

Secure Coding

Shruti Kalsi

Consultant

Indian Computer emergency Response Team

File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

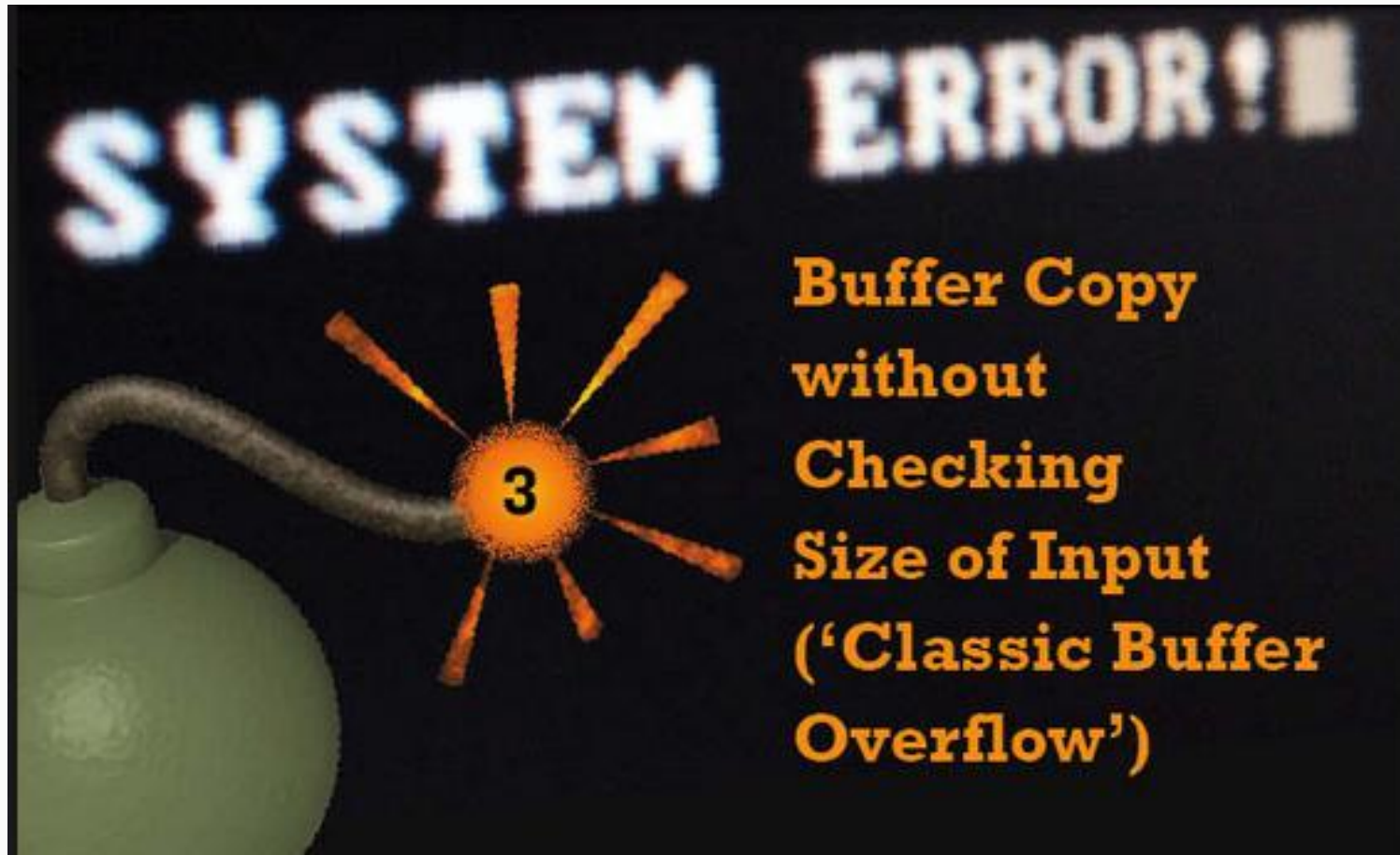


action.php index.html savecomment.php

```
1 <?php
2 if ($_POST['kommentar'] != "") {
3     include("env_db.php");
4     include("language.php");
5     initDB();
6     $recipe = $_POST['id'];
7     $comment = $_POST['kommentar'];
8     $pos = strpos($comment, "<");
9     if ($pos === false) {
10         $datum = date('Y-m-d');
11         $user = $_POST['user'];
12         $query = "INSERT INTO dat_comments (recipe, comment, datum, user) VALUES ($recipe, '$comment', '$datum', '$user')";
13         $result = mysql_query($query);
14         header("Location: ./rezeptanzeige.php?currid=$recipe");
15     }
16     else {
17         echo "<script>alert('$sys_com_err');location.href='./rezeptanzeige.php?currid=$recipe';</script>\n";
18     }
19 }
20 ?>
```

An illustration of <PHP> source code

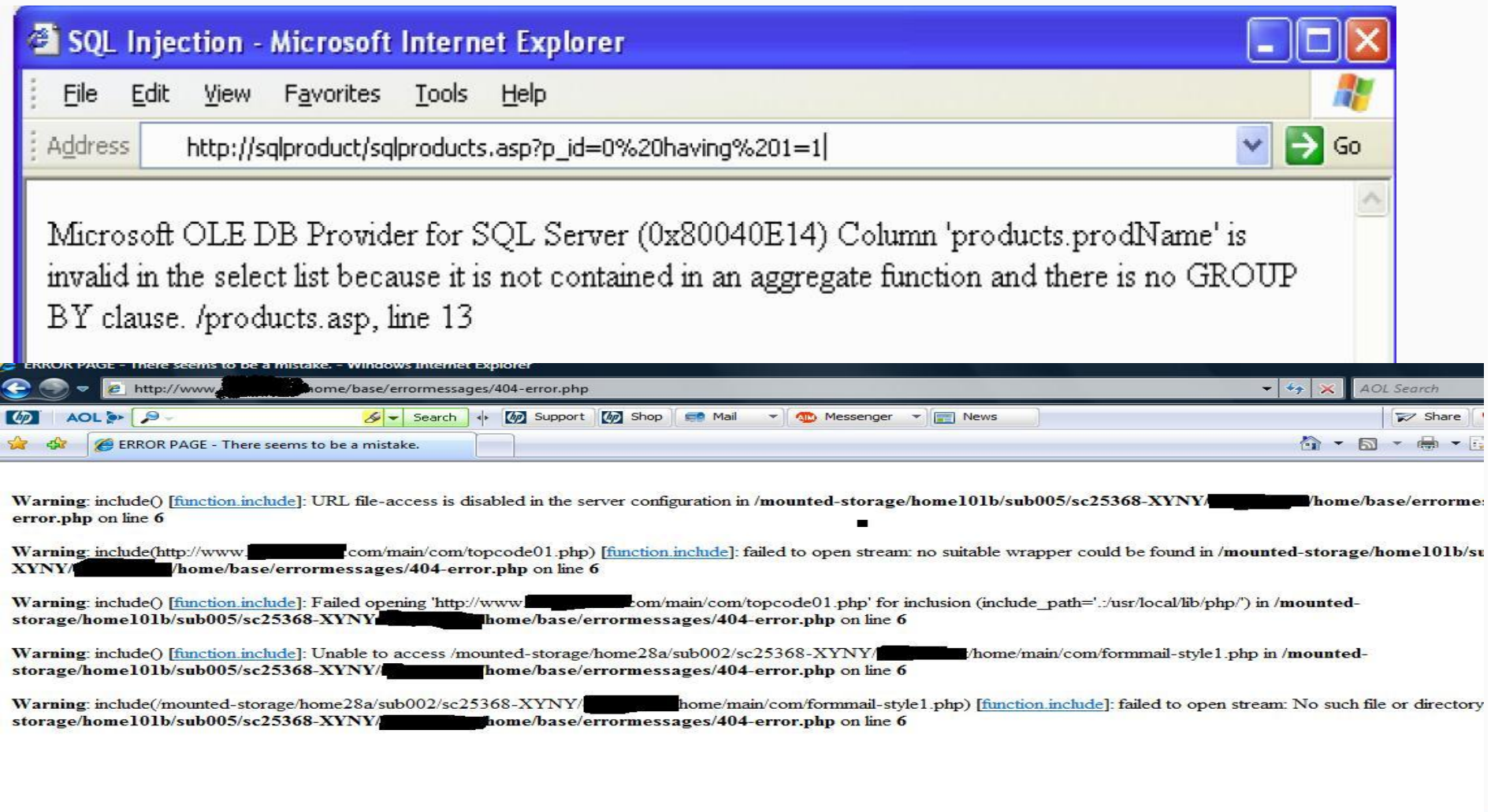
SANS TOP 25 Programming Errors



- **Insecure Interaction Between Components**
- **Risky Resource Management**
- **Porous Defences**

- **Insecure Interaction Between Components**
- SQL Injection
- OS Command Injection
- Cross-site Scripting
- Unrestricted Upload of File
- Cross-Site Request Forgery (CSRF)
- URL Redirection to Untrusted Site ('Open Redirect')

Error messages



SQL Injection - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address `http://sqlproduct/sqlproducts.asp?p_id=0%20having%201=1` Go

Microsoft OLE DB Provider for SQL Server (0x80040E14) Column 'products.prodName' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause. /products.asp, line 13

ERROR PAGE - There seems to be a mistake. - Windows Internet Explorer

`http://www.██████████.home/base/errormessages/404-error.php`

hp AOL Search Support Shop Mail Messenger News Share

ERROR PAGE - There seems to be a mistake.

Warning: include() [function.include]: URL file-access is disabled in the server configuration in /mounted-storage/home101b/sub005/sc25368-XYNY/██████████/home/base/errorme: error.php on line 6

Warning: include(http://www.██████████.com/main/com/topcode01.php) [function.include]: failed to open stream: no suitable wrapper could be found in /mounted-storage/home101b/sub005/sc25368-XYNY/██████████/home/base/errormessages/404-error.php on line 6

Warning: include() [function.include]: Failed opening 'http://www.██████████.com/main/com/topcode01.php' for inclusion (include_path='.:usr/local/lib/php/') in /mounted-storage/home101b/sub005/sc25368-XYNY/██████████/home/base/errormessages/404-error.php on line 6

Warning: include() [function.include]: Unable to access /mounted-storage/home28a/sub002/sc25368-XYNY/██████████/home/main/com/formmail-style1.php in /mounted-storage/home101b/sub005/sc25368-XYNY/██████████/home/base/errormessages/404-error.php on line 6

Warning: include(/mounted-storage/home28a/sub002/sc25368-XYNY/██████████/home/main/com/formmail-style1.php) [function.include]: failed to open stream: No such file or directory storage/home101b/sub005/sc25368-XYNY/██████████/home/base/errormessages/404-error.php on line 6

- **Risky Resource Management**
- Buffer Overflow
- Path Traversal
- Download of Code Without Integrity Check
- Inclusion of Functionality from Untrusted Control Sphere
- Use of Potentially Dangerous Function
- Incorrect Calculation of Buffer Size
- Integer Overflow or Wraparound

- **Porous Defences**
- Missing Authentication for Critical Function
- Missing Authorization
- Use of Hard-coded Credentials
- Missing Encryption of Sensitive Data
- Reliance on Untrusted Inputs in a Security Decision
- Execution with Unnecessary Privileges
- Incorrect Authorization
- Incorrect Permission Assignment for Critical Resource

- **Porous Defences (cont..)**
- Use of a Broken or Risky Cryptographic Algorithm
- Improper Restriction of Excessive Authentication Attempts

Secure Coding Practices.

Input Handling

- Conduct all data validation on a trusted system.
- Validate all input against a "white" list of allowed characters, whenever possible.
- Validate data from redirects.

Escaping

- Using escape Functions/strings for escaping certain characters.

Safe HTML(Sanitization)

- Allowing/Disallowing certain HTML Tags.

File Handling

- Do not pass user supplied data directly to any dynamic include function
- Require authentication before allowing a file to be uploaded
- Limit the type of files that can be uploaded to only those types that are needed
- Turn off execution privileges on file upload directories

Cryptographic Practices

- All cryptographic functions used to protect secrets from the application user must be implemented on a trusted system.
- All random numbers, random file names using the cryptographic module's approved random number generator when these random values are intended to be un-guessable .

Error Handling & Exceptions

- Do not disclose sensitive information in error responses.
- Error handling logic associated with security controls should deny access by default
- Log all input validation failures
- Log all authentication attempts, especially failures

Authenticity Validation

- Who is a valid user to access the website.

Resources for the developers- OWASP, PHPSC.

- PHP Security Consortium (PHPSC) is an international group of PHP experts dedicated to promoting secure programming practices within the PHP community.

References

- <http://www.sans.org>
- www.securecoding.cert.org
- <http://phpsec.org/>

Security is a path, not a destination

