SQLi Scan Report

Generated: 2025-08-28 19:15:14

Findings: 24

Technique	Risk	URL	Param	Evidence
error-based	High	http://localhost:8000/cart.php	product_id	SQLSTATE\[[A-Z0-9]+\]
error-based	High	http://localhost:8000/view_upload.php	id	SQLSTATE\[[A-Z0-9]+\]
error-based	High	http://localhost:8000/admin.php	user_id	SQLSTATE\[[A-Z0-9]+\]
error-based	High	http://localhost:8000/products.php	q	SQLSTATE\[[A-Z0-9]+\]
error-based	High	http://localhost:8000/search.php	q	SQLSTATE\[[A-Z0-9]+\]
error-based	High	http://localhost:8000/index.php	q	SQLSTATE\[[A-Z0-9]+\]
error-based	High	http://localhost:8000/index.php	user_id	SQLSTATE\[[A-Z0-9]+\]
error-based	High	http://localhost:8000/admin.php	comment_id	SQLSTATE\[[A-Z0-9]+\]
error-based	High	http://localhost:8000/login.php	username	SQLSTATE\[[A-Z0-9]+\]
error-based	High	http://localhost:8000/login.php	password	SQLSTATE\[[A-Z0-9]+\]
error-based	High	http://localhost:8000/cart.php	note	SQLSTATE\[[A-Z0-9]+\]
error-based	High	http://localhost:8000/index.php	comment	SQLSTATE\[[A-Z0-9]+\]
boolean-blind	Medium	http://localhost:8000/view_upload.php	id	rounds=3 diffs=3 sim_avg=0.015
error-based	High	http://localhost:8000/index.php	add_comment	SQLSTATE\[[A-Z0-9]+\]
boolean-blind	Medium	http://localhost:8000/products.php	q	rounds=3 diffs=3 sim_avg=0.522
union-confirmed	Critical	http://localhost:8000/cart.php	product_id	columns=1
union-confirmed	Critical	http://localhost:8000/view_upload.php	id	columns=3
union-confirmed	Critical	http://localhost:8000/products.php	q	columns=5
union-confirmed	Critical	http://localhost:8000/search.php	q	columns=3
union-confirmed	Critical	http://localhost:8000/index.php	q	columns=3
union-confirmed	Critical	http://localhost:8000/cart.php	note	columns=1
union-confirmed	Critical	http://localhost:8000/login.php	username	columns=3
union-confirmed	Critical	http://localhost:8000/login.php	password	columns=3
union-confirmed	Critical	http://localhost:8000/index.php	comment	columns=1

Sample secure query snippet (example):

```
// PHP PDO example $stmt = $pdo->prepare('SELECT * FROM table WHERE product_id = ?');
$stmt->execute([$value]); $row = $stmt->fetch();
```