The background of the slide is a vibrant orange color, decorated with several overlapping, semi-transparent shapes in various shades of orange and yellow. These shapes include circles, rectangles, and irregular polygons, creating a modern, layered aesthetic. The shapes are positioned in the top and bottom portions of the slide, framing a central white horizontal band.

Improving Compliance and Performance at the Code Level

Sebastian Schinzel – Virtual Forge GmbH

- **SQL-Injection Demo**
- **Example of bad coding**
- **Finding bad coding using Source Code Analysis (SCA) and Data Flow Analysis (DFA)**
- **Preventing bad coding in the first place**

>> SQL Injection Demo



>> SQL Injection Demo

Business Impact:

- Attackers are able to view arbitrary credit card transactions

PCI-DSS:

“Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. [...] Cover prevention of common coding vulnerabilities in software development processes, to include the following:

- [...]
- 6.5.6 Injection flaws (for example, structured query language (SQL) injection)”

>> Example Coding

* Read user input

1. `input_year = request->get_form_field('input_year');`
2. `input_month = request->get_form_field('input_month');`

* Create and execute the SQL query

3. `CONCATENATE `uname = ' ` sy-uname ` ` INTO cl where.`
4. `CONCATENATE cl_where ` AND ta_date LIKE ' ` input_year input_month `%' ` INTO cl where.`
5. `SELECT * FROM ZCCINFO INTO CORRESPONDING FIELDS OF TABLE itab_zccinfo WHERE (cl where) ORDER BY ta_date.`

>> Example Coding

Normal Request:

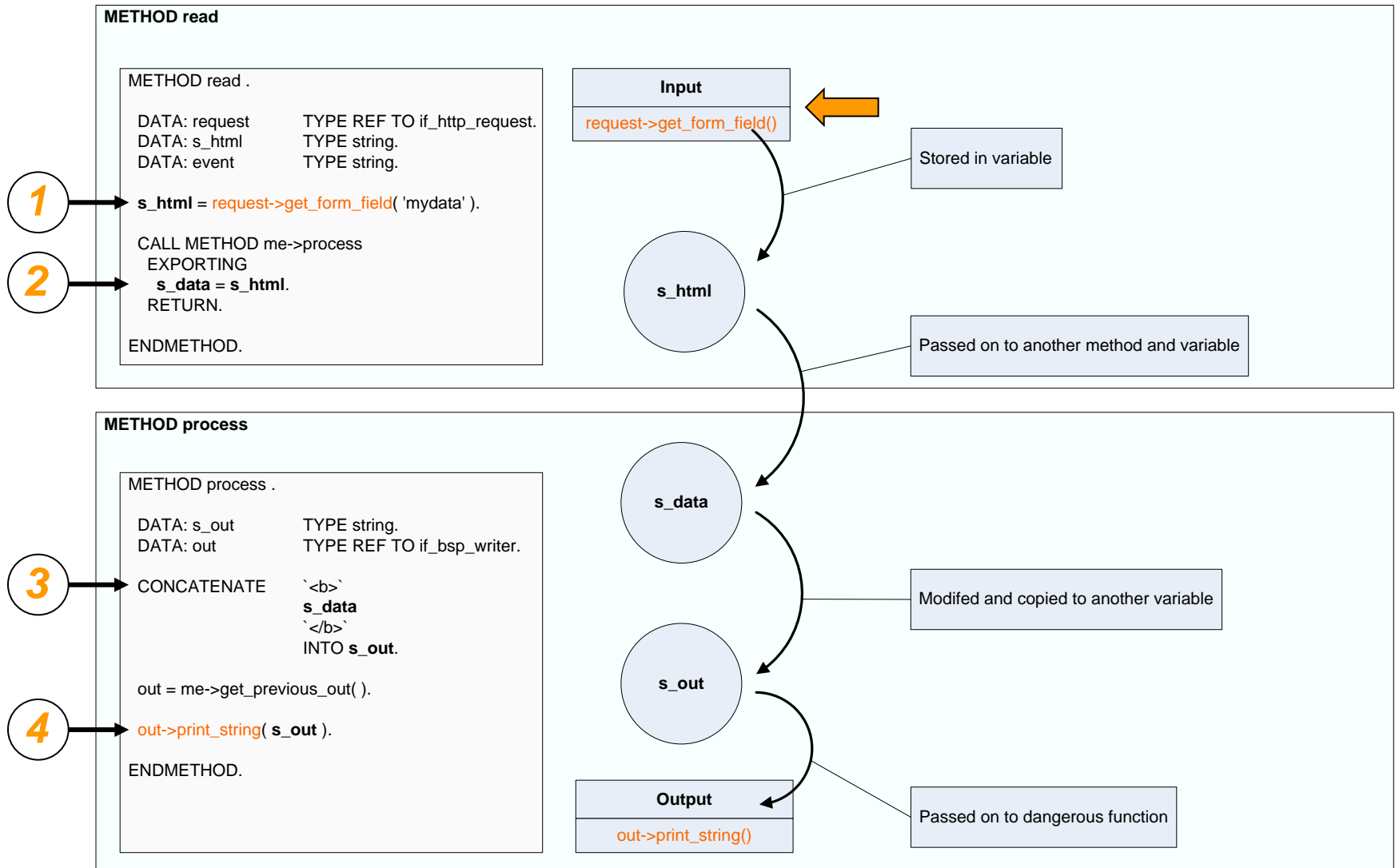
```
SELECT *  
  FROM ZCCINFO  
 INTO CORRESPONDING FIELDS OF TABLE itab_zccinfo  
 WHERE uname='user'  
 AND ta_date LIKE '200801%'  
 ORDER BY ta_date.
```

>> Example Coding

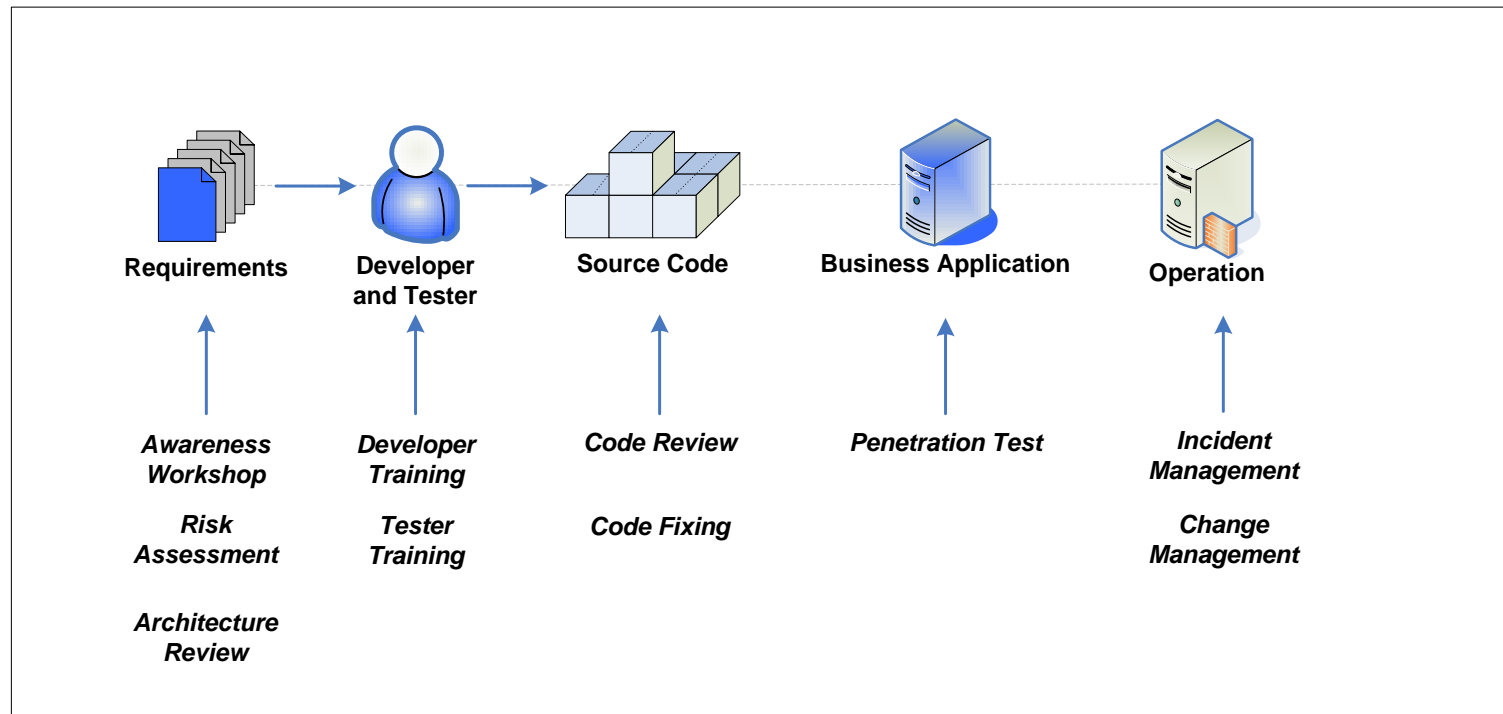
Attack:

```
SELECT *  
  FROM ZCCINFO  
  INTO CORRESPONDING FIELDS OF TABLE itab_zccinfo  
 WHERE uname='user'  
 AND ta_date LIKE '200801' OR mandt LIKE '%%'  
 ORDER BY ta_date.
```

>> Finding bad coding



>> Preventing bad coding in the first place



Questions? Comments?

Thank you for your attendance!

>> SQL Injection

Show your recent transactions - Mozilla Firefox

File Edit View History Bookmarks Tools Help

ccdata_demo/details.htm?input_year=2008&input_month=01

Please select year and month to filter your transactions:

Year Month

Results:

Your recent credit card transactions

CC_NUMBER	CC_EXPIRE	CC_NAME	TA_DESCRIPTION	TA_AMOUNT	TA_DATE
4149253627344523	11/09	PETER JACKSON	DRUG STORE	65,00	15.01.2008
4149253627344523	11/09	PETER JACKSON	PLANE TICKET	80,00	19.01.2008

Page 1 of 1

Done

>> SQL Injection

Business Server Page (BSP) error

What happened?

Calling the BSP page was terminated due to an error.

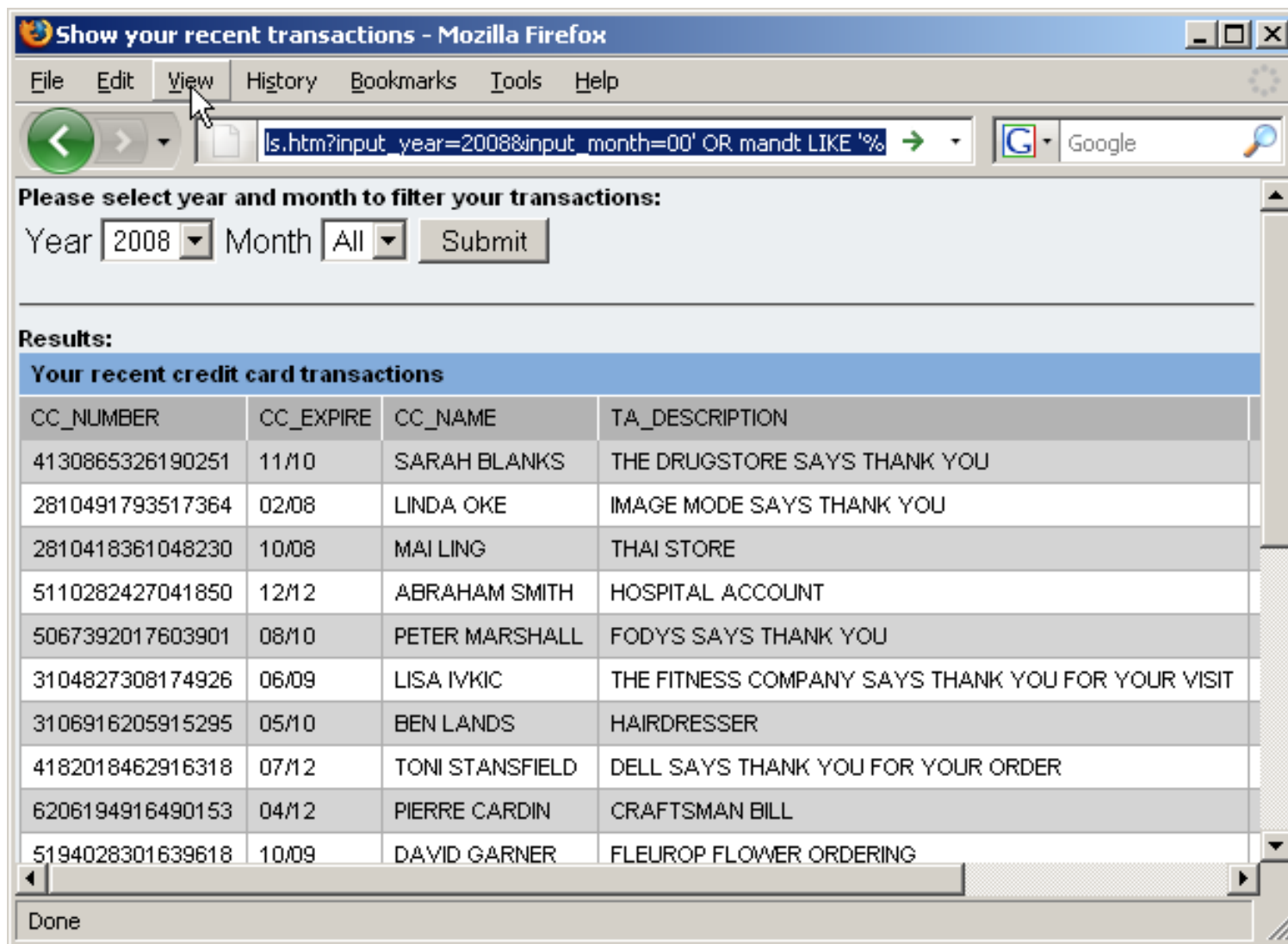
SAP Note

- **The following error text was processed in the system:**
An exception with the type CX_SY_DYNAMIC_OSQSQL_SYNTAX occurred, but was neither handled locally, nor declared in a RAISING clause

Exception Class	CX_SY_DYNAMIC_OSQSQL_SYNTAX
Error Name	SAPSQL_WHERE_PARENTHESES
Program	CL_O27VCP9ZMBO80HYLVYZQJUJ9EFLCP
Include	CL_O27VCP9ZMBO80HYLVYZQJUJ9EFLCM008
ABAP Class	CL_O27VCP9ZMBO80HYLVYZQJUJ9EFL
Method	_ONREQUEST
BSP Application	ZVF_CCDATA_DEMO

Done

>> SQL Injection



Show your recent transactions - Mozilla Firefox

File Edit **View** History Bookmarks Tools Help

ls.htm?input_year=2008&input_month=00' OR mandt LIKE '%

Please select year and month to filter your transactions:

Year Month

Results:

Your recent credit card transactions

CC_NUMBER	CC_EXPIRE	CC_NAME	TA_DESCRIPTION
4130865326190251	11/10	SARAH BLANKS	THE DRUGSTORE SAYS THANK YOU
2810491793517364	02/08	LINDA OKE	IMAGE MODE SAYS THANK YOU
2810418361048230	10/08	MAI LING	THAI STORE
5110282427041850	12/12	ABRAHAM SMITH	HOSPITAL ACCOUNT
5067392017603901	08/10	PETER MARSHALL	FODYS SAYS THANK YOU
3104827308174926	06/09	LISA IVKIC	THE FITNESS COMPANY SAYS THANK YOU FOR YOUR VISIT
3106916205915295	05/10	BEN LANDS	HAIRDRESSER
4182018462916318	07/12	TONI STANSFIELD	DELL SAYS THANK YOU FOR YOUR ORDER
6206194916490153	04/12	PIERRE CARDIN	CRAFTSMAN BILL
5194028301639618	10/09	DAVID GARNER	FLEUROP FLOWER ORDERING

Done