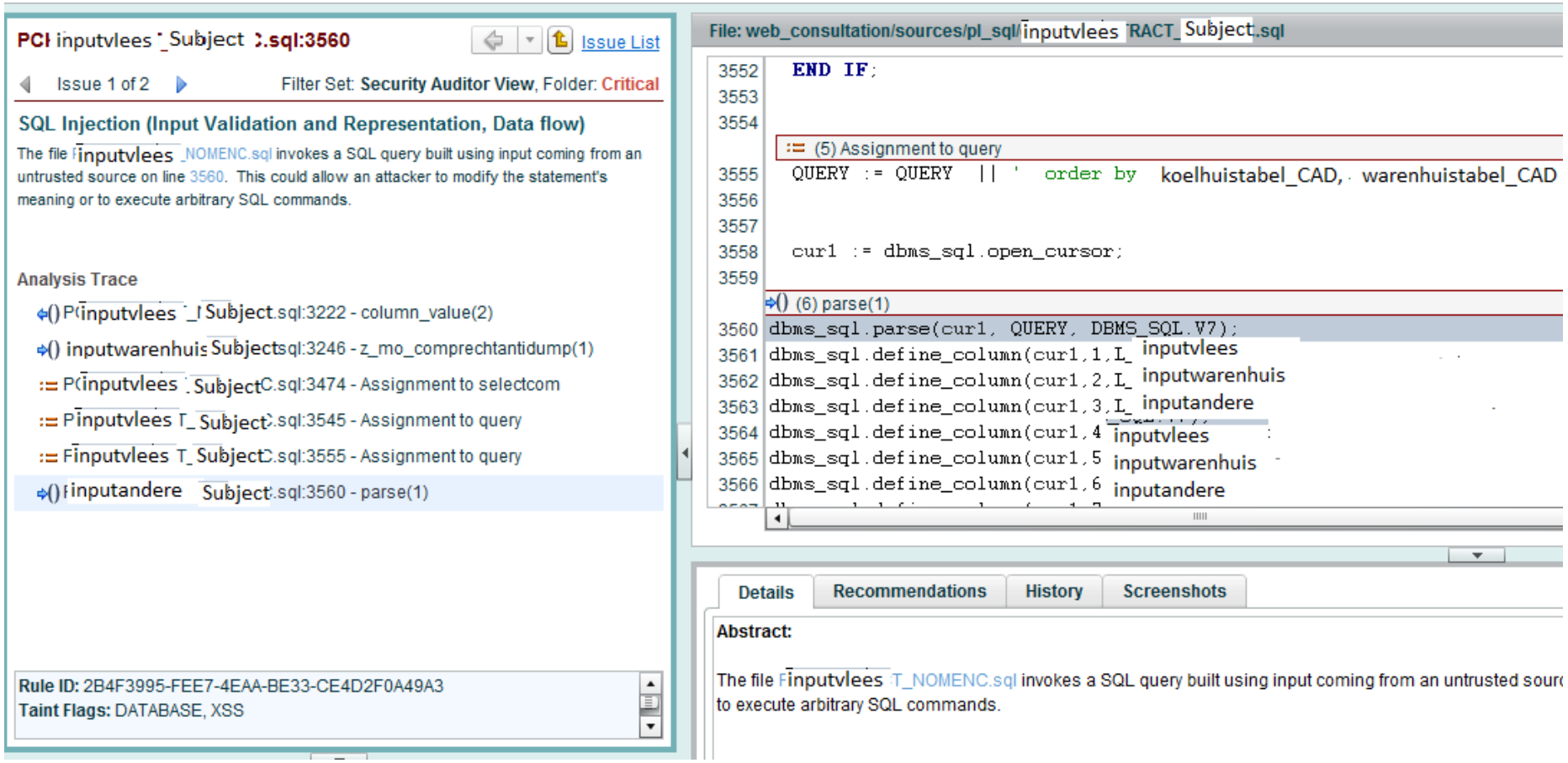
Dear [TrustedCompany] customer

[TrustedCompany] organizes a great game, fabulous prices to win! Just log on to our site using the following link:

- wwwTrustedCompany.com/application/maliousinput

People trust this

Comparing white hat vs black hat



Source: screenshot from Fortify (anonymized); similar output from Appscan Source

Conclusion