Faculdade FGA – UnB Gama

Disciplina: Tecnicas de programação

Professor: Maurício Serrano

Alunos: Fagner Rodrigues – 09/0112750

Geison de Souza – 10/0029990

Thaiane Braga – 12/0136198

Thomaz Martins – 11/0066855

Análise estática do projeto C-L

Uma vez que a complexidade entrou na equação ela traz o seu efeito colateral: situações inesperadas. Quando temos um ciclo de vida em nossa aplicação que não contempla o devido cuidado com segurança, temos implicações de diversos níveis. A maior delas é que em geral problemas que a primeira vista são simples e pequenos, acabam se tornando verdadeiros pesadelos.

Análise Estática do Código consiste basicamente em antever problemas de segurança efetuando uma auditoria no código, sem executá-lo. Isso pode se tornar uma tarefa muito trabalhosa, especialmente quando o desenvolvedor não tem experiência com segurança e se não existe um framework de desenvolvimento seguro em uso no projeto.

As aplicações web são alvos constantes de ataques, quase que 24 horas por dia. Temos estatiscas de que muitas vezes, 60% do tráfego diário que chega a um website é gerado por bots que em sua grande maioria estão procurando por scripts vulneráveis para efetuar ataques, comprometer o servidor e a aplicação e fazê-la parte de sua rede de zumbis. Não seria nada legal ter seu e-Commerce em uma lista de hosts que estão disseminando Malwares para os usuários. Isto pode comprometer gravemente os negócios.

Para auxiliar desenvolvedores neste árduo processo de análise estática, temos algumas aplicações muito interessantes e que podem realmente trazer a tona, muitas vezes problemas de segurança que não eram imaginados durante o desenvolvimento. Talvez aquele “warning” que seu compilador cuspiu na tela e você pensou “ah mas é apenas um warning, não tem nada de grave ai..” esconda muito mais do que imagina.

Em relação a análise estática, foi utilizado a ferramenta Rips. RIPS é uma ferramenta escrita em PHP para encontrar vulnerabilidades em aplicações PHP utilizando o conceito de análise estática do código. Utilizando tokenização e parseando todos os arquivos de código PHP, ele consegue transformar seu código fonte PHP em program model e detectar sinks sensíveis (pontecialmente funções vulneráveis) que poderiam ser manipuladas por um userinput (influenciada por um usuário malicioso) durante o fluxo do programa. Além disto,

baseado na estrutura de output de uma vulnerabilidade encontrada, RIPS também oferece um framework integrado de code audit para que você possa fazer uma análise manual.

RIPS consegue identificar por padrão diversas vulnerabilidades em sua aplicação, em sua grande maioria as listadas no OWASP Top 10 são identificadas. Segue abaixo uma pequena lista das principais vulnerabilidades identificadas pela aplicação:

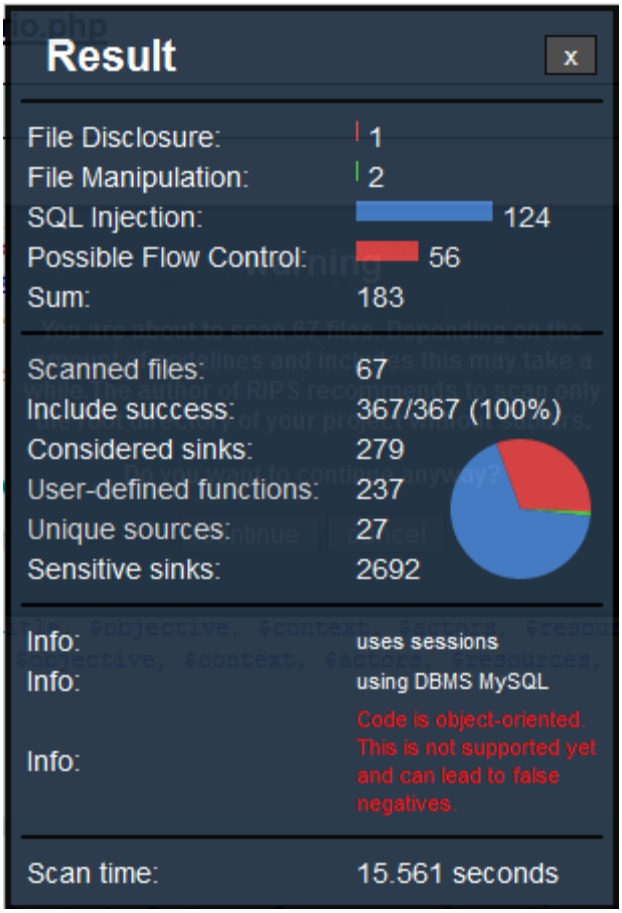
- Code Execution
- Command Execution
- Cross-Site Scripting
- Header Injection
- File Disclosure
- File Inclusion
- File Manipulation
- LDAP Injection
- SQL Injection
- XPath Injection

A interface de auditoria de código do RIPS consiste de algumas funcionalidades muito interessantes, entre elas podemos citar:

- Estatísticas referentes ao Scans e as vulnerabilidades da aplicação
- Linhas de código vulneraveis são agrupadas
- Descrição das Vulnerabilidades com exemplo de código, PoC e patch
- Engine que permite a criação do Exploit para explorer a vulnerabilidade encontrada
- Exibição gráfica de arquivos (conectada pelos includes)
- Exibição gráfica de funções (conectadas pelas calls)
- Userinput list (parámetros da aplicação)
- Visualização do código fonte com destaque em funções e parametros

Entre muitas outras que permitem que você faça o debug da aplicação utilizando inclusive expressões regulares. Efetuando a análise estática do código com RIPs, você consegue rapidez ao executar a análise (executar uma análise estática manualmente pode ser dolorosamente demorado). Você consegue identificar blind/non-blind SQL exploitation, detectar backdoors em seu código entre outras vantagens.

Abaixo segue o resultado da análise estática feita com a ferramenta do nosso projeto C-L:



path / file: C:\xampp-portable\htdocs\C-L\cel\aplicacao subdirs
verbosity level: 1. user tainted only vuln type: All server-side scan
code style: phps bottom-up /regex/: search
windows
files user input
stats functions 0.54
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_cenario.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
51: mysql_query mysql_query(**$commandSQL**) or // funcoes_genericas.php
46: $commandSQL = "INSERT INTO cenario (id_projeto,data, titulo, objetivo, contexto, atores, recursos, excecao, episodios) VALUES (**$idProject**,'$date', '" . prepara_dado (strtolower($title)) . "', '" . prepara_dado ($objective) . "', '" . prepara_dado ($context) . "', '" . prepara_dado ($actors) . "', '" . prepara_dado ($resources) . "', '" . prepara_dado ($exception) // funcoes_genericas.php
42: _ function scenarioincludes($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
45: $date = date("Y-m-d"); // funcoes_genericas.php
requires:
40: if(!(function_exists("scenarioIncludes")))
Userinput is passed through function parameters.
270: _ $idIncluded = scenarioincludes ($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php
266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
requires:
264: if(!(function_exists("addScenario")))
Userinput is passed through function parameters.

1335: _addscenario ($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
requires:
1304: if(!(function_exists("inserirPedidoAdicionarCenario")))
1334: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
76: _inserirpedidoadicionarcenario ($_SESSION['id_projeto_corrente'], $title, $objective, $context, $actors, $resources, $exception, $episodes, $_SESSION['id_usuario_corrente']);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
68: $title = str_replace(">", " ", str_replace("<", " ", **$title**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
69: $objective = str_replace(">", " ", str_replace("<", " ", **$objective**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
70: $context = str_replace(">", " ", str_replace("<", " ", **$context**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
71: $actors = str_replace(">", " ", str_replace("<", " ", **$actors**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
72: $resources = str_replace(">", " ", str_replace("<", " ", **$resources**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
52: if(isset($submit))
63: if($returnCheck == true)
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

231: **mysql_query $requestResultSQL** = mysql_query($commandSQL) or die ("Erro ao enviar a query"); // funcoes_genericas.php

230: $commandSQL = "SELECT **$field** FROM $table WHERE $where"; // funcoes_genericas.php

227: _ funcTion simple_query($field, $table, $where)

227: _ funcTion simple_query($field, $table, $where)

227: _ funcTion simple_query($field, $table, $where)

requires:

225: if(!(function_exists("simple_query")))

Userinput returned by function *import_request_variables()* reaches sensitive sink.

108: _ $nameProject = simple_query ("nome", "projeto", "id_projeto = " . $_SESSION['id_projeto_corrente']);

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

requires:

106: if(isset($submit)) else

Vulnerability is also triggered in:

C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

278: **mysql_query $requestResultSQL** = mysql_query($commandSQL) or die ("Erro ao enviar a query de SELECT
" . mysql_error() . "<br>" . __FILE__ . __LINE__);

funcoes_genericas.php

272: $commandSQL = "SELECT id_cenario, titulo, contexto, episodios FROM cenario WHERE id_projeto = **$idProject** AND id_cenario != $idIncluded ORDER BY CHAR_LENGTH(titulo) DESC"; // funcoes_genericas.php

266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)

270: $idIncluded = scenarioincludes ($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php

266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)

266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)

266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)

266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)

266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)

266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)

266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)

requires:

264: if(!(function_exists("addScenario")))

Userinput is passed through function parameters.

1335: _ addscenario ($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

requires:

1304: if(!(function_exists("inserirPedidoAdicionarCenario")))

1334: if($resultArray == false) else

Userinput returned by function *import_request_variables()* reaches sensitive sink.

76: _ inserirpedidoadicionarcenario ($_SESSION['id_projeto_corrente'], $title, $objective, $context, $actors, $resources, $exception, $episodes, $_SESSION['id_usuario_corrente']);

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
68: $title = str_replace(">", " ", str_replace("<", " ", **$title**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
69: $objective = str_replace(">", " ", str_replace("<", " ", **$objective**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
70: $context = str_replace(">", " ", str_replace("<", " ", **$context**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
71: $actors = str_replace(">", " ", str_replace("<", " ", **$actors**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
72: $resources = str_replace(">", " ", str_replace("<", " ", **$resources**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
52: if(isset($submit))
63: if($returnCheck == true)
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
293: **mysql_query** mysql_query(**$commandSQL**) or // funcoes_genericas.php
290: $commandSQL = "INSERT INTO centocen (id_cenario_from, id_cenario_to) VALUES (" . $result['id_cenario'] . ", **$idIncluded**)"; // funcoes_genericas.php
282: $result = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php
278: $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de SELECT
" . mysql_error() . "<br>" . __FILE__ . __LINE__ funcoes_genericas.php, trace stopped
270: $idIncluded = scenarioincludes (**$idProject**, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php
266: _function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
266: _function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
266: _function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
266: _function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
266: _function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
266: _function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
266: _function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
266: _function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
requires:
264: if(!(function_exists("addScenario")))
282: _function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
288: if((preg_match($regex, $result['contexto']) != 0) || (preg_match($regex, $result['episodios']) != 0))
Userinput is passed through function parameters.
1335: _addscenario ($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
requires:
1304: if(!(function_exists("inserirPedidoAdicionarCenario")))
1334: if($resultArray == false) else

Userinput returned by function *import_request_variables()* reaches sensitive sink.
76: _inserirpedidoadicionarcenario ($_SESSION['id_projeto_corrente'], $title, $objective, $context, $actors, $resources, $exception, $episodes, $_SESSION['id_usuario_corrente']);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
68: $title = str_replace(">", " ", str_replace("<", " ", **$title**));

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
69: $objective = str_replace(">", " ", str_replace("<", " ", **$objective**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
70: $context = str_replace(">", " ", str_replace("<", " ", **$context**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
71: $actors = str_replace(">", " ", str_replace("<", " ", **$actors**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
72: $resources = str_replace(">", " ", str_replace("<", " ", **$resources**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
52: if(isset($submit))
63: if($returnCheck == true)
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
308: mysql_query mysql_query(**$commandSQL**) or // funcoes_genericas.php
305: $commandSQL = "INSERT INTO centocen (id_cenario_from, id_cenario_to)

```
VALUES ($idIncluded, " . $result['id_cenario'] . ")"; // funcoes_genericas.php
270: $idIncluded = scenarioincludes ($idProject, $title, $objective, $context,
$actors, $resources, $exception, $episodes); // funcoes_genericas.php
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
282: $result = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php
278: $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a
query de SELECT<br>" . mysql_error() . "<br>" . __FILE__ . __LINE__
funcoes_genericas.php, trace stopped
requires:
264: if(!(function_exists("addScenario")))
282: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
303: if((preg_match($regex, $context) != 0) || (preg_match($regex, $episodes)
!= 0))
Userinput is passed through function parameters.
1335: _ addscenario ($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes); // funcoes_genericas.php
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
requires:
1304: if(!(function_exists("inserirPedidoAdicionarCenario")))
1334: if($resultArray == false) else
```



```
Userinput returned by function import_request_variables() reaches sensitive sink.
76: _ inserirpedidoadicionarcenario
($_SESSION['id_projeto_corrente'], $title, $objective, $context, $actors,
$resources, $exception, $episodes, $_SESSION['id_usuario_corrente']);
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
68: $title = str_replace(">", " ", str_replace("<", " ", $title));
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
69: $objective = str_replace(">", " ", str_replace("<", " ", $objective));
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
```

13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
70: $context = str_replace(">", " ", str_replace("<", " ", **$context**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
71: $actors = str_replace(">", " ", str_replace("<", " ", **$actors**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
72: $resources = str_replace(">", " ", str_replace("<", " ", **$resources**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
52: if(isset($submit))
63: if($returnCheck == true)
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
317: mysql_query $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de SELECT 3
" . mysql_error() . "<br>" . __FILE__ . __LINE__
funcoes_genericas.php
315: $commandSQL = "SELECT id_lexico, nome FROM lexico WHERE id_projeto = **$idProject** "; // funcoes_genericas.php
266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
requires:
264: if(!(function_exists("addScenario")))
Userinput is passed through function parameters.

1335: _addscenario ($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
requires:
1304: if(!(function_exists("inserirPedidoAdicionarCenario")))
1334: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
76: _inserirpedidoadicionarcenario ($_SESSION['id_projeto_corrente'], $title, $objective, $context, $actors, $resources, $exception, $episodes, $_SESSION['id_usuario_corrente']);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
68: $title = str_replace(">", " ", str_replace("<", " ", **$title**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
69: $objective = str_replace(">", " ", str_replace("<", " ", **$objective**));

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
70: $context = str_replace(">", " ", str_replace("<", " ", **$context**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
71: $actors = str_replace(">", " ", str_replace("<", " ", **$actors**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
72: $resources = str_replace(">", " ", str_replace("<", " ", **$resources**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
52: if(isset($submit))
63: if($returnCheck == true)
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

```
Userinput reaches sensitive sink.
334: mysql_query $queryScenarioResult = mysql_query($queryScenario) or die ("Erro ao enviar a query de select no centolex<br>" . mysql_error() . "<br>" . __FILE__
332: $queryScenario = "SELECT * FROM centolex WHERE id_cenario = $idIncluded AND id_lexico = " . $result2['id_lexico']; // funcoes_genericas.
270: $idIncluded = scenarioincludes ($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php
266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)
319: $result2 = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php
317: $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de SELECT 3<br>" . mysql_error() . "<br>" . __FILE__ . __LINE__
requires:
264: if(!(function_exists("addScenario")))
330: if((preg_match($regex, $title) != 0) || (preg_match($regex, $objective) != 0) || (preg_match($regex, $context) != 0) || (preg_match($regex, $actors
Userinput is passed through function parameters.
1335: _ addscenario ($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
```

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
requires:
1304: if(!(function_exists("inserirPedidoAdicionarCenario")))
1334: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
76: _ inserirpedidoadicionarcenario ($_SESSION['id_projeto_corrente'], $title, $objective, $context, $actors, $resources, $exception, $episodes, $_SESSION['id_usuario_corrente']);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
68: $title = str_replace(">", " ", str_replace("<", " ", **$title**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
69: $objective = str_replace(">", " ", str_replace("<", " ", **$objective**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
70: $context = str_replace(">", " ", str_replace("<", " ", **$context**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
71: $actors = str_replace(">", " ", str_replace("<", " ", **$actors**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
72: $resources = str_replace(">", " ", str_replace("<", " ", **$resources**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
52: if(isset($submit))
63: if($returnCheck == true)
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

```
Userinput reaches sensitive sink. (Blind exploitation)
342: mysql_query mysql_query($commandSQL) or // funcoes_genericas.php
340: $commandSQL = "INSERT INTO centolex (id_cenario, id_lexico) VALUES
($idIncluded, " . $result2['id_lexico'] .
270: $idIncluded = scenarioincludes ($idProject, $title, $objective, $context,
$actors, $resources, $exception, $episodes); // funcoes_genericas.php
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
319: $result2 = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php
317: $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a
query de SELECT 3<br>" . mysql_error() . "<br>" . __FILE__ . __LINE__
requires:
264: if(!(function_exists("addScenario")))
330: if((preg_match($regex, $title) != 0) || (preg_match($regex, $objective) !=
0) || (preg_match($regex, $context) != 0) || (preg_match($regex, $actors
339: if($resultArrayScenario == false)
Userinput is passed through function parameters.
1335: _ addscenario ($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes); // funcoes_genericas.php
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
requires:
1304: if(!(function_exists("inserirPedidoAdicionarCenario")))
```

1334: `if($resultArray == false) else`
Userinput returned by function *import_request_variables()* reaches sensitive sink.
76: `_inserirpedidoadicionarcenario ($_SESSION['id_projeto_corrente'], $title, $objective, $context, $actors, $resources, $exception, $episodes, $_SESSION['id_usuario_corrente']);`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
68: `$title = str_replace(">", " ", str_replace("<", " ", $title));`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
69: `$objective = str_replace(">", " ", str_replace("<", " ", $objective));`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
70: `$context = str_replace(">", " ", str_replace("<", " ", $context));`

14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
71: `$actors = str_replace(">", " ", str_replace("<", " ", $actors));`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
72: `$resources = str_replace(">", " ", str_replace("<", " ", $resources));`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
52: `if(isset($submit))`
63: `if($returnCheck == true)`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

356: **mysql_query** **$query_synonymous_result** = mysql_query($query_synonymous) or die ("Erro ao enviar a query
" . mysql_error() . "<br>" . __FILE__ . __LINE__
funcoes_genericas.php

354: $query_synonymous = "SELECT nome, id_lexico FROM sinonimo WHERE id_projeto = **$idProject** AND id_pedidolex = 0"; // funcoes_genericas.php

266: _ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)

requires:

264: if(!(function_exists("addScenario")))

Userinput is passed through function parameters.

1335: _ addscenario ($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

requires:

1304: if(!(function_exists("inserirPedidoAdicionarCenario")))

1334: if($resultArray == false) else

Userinput returned by function *import_request_variables()* reaches sensitive sink.

76: _ inserirpedidoadicionarcenario ($_SESSION['id_projeto_corrente'], $title, $objective, $context, $actors, $resources, $exception, $episodes, $_SESSION['id_usuario_corrente']);

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

68: $title = str_replace(">", " ", str_replace("<", " ", **$title**));

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

69: $objective = str_replace(">", " ", str_replace("<", " ", **$objective**));

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

70: $context = str_replace(">", " ", str_replace("<", " ", **$context**));

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

71: $actors = str_replace(">", " ", str_replace("<", " ", **$actors**));

14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
72: `$resources = str_replace(">", " ", str_replace("<", " ", $resources));`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`

requires:
52: `if(isset($submit))`
63: `if($returnCheck == true)`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
376: `mysql_query $requestResultSQL = mysql_query($query_scenario) or die ("Erro ao enviar a query de busca<br>" . mysql_error() . "<br>" . __FILE__ . __LINE__ funcoes_genericas.php`
368: `$query_scenario = "SELECT id_cenario, titulo, contexto, episodios, objetivo, atores, recursos, excecao FROM cenario WHERE id_projeto = $idProject AND id_cenario = $idIncluded"; // funcoes_genericas.php`
266: `_ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
270: `$idIncluded = scenarioincludes ($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php`
266: `_ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
266: `_ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
266: `_ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
266: `_ function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)`

```
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
requires:
264: if(!(function_exists("addScenario")))
Userinput is passed through function parameters.
1335: _ addscenario ($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes); // funcoes_genericas.php
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective,
$context, $actors, $resources, $exception, $episodes, $id_usuario)
requires:
1304: if(!(function_exists("inserirPedidoAdicionarCenario")))
1334: if($resultArray == false) else
Userinput returned by function import_request_variables() reaches sensitive sink.
76: _ inserirpedidoadicionarcenario
($_SESSION['id_projeto_corrente'], $title, $objective, $context, $actors,
$resources, $exception, $episodes, $_SESSION['id_usuario_corrente']);
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
68: $title = str_replace(">", " ", str_replace("<", " ", $title));
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
69: $objective = str_replace(">", " ", str_replace("<", " ", $objective));
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
70: $context = str_replace(">", " ", str_replace("<", " ", $context));
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
71: $actors = str_replace(">", " ", str_replace("<", " ", $actors));
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
72: $resources = str_replace(">", " ", str_replace("<", " ", $resources));
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
```

12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
52: `if(isset($submit))`

63: `if($returnCheck == true)`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
393: **mysql_query $queryScenarioResult** `= mysql_query($queryScenario) or die ("Erro ao enviar a query de select no centolex<br>" . mysql_error() . "<br>" . __FILE__`
391: `$queryScenario = "SELECT * FROM centolex WHERE id_cenario =` **$idIncluded** `AND id_lexico = $id_lexiconSynonymous`
270: `$idIncluded = scenarioincludes (`**$idProject**`, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php`
266: `_function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
266: `_function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
266: `_function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
266: `_function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
266: `_function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
266: `_function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
266: `_function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
266: `_function addscenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
365: `$id_lexiconSynonymous[] = $rowSinonimo['id_lexico']; // funcoes_genericas.php`
362: `$rowSinonimo = mysql_fetch_array($query_synonymous_result)){ // funcoes_genericas.php`
356: `$query_synonymous_result = mysql_query($query_synonymous) or die ("Erro ao enviar a query<br>" . mysql_error() . "<br>" . __FILE__`
requires:

264: if(!(function_exists("addScenario")))
389: if((preg_match($regex, $objective) != 0) || (preg_match($regex, $context) != 0) || (preg_match($regex, $actors) != 0) || (preg_match($regex,
Userinput is passed through function parameters.
1335: _addscenario ($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
requires:
1304: if(!(function_exists("inserirPedidoAdicionarCenario")))
1334: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
76: _inserirpedidoadicionarcenario ($_SESSION['id_projeto_corrente'], $title, $objective, $context, $actors, $resources, $exception, $episodes, $_SESSION['id_usuario_corrente']);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
68: $title = str_replace(">", " ", str_replace("<", " ", **$title**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
69: $objective = str_replace(">", " ", str_replace("<", " ", **$objective**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
70: $context = str_replace(">", " ", str_replace("<", " ", **$context**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
71: $actors = str_replace(">", " ", str_replace("<", " ", **$actors**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
72: $resources = str_replace(">", " ", str_replace("<", " ", **$resources**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
52: if(isset($submit))
63: if($returnCheck == true)

Vulnerability is also triggered in:

C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

```
Userinput reaches sensitive sink. (Blind exploitation)
399: mysql_query mysql_query($commandSQL) or // funcoes_genericas.php
397: $commandSQL = "INSERT INTO centolex (id_cenario, id_lexico) VALUES
($idIncluded, $id_lexiconSynonymous[$i
270: $idIncluded = scenarioincludes ($idProject, $title, $objective, $context,
$actors, $resources, $exception, $episodes); // funcoes_genericas.php
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
266: _ function addscenario($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes)
365: $id_lexiconSynonymous[] = $rowSinonimo['id_lexico']; //
funcoes_genericas.php
362: $rowSinonimo = mysql_fetch_array($query_synonymous_result)){ //
funcoes_genericas.php
356: $query_synonymous_result = mysql_query($query_synonymous) or die ("Erro ao
enviar a query<br>" . mysql_error() . "<br>" . __FILE__
requires:
264: if(!(function_exists("addScenario")))
389: if((preg_match($regex, $objective) != 0) || (preg_match($regex, $context)
!= 0) || (preg_match($regex, $actors) != 0) || (preg_match($regex,
396: if($resultArrayScenario == false)
Userinput is passed through function parameters.
1335: _ addscenario ($idProject, $title, $objective, $context, $actors,
$resources, $exception, $episodes); // funcoes_genericas.php
```

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)
requires:
1304: if(!(function_exists("inserirPedidoAdicionarCenario")))
1334: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
76: _ inserirpedidoadicionarcenario ($_SESSION['id_projeto_corrente'], $title, $objective, $context, $actors, $resources, $exception, $episodes, $_SESSION['id_usuario_corrente']);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
68: $title = str_replace(">", " ", str_replace("<", " ", **$title**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
69: $objective = str_replace(">", " ", str_replace("<", " ", **$objective**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
70: $context = str_replace(">", " ", str_replace("<", " ", **$context**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
71: $actors = str_replace(">", " ", str_replace("<", " ", **$actors**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
72: $resources = str_replace(">", " ", str_replace("<", " ", **$resources**));
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
52: if(isset($submit))
63: if($returnCheck == true)
Vulnerability is also triggered in:

C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

1283: **mysql_query** **$qr** = mysql_query($commandSQL) or die ("Erro ao enviar a query de select no cenario
" . mysql_error() . "<br>" . __FILE__ . __LINE__);
funcoes_genericas.php

1282: $commandSQL = "SELECT * FROM cenario WHERE id_projeto = **$projeto** AND titulo = '$title' "; // funcoes_genericas.php

1278: _ function checarcenarioexistente($projeto, $title)

1278: _ function checarcenarioexistente($projeto, $title)

Userinput returned by function *import_request_variables()* reaches sensitive sink.

54: _ $returnCheck = checarcenarioexistente ($_SESSION['id_projeto_corrente'], $title);

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

requires:

52: if(isset($submit))

Vulnerability is also triggered in:

C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

1313: **mysql_query $qr** = mysql_query($commandSQL) or die ("Erro ao enviar a query de select no participa
" . mysql_error() . "<br>" . __FILE__ . __LINE__);
funcoes_genericas.php

1312: $commandSQL = "SELECT * FROM participa WHERE gerente = 1 AND id_usuario = **$id_usuario** AND id_projeto = $idProject "; // funcoes_genericas.php

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

1306: _ function inserirpedidoadicionarcenario($idProject, $title, $objective, $context, $actors, $resources, $exception, $episodes, $id_usuario)

requires:

1304: if(!(function_exists("inserirPedidoAdicionarCenario")))

Userinput returned by function *import_request_variables()* reaches sensitive sink.

76: _ inserirpedidoadicionarcenario ($_SESSION['id_projeto_corrente'], $title, $objective, $context, $actors, $resources, $exception, $episodes, $_SESSION['id_usuario_corrente']);

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

68: $title = str_replace(">", " ", str_replace("<", " ", **$title**));

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

69: $objective = str_replace(">", " ", str_replace("<", " ", **$objective**));

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

70: $context = str_replace(">", " ", str_replace("<", " ", **$context**));

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

71: $actors = str_replace(">", " ", str_replace("<", " ", **$actors**));

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

72: $resources = str_replace(">", " ", str_replace("<", " ", **$resources**));

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

requires:

52: `if(isset($submit))`
63: `if($returnCheck == true)`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: `$a $a = $valor; // httprequest.inc`
6: `$a = $chave; // httprequest.inc`
5: `list($chave, $valor) = each($_GET)){ // httprequest.inc list()`
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: `$a $a = $valor; // httprequest.inc`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_lexico.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
86: `mysql_query mysql_query($commandSQL) or // funcoes_genericas.php`
82: `$commandSQL = "INSERT INTO lexico (id_projeto, data, nome, nocao, impacto, tipo)
VALUES ($idProject , '$date', '" . prepara_dado (strtolower($name)) . "', '" . prepara_dado
($notion) . "', '" . prepara_dado ($impact) . "', '$classification')"; // funcoes_genericas.php`
76: `_ function lexiconincludes($idProject, $name, $notion, $impact, $synonyms, $classification)`
79: `$date = date("Y-m-d"); // funcoes_genericas.php`
76: `_ function lexiconincludes($idProject, $name, $notion, $impact, $synonyms, $classification)`
requires:
74: `if(!(function_exists("lexiconIncludes")))`
Userinput is passed through function parameters.
443: `_ $idIncluded = lexiconincludes ($idProject, $name, $notion, $impact, $synonyms, $classification); // funcoes_genericas.php`
439: `_ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)`

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
requires:

437: if(!(function_exists("addLexicon")))
Userinput is passed through function parameters.
1507: _ addlexicon ($idProject, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
requires:
1454: if(!(function_exists("inserirPedidoAdicionarLexico")))
1506: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
58: $id_usuario_corrente = **$_SESSION**['id_usuario_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
48: $listSinonimo = array(); // if(!isset($listSinonimo)),
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
requires:
43: if(isset($submit))
56: if(($returnCheck == true) AND ($returnCheckTheSynonym == true))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink. (Blind exploitation)

103: mysql_query mysql_query(**$commandSQL**, $$SgbdConnectStatus) or // funcoes_genericas.php

101: $commandSQL = "INSERT INTO sinonimo (id_lexico, nome, id_projeto) VALUES ($newLexId, '" . prepara_dado (strtolower($newSynonymous)) . "', **$idProject**)"; // funcoes_genericas.php

89: $newLexId = mysql_insert_id($$SgbdConnectStatus); // funcoes_genericas.php

99: foreach($synonyms as $newSynonymous) // funcoes_genericas.php

93: $synonyms = array(); // funcoes_genericas.phpif(!is_array($synonyms)),

76: _ function lexiconincludes($idProject, $name, $notion, $impact, $synonyms, $classification)

requires:

74: if(!(function_exists("lexiconIncludes")))

Userinput is passed through function parameters.

443: _ $idIncluded = lexiconincludes ($idProject, $name, $notion, $impact, $synonyms, $classification); // funcoes_genericas.php

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

requires:

437: if(!(function_exists("addLexicon")))

Userinput is passed through function parameters.

1507: _ addlexicon ($idProject, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

requires:

1454: if(!(function_exists("inserirPedidoAdicionarLexico")))

1506: if($resultArray == false) else

Userinput returned by function *import_request_variables()* reaches sensitive sink.

59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

58: $id_usuario_corrente = **$_SESSION**['id_usuario_corrente'];

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

48: $listSinonimo = array(); // if(!isset($listSinonimo)),

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

requires:

43: if(isset($submit))

56: if(($returnCheck == true) AND ($returnCheckTheSynonym == true))

Vulnerability is also triggered in:

C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

449: **mysql_query $requestResultSQL** = mysql_query($query_result) or die ("Erro ao enviar a query de SELECT 1
" . mysql_error() . "<br>" . __FILE__ . __LINE__
funcoes_genericas.php
445: $query_result = "SELECT id_cenario, titulo, objetivo, contexto, atores, recursos, excecao, episodios FROM cenario
WHERE id_projeto = **$idProject** "; // funcoes_genericas.php
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
requires:
437: if(!(function_exists("addLexicon")))
Userinput is passed through function parameters.
1507: _ addlexicon ($idProject, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
requires:
1454: if(!(function_exists("inserirPedidoAdicionarLexico")))
1506: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.

59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
58: $id_usuario_corrente = **$_SESSION**['id_usuario_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
48: $listSinonimo = array(); // if(!isset($listSinonimo)),
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
43: `if(isset($submit))`
56: `if(($returnCheck == true) AND ($returnCheckTheSynonym == true))`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
465: `mysql_query mysql_query($commandSQL) or // funcoes_genericas.php`
462: `$commandSQL = "INSERT INTO centolex (id_cenario, id_lexico) VALUES (" . $result['id_cenario'] . ", $idIncluded)"; // funcoes_genericas.`**451:** `$result = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php`
449: `$requestResultSQL = mysql_query($query_result) or die ("Erro ao enviar a query de SELECT 1<br>" . mysql_error() . "<br>" . __FILE__ . __LINE__`
443: `$idIncluded = lexiconincludes ($idProject, $name, $notion, $impact, $synonyms, $classification); // funcoes_genericas.php`
439: `_ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)`
439: `_ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)`
439: `_ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)`
439: `_ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)`
439: `_ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)`
439: `_ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)`
requires:
437: `if(!(function_exists("addLexicon")))`
451: `_ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)`
461: `if((preg_match($regex, $result['objetivo']) != 0) || (preg_match($regex, $result['contexto']) != 0) || (preg_match($regex, $result['atores'])`

Userinput is passed through function parameters.
1507: _ addlexicon ($idProject, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
requires:
1454: if(!(function_exists("inserirPedidoAdicionarLexico")))
1506: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
58: $id_usuario_corrente = **$_SESSION**['id_usuario_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
48: $listSinonimo = array(); // if(!isset($listSinonimo)),
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
requires:
43: if(isset($submit))
56: if(($returnCheck == true) AND ($returnCheckTheSynonym == true))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
478: mysql_query $requestResultSQL = mysql_query($query_result) or die ("Erro ao enviar a query de SELECT 2
" . mysql_error() . "<br>" . __FILE__ . __LINE__
funcoes_genericas.php
445: $query_result = "SELECT id_cenario, titulo, objetivo, contexto, atores, recursos, excecao, episodios FROM cenario
WHERE id_projeto = **$idProject** "; // funcoes_genericas.php
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
requires:
437: if(!(function_exists("addLexicon")))
Userinput is passed through function parameters.
1507: _ addlexicon ($idProject, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
requires:
1454: if(!(function_exists("inserirPedidoAdicionarLexico")))
1506: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
58: `$id_usuario_corrente = $_SESSION['id_usuario_corrente'];`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
48: `$listSinonimo = array(); // if(!isset($listSinonimo)),`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`

12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
43: `if(isset($submit))`
56: `if(($returnCheck == true) AND ($returnCheckTheSynonym == true))`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
494: `mysql_query $query_lexiconResult = mysql_query($query_lexicon) or die ("Erro ao enviar a query de select no centolex<br>" . mysql_error() . "<br>" . __FILE__`
493: `$query_lexicon = "SELECT * FROM centolex WHERE id_cenario = " . $result2['id_cenario'] . " AND id_lexico = $idIncluded "; // funcoes_genericas.php`
481: `$result2 = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php`

478: $requestResultSQL = mysql_query($query_result) or die ("Erro ao enviar a query de SELECT 2
" . mysql_error() . "<br>" . __FILE__ . __LINE__
443: $idIncluded = lexiconincludes (**$idProject**, $name, $notion, $impact, $synonyms, $classification); // funcoes_genericas.php
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
requires:
437: if(!(function_exists("addLexicon")))
491: if((preg_match($regex, $result2['objetivo']) != 0) || (preg_match($regex, $result2['contexto']) != 0) || (preg_match($regex, $result2['atores']
Userinput is passed through function parameters.
1507: _ addlexicon ($idProject, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
requires:
1454: if(!(function_exists("inserirPedidoAdicionarLexico")))
1506: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
58: $id_usuario_corrente = **$_SESSION**['id_usuario_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
48: $listSinonimo = array(); // if(!isset($listSinonimo)),
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
requires:
43: if(isset($submit))
56: if(($returnCheck == true) AND ($returnCheckTheSynonym == true))

Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
502: **mysql_query** mysql_query(**$commandSQL**) or // funcoes_genericas.php
499: $commandSQL = "INSERT INTO centolex (id_cenario, id_lexico) VALUES (" . $result2['id_cenario'] . ", **$idIncluded**)";
481: $result2 = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php
478: $requestResultSQL = mysql_query($query_result) or die ("Erro ao enviar a query de SELECT 2
" . mysql_error() . "<br>" . __FILE__ . __LINE__
443: $idIncluded = lexiconincludes (**$idProject**, $name, $notion, $impact, $synonyms, $classification); // funcoes_genericas.php
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
requires:
437: if(!(function_exists("addLexicon")))
491: if((preg_match($regex, $result2['objetivo']) != 0) || (preg_match($regex, $result2['contexto']) != 0) || (preg_match($regex, $result2['atores'

497: if($resultArraylex == false)
Userinput is passed through function parameters.
1507: _ addlexicon ($idProject, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
requires:
1454: if(!(function_exists("inserirPedidoAdicionarLexico")))
1506: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
58: $id_usuario_corrente = **$_SESSION**['id_usuario_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
48: $listSinonimo = array(); // if(!isset($listSinonimo)),
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
requires:
43: if(isset($submit))
56: if(($returnCheck == true) AND ($returnCheckTheSynonym == true))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
RIPS - A static source code analyser for vulnerabilities in PHP scripts http://localhost/rips-0.54/

C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

521: mysql_query $requestResultSQL = mysql_query($query_otherLexicon) or die ("Erro ao enviar a query de SELECT no LEXICO
" . mysql_error() . "<br>" . __FILE__ funcoes_genericas.php

515: $query_otherLexicon = "SELECT id_lexico, nome, nocao, impacto, tipo FROM lexico WHERE id_projeto = **$idProject**
AND id_lexico != $idIncluded"; // funcoes_genericas.php

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

443: $idIncluded = lexiconincludes ($idProject, $name, $notion, $impact, $synonyms, $classification); // funcoes_genericas.php

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

requires:

437: if(!(function_exists("addLexicon")))

Userinput is passed through function parameters.

1507: _ addlexicon ($idProject, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

requires:

1454: if(!(function_exists("inserirPedidoAdicionarLexico")))

1506: if($resultArray == false) else

Userinput returned by function *import_request_variables()* reaches sensitive sink.

59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
58: $id_usuario_corrente = **$_SESSION**['id_usuario_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
48: $listSinonimo = array(); // if(!isset($listSinonimo)),
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
requires:
43: if(isset($submit))
56: if(($returnCheck == true) AND ($returnCheckTheSynonym == true))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

532: **mysql_query** **$query_lexiconResult** = mysql_query($query_lexicon) or die ("Erro ao enviar a query de select no lextolex
" . mysql_error() . "<br>" . __FILE__ funcoes_genericas.php

531: $query_lexicon = "SELECT * FROM lextolex WHERE id_lexico_from = " . $result['id_lexico'] . " AND id_lexico_to = **$idIncluded**"; // funcoes_genericas.php

523: $result = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php

521: $requestResultSQL = mysql_query($query_otherLexicon) or die ("Erro ao enviar a query de SELECT no LEXICO
" . mysql_error() . "<br>" . funcoes_genericas.php, trace stopped

443: $idIncluded = lexiconincludes (**$idProject**, $name, $notion, $impact, $synonyms, $classification); // funcoes_genericas.php

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

requires:

437: if(!(function_exists("addLexicon")))

529: if((preg_match($regex, $result['nocao']) != 0) || (preg_match($regex, $result['impacto']) != 0))

Userinput is passed through function parameters.

1507: _ addlexicon ($idProject, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

requires:

1454: if(!(function_exists("inserirPedidoAdicionarLexico")))

1506: if($resultArray == false) else

Userinput returned by function *import_request_variables()* reaches sensitive sink.

59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
58: `$id_usuario_corrente = $_SESSION['id_usuario_corrente'];`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
48: `$listSinonimo = array(); // if(!isset($listSinonimo)),`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
43: `if(isset($submit))`
56: `if(($returnCheck == true) AND ($returnCheckTheSynonym == true))`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
540: **mysql_query** `mysql_query($commandSQL) or // funcoes_genericas.php`
537: `$commandSQL = "INSERT INTO lextolex (id_lexico_from, id_lexico_to) VALUES (" . $result['id_lexico'] . ", $idIncluded)";`
523: `$result = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php`
521: `$requestResultSQL = mysql_query($query_otherLexicon) or die ("Erro ao enviar a query de SELECT no LEXICO<br>" . mysql_error() . "<br>" . funcoes_genericas.php, trace stopped`

443: $idIncluded = lexiconincludes (**$idProject**, $name, $notion, $impact, $synonyms, $classification); // funcoes_genericas.php
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
requires:
437: if(!(function_exists("addLexicon")))
529: if((preg_match($regex, $result['nocao']) != 0) || (preg_match($regex, $result['impacto']) != 0))
535: if($resultArraylex == false)
Userinput is passed through function parameters.
1507: _ addlexicon ($idProject, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
requires:
1454: if(!(function_exists("inserirPedidoAdicionarLexico")))
1506: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
58: $id_usuario_corrente = **$_SESSION**['id_usuario_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
48: $listSinonimo = array(); // if(!isset($listSinonimo)),
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
requires:
43: if(isset($submit))
56: if(($returnCheck == true) AND ($returnCheckTheSynonym == true))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
558: **mysql_query** mysql_query(**$commandSQL**) or // funcoes_genericas.php
556: $commandSQL = "INSERT INTO lextolex (id_lexico_from, id_lexico_to) VALUES (**$idIncluded**, " . $result['id_lexico'] . ")"; // funcoes_genericas.php
443: $idIncluded = lexicon**includes** (**$idProject**, $name, $notion, $impact, $synonyms, $classification); // funcoes_genericas.php
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
523: $result = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php
521: $requestResultSQL = mysql_query($query_otherLexicon) or die ("Erro ao enviar a query de SELECT no LEXICO
" . mysql_error() . "<br>" . funcoes_genericas.php, trace stopped
requires:
437: if(!(function_exists("addLexicon")))
554: if((preg_match($regex, $notion) != 0) || (preg_match($regex, $impact) != 0))

Userinput is passed through function parameters.
1507: _ addlexicon ($idProject, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
requires:
1454: if(!(function_exists("inserirPedidoAdicionarLexico")))
1506: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
58: $id_usuario_corrente = **$_SESSION**['id_usuario_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
48: $listSinonimo = array(); // if(!isset($listSinonimo)),
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
requires:
43: if(isset($submit))
56: if(($returnCheck == true) AND ($returnCheckTheSynonym == true))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

571: **mysql_query $requestResultSQL** = mysql_query($query_Lexicon) or die ("Erro ao enviar a query de select no lexico
" . mysql_error() . "<br>" . __FILE__ funcoes_genericas.php
566: $query_Lexicon = "SELECT id_lexico, nome, nocao, impacto FROM lexico WHERE id_projeto = **$idProject**
AND id_lexico != $idIncluded"; // funcoes_genericas.php
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
443: $idIncluded = lexiconincludes ($idProject, $name, $notion, $impact, $synonyms, $classification); // funcoes_genericas.php
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
requires:
437: if(!(function_exists("addLexicon")))
Userinput is passed through function parameters.
1507: _ addlexicon ($idProject, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
requires:
1454: if(!(function_exists("inserirPedidoAdicionarLexico")))
1506: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.

59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
58: $id_usuario_corrente = **$_SESSION**['id_usuario_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
48: $listSinonimo = array(); // if(!isset($listSinonimo)),
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
requires:
43: if(isset($submit))
56: if(($returnCheck == true) AND ($returnCheckTheSynonym == true))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

586: **mysql_query $query_lexiconResult** = mysql_query($query_lexicon) or die ("Erro ao enviar a query de select no lextolex
" . mysql_error() . "<br>" . __FILE__ funcoes_genericas.php

585: $query_lexicon = "SELECT * FROM lextolex WHERE id_lexico_from = " . $resultl['id_lexico'] . " AND id_lexico_to = **$idIncluded**"; // funcoes_genericas.php

577: $resultl = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php

571: $requestResultSQL = mysql_query($query_Lexicon) or die ("Erro ao enviar a query de select no lexico
" . mysql_error() . "<br>" . __FILE__ funcoes_genericas.php, trace stopped

443: $idIncluded = lexiconincludes (**$idProject**, $name, $notion, $impact, $synonyms, $classification); // funcoes_genericas.php

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)

requires:

437: if(!(function_exists("addLexicon")))

583: if((preg_match($regex, $resultl['nocao']) != 0) || (preg_match($regex, $resultl['impacto']) != 0))

Userinput is passed through function parameters.

1507: _ addlexicon ($idProject, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)

requires:

1454: if(!(function_exists("inserirPedidoAdicionarLexico")))

1506: if($resultArray == false) else

Userinput returned by function *import_request_variables()* reaches sensitive sink.

59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
58: `$id_usuario_corrente = $_SESSION['id_usuario_corrente'];`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
48: `$listSinonimo = array(); // if(!isset($listSinonimo)),`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
43: `if(isset($submit))`
56: `if(($returnCheck == true) AND ($returnCheckTheSynonym == true))`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
594: **mysql_query** `mysql_query($commandSQL) or // funcoes_genericas.php`
591: `$commandSQL = "INSERT INTO lextolex (id_lexico_from, id_lexico_to) VALUES (" . $resultl['id_lexico'] . ", $idIncluded)";`
funcoes_genericas.php
577: `$resultl = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php`
571: `$requestResultSQL = mysql_query($query_Lexicon) or die ("Erro ao enviar a query de select no lexico<br>" . mysql_error() . "<br>" . __FILE__`
funcoes_genericas.php, trace stopped
443: `$idIncluded = lexiconincludes ($idProject, $name, $notion, $impact, $synonyms, $classification); // funcoes_genericas.php`

```
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms,
$classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms,
$classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms,
$classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms,
$classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms,
$classification)
439: _ function addlexicon($idProject, $name, $notion, $impact, $synonyms,
$classification)
```


requires:

```
437: if(!(function_exists("addLexicon")))
583: if((preg_match($regex, $resultl['nocao']) != 0) || (preg_match($regex,
$resultl['impacto']) != 0))
589: if($resultArraylex == false)
```

Userinput is passed through function parameters.

```
1507: _ addlexicon ($idProject, $name, $notion, $impact, $sinonimos,
$classificacao); // funcoes_genericas.php
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion,
$impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion,
$impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion,
$impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion,
$impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion,
$impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion,
$impact, $id_usuario, $sinonimos, $classificacao)
```

requires:

```
1454: if(!(function_exists("inserirPedidoAdicionarLexico")))
1506: if($resultArray == false) else
```

Userinput returned by function *import_request_variables()* reaches sensitive sink.

```
59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact,
$id_usuario_corrente, $listSinonimo, $classificacao);
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
58: $id_usuario_corrente = $_SESSION['id_usuario_corrente'];
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
48: $listSinonimo = array(); // if(!isset($listSinonimo)),
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
```

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
requires:
43: if(isset($submit))
56: if(($returnCheck == true) AND ($returnCheckTheSynonym == true))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
610: **mysql_query $query_SynonymousResult** = mysql_query($query_Synonymous) or die ("Erro ao enviar a query de select no sinonimo
" . mysql_error() . "<br>"
funcoes_genericas.php
606: $query_Synonymous = "SELECT nome, id_lexico FROM sinonimo WHERE id_projeto = **$idProject**
AND id_lexico != $idIncluded AND id_pedidolex = 0"; // funcoes_genericas.php
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
443: $idIncluded = lexiconincludes ($idProject, $name, $notion, $impact, $synonyms, $classification); // funcoes_genericas.php
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
439: _function addlexicon($idProject, $name, $notion, $impact, $synonyms, $classification)
requires:
437: if(!(function_exists("addLexicon")))
Userinput is passed through function parameters.
1507: _addlexicon ($idProject, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
requires:
1454: if(!(function_exists("inserirPedidoAdicionarLexico")))
1506: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
58: $id_usuario_corrente = **$_SESSION**['id_usuario_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
48: $listSinonimo = array(); // if(!isset($listSinonimo)),
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
requires:
43: if(isset($submit))
56: if(($returnCheck == true) AND ($returnCheckTheSynonym == true))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

1204: `mysql_query $qr = mysql_query($commandSQL) or die ("Erro ao enviar a query de select no lexico<br>" . mysql_error() . "<br>" . __FILE__ . __LINE__); // funcoes_genericas.php`

1203: `$commandSQL = "SELECT * FROM lexico WHERE id_projeto = $projeto AND nome = '$name' "; // funcoes_genericas.php`

1199: `_ function checarlexicoexistente($projeto, $name)`

1199: `_ function checarlexicoexistente($projeto, $name)`

Userinput returned by function *import_request_variables()* reaches sensitive sink.

45: `_ $returnCheck = checarlexicoexistente ($_SESSION['id_projeto_corrente'], $name);`

14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`

13: `$a = $chave; // httprequest.inc`

12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`

12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`

14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`

13: `$a = $chave; // httprequest.inc`

12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`

12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`

requires:

43: `if(isset($submit))`

Vulnerability is also triggered in:

C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
1214: **mysql_query $qr** = mysql_query($commandSQL) or die ("Erro ao enviar a query de select no lexico
" . mysql_error() . "<br>" . __FILE__ . __LINE__); // funcoes_genericas.php
1213: $commandSQL = "SELECT * FROM sinonimo WHERE id_projeto = **$projeto** AND nome = '$name' "; // funcoes_genericas.php
1199: _ function checarlexicoexistente($projeto, $name)
1199: _ function checarlexicoexistente($projeto, $name)
Userinput returned by function *import_request_variables()* reaches sensitive sink.
45: _ $returnCheck = checarlexicoexistente ($_SESSION['id_projeto_corrente'], $name);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
43: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.

1244: **mysql_query** **$qr** = mysql_query($commandSQL) or die ("Erro ao enviar a query de select no sinonimo
" . mysql_error() . "<br>" . __FILE__ . __LINE__);
funcoes_genericas.php
1243: $commandSQL = "SELECT * FROM sinonimo WHERE id_projeto = **$projeto** AND nome = '$sinonimo' "; // funcoes_genericas.php
1236: _ function checarsinonimo($projeto, $listSinonimo)
1241: foreach($listSinonimo as $sinonimo) // funcoes_genericas.php
1236: _ function checarsinonimo($projeto, $listSinonimo)
requires:
1241: _ function checarsinonimo($projeto, $listSinonimo)
Userinput returned by function *import_request_variables()* reaches sensitive sink.
54: _ $returnCheckTheSynonym = checarsinonimo ($_SESSION['id_projeto_corrente'], $listSinonimo);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
48: $listSinonimo = array(); // if(!isset($listSinonimo)),
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
43: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
1255: **mysql_query** **$qr** = mysql_query($commandSQL) or die ("Erro ao enviar a query de select no sinonimo
" . mysql_error() . "<br>" . __FILE__ . __LINE__);
funcoes_genericas.php
1254: $commandSQL = "SELECT * FROM lexico WHERE id_projeto = **$projeto** AND nome = '$sinonimo' "; // funcoes_genericas.php
1236: _ function checarsinonimo($projeto, $listSinonimo)
1241: foreach($listSinonimo as $sinonimo) // funcoes_genericas.php
1236: _ function checarsinonimo($projeto, $listSinonimo)

requires:
1241: _ function checarsinonimo($projeto, $listSinonimo)
Userinput returned by function *import_request_variables()* reaches sensitive sink.
54: _ $returnCheckTheSynonym = checarsinonimo ($_SESSION['id_projeto_corrente'], $listSinonimo);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
48: $listSinonimo = array(); // if(!isset($listSinonimo)),
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
43: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
1464: mysql_query $qr = mysql_query($commandSQL) or die ("Erro ao enviar a query de select no participa
" . mysql_error() . "<br>" . __FILE__ . __LINE__);
funcoes_genericas.php
1463: $commandSQL = "SELECT * FROM participa WHERE gerente = 1 AND id_usuario = **$id_usuario** AND id_projeto = $idProject "; // funcoes_genericas.php

1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
1456: _ function inserirpedidoadicionarlexico($idProject, $name, $notion, $impact, $id_usuario, $sinonimos, $classificacao)
requires:
1454: if(!(function_exists("inserirPedidoAdicionarLexico")))
Userinput returned by function *import_request_variables()* reaches sensitive sink.
59: _ inserirpedidoadicionarlexico ($idProject, $name, $notion, $impact, $id_usuario_corrente, $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

```
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
58: $id_usuario_corrente = $_SESSION['id_usuario_corrente'];
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
48: $listSinonimo = array(); // if(!isset($listSinonimo)),
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
43: if(isset($submit))
56: if(($returnCheck == true) AND ($returnCheckTheSynonym == true))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
```

Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
90: **mysql_query** **$requestResultSQL** = mysql_query($commandSQL) or die ("Erro ao executar a query");
89: $commandSQL = "SELECT nome FROM projeto WHERE id_projeto = **$idProject** ";
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
87: if(isset($submit)) else
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_projeto.php
RIPS - A static source code analyser for vulnerabilities in PHP scripts http://localhost/rips-0.54/
30 de 68 29/11/2013 13:14
SQL Injection
Userinput reaches sensitive sink.
131: **mysql_query** **$queryVerifiesResult** = mysql_query($queryVerifies) or die ("Erro ao enviar a query de select
" . mysql_error() . "<br>" . __FILE__ . __LINE__ funcoes_genericas.php
130: $queryVerifies = "SELECT * FROM projeto WHERE nome = '**$name**'"; // funcoes_genericas.php
125: _ function projectincludes($name, $description)
requires:
123: if(!(function_exists("projectIncludes")))
Userinput returned by function *import_request_variables()* reaches sensitive sink.
30: _ $id_projeto_incluido = projectincludes ($name, $description);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
28: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

Possible Flow Control

Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.

7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()

Possible Flow Control

Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.

14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

SQL Injection

Userinput returned by function *import_request_variables()* reaches sensitive sink. (Blind exploitation)

38: **mysql_query** mysql_query(**$commandSQL**) or
37: $commandSQL = "INSERT INTO participa (id_usuario, id_projeto, gerente) VALUES (**$id_usuario_corrente**, $id_projeto_incluido, $gerente)";
36: $id_usuario_corrente = **$_SESSION**['id_usuario_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
30: $id_projeto_incluido = projectincludes ($name, $description);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
35: $gerente = 1;

requires:

28: if(isset($submit))
32: if($id_projeto_incluido != - 1)

hide all

File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/add_usuario.php

Possible Flow Control

Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.

7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()

Possible Flow Control

Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.

14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

SQL Injection

Userinput returned by function *import_request_variables()* reaches sensitive sink.
55: **mysql_query** **$requestResultSQL** = mysql_query($commandSQL) or die ("Erro ao enviar a query");
54: $commandSQL = "SELECT id_usuario FROM usuario WHERE login = '**$login**'";

14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
12: `if(isset($submit))`
22: `if($name == "" || $email == "" || $login == "" || $password == "" || $senha_conf == "") else`
30: `if($password != $senha_conf) else`
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink. (Blind exploitation)
90: **mysql_query** `mysql_query($commandSQL) or`
89: `$commandSQL = "INSERT INTO usuario (nome, login, email, senha) VALUES ('$name', '$login', '$email', '$password')";`
84: `$name = str_replace(">", " ", str_replace("<", " ", $name));`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
85: `$login = str_replace(">", " ", str_replace("<", " ", $login));`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
86: `$email = str_replace(">", " ", str_replace("<", " ", $email));`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
88: `$password = md5($password);`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
12: `if(isset($submit))`
22: `if($name == "" || $email == "" || $login == "" || $password == "" || $senha_conf == "") else`
30: `if($password != $senha_conf) else`
82: `if(mysql_num_rows($requestResultSQL)) else`
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink. (Blind exploitation)
142: **mysql_query** `mysql_query($commandSQL) or`
139: `$commandSQL = "INSERT INTO participa (id_usuario, id_projeto) VALUES ($id_usuario_incluido, " . $_SESSION['id_projeto_corrente'] . ")";`
137: `$id_usuario_incluido = simple_query ("id_usuario", "usuario", "login = '$login'");`
85: `$login = str_replace(">", " ", str_replace("<", " ", $login)); // if(isset($submit)), if($name == "" || $email == "" || $login == "" || $password == "" || $senha_conf == "") else , if($password != $senha_conf) else , if(mysql_num_rows($requestResultSQL)) else ,`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:

98: if(isset($cadastrado))
131: if($novo == "true") else
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/algoritmo_inicio.php
SQL Injection
Userinput reaches sensitive sink.
121: mysql_query $result = mysql_query($query) or die ("A consulta ao BD falhou : " . mysql_error() . __LINE__); // auxiliar_bd.php
118: $query = "update lexico set tipo = '**$type**' where id_lexico = '$id_lexico';"; // auxiliar_bd.phpif($type == "null") else ,
99: _ function atualiza_tipo($id_lexico, $type)
99: _ function atualiza_tipo($id_lexico, $type)
Userinput is passed through function parameters.
466: _ atualiza_tipo ($term, $aux)) // auxiliar_bd.php
463: foreach($list as $key=>$term) // auxiliar_bd.php
461: $list = verifica_tipo (); // auxiliar_bd.php
464: $aux = **$_POST**["type".$key]; // auxiliar_bd.php
requires:
454: if(isset($_SESSION['tipos']))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/arv_interface.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/auxiliar_bd.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/scrip_bd2.php

hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_cenario.php
SQL Injection
Userinput reaches sensitive sink.
698: mysql_query $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de SELECT
" . mysql_error() . "<br>" . __FILE__ . __LINE__);
funcoes_genericas.php
692: $commandSQL = "SELECT id_cenario, titulo, contexto, episodios FROM cenario WHERE id_projeto = **$idProject** AND id_cenario != $idScenario ORDER BY CHAR_LENGTH(titulo) DESC"; // funcoes_genericas.php
663: _ function changescenario($idProject, $idScenario, $title, $objective, $context, $actors, $resources, $exception, $episodes)
663: _ function changescenario($idProject, $idScenario, $title, $objective, $context, $actors, $resources, $exception, $episodes)
requires:
661: if(!(function_exists("changeScenario")))
Userinput is passed through function parameters.
1385: _ changescenario ($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php
1355: _ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa
1355: _ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa
requires:
1353: if(!(function_exists("inserirPedidoAlterarCenario")))
1384: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
14: _ inserirpedidoalterarcenario ($_SESSION['id_projeto_corrente'], $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa, $_SESSION['id_usuario_corrente'
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
12: `if(isset($submit))`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
710: `mysql_query mysql_query($commandSQL) or // funcoes_genericas.php`
708: `$commandSQL = "INSERT INTO centocen (id_cenario_from, id_cenario_to) VALUES (" . $result['id_cenario'] . ", $idScenario)";`
funcoes_genericas.php
700: `$result = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php`
698: `$requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de SELECT<br>" . mysql_error() . "<br>" . __FILE__ . __LINE__`
funcoes_genericas.php, trace stopped
663: `_ function changescenario($idProject, $idScenario, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
requires:
661: `if(!(function_exists("changeScenario")))`
700: `_ function changescenario($idProject, $idScenario, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
706: `if((preg_match($regex, $result['contexto']) != 0) || (preg_match($regex, $result['episodios']) != 0))`
Userinput is passed through function parameters.
1385: `_ changescenario ($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php`
1355: `_ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa`
1355: `_ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa`
requires:
1353: `if(!(function_exists("inserirPedidoAlterarCenario")))`
1384: `if($resultArray == false) else`
Userinput returned by function *import_request_variables()* reaches sensitive sink.
14: `_ inserirpedidoalterarcenario ($_SESSION['id_projeto_corrente'], $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa, $_SESSION['id_usuario_corrente'`

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
12: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
723: mysql_query mysql_query(**$commandSQL**) or // funcoes_genericas.php
721: $commandSQL = "INSERT INTO centocen (id_cenario_from, id_cenario_to) VALUES (**$idScenario**, " . $result['id_cenario'] . ")"; // funcoes_genericas.php
663: _function changescenario($idProject, $idScenario, $title, $objective, $context, $actors, $resources, $exception, $episodes)
700: $result = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php
698: $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de SELECT
" . mysql_error() . "<br>" . __FILE__ . __LINE__ funcoes_genericas.php, trace stopped
requires:
661: if(!(function_exists("changeScenario")))
700: _function changescenario($idProject, $idScenario, $title, $objective, $context, $actors, $resources, $exception, $episodes)
720: if((preg_match($regex, $context) != 0) || (preg_match($regex, $episodes) != 0))
Userinput is passed through function parameters.
1385: _changescenario ($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php
1355: _function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa

1355: _ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa
requires:
1353: if(!(function_exists("inserirPedidoAlterarCenario")))
1384: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
14: _ inserirpedidoalterarcenario
($_SESSION['id_projeto_corrente'], $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa, $_SESSION['id_usuario_corrente']
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
12: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
733: **mysql_query $requestResultSQL** = mysql_query($commandSQL) or die ("Erro ao enviar a query de SELECT 3
" . mysql_error() . "<br>" . __FILE__ . __LINE__
funcoes_genericas.php
731: $commandSQL = "SELECT id_lexico, nome FROM lexico WHERE id_projeto = **$idProject** "; // funcoes_genericas.php
663: _ function changescenario($idProject, $idScenario, $title, $objective, $context, $actors, $resources, $exception, $episodes)
requires:
661: if(!(function_exists("changeScenario")))

Userinput is passed through function parameters.

1385: _ changescenario ($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php

1355: _ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa

1355: _ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa

requires:

1353: if(!(function_exists("inserirPedidoAlterarCenario")))

1384: if($resultArray == false) else

Userinput returned by function *import_request_variables()* reaches sensitive sink.

14: _ inserirpedidoalterarcenario ($_SESSION['id_projeto_corrente'], $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa, $_SESSION['id_usuario_corrente'

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

requires:

12: if(isset($submit))

Vulnerability is also triggered in:

C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

749: mysql_query $query_ScenarioResult = mysql_query($query_Scenario) or die ("Erro ao enviar a query de select no centolex
" . mysql_error() . "<br>" . __FILE__

748: $query_Scenario = "SELECT * FROM centolex WHERE id_cenario = **$idScenario** AND id_lexico = " . $result2['id_lexico']; // funcoes_genericas.php

663: _ function changescenario($idProject, $idScenario, $title, $objective, $context, $actors, $resources, $exception, $episodes)
735: $result2 = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php
733: $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de SELECT 3
" . mysql_error() . "<br>" . __FILE__ . __LINE__
requires:
661: if(!(function_exists("changeScenario")))
746: if((preg_match($regex, $title) != 0) || (preg_match($regex, $objective) != 0) || (preg_match($regex, $context) != 0) || (preg_match($regex, $actors
Userinput is passed through function parameters.
1385: _ changescenario ($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php
1355: _ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa
1355: _ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa
requires:
1353: if(!(function_exists("inserirPedidoAlterarCenario")))
1384: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.

14: _ inserirpedidoalterarcenario ($_SESSION['id_projeto_corrente'], $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa, $_SESSION['id_usuario_corrente'
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
12: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
755: **mysql_query** `mysql_query(`**$commandSQL**`) or // funcoes_genericas.php`
754: `$commandSQL = "INSERT INTO centolex (id_cenario, id_lexico) VALUES (`**$idScenario**`, " . $result2['id_lexico'] . ")"; // funcoes_genericas.php`
663: `_function changescenario($idProject, $idScenario, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
735: `$result2 = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php`
733: `$requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de SELECT 3<br>" . mysql_error() . "<br>" . __FILE__ . __LINE__`
requires:
661: `if(!(function_exists("changeScenario")))`
746: `if((preg_match($regex, $title) != 0) || (preg_match($regex, $objective) != 0) || (preg_match($regex, $context) != 0) || (preg_match($regex, $actors`
752: `if($resultArrayScen == false)`
Userinput is passed through function parameters.
1385: `_changescenario ($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php`
1355: `_function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa`
1355: `_function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa`
requires:
1353: `if(!(function_exists("inserirPedidoAlterarCenario")))`
1384: `if($resultArray == false) else`
Userinput returned by function *import_request_variables()* reaches sensitive sink.
14: `_inserirpedidoalterarcenario ($_SESSION['id_projeto_corrente'], $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa, $_SESSION['id_usuario_corrente'`
14: `$$a = `**$valor**`; // is like import_request_variables() // httprequest.incsee above`
13: `$a = `**$chave**`; // httprequest.inc`
12: `list($chave, `**$valor**`) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = `**$valor**`; // is like import_request_variables() // httprequest.incsee above`
13: `$a = `**$chave**`; // httprequest.inc`
12: `list($chave, `**$valor**`) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = `**$valor**`; // is like import_request_variables() // httprequest.incsee above`
13: `$a = `**$chave**`; // httprequest.inc`
12: `list($chave, `**$valor**`) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
12: `if(isset($submit))`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
770: `mysql_query $query_synonymousResult = mysql_query($query_synonymous) or die ("Erro ao enviar a query<br>" . mysql_error() . "<br>" . __FILE__ . __LINE__`
funcoes_genericas.php
767: `$query_synonymous = "SELECT nome, id_lexico FROM sinonimo WHERE id_projeto = $idProject AND id_pedidolex = 0"; //`
funcoes_genericas.php
663: `_ function changescenario($idProject, $idScenario, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
requires:
661: `if(!(function_exists("changeScenario")))`
Userinput is passed through function parameters.
1385: `_ changescenario ($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php`
1355: `_ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa`
1355: `_ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa`
requires:
1353: `if(!(function_exists("inserirPedidoAlterarCenario")))`
1384: `if($resultArray == false) else`
Userinput returned by function *import_request_variables()* reaches sensitive sink.
14: `_ inserirpedidoalterarcenario ($_SESSION['id_projeto_corrente'], $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa, $_SESSION['id_usuario_corrente'`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
12: `if(isset($submit))`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

791: mysql_query $requestResultSQL = mysql_query($query_LexiconScenario) or die ("Erro ao enviar a query de busca
" . mysql_error() . "<br>" . __FILE__ . funcoes_genericas.php

782: $query_LexiconScenario = "SELECT id_cenario, titulo, contexto, episodios, objetivo, atores, recursos, excecao FROM cenario WHERE id_projeto = **$idProject** AND id_cenario = $idScenario"; // funcoes_genericas.php

663: _ function changescenario($idProject, $idScenario, $title, $objective, $context, $actors, $resources, $exception, $episodes)

663: _ function changescenario($idProject, $idScenario, $title, $objective, $context, $actors, $resources, $exception, $episodes)

requires:

661: if(!(function_exists("changeScenario")))

Userinput is passed through function parameters.

1385: _ changescenario ($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php

1355: _ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa

1355: _ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa

requires:

1353: if(!(function_exists("inserirPedidoAlterarCenario")))

1384: if($resultArray == false) else

Userinput returned by function *import_request_variables()* reaches sensitive sink.

14: _ inserirpedidoalterarcenario ($_SESSION['id_projeto_corrente'], $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa, $_SESSION['id_usuario_corrente'

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

requires:

12: if(isset($submit))

Vulnerability is also triggered in:

C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

806: **mysql_query $query_ScenarioResult** = mysql_query($query_Scenario) or die ("Erro ao enviar a query de select no centolex
" . mysql_error() . "<br>" . __FILE__

805: $query_Scenario = "SELECT * FROM centolex WHERE id_cenario = **$idScenario** AND id_lexico = $id_lexiconSynonymous[$i] "; // funcoes_genericas.php

663: _ function changescenario($idProject, $idScenario, $title, $objective, $context, $actors, $resources, $exception, $episodes)

779: $id_lexiconSynonymous[] = $rowSynonymous['id_lexico']; // funcoes_genericas.php

776: $rowSynonymous = mysql_fetch_array($query_synonymousResult)){ // funcoes_genericas.php

770: $query_synonymousResult = mysql_query($query_synonymous) or die ("Erro ao enviar a query
" . mysql_error() . "<br>" . __FILE__ .

requires:

661: if(!(function_exists("changeScenario")))

803: if((preg_match($regex, $objective) != 0) || (preg_match($regex, $context) != 0) || (preg_match($regex, $actors) != 0) || (preg_match($regex,

Userinput is passed through function parameters.

1385: _ changescenario ($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php

1355: _ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa

1355: _ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa

requires:

1353: if(!(function_exists("inserirPedidoAlterarCenario")))

1384: if($resultArray == false) else

Userinput returned by function *import_request_variables()* reaches sensitive sink.

14: _ inserirpedidoalterarcenario ($_SESSION['id_projeto_corrente'], $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa, $_SESSION['id_usuario_corrente'

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
12: `if(isset($submit))`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
811: **mysql_query** `mysql_query($commandSQL) or // funcoes_genericas.php`
810: `$commandSQL = "INSERT INTO centolex (id_cenario, id_lexico) VALUES ($idScenario, $id_lexiconSynonymous[$i])"; // funcoes_genericas.php`
663: `_ function changescenario($idProject, $idScenario, $title, $objective, $context, $actors, $resources, $exception, $episodes)`
779: `$id_lexiconSynonymous[] = $rowSynonymous['id_lexico']; // funcoes_genericas.php`
776: `$rowSynonymous = mysql_fetch_array($query_synonymousResult)){ // funcoes_genericas.php`
770: `$query_synonymousResult = mysql_query($query_synonymous) or die ("Erro ao enviar a query<br>" . mysql_error() . "<br>" . __FILE__ .`
requires:
661: `if(!(function_exists("changeScenario")))`
803: `if((preg_match($regex, $objective) != 0) || (preg_match($regex, $context) != 0) || (preg_match($regex, $actors) != 0) || (preg_match($regex,`
809: `if($resultArrayScen == false)`
Userinput is passed through function parameters.
1385: `_ changescenario ($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes); // funcoes_genericas.php`
1355: `_ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa`
1355: `_ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa`
requires:
1353: `if(!(function_exists("inserirPedidoAlterarCenario")))`

1384: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
14: _ inserirpedidoalterarcenario
($_SESSION['id_projeto_corrente'], $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa, $_SESSION['id_usuario_corrente'
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
12: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
1362: mysql_query $qr = mysql_query($commandSQL) or die ("Erro ao enviar a query de select no participa
" . mysql_error() . "<br>" . __FILE__ . __LINE__);
1361: $commandSQL = "SELECT * FROM participa WHERE gerente = 1 AND id_usuario = **$id_usuario** AND id_projeto = $idProject "; // funcoes_genericas.php
1355: _ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa
1355: _ function inserirpedidoalterarcenario($idProject, $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa
requires:
1353: if(!(function_exists("inserirPedidoAlterarCenario")))
Userinput returned by function *import_request_variables()* reaches sensitive sink.
14: _ inserirpedidoalterarcenario

($_SESSION['id_projeto_corrente'], $id_cenario, $title, $objective, $context, $actors, $resources, $exception, $episodes, $justificativa, $_SESSION['id_usuario_corrente'
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
12: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
42: **mysql_query** **$requestResultSQL** = mysql_query($commandSQL) or die ("Erro ao executar a query");
41: $commandSQL = "SELECT * FROM cenario WHERE id_cenario = **$id_cenario**";
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
37: `if(isset($submit)) else`
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_conceito.php
SQL Injection
Userinput reaches sensitive sink.
1122: `mysql_query $requestResultSQL = mysql_query($qr) or die ("Erro ao enviar a query de SELECT<br>" . mysql_error() . "<br>" . __FILE__ . __LINE__); // funcoes_genericas.php`
1120: `$qr = "SELECT * FROM conceito WHERE id_projeto = $idProject AND id_conceito != $id_conceito"; // funcoes_genericas.php`
1092: `_ function removeconcept($idProject, $id_conceito)`
1092: `_ function removeconcept($idProject, $id_conceito)`
requires:
1090: `if(!(function_exists("removeConcept")))`
Userinput is passed through function parameters.
1682: `_ removeconcept ($idProject, $id_conceito); // funcoes_genericas.php`
1652: `_ function inserirpedidoalterarconceito($idProject, $id_conceito, $name, $description, $namespace, $justificativa, $id_usuario)`
1652: `_ function inserirpedidoalterarconceito($idProject, $id_conceito, $name, $description, $namespace, $justificativa, $id_usuario)`
requires:
1650: `if(!(function_exists("inserirPedidoAlterarCenario")))`
1681: `if($resultArray == false) else`
Userinput returned by function *import_request_variables()* reaches sensitive sink.
20: `_ inserirpedidoalterarconceito ($_SESSION['id_projeto_corrente'], $id_conceito, $name, $description, $namespace, $justificativa, $_SESSION['id_usuario_corrente']);`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`

14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
19: `if(isset($submit))`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.
1659: mysql_query $qr = mysql_query($commandSQL) or die ("Erro ao enviar a query de select no participa
" . mysql_error() . "<br>" . __FILE__ . __LINE__); funcoes_genericas.php
1658: $commandSQL = "SELECT * FROM participa WHERE gerente = 1 AND id_usuario = **$id_usuario** AND id_projeto = $idProject "; // funcoes_genericas.php
1652: _ function inserirpedidoalterarconceito($idProject, $id_conceito, $name, $description, $namespace, $justificativa, $id_usuario)
1652: _ function inserirpedidoalterarconceito($idProject, $id_conceito, $name, $description, $namespace, $justificativa, $id_usuario)
requires:
1650: if(!(function_exists("inserirPedidoAlterarCenario")))
Userinput returned by function *import_request_variables()* reaches sensitive sink.
20: _ inserirpedidoalterarconceito ($_SESSION['id_projeto_corrente'], $id_conceito, $name, $description, $namespace, $justificativa, $_SESSION['id_usuario_corrente']);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
19: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: $a $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()

Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: $a $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
45: mysql_query $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao executar a query");
44: $commandSQL = "SELECT * FROM conceito WHERE id_conceito = **$id_conceito**";
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
40: if(isset($submit)) else
hide all

File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/alt_lexico.php

SQL Injection
Userinput reaches sensitive sink.
885: mysql_query $requestResultSQL = mysql_query($query_result) or die ("Erro ao enviar a query de SELECT 1
" . mysql_error() . "<br>" . __FILE__ . __LINE__ funcoes_genericas.php
881: $query_result = "SELECT id_cenario, titulo, objetivo, contexto, atores, recursos, excecao, episodios FROM cenario
WHERE id_projeto = **$idProject** "; // funcoes_genericas.php
857: _ function changelexicon($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao)
requires:
855: if(!(function_exists("changeLexicon")))
Userinput is passed through function parameters.
1574: _ changelexicon ($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
requires:
1525: if(!(function_exists("inserirPedidoAlterarLexico")))
1573: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
39: _ inserirpedidoalterarlexico ($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $_SESSION['id_usuario_corrente'], $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:

13: `if(isset($submit))`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
902: **mysql_query** `mysql_query(`**$commandSQL**`) or // funcoes_genericas.php`
899: `$commandSQL = "INSERT INTO centolex (id_cenario, id_lexico) VALUES (" . $result['id_cenario'] . ", `**$id_lexico**`)";`
887: `$result = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php`
885: `$requestResultSQL = mysql_query($query_result) or die ("Erro ao enviar a query de SELECT 1<br>" . mysql_error() . "<br>" . __FILE__ . __LINE__`
857: `_ function changelexicon($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao)`

requires:
855: `if(!(function_exists("changeLexicon")))`
887: `_ function changelexicon($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao)`
897: `if((preg_match($regex, $result['objetivo']) != 0) || (preg_match($regex, $result['contexto']) != 0) || (preg_match($regex, $result['atores'])`
Userinput is passed through function parameters.
1574: `_ changelexicon ($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php`
1527: `_ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)`
1527: `_ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)`
requires:
1525: `if(!(function_exists("inserirPedidoAlterarLexico")))`
1573: `if($resultArray == false) else`
Userinput returned by function *import_request_variables()* reaches sensitive sink.
39: `_ inserirpedidoalterarlexico ($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $_SESSION['id_usuario_corrente'], $listSinonimo, $classificacao);`
14: `$$a = `**$valor**`; // is like import_request_variables() // httpprequest.incsee above`
13: `$a = `**$chave**`; // httprequest.inc`
12: `list($chave, `**$valor**`) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = `**$valor**`; // is like import_request_variables() // httpprequest.incsee above`
13: `$a = `**$chave**`; // httprequest.inc`
12: `list($chave, `**$valor**`) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
13: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
914: **mysql_query $requestResultSQL** = mysql_query($query_result) or die ("Erro ao enviar a query de SELECT 2
" . mysql_error() . "<br>" . __FILE__ . __LINE__
funcoes_genericas.php
881: $query_result = "SELECT id_cenario, titulo, objetivo, contexto, atores, recursos, excecao, episodios FROM cenario
WHERE id_projeto = **$idProject** "; // funcoes_genericas.php
857: _function changelexicon($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao)
requires:
855: if(!(function_exists("changeLexicon")))
Userinput is passed through function parameters.
1574: _changelexicon ($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1527: _function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
1527: _function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
requires:
1525: if(!(function_exists("inserirPedidoAlterarLexico")))
1573: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
39: _inserirpedidoalterarlexico
($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $_SESSION['id_usuario_corrente'], $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
13: `if(isset($submit))`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
RIPS - A static source code analyser for vulnerabilities in PHP scripts http://localhost/rips-0.54/
43 de 68 29/11/2013 13:14
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
952: `mysql_query $requestResultSQL = mysql_query($qlo) or die ("Erro ao enviar a query de SELECT no LEXICO<br>" . mysql_error() . "<br>" . __FILE__ . __LINE__ funcoes_genericas.php`
947: `$qlo = "SELECT id_lexico, nome, nocao, impacto, tipo FROM lexico WHERE id_projeto = $idProject AND id_lexico <> $id_lexico"; // funcoes_genericas.php`
857: `_ function changelexicon($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao)`
857: `_ function changelexicon($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao)`
requires:
855: `if(!(function_exists("changeLexicon")))`
Userinput is passed through function parameters.
1574: `_ changelexicon ($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php`
1527: `_ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)`
1527: `_ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)`
requires:
1525: `if(!(function_exists("inserirPedidoAlterarLexico")))`
1573: `if($resultArray == false) else`
Userinput returned by function *import_request_variables()* reaches sensitive sink.
39: `_ inserirpedidoalterarlexico ($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $_SESSION['id_usuario_corrente'], $listSinonimo, $classificacao);`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
13: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
965: mysql_query mysql_query(**$commandSQL**) or // funcoes_genericas.php
962: $commandSQL = "INSERT INTO lextolex (id_lexico_from, id_lexico_to) VALUES (" . $result['id_lexico'] . ", **$id_lexico**)"; // funcoes_genericas.php
954: $result = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php
952: $requestResultSQL = mysql_query($qlo) or die ("Erro ao enviar a query de SELECT no LEXICO
" . mysql_error() . "<br>" . __FILE__ . __LINE__
funcoes_genericas.php, trace stopped
857: _ function changelexicon($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao)
requires:
855: if(!(function_exists("changeLexicon")))

961: if((preg_match($regex, $result['nocao']) != 0) || (preg_match($regex, $result['impacto']) != 0))
Userinput is passed through function parameters.
1574: _ changelexicon ($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
requires:
1525: if(!(function_exists("inserirPedidoAlterarLexico")))
1573: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
39: _ inserirpedidoalterarlexico

($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $_SESSION['id_usuario_corrente'], $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
13: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
981: mysql_query mysql_query(**$commandSQL**) or // funcoes_genericas.php
978: $commandSQL = "INSERT INTO lextolex (id_lexico_from, id_lexico_to) VALUES (**$id_lexico**, " . $result['id_lexico'] . ")"; // funcoes_genericas.php
857: _ function changelexicon($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao)
954: $result = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php
952: $requestResultSQL = mysql_query($qlo) or die ("Erro ao enviar a query de SELECT no LEXICO
" . mysql_error() . "<br>" . __FILE__ . __LINE__ funcoes_genericas.php, trace stopped
requires:
855: if(!(function_exists("changeLexicon")))
977: if((preg_match($regex, $notion) != 0) || (preg_match($regex, $impact) != 0))
Userinput is passed through function parameters.
1574: _ changelexicon ($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
requires:

1525: if(!(function_exists("inserirPedidoAlterarLexico")))
1573: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
39: _ inserirpedidoalterarlexico
($idProject, $id_lexico, $name, $notion, $impact, $justificativa,
$_SESSION['id_usuario_corrente'], $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee
above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee
above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee
above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
13: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
1000: mysql_query $requestResultSQL = mysql_query($sql) or die ("Erro ao enviar a
query de select no lexico
" . mysql_error() . "<br>" . __FILE__ . __LINE__
funcoes_genericas.php
989: $sql = "SELECT id_lexico, nome, nocao, impacto FROM lexico WHERE id_projeto
= **$idProject**
AND id_lexico <> $id_lexico"; // funcoes_genericas.php
857: _ function changelexicon($idProject, $id_lexico, $name, $notion, $impact,
$sinonimos, $classificacao)
857: _ function changelexicon($idProject, $id_lexico, $name, $notion, $impact,
$sinonimos, $classificacao)
requires:
855: if(!(function_exists("changeLexicon")))
Userinput is passed through function parameters.
1574: _ changelexicon ($idProject, $id_lexico, $name, $notion, $impact,
$sinonimos, $classificacao); // funcoes_genericas.php

1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
requires:
1525: if(!(function_exists("inserirPedidoAlterarLexico")))
1573: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
39: _ inserirpedidoalterarlexico ($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $_SESSION['id_usuario_corrente'], $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
13: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
1014: **mysql_query $result** = mysql_query($qverif) or die ("Erro ao enviar query de select no lextolex
" . mysql_error() . "<br>" . __FILE__ . __LINE__); // funcoes_genericas.php
1012: $qverif = "SELECT * FROM lextolex where id_lexico_from=" . $result1['id_lexico'] . " and id_lexico_to=**$id_lexico**"; // funcoes_genericas.php
1001: $result1 = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php
1000: $requestResultSQL = mysql_query($sql) or die ("Erro ao enviar a query de select no lexico
" . mysql_error() . "<br>" . __FILE__ . __LINE__ funcoes_genericas.php, trace stopped
857: _ function changelexicon($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao)
requires:
855: if(!(function_exists("changeLexicon")))

1009: if((preg_match($regex, $resultl['nocao']) != 0) || (preg_match($regex, $resultl['impacto']) != 0))

Userinput is passed through function parameters.
1574: _ changelexicon ($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
requires:
1525: if(!(function_exists("inserirPedidoAlterarLexico")))
1573: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
39: _ inserirpedidoalterarlexico ($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $_SESSION['id_usuario_corrente'], $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
13: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink. (Blind exploitation)
1018: **mysql_query** mysql_query(**$commandSQL**) or // funcoes_genericas.php
1016: $commandSQL = "INSERT INTO lextolex (id_lexico_from, id_lexico_to) VALUES (" . $resultl['id_lexico'] . ", **$id_lexico**)"; // funcoes_genericas.php
1001: $resultl = mysql_fetch_array($requestResultSQL)){ // funcoes_genericas.php

1000: $requestResultSQL = mysql_query($ql) or die ("Erro ao enviar a query de select no lexico
" . mysql_error() . "<br>" . __FILE__ . __LINE__
funcoes_genericas.php, trace stopped
857: _ function changelexicon($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao)
requires:
855: if(!(function_exists("changeLexicon")))
1009: if((preg_match($regex, $resultl['nocao']) != 0) || (preg_match($regex, $resultl['impacto']) != 0))
1015: if(!resultado)
Userinput is passed through function parameters.
1574: _ changelexicon ($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
requires:
1525: if(!(function_exists("inserirPedidoAlterarLexico")))
1573: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
39: _ inserirpedidoalterarlexico ($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $_SESSION['id_usuario_corrente'], $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
13: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection
Userinput reaches sensitive sink.
1034: mysql_query $qrrSinonimos = mysql_query($qSinonimos) or die ("Erro ao enviar a query de select no sinonimo
" . mysql_error() . "<br>" . __FILE__ . __LINE__
funcoes_genericas.php
1028: $qSinonimos = "SELECT nome, id_lexico FROM sinonimo WHERE id_projeto = **$idProject** AND id_lexico <> $id_lexico
AND id_pedidolex = 0"; // funcoes_genericas.php
857: _ function changelexicon($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao)
857: _ function changelexicon($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao)
requires:
855: if(!(function_exists("changeLexicon")))
Userinput is passed through function parameters.
1574: _ changelexicon ($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
requires:
1525: if(!(function_exists("inserirPedidoAlterarLexico")))
1573: if($resultArray == false) else
Userinput returned by function *import_request_variables()* reaches sensitive sink.
39: _ inserirpedidoalterarlexico
($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $_SESSION['id_usuario_corrente'], $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
13: if(isset($submit))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

1048: **mysql_query $result** = mysql_query($qv) or die ("Erro ao enviar query de select no lextolex
" . mysql_error() . "<br>" . __FILE__ . __LINE__); // funcoes_genericas.php
1047: $qv = "SELECT * FROM lextolex where id_lexico_from=**$id_lexico** and id_lexico_to=" . $rowSinonimo['id_lexico']; // funcoes_genericas.php
857: _ function changelexicon($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao)
1039: $rowSinonimo = mysql_fetch_array($qrrSinonimos)){ // funcoes_genericas.php
1034: $qrrSinonimos = mysql_query($qSinonimos) or die ("Erro ao enviar a query de select no sinonimo
" . mysql_error() . "<br>" . __FILE__ funcoes_genericas.php, trace stopped
requires:
855: if(!(function_exists("changeLexicon")))
1044: if((preg_match($regex, $notion) != 0) || (preg_match($regex, $impact) != 0))

Userinput is passed through function parameters.
1574: _ changelexicon ($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
requires:
1525: if(!(function_exists("inserirPedidoAlterarLexico")))
1573: if($resultArray == false) else

Userinput returned by function *import_request_variables()* reaches sensitive sink.
39: _ inserirpedidoalterarlexico ($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $_SESSION['id_usuario_corrente'], $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
13: if(isset($submit))

Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink. (Blind exploitation)

1053: **mysql_query** mysql_query(**$commandSQL**) or // funcoes_genericas.php
1050: $commandSQL = "INSERT INTO lextolex (id_lexico_from, id_lexico_to) VALUES (**$id_lexico**, " . $rowSinonimo['id_lexico'] . ")"
funcoes_genericas.php
857: _ function changelexicon($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao)
1039: $rowSinonimo = mysql_fetch_array($qrrSinonimos)){ // funcoes_genericas.php
1034: $qrrSinonimos = mysql_query($qSinonimos) or die ("Erro ao enviar a query de select no sinonimo
" . mysql_error() . "<br>" . __FILE__
funcoes_genericas.php, trace stopped
requires:
855: if(!(function_exists("changeLexicon")))
1044: if((preg_match($regex, $notion) != 0) || (preg_match($regex, $impact) != 0))
1049: if(!resultado)

Userinput is passed through function parameters.

1574: _ changelexicon ($idProject, $id_lexico, $name, $notion, $impact, $sinonimos, $classificacao); // funcoes_genericas.php
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
requires:
1525: if(!(function_exists("inserirPedidoAlterarLexico")))
1573: if($resultArray == false) else

Userinput returned by function *import_request_variables()* reaches sensitive sink.

39: _ inserirpedidoalterarlexico ($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $_SESSION['id_usuario_corrente'], $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
13: if(isset($submit))

Vulnerability is also triggered in:

C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

```
Userinput reaches sensitive sink. (Blind exploitation)
1077: mysql_query mysql_query($commandSQL, $SgbdConnectStatus) or //
funcoes_genericas.php
1074: $commandSQL = "INSERT INTO sinonimo (id_lexico, nome, id_projeto) VALUES
($id_lexico, '" . prepara_dado
(strtolower($novoSin)) . "', $idProject )"; // funcoes_genericas.php
857: _ function changelexicon($idProject, $id_lexico, $name, $notion, $impact,
$sinonimos, $classificacao)
1073: foreach($sinonimos as $novoSin) // funcoes_genericas.php
1067: $sinonimos = array(); // funcoes_genericas.phpif(!is_array($sinonimos)),
857: _ function changelexicon($idProject, $id_lexico, $name, $notion, $impact,
$sinonimos, $classificacao)
requires:
855: if(!(function_exists("changeLexicon")))
Userinput is passed through function parameters.
1574: _ changelexicon ($idProject, $id_lexico, $name, $notion, $impact,
$sinonimos, $classificacao); // funcoes_genericas.php
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name,
$notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name,
$notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao)
requires:
1525: if(!(function_exists("inserirPedidoAlterarLexico")))
1573: if($resultArray == false) else
Userinput returned by function import_request_variables() reaches sensitive sink.
39: _ inserirpedidoalterarlexico
($idProject, $id_lexico, $name, $notion, $impact, $justificativa,
$_SESSION['id_usuario_corrente'], $listSinonimo, $classificacao);
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
13: if(isset($submit))
Vulnerability is also triggered in:
```

C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

SQL Injection

Userinput reaches sensitive sink.

1535: **mysql_query $qr** = mysql_query($commandSQL) or die ("Erro ao enviar a query de select no participa
" . mysql_error() . "<br>" . __FILE__ . __LINE__);
funcoes_genericas.php
1534: $commandSQL = "SELECT * FROM participa WHERE gerente = 1 AND id_usuario = **$id_usuario** AND id_projeto = $idProject "; // funcoes_genericas.php
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao
1527: _ function inserirpedidoalterarlexico($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $id_usuario, $sinonimos, $classificacao
requires:
1525: if(!(function_exists("inserirPedidoAlterarLexico")))

Userinput returned by function *import_request_variables()* reaches sensitive sink.

39: _ inserirpedidoalterarlexico ($idProject, $id_lexico, $name, $notion, $impact, $justificativa, $_SESSION['id_usuario_corrente'], $listSinonimo, $classificacao);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
13: if(isset($submit))

Vulnerability is also triggered in:

C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

Possible Flow Control

```
Userinput is used to build the variable name. Arbitrary variables may be
overwritten/initialized which may lead to further vulnerabilities.
7: $a $$a = $valor; // httprequest.inc
6: $a = $chave; // httprequest.inc
5: list($chave, $valor) = each($_GET)){ // httprequest.inc list()
```

Possible Flow Control

```
Userinput is used to build the variable name. Arbitrary variables may be
overwritten/initialized which may lead to further vulnerabilities.
14: $a $$a = $valor; // httprequest.inc
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
```

SQL Injection

```
Userinput returned by function import_request_variables() reaches sensitive sink.
67: mysql_query $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao
executar a query");
66: $commandSQL = "SELECT * FROM lexico WHERE id_lexico = $id_lexico";
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
63: if(isset($submit)) else
```

SQL Injection

```
Userinput returned by function import_request_variables() reaches sensitive sink.
76: mysql_query $requestResultSQLSinonimo = mysql_query($commandSQLSinonimo) or die
("Erro ao executar a query");
75: $commandSQLSinonimo = "SELECT nome FROM sinonimo WHERE id_lexico =
$id_lexico";
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee
above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
63: if(isset($submit)) else
```

hide all

File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/code.php

SQL Injection

```
Userinput reaches sensitive sink.
2097: mysql_query $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao
enviar a query<br>" . mysql_error() . "<br>" . __FILE__ . __LINE__); //
funcoes_genericas.php
2093: $commandSQL = "SELECT * FROM participa WHERE id_usuario = $id_usuario
AND id_projeto = $idProject "; // funcoes_genericas.php
2091: _ function permissionchecktoproject($id_usuario, $idProject)
2091: _ function permissionchecktoproject($id_usuario, $idProject)
requires:
```



```
2089: if(!(function_exists("permissionCheckToProject")))
Userinput is passed through function parameters.
25: _ permissionchecktoproject ($_SESSION['id_usuario_corrente'], $idProject) or
11: $idProject = $_GET['id_projeto']; // if(isset($_GET)),
requires:
23: if(isset($idProject))
```

Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/form_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/funcoes_genericas.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
SQL Injection
Userinput reaches sensitive sink.
28: `mysql_query $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query");`
27: `$commandSQL = "SELECT nome FROM projeto WHERE id_projeto = $idProject ";`
11: `$idProject = $_GET['id_projeto']; // if(isset($_GET)),`
requires:
23: `if(isset($idProject))`
SQL Injection
Userinput reaches sensitive sink.
85: `mysql_query $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de selecao");`
80: `$commandSQL = "SELECT id_cenario, titulo FROM cenario WHERE id_projeto = $idProject ORDER BY titulo";`
11: `$idProject = $_GET['id_projeto']; // if(isset($_GET)),`
SQL Injection
Userinput reaches sensitive sink.
149: `mysql_query $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de selecao");`
144: `$commandSQL = "SELECT id_lexico, nome FROM lexico WHERE id_projeto = $idProject ORDER BY nome";`
11: `$idProject = $_GET['id_projeto']; // if(isset($_GET)),`
SQL Injection
Userinput reaches sensitive sink.
205: `mysql_query $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de selecao");`
200: `$commandSQL = "SELECT id_conceito, nome FROM conceito WHERE id_projeto = $idProject ORDER BY nome";`
11: `$idProject = $_GET['id_projeto']; // if(isset($_GET)),`
SQL Injection
Userinput reaches sensitive sink.
225: `mysql_query $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de selecao");`
220: `$commandSQL = "SELECT id_relacao, nome FROM relacao r WHERE id_projeto = $idProject ORDER BY nome";`
11: `$idProject = $_GET['id_projeto']; // if(isset($_GET)),`
SQL Injection
Userinput reaches sensitive sink.
245: `mysql_query $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de selecao");`

240: `$commandSQL = "SELECT id_axioma, axioma FROM axioma WHERE id_projeto = $idProject ORDER BY axioma";`
11: `$idProject = $_GET['id_projeto']; // if(isset($_GET)),`
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/create.php
SQL Injection
Userinput reaches sensitive sink.
121: **mysql_query $result** `= mysql_query($query) or die ("A consulta ao BD falhou : " . mysql_error() . __LINE__); // auxiliar_bd.php`
118: `$query = "update lexico set tipo = '$type' where id_lexico = '$id_lexico';"; // auxiliar_bd.phpif($type == "null") else ,`
99: `_ function atualiza_tipo($id_lexico, $type)`

99: `_ function atualiza_tipo($id_lexico, $type)`
Userinput is passed through function parameters.
466: `_ atualiza_tipo ($term, $aux)) // auxiliar_bd.php`
463: `foreach($list as $key=>$term) // auxiliar_bd.php`
461: `$list = verifica_tipo (); // auxiliar_bd.php`
464: `$aux = $_POST["type".$key]; // auxiliar_bd.php`
requires:
454: `if(isset($_SESSION['tipos']))`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_daml.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/inicio.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/script_bd2.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/teste_daml.php
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/enviar_senha.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** `$` **$a** `= $valor; // httprequest.inc`
6: `$a =` **$chave** `; // httprequest.inc`
5: `list($chave,` **$valor** `) = each($_GET)){ // httprequest.inc list()`
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** `$` **$a** `= $valor; // httprequest.inc`
13: `$a =` **$chave** `; // httprequest.inc`
12: `list($chave,` **$valor** `) = each($_POST)){ // httprequest.inc list()`
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
27: **mysql_query $requestResultSQL** `= mysql_query($commandSQL) or die ("Erro ao executar a query");`
25: `$commandSQL = "SELECT * FROM usuario WHERE login='` **$login** `'";`
14: `$$a =` **$valor** `; // is like import_request_variables() // httprequest.incsee above`
13: `$a =` **$chave** `; // httprequest.inc`
12: `list($chave,` **$valor** `) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_daml.php
File Manipulation
Userinput reaches sensitive sink. (Blind exploitation)
34: **fwrite** `fwrite(` **$fp** `,` **$header** `)) // daml.php`
22: `$fp = fopen(` **$address** `, "w")){ // daml.php`
19: `$address =` **$directory** `. $file; // daml.php`
15: `_ function savedaml($urlOntology, $directory, $file, $arrayInformation, $conceptsList, $relationsList, $axiomsList)`
15: `_ function savedaml($urlOntology, $directory, $file, $arrayInformation, $conceptsList, $relationsList, $axiomsList)`
32: `$header = $header .` **$arrayInformation** `['title'] . '="' . $url . '#">'; // daml.php`
31: `$header = $header . '<rdf:RDF xmlns:daml="http://www.daml.org/2001/03/daml+oil#" xmlns:dc="http://purl.org/dc/elements /1.1/" xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#" xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#" xmlns:xsd="http:`

```
//www.w3.org/2000/10/XMLSchema#" xmlns:'; // daml.php
30: $header = '<?xml version="1.0" encoding="ISO-8859-1" ?>'; // daml.php
15: _ function savedaml($urlOntology, $directory, $file, $arrayInformation,
$conceptsList, $relationsList, $axiomsList)
18: $url = $urlOntology . $file; // daml.php
15: _ function savedaml($urlOntology, $directory, $file, $arrayInformation,
$conceptsList, $relationsList, $axiomsList)
15: _ function savedaml($urlOntology, $directory, $file, $arrayInformation,
$conceptsList, $relationsList, $axiomsList)
Userinput is passed through function parameters.
42: _ $daml = savedaml ($site, $dir, $archive, $i, $lista_conceitos,
$relationsList, $lista_axiomas);
27: $site = $_SESSION['site'];
28: $dir = $_SESSION['diretorio'];
29: $archive = strtr($project, "
_____
", "aaaooo") . "__" . date("j-m-Y_H-i-s") . ".daml";
25: $project = $resultArray[0];
24: $resultArray = mysql_fetch_array($query_project);
23: $query_project = mysql_query($sql_project) or die ("Erro ao verificar
usu&aacute;rio!" . mysql_error()); // , trace stopped
31: $i["versionInfo"] = $_POST['versionInfo'] // array()
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/teste_daml.php
File Manipulation
Userinput reaches sensitive sink. (Blind exploitation)
93: fwrite fwrite($fp, $information)) // daml.php
22: $fp = fopen($address, "w")){ // daml.php
19: $address = $directory . $file; // daml.php
15: _ function savedaml($urlOntology, $directory, $file, $arrayInformation,
$conceptsList, $relationsList, $axiomsList)
15: _ function savedaml($urlOntology, $directory, $file, $arrayInformation,
$conceptsList, $relationsList, $axiomsList)
91: $information = $information . '</daml:Ontology>'; // daml.php
88: $information = $information . '<daml:versionInfo>' .
$arrayInformation['versionInfo'] . '</daml:versionInfo>'; //
daml.phpif($arrayInformation == "") else 84: $information = $information .
'<daml:versionInfo />'; // daml.phpif($arrayInformation == ""),
79: $information = $information . '<dc:subject>' . $arrayInformation['subject'] .
'</dc:subject>'; // daml.phpif($arrayInformation == "") else ,
75: $information = $information . '<dc:subject />'; //
daml.phpif($arrayInformation == ""),
70: $information = $information . '<dc:description>' .
$arrayInformation['description'] . '</dc:description>'; //
daml.phpif($arrayInformati
else ,
66: $information = $information . '<dc:description />'; //
daml.phpif($arrayInformation == ""),
61: $information = $information . '<dc:creator>' . $arrayInformation['creator'] .
'</dc:creator>'; // daml.phpif($arrayInformatio
else ,
57: $information = $information . '<dc:creator />'; //
daml.phpif($arrayInformation == ""),
```

```
53: $information = $information . '<dc:date>' . date("j-m-Y H:i:s") .
'</dc:date>'; // daml.php
50: $information = $information . '<dc:title>' . $arrayInformation['title'] .
'</dc:title>'; //
daml.phpif($arrayInformation == "") else ,
46: $information = $information . '<dc:title />'; //
daml.phpif($arrayInformation == ""),
42: $information = '<daml:Ontology rdf:about="">'; // daml.php
42: $information = '<daml:Ontology rdf:about="">'; // daml.php
:
15: _ function savedaml($urlOntology, $directory, $file, $arrayInformation,
$conceptsList,
15: _ function savedaml($urlOntology, $directory, $file, $arrayInformation,
$conceptsList, $relationsList, $axiomsList
15: _ function savedaml($urlOntology, $directory, $file, $arrayInformation,
$conceptsList, $relationsList, $axiomsList)
```

15: _ function savedaml($urlOntology, $directory, $file, $arrayInformation, $conceptsList, $relationsList, $axiomsList)
15: _ function savedaml($urlOntology, $directory, $file, $arrayInformation, $conceptsList, $relationsList, $axiomsList)
Userinput is passed through function parameters.
42: _ $daml = savedaml ($site, $dir, $archive, $i, $lista_conceitos, $relationsList, $lista_axiomas);
27: $site = $_SESSION['site'];
28: $dir = $_SESSION['diretorio'];
29: $archive = strtr($project, "
_____
", "aaaooo") . "__" . date("j-m-Y_H-i-s") . ".daml";
25: $project = $resultArray[0];
24: $resultArray = mysql_fetch_array($query_project);
23: $query_project = mysql_query($sql_project) or die ("Erro ao verificar usuário!" . mysql_error()); // , trace stopped
31: $i["versionInfo"] = **$_POST**['versionInfo'] // array()
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/teste_daml.php
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml-ANTIGO.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
SQL Injection
Userinput reaches sensitive sink.
55: **mysql_query** **$tb_nome** = mysql_query($qry_nome) or die ("Erro ao enviar a query de selecao.");
51: $qry_nome = "SELECT nome FROM projeto WHERE id_projeto = " . **$idProject**;
40: _ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)
Userinput returned by function *import_request_variables()* reaches sensitive sink.
183: _ $str_xml = gerar_xml ($bd_trabalho, $idProject, $data_pesquisa, $flag_formatado);
172: $idProject = **$_SESSION**['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
173: $data_pesquisa = **$data_ano** . "-" . $data_mes . "-" . $data_dia;
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
181: if(!mysql_num_rows($qrrVerifica))
SQL Injection
Userinput reaches sensitive sink.
66: **mysql_query** **$tb_cenario** = mysql_query($qry_cenario) or die ("Erro ao enviar a query de selecao.");

59: $qry_cenario = "SELECT id_cenario, titulo, objetivo, contexto , atores , recursos, episodios, excecao
FROM cenario WHERE (id_projeto = " . **$idProject** . ")
AND (data <=" . " '" . $data_pesquisa . "'" . ") ORDER BY id_cenario,data DESC";
40: _ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)
40: _ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)
Userinput returned by function *import_request_variables()* reaches sensitive sink.
183: _ $str_xml = gerar_xml ($bd_trabalho, $idProject, $data_pesquisa, $flag_formatado);
172: $idProject = **$_SESSION**['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
173: $data_pesquisa = **$data_ano** . "-" . $data_mes . "-" . $data_dia;
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
181: if(!mysql_num_rows($qrrVerifica))
SQL Injection
Userinput reaches sensitive sink.
126: **mysql_query** **$tb_lexico** = mysql_query($qry_lexico) or die ("Erro ao enviar a query de selecao.");
120: $qry_lexico = "SELECT id_lexico, nome, nocao, impacto FROM lexico
WHERE (id_projeto = " . **$idProject** . ") AND (data <=" . " '" . $data_pesquisa . "'" . ")
ORDER BY id_lexico,data DESC";
40: _ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)
40: _ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)
Userinput returned by function *import_request_variables()* reaches sensitive sink.
183: _ $str_xml = gerar_xml ($bd_trabalho, $idProject, $data_pesquisa, $flag_formatado);
172: $idProject = **$_SESSION**['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
173: $data_pesquisa = **$data_ano** . "-" . $data_mes . "-" . $data_dia;
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
181: if(!mysql_num_rows($qrrVerifica))
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
179: mysql_query $qrrVerifica = mysql_query($qVerifica);
178: $qVerifica = "SELECT * FROM publicacao WHERE id_projeto = '**$idProject** ' AND versao = '$version' ";
172: $idProject = **$_SESSION**['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink. (Blind exploitation)
193: mysql_query mysql_query(**$commandSQL**) or
188: $commandSQL = "INSERT INTO publicacao (id_projeto, data_publicacao, versao, XML)
VALUES ('**$idProject** ', '$data_pesquisa', '$version', '$xml_resultante')";
172: $idProject = **$_SESSION**['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
173: $data_pesquisa = $data_ano . "-" . $data_mes . "-" . $data_dia;
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
185: $xml_resultante = "<?xml version=''1.0'' encoding=''ISO-8859-1'' ?>\n" . $str_xml;
183: $str_xml = gerar_xml ($bd_trabalho, $idProject, $data_pesquisa, $flag_formatado);
176: $bd_trabalho = bd_connect () or die ("Erro ao conectar ao SGBD");
172: $idProject = $_SESSION['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
requires:
181: if(!mysql_num_rows($qrrVerifica))
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
196: mysql_query $requestResultSQL = mysql_query($queryResult) or die ("Erro ao enviar a query");

195: `$queryResult = "select * from publicacao where id_projeto = $idProject ";`
172: `$idProject = $_SESSION['id_projeto_corrente'];`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
181: `if(!mysql_num_rows($qrrVerifica))`
SQL Injection
RIPS - A static source code analyser for vulnerabilities in PHP scripts http://localhost/rips-0.54/
55 de 68 29/11/2013 13:14
Userinput returned by function *import_request_variables()* reaches sensitive sink.
204: `mysql_query $qrrRecupera = mysql_query($qRecupera) or die ("Erro ao enviar a query de busca!");`
203: `$qRecupera = "SELECT * FROM publicacao WHERE id_projeto = '$idProject ' AND versao = '$version'";`
172: `$idProject = $_SESSION['id_projeto_corrente'];`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
181: `if(!mysql_num_rows($qrrVerifica))`
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerador_xml.php
SQL Injection
Userinput reaches sensitive sink.
31: `mysql_query $queryLexiconsResult = mysql_query($queryLexicons) or die ("Erro ao enviar a query de selecao na tabela lexicos !" . mysql_error()); // coloca_links.php`
21: `$queryLexicons = "SELECT id_lexico, nome FROM lexico WHERE id_projeto = '$idProject ' ORDER BY nome DESC"; // coloca_links.phpif($noCurrent) else ,`
3: `_ function load_arraylexicon($idProject, $idCurrentLexicon, $noCurrent)`
Userinput is passed through function parameters.
74: `_ $vetor_todos_lexicos = load_arraylexicon ($idProject, 0, false);`
41: `_ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)`
requires:
39: `if(!(function_exists("gerar_xml")))`
Userinput is passed through function parameters.
137: `_ $vector_lexicons = load_arraylexicon ($idProject, $row[0], true);`
41: `_ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)`
requires:
39: `if(!(function_exists("gerar_xml")))`
Userinput returned by function *import_request_variables()* reaches sensitive sink.
373: `_ $str_xml = gerar_xml ($bd_trabalho, $idProject, $data_pesquisa, $flag_formatado);`
361: `$idProject = $_SESSION['id_projeto_corrente'];`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
362: `$data_pesquisa = $data_ano . "-" . $data_mes . "-" . $data_dia;`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`

12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
371: `if(!mysql_num_rows($qrrVerifica))`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/monta_relacoes.php
SQL Injection
Userinput reaches sensitive sink.
41: **mysql_query** **$querySynonymsResult** `= mysql_query($querySynonyms) or die ("Erro ao enviar a query de selecao na tabela sinonimos !" . mysql_error()); // coloca_links.php`
26: `$querySynonyms = "SELECT id_lexico, nome FROM sinonimo WHERE id_projeto = '`**$idProject**`' ORDER BY nome DESC"; // coloca_links.phpif($noCurrent) else ,`
3: `_ function load_arraylexicon($idProject, $idCurrentLexicon, $noCurrent)`
Userinput is passed through function parameters.
74: `_ $vetor_todos_lexicos = load_arraylexicon ($idProject, 0, false);`
41: `_ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)`
requires:
39: `if(!(function_exists("gerar_xml")))`
Userinput is passed through function parameters.
137: `_ $vector_lexicons = load_arraylexicon ($idProject, $row[0], true);`
41: `_ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)`
requires:
39: `if(!(function_exists("gerar_xml")))`
Userinput returned by function *import_request_variables()* reaches sensitive sink.
373: `_ $str_xml = gerar_xml ($bd_trabalho, $idProject, $data_pesquisa, $flag_formatado);`
361: `$idProject = `**$_SESSION**`['id_projeto_corrente'];`
14: `$$a = `**$valor**`; // is like import_request_variables() // httprequest.incsee above`
13: `$a = `**$chave**`; // httprequest.inc`
12: `list($chave, `**$valor**`) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`

362: `$data_pesquisa = `**$data_ano**` . "-" . $data_mes . "-" . $data_dia;`
14: `$$a = `**$valor**`; // is like import_request_variables() // httprequest.incsee above`
13: `$a = `**$chave**`; // httprequest.inc`
12: `list($chave, `**$valor**`) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = `**$valor**`; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a = `**$valor**`; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
371: `if(!mysql_num_rows($qrrVerifica))`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/monta_relacoes.php
SQL Injection
Userinput reaches sensitive sink.
77: **mysql_query** **$queryScenariosResult** `= mysql_query($queryScenarios) or die ("Erro ao enviar a query de selecao !!" . mysql_error()); // coloca_links.php`

71: $queryScenarios = "SELECT id_cenario, titulo FROM cenario WHERE id_projeto = '**$idProject** ' ORDER BY titulo DESC"; //
coloca_links.phpif($noCurrent) else ,
52: _ function loadscenariosvector($idProject, $idCurrentScenario, $noCurrent)
Userinput is passed through function parameters.
79: _ $vector_scenarios = loadscenariosvector ($idProject, $idCurrentScenario, true);
41: _ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)
requires:
39: if(!(function_exists("gerar_xml")))
Userinput returned by function *import_request_variables()* reaches sensitive sink.
373: _ $str_xml = gerar_xml ($bd_trabalho, $idProject, $data_pesquisa, $flag_formatado);
361: $idProject = **$_SESSION**['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
362: $data_pesquisa = **$data_ano** . "-" . $data_mes . "-" . $data_dia;
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
371: if(!mysql_num_rows($qrrVerifica))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/monta_relacoes.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
SQL Injection
Userinput reaches sensitive sink.
57: **mysql_query** **$tb_nome** = mysql_query($qry_nome) or die ("Erro ao enviar a query de selecao.");
54: $qry_nome = "SELECT nome FROM projeto WHERE id_projeto = " . **$idProject**;
41: _ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)
requires:
39: if(!(function_exists("gerar_xml")))
Userinput returned by function *import_request_variables()* reaches sensitive sink.
373: _ $str_xml = gerar_xml ($bd_trabalho, $idProject, $data_pesquisa, $flag_formatado);
361: $idProject = **$_SESSION**['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

362: $data_pesquisa = **$data_ano** . "-" . $data_mes . "-" . $data_dia;
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
371: if(!mysql_num_rows($qrrVerifica))
SQL Injection
Userinput reaches sensitive sink.
68: mysql_query $tb_cenario = mysql_query($qry_cenario) or die ("Erro ao enviar a query de selecao.");
61: $qry_cenario = "SELECT id_cenario, titulo, objetivo, contexto, atores, recursos, episodios, excecao
FROM cenario WHERE (id_projeto = " . **$idProject** . ")
AND (data <=" . " '" . $data_pesquisa . "'" . ") ORDER BY id_cenario,data DESC";
41: _ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)
41: _ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)
requires:
39: if(!(function_exists("gerar_xml")))
Userinput returned by function *import_request_variables()* reaches sensitive sink.
373: _ $str_xml = gerar_xml ($bd_trabalho, $idProject, $data_pesquisa, $flag_formatado);
361: $idProject = **$_SESSION**['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
362: $data_pesquisa = **$data_ano** . "-" . $data_mes . "-" . $data_dia;
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
371: if(!mysql_num_rows($qrrVerifica))
SQL Injection
Userinput reaches sensitive sink.
130: mysql_query $tb_lexico = mysql_query($qry_lexico) or die ("Erro ao enviar a query de selecao.");
124: $qry_lexico = "SELECT id_lexico, nome, nocao, impacto FROM lexico
WHERE (id_projeto = " . **$idProject** . ") AND (data <=" . " '" . $data_pesquisa . "'" . ")
ORDER BY id_lexico,data DESC";
41: _ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)

41: _ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)
requires:
39: if(!(function_exists("gerar_xml")))
Userinput returned by function *import_request_variables()* reaches sensitive sink.
373: _ $str_xml = gerar_xml ($bd_trabalho, $idProject, $data_pesquisa, $flag_formatado);
361: $idProject = **$_SESSION**['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
362: $data_pesquisa = **$data_ano** . "-" . $data_mes . "-" . $data_dia;
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
371: if(!mysql_num_rows($qrrVerifica))
SQL Injection
Userinput reaches sensitive sink.
150: **mysql_query** **$resultSinonimos** = mysql_query($querySinonimo) or die ("Erro ao enviar a query de selecao de sinonimos.");
145: $querySinonimo = "SELECT nome FROM sinonimo WHERE (id_projeto = " . **$idProject** . ") AND (id_lexico = " . $row[0] . ")";
41: _ function gerar_xml($bd, $idProject, $data_pesquisa, $flag_formatado)
136: $row = mysql_fetch_row($tb_lexico)){
130: $tb_lexico = mysql_query($qry_lexico) or die ("Erro ao enviar a query de selecao."); // , trace stopped
requires:
39: if(!(function_exists("gerar_xml")))
141: if(($id_temp != $id_lexico) or (primeiro))
Userinput returned by function *import_request_variables()* reaches sensitive sink.
373: _ $str_xml = gerar_xml ($bd_trabalho, $idProject, $data_pesquisa, $flag_formatado);
361: $idProject = **$_SESSION**['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
362: $data_pesquisa = **$data_ano** . "-" . $data_mes . "-" . $data_dia;
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc

12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
371: if(!mysql_num_rows($qrrVerifica))
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
368: mysql_query $qrrVerifica = mysql_query($qVerifica);
367: $qVerifica = "SELECT * FROM publicacao WHERE id_projeto = '**$idProject** ' AND versao = '$version' ";
361: $idProject = **$_SESSION**['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink. (Blind exploitation)
380: mysql_query mysql_query(**$commandSQL**) or
377: $commandSQL = "INSERT INTO publicacao (id_projeto, data_publicacao, versao, XML)
VALUES ('**$idProject** ', '$data_pesquisa', '$version', '" . mysql_real_escape_string($xml_resultante) . "')";
361: $idProject = **$_SESSION**['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
362: $data_pesquisa = $data_ano . "-" . $data_mes . "-" . $data_dia;
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
375: $xml_resultante = "<?xml version='1.0' encoding='ISO-8859-1' ?>\n" . $str_xml;
373: $str_xml = gerar_xml ($bd_trabalho, $idProject, $data_pesquisa, $flag_formatado);
365: $bd_trabalho = bd_connect () or die ("Erro ao conectar ao SGBD");
361: $idProject = $_SESSION['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
requires:
371: if(!mysql_num_rows($qrrVerifica))
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/gerarGrafo.php
Possible Flow Control

Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
31: **mysql_query** **$requestResultSQL** = mysql_query($commandSQL) or die ("Erro ao enviar a query");
30: $commandSQL = "SELECT * FROM publicacao WHERE id_projeto = '**$idProject** '";
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/heading.php
SQL Injection
Userinput reaches sensitive sink.
2118: **mysql_query** **$qr** = mysql_query($commandSQL) or die ("Erro ao enviar a query de select no participa
" . mysql_error() . "<br>" . __FILE__ . __LINE__);
funcoes_genericas.php

2117: $commandSQL = "SELECT * FROM participa WHERE gerente = 1 AND id_usuario = **$id_usuario** AND id_projeto = $idProject "; // funcoes_genericas.php
2115: _ function verificagerente($id_usuario, $idProject)
2115: _ function verificagerente($id_usuario, $idProject)
Userinput is passed through function parameters.
204: _ $returnCheck = verificagerente ($id_user, $idProject);
203: $id_user = $_SESSION['id_usuario_corrente'];
25: $idProject = **$_GET**['id_projeto']; // if(isset($_GET)),
requires:
201: if(isset($idProject))
Userinput is passed through function parameters.
328: _ $returnCheck = verificagerente ($id_user, $idProject);
327: $id_user = $_SESSION['id_usuario_corrente'];
25: $idProject = **$_GET**['id_projeto']; // if(isset($_GET)),
requires:
325: if(isset($idProject))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/index.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/httprequest.inc
Possible Flow Control

Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor;
6: $a = **$chave**;
5: list($chave, **$valor**) = each($_GET)){ // list()
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor;
13: $a = **$chave**;
12: list($chave, **$valor**) = each($_POST)){ // list()
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/login.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/main.php
SQL Injection
Userinput reaches sensitive sink.
2079: **mysql_query** **$requestResultSQL** = mysql_query($commandSQL) or die ("Erro ao enviar a query
" . mysql_error() . "<br>" . __FILE__ . __LINE__); // funcoes_genericas.php
2074: $commandSQL = "SELECT * FROM participa WHERE id_usuario = **$id_usuario** AND id_projeto = $idProject AND gerente = 1"; // funcoes_genericas.php
2072: _ function is_admin($id_usuario, $idProject)
2072: _ function is_admin($id_usuario, $idProject)
requires:
2070: if(!(function_exists("is_admin")))
Userinput returned by function *import_request_variables()* reaches sensitive sink.

917: _ is_admin ($_SESSION['id_usuario_corrente'], $idProject))
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
688: $idProject = **$_SESSION**['id_projeto_corrente']; // if(isset($id) && isset($term)), if($term == "1"),
33: $_SESSION['id_projeto_corrente'] = ""; // if(!isset($_SESSION)),
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
861: if(isset($idProject))
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/projetos.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto_base.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php

Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()

Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()

SQL Injection
Userinput reaches sensitive sink.
24: **mysql_query** **$tbScenario** = mysql_query($queryScenario) or die ("Erro ao enviar a query de selecao."); // frame_inferior.php
19: $queryScenario = "SELECT id_cenario, titulo FROM cenario, centocen WHERE id_cenario = id_cenario_from AND id_cenario_to = " . **$id**; // frame_inferior.php
11: _function bottom_frame($bd, $type, $id)
requires:
17: if($type == "c")
Userinput returned by function *import_request_variables()* reaches sensitive sink.
859: _bottom_frame ($SgbdConnect, $term, $id);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
507: if(isset($id) && isset($term))

SQL Injection
Userinput reaches sensitive sink.
55: **mysql_query** **$tbScenario** = mysql_query($queryScenario) or die ("Erro ao enviar a query de selecao."); // frame_inferior.php
50: $queryScenario = "SELECT c.id_cenario, c.titulo FROM cenario c, centolex cl WHERE c.id_cenario = cl.id_cenario AND cl.id_lexico = " . **$id**; // frame_inferior.php
11: _function bottom_frame($bd, $type, $id)
requires:
48: if($type == "l")
Userinput returned by function *import_request_variables()* reaches sensitive sink.
859: _bottom_frame ($SgbdConnect, $term, $id);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
507: if(isset($id) && isset($term))

SQL Injection
Userinput reaches sensitive sink.
64: **mysql_query** **$tbLexicon** = mysql_query($queryLexicon) or die ("Erro ao enviar a query de selecao."); // frame_inferior.php
59: $queryLexicon = "SELECT id_lexico, nome FROM lexico, lextolex WHERE id_lexico = id_lexico_from AND id_lexico_to = " . **$id**; // frame_inferior.php
11: _function bottom_frame($bd, $type, $id)

requires:
48: if($type == "l")
Userinput returned by function *import_request_variables()* reaches sensitive sink.
859: _bottom_frame ($SgbdConnect, $term, $id);

14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
507: if(isset($id) && isset($term))
SQL Injection
Userinput reaches sensitive sink.
129: **mysql_query $result** = mysql_query($commandSQL) or die ("Erro ao enviar a query de selecao !!" . mysql_error()); // frame_inferior.php
122: $commandSQL = "SELECT r.id_relacao, r.nome, predicado FROM conceito c, relacao_conceito rc, relacao r
WHERE c.id_conceito = **$id** AND c.id_conceito = rc.id_conceito
AND r.id_relacao = rc.id_relacao ORDER BY r.nome "; // frame_inferior.php
11: _function bottom_frame($bd, $type, $id)
requires:
120: if($type == "oc")
Userinput returned by function *import_request_variables()* reaches sensitive sink.
859: _bottom_frame ($SgbdConnect, $term, $id);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
507: if(isset($id) && isset($term))
SQL Injection
Userinput reaches sensitive sink.
147: **mysql_query $result** = mysql_query($commandSQL) or die ("Erro ao enviar a query de selecao !!" . mysql_error()); // frame_inferior.php
140: $commandSQL = "SELECT DISTINCT c.id_conceito, c.nome FROM conceito c, relacao_conceito rc, relacao r
WHERE r.id_relacao = **$id** AND c.id_conceito = rc.id_conceito
AND r.id_relacao = rc.id_relacao ORDER BY r.nome "; // frame_inferior.php
11: _function bottom_frame($bd, $type, $id)
requires:
138: if($type == "or")
Userinput returned by function *import_request_variables()* reaches sensitive sink.
859: _bottom_frame ($SgbdConnect, $term, $id);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
507: if(isset($id) && isset($term))
SQL Injection
Userinput reaches sensitive sink.
162: **mysql_query $result** = mysql_query($commandSQL) or die ("Erro ao enviar a query de selecao !!" . mysql_error()); // frame_inferior.php
158: $commandSQL = "SELECT * FROM axioma WHERE id_axioma = \"**$id**\";"; // frame_inferior.php
11: _function bottom_frame($bd, $type, $id)
requires:
156: if($type == "oa")
Userinput returned by function *import_request_variables()* reaches sensitive sink.
859: _bottom_frame ($SgbdConnect, $term, $id);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
507: if(isset($id) && isset($term))
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
550: **mysql_query $requestResultSQL** = mysql_query($commandSQL) or die ("Erro ao enviar a query de selecao !!" . mysql_error());

545: `$commandSQL = "SELECT id_cenario, titulo, objetivo, contexto, atores, recursos, excecao, episodios, id_projeto FROM cenario WHERE id_cenario = $id";`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
507: `if(isset($id) && isset($term))`
543: `if($term == "c")`
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
651: `mysql_query $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de selecao !!" . mysql_error());`

647: `$commandSQL = "SELECT id_lexico, nome, nocao, impacto, tipo, id_projeto FROM lexico WHERE id_lexico = $id";`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
507: `if(isset($id) && isset($term))`
645: `if($term == "l")`
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
692: `mysql_query $requestResultSQL = mysql_query($querySynonym) or die ("Erro ao enviar a query de Sinonimos" . mysql_error());`
690: `$querySynonym = "SELECT * FROM sinonimo WHERE id_lexico = $id";`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
507: `if(isset($id) && isset($term))`
645: `if($term == "l")`
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
758: `mysql_query $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de selecao !!" . mysql_error());`
754: `$commandSQL = "SELECT id_conceito, nome, descricao FROM conceito WHERE id_conceito = $id";`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
507: `if(isset($id) && isset($term))`
752: `if($term == "oc")`
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
796: `mysql_query $requestResultSQL = mysql_query($commandSQL) or die ("Erro ao enviar a query de selecao !!" . mysql_error());`
792: `$commandSQL = "SELECT id_relacao, nome FROM relacao WHERE id_relacao = $id";`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
507: `if(isset($id) && isset($term))`
790: `elseif($term == "or")`

hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostrarProjeto.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
21: **mysql_query** **$requestResultSQL** = mysql_query($queryResult) or die ("Erro ao enviar a query");
19: $queryResult = "SELECT * FROM publicacao WHERE id_projeto = **$idProject** AND versao = $version";
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/mostraXML.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()

Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
26: **mysql_query** **$requestResultSQL** = mysql_query($queryResult) or die ("Erro ao enviar a query");
24: $queryResult = "SELECT * FROM publicacao WHERE id_projeto = **$idProject** AND versao = $version";
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/recuperarXML.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()

Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
42: **mysql_query** **$requestResultSQLDelete** = mysql_query($queryDelete);
41: $queryDelete = "DELETE FROM publicacao WHERE id_projeto = '**$idProject** ' AND versao = '$version' ";
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
38: if(isset($delete))
40: if($delete)
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
53: **mysql_query** **$requestResultSQL** = mysql_query($commandSQL) or die ("Erro ao enviar a query");
52: $commandSQL = "SELECT * FROM publicacao WHERE id_projeto = '**$idProject** '";
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/rel_usuario.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink. (Blind exploitation)
19: **mysql_query** mysql_query(**$commandSQL**) or
15: $commandSQL = "DELETE FROM participa WHERE id_usuario != " . **$_SESSION**['id_usuario_corrente'] . "
AND id_projeto = " . $_SESSION['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()

12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
requires:
13: if(isset($submit))

SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink. (Blind exploitation)
28: **mysql_query** `mysql_query(`**$commandSQL**`) or`
25: `$commandSQL = "INSERT INTO participa (id_usuario, id_projeto) VALUES (" .` **$users**`[$i] . ", " . $_SESSION['id_projeto_corrente'] . ")";`
14: `$$a =` **$valor**`; // is like import_request_variables() // httprequest.incsee above`
13: `$a =` **$chave**`; // httprequest.inc`
12: `list($chave,` **$valor**`) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a =` **$valor**`; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
13: `if(isset($submit))`
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
133: **mysql_query** **$requestResultSQL** `= mysql_query($commandSQL) or die ("Erro ao enviar a query");`
127: `$commandSQL = "SELECT u.id_usuario, login FROM usuario u, participa p WHERE u.id_usuario = p.id_usuario AND p.id_projeto = " .` **$_SESSION**`['id_projeto_corrente'] . " AND u.id_usuario != " . $_SESSION['id_usuario_corrente'];`
14: `$$a =` **$valor**`; // is like import_request_variables() // httprequest.incsee above`
13: `$a =` **$chave**`; // httprequest.inc`
12: `list($chave,` **$valor**`) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
14: `$$a =` **$valor**`; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
43: `if(isset($submit)) else`
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
158: **mysql_query** **$subRequestResultSQL** `= mysql_query($subQuery) or die ("Erro ao enviar a subquery");`
157: `$subQuery = "SELECT id_usuario FROM participa WHERE participa.id_projeto =" .` **$_SESSION**`['id_projeto_corrente'];`
14: `$$a =` **$valor**`; // is like import_request_variables() // httprequest.incsee above`
13: `$a =` **$chave**`; // httprequest.inc`
12: `list($chave,` **$valor**`) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
requires:
43: `if(isset($submit)) else`
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
180: **mysql_query** **$requestResultSQL** `= mysql_query($commandSQL) or die ("Erro ao enviar a query");`
175: `$commandSQL = "SELECT usuario.id_usuario, usuario.login FROM usuario where usuario.id_usuario not in " .` **$resultSubQuery**`;`
169: `$resultSubQuery = "`**$resultSubQuery** `)"; // if($subRequestResultSQL != 0),`
168: `$resultSubQuery = "`**$resultSubQuery** `, $row[0]"; // if($subRequestResultSQL != 0),`
164: `$resultSubQuery = "(` **$row**`[0]"; // if($subRequestResultSQL != 0),`
163: `$row = mysql_fetch_row($subRequestResultSQL); // if($subRequestResultSQL != 0),`
158: `$subRequestResultSQL = mysql_query($subQuery) or die ("Erro ao enviar a subquery"); // , trace stopped`
14: `$$a =` **$valor**`; // is like import_request_variables() // httprequest.incsee above`
13: `$a =` **$chave**`; // httprequest.inc`
12: `list($chave,` **$valor**`) = each($_POST)){ // httprequest.inc list()`

12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
166: `$row = mysql_fetch_row($subRequestResultSQL)){ // if($subRequestResultSQL != 0),`
158: `$subRequestResultSQL = mysql_query($subQuery) or die ("Erro ao enviar a subquery"); // , trace stopped`
requires:
43: `if(isset($submit)) else`
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/remove_projeto.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink.
39: **mysql_query** **$qvr** = mysql_query($qv) or die ("Erro ao enviar a query de select no projeto");
38: $qv = "SELECT * FROM projeto WHERE id_projeto = '**$idProject** ' ";
33: $idProject = **$_SESSION**['id_projeto_corrente'];
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above

13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_cenario.php
SQL Injection
Userinput reaches sensitive sink.
1412: **mysql_query** **$qr** = mysql_query($commandSQL) or die ("Erro ao enviar a query de select no participa
" . mysql_error() . "<br>" . __FILE__ . __LINE__);
funcoes_genericas.php
1411: $commandSQL = ("SELECT * FROM participa WHERE gerente = 1 AND id_usuario = **$id_usuario** AND id_projeto = $idProject "); // funcoes_genericas.php
1405: _ function inserirpedidoremovercenario($idProject, $id_cenario, $id_usuario)
1405: _ function inserirpedidoremovercenario($idProject, $id_cenario, $id_usuario)
requires:
1403: `if(!(function_exists("inserirPedidoRemoverCenario")))`
Userinput returned by function *import_request_variables()* reaches sensitive sink.
27: _ inserirpedidoremovercenario ($_SESSION['id_projeto_corrente'], $id_cenario, $_SESSION['id_usuario_corrente']);
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php

C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: `$a $$a = $valor; // httprequest.inc`
6: `$a = $chave; // httprequest.inc`
5: `list($chave, $valor) = each($_GET)){ // httprequest.inc list()`
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: `$a $$a = $valor; // httprequest.inc`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_conceito.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: `$a $$a = $valor; // httprequest.inc`
6: `$a = $chave; // httprequest.inc`
5: `list($chave, $valor) = each($_GET)){ // httprequest.inc list()`
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: `$a $$a = $valor; // httprequest.inc`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_lexico.php
SQL Injection
Userinput reaches sensitive sink.
1600: `mysql_query $qr = mysql_query($commandSQL) or die ("Erro ao enviar a query de select no participa<br>" . mysql_error() . "<br>" . __FILE__ . __LINE__);`
funcoes_genericas.php
1599: `$commandSQL = "SELECT * FROM participa WHERE gerente = 1 AND id_usuario = $id_usuario AND id_projeto = $idProject "; // funcoes_genericas.php`
1593: `_ function inserirpedidoremoverlexico($idProject, $id_lexico, $id_usuario)`
1593: `_ function inserirpedidoremoverlexico($idProject, $id_lexico, $id_usuario)`
requires:
1591: `if(!(function_exists("inserirPedidoRemoverLexico")))`
Userinput returned by function *import_request_variables()* reaches sensitive sink.
26: `_ inserirpedidoremoverlexico ($id_project, $id_lexicon, $_SESSION['id_usuario_corrente']);`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`

14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
Vulnerability is also triggered in:
C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: `$a $$a = $valor; // httprequest.inc`
6: `$a = $chave; // httprequest.inc`
5: `list($chave, $valor) = each($_GET)){ // httprequest.inc list()`

Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/rmv_relacao.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/showSource.php
File Disclosure
Userinput reaches sensitive sink. (Blind exploitation)
6: **show_source** show_source(**$file**);
3: $file = **$_GET**['file'];
requires:
4: if(isset($_GET['file']))
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/updUser.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: **$a** $**$a** = $valor; // httprequest.inc
6: $a = **$chave**; // httprequest.inc
5: list($chave, **$valor**) = each($_GET)){ // httprequest.inc list()
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: **$a** $**$a** = $valor; // httprequest.inc
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
SQL Injection
Userinput returned by function *import_request_variables()* reaches sensitive sink. (Blind exploitation)
36: **mysql_query** mysql_query(**$query_user**) or
34: $query_user = "UPDATE usuario SET nome ='**$name**' , login = '$login' , email = '$email' , senha = '$criptPassword' WHERE id_usuario='$id_user'";
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = **$chave**; // httprequest.inc
12: list($chave, **$valor**) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
14: $$a = **$valor**; // is like import_request_variables() // httprequest.incsee above
13: $a = $chave; // httprequest.inc
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
12: list($chave, $valor) = each($_POST)){ // httprequest.inc list()
33: $criptPassword = md5($password);
14: $$a = $valor; // is like import_request_variables() // httprequest.incsee above

13: $a = $chave; // httprequest.inc

12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
8: `$id_user = $_SESSION['id_usuario_corrente'];`
14: `$$a = $valor; // is like import_request_variables() // httprequest.incsee above`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_cenario.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: `$a $$a = $valor; // httprequest.inc`
6: `$a = $chave; // httprequest.inc`
5: `list($chave, $valor) = each($_GET)){ // httprequest.inc list()`
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: `$a $$a = $valor; // httprequest.inc`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_conceito.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: `$a $$a = $valor; // httprequest.inc`
6: `$a = $chave; // httprequest.inc`
5: `list($chave, $valor) = each($_GET)){ // httprequest.inc list()`
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: `$a $$a = $valor; // httprequest.inc`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_lexico.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: `$a $$a = $valor; // httprequest.inc`
6: `$a = $chave; // httprequest.inc`
5: `list($chave, $valor) = each($_GET)){ // httprequest.inc list()`
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: `$a $$a = $valor; // httprequest.inc`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
hide all
File: C:\xampp-portable\htdocs\C-L\cel\aplicacao/ver_pedido_relacao.php
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
7: `$a $$a = $valor; // httprequest.inc`
6: `$a = $chave; // httprequest.inc`
5: `list($chave, $valor) = each($_GET)){ // httprequest.inc list()`
Possible Flow Control
Userinput is used to build the variable name. Arbitrary variables may be overwritten/initialized which may lead to further vulnerabilities.
14: `$a $$a = $valor; // httprequest.inc`
13: `$a = $chave; // httprequest.inc`
12: `list($chave, $valor) = each($_POST)){ // httprequest.inc list()`
hide all

Pela análise, verificamos em demasiado problemas com sql injection sendo que de certa forma as entradas do usuário atinge de forma sensível a renovação, a entrada de usuários é passada através de parâmetros da função em vários arquivos. As entradas de usuário são retornadas por funções que atinge de forma sensível a renovação.

Verificamos também problemas com o arquivo httprequest.inc que afeta vários outros arquivos pelo modo que ele passa as variáveis dentro das funções.

Cocluíndo, necessitamos resolver esses problemas para acabar ou pelo menos diminuir essas vulnerabilidades.