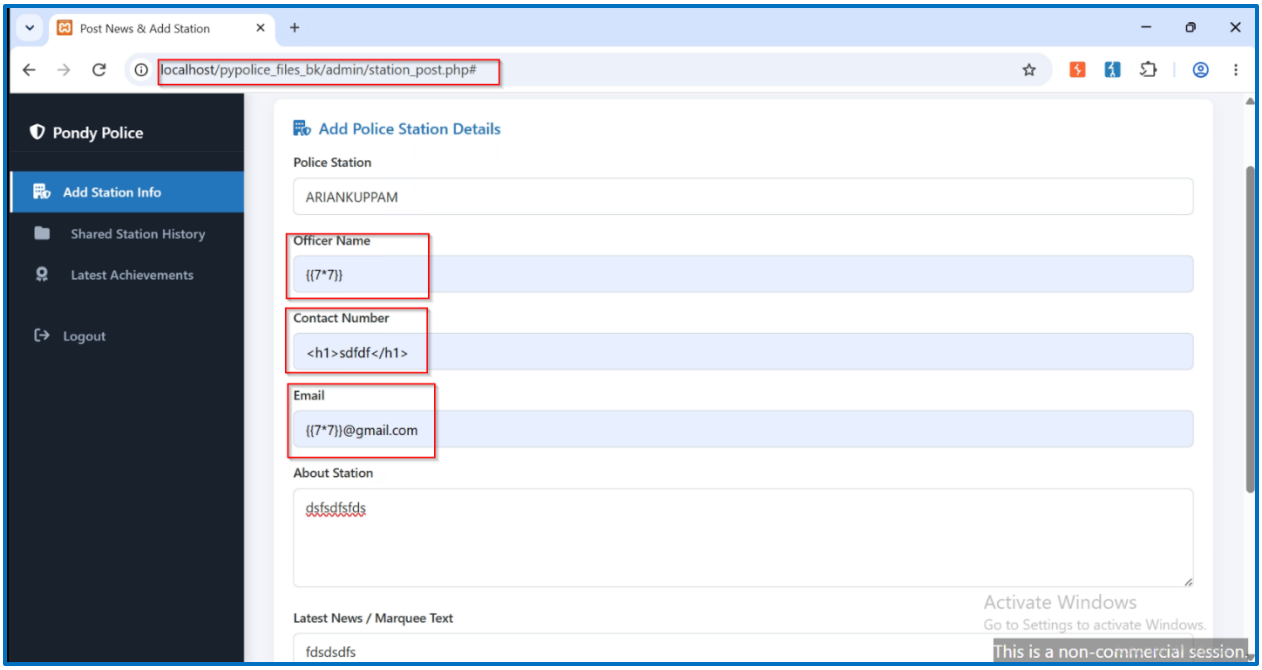
5.4 Improper Input Validation

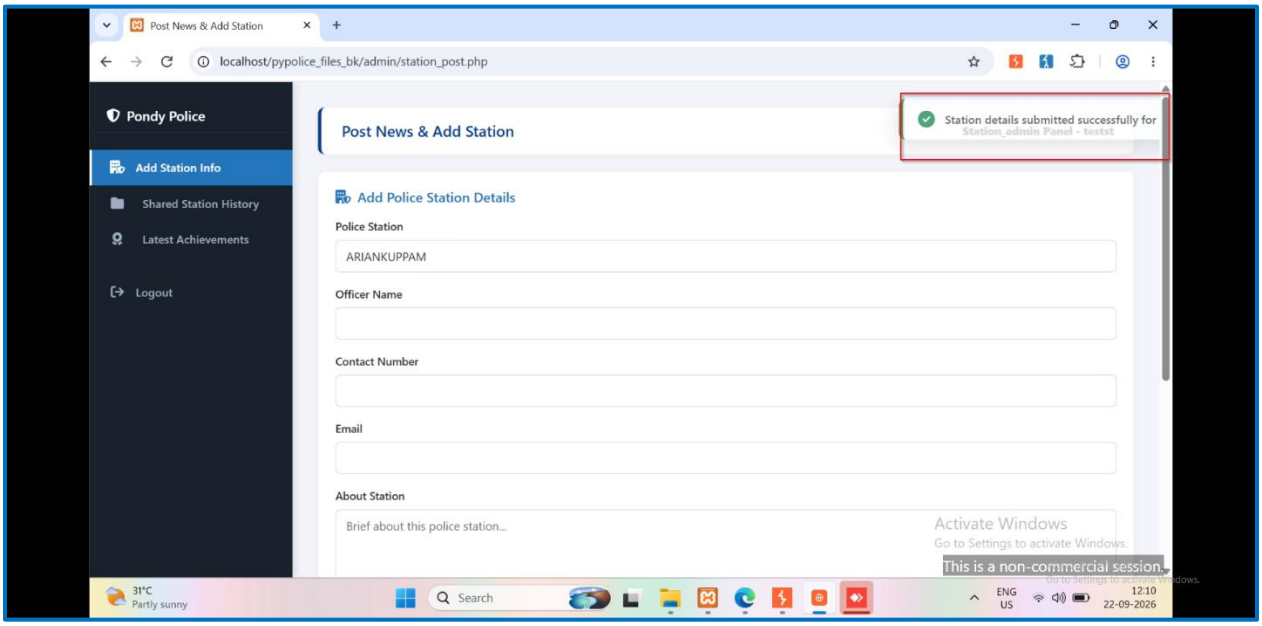
Threat Description: Low

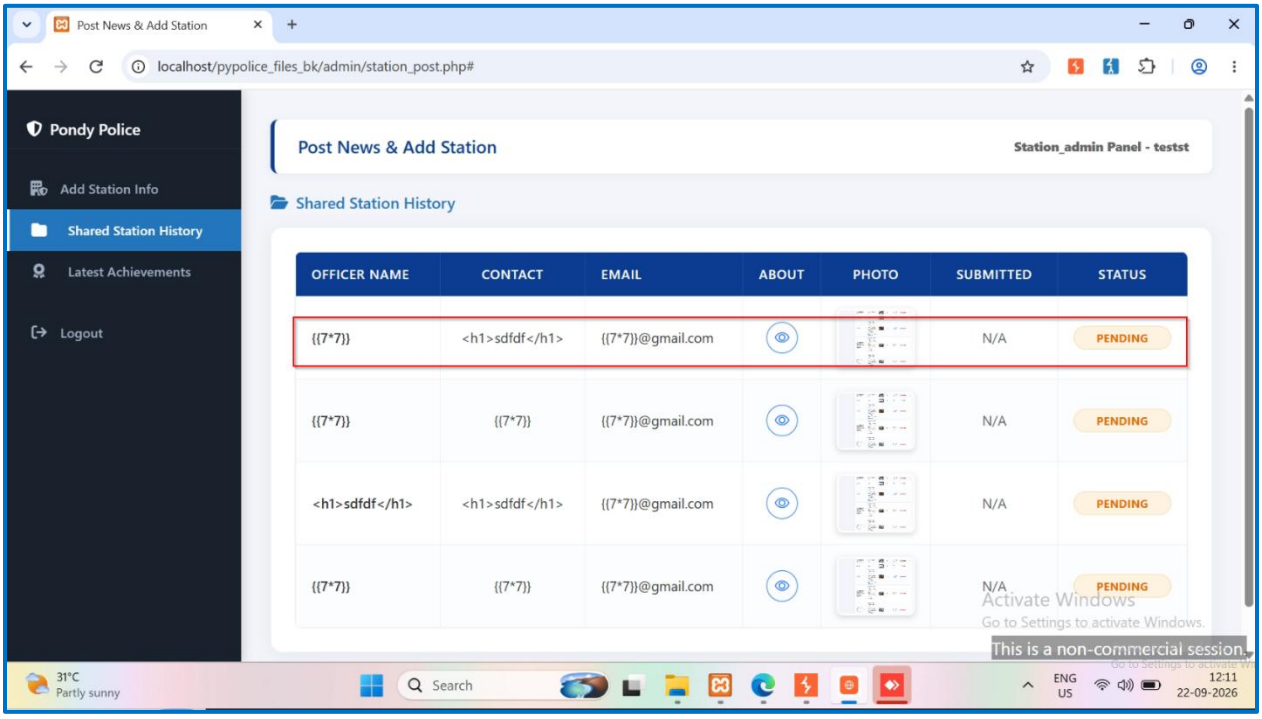
Improper Input Validation occurs when an application fails to adequately validate, sanitize, normalize, or constrain data received from users before processing it. Input validation ensures that application components receive data that conforms to the expected format, type, length, and business rules. Weak validation may allow unexpected, malformed, or unauthorized values to be accepted by application functionality. This weakness commonly results from relying on client-side validation, insufficient server-side validation, or failure to enforce application-specific business rules. Effective validation requires all untrusted input to be validated server-side according to the expected data type and contextual requirements.

Methodology:

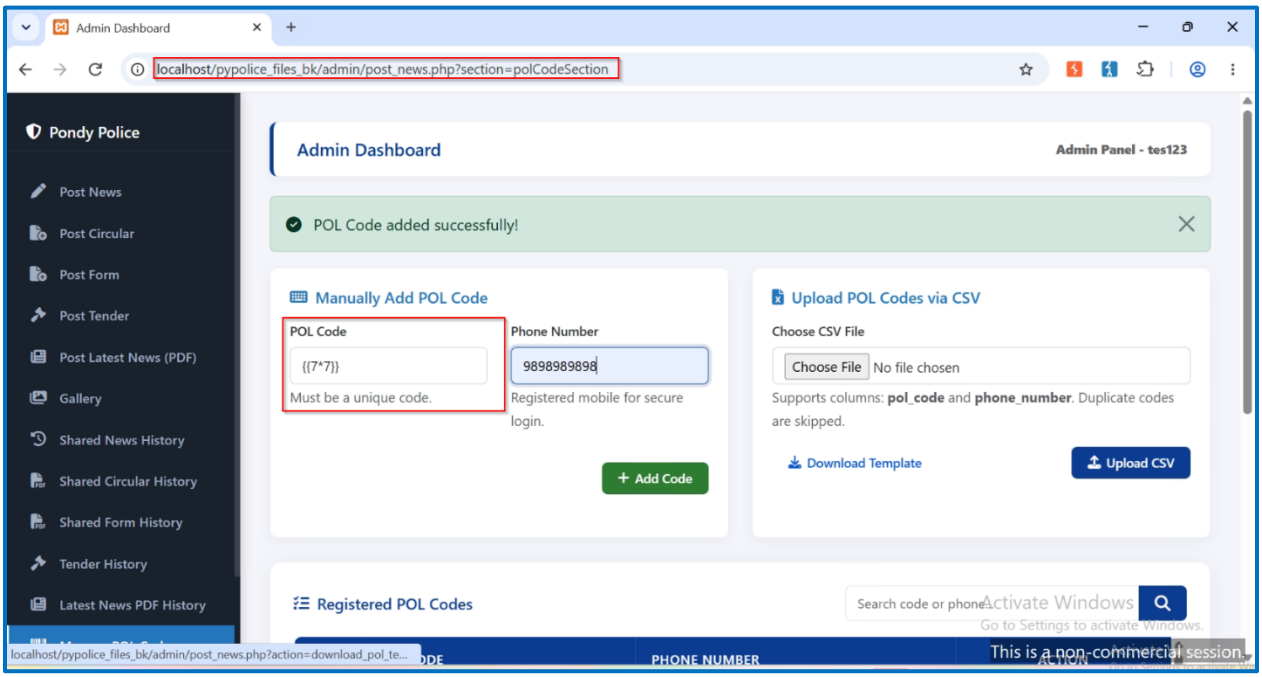
During the assessment, we observed that the web application is vulnerable to Improper Input Validation.

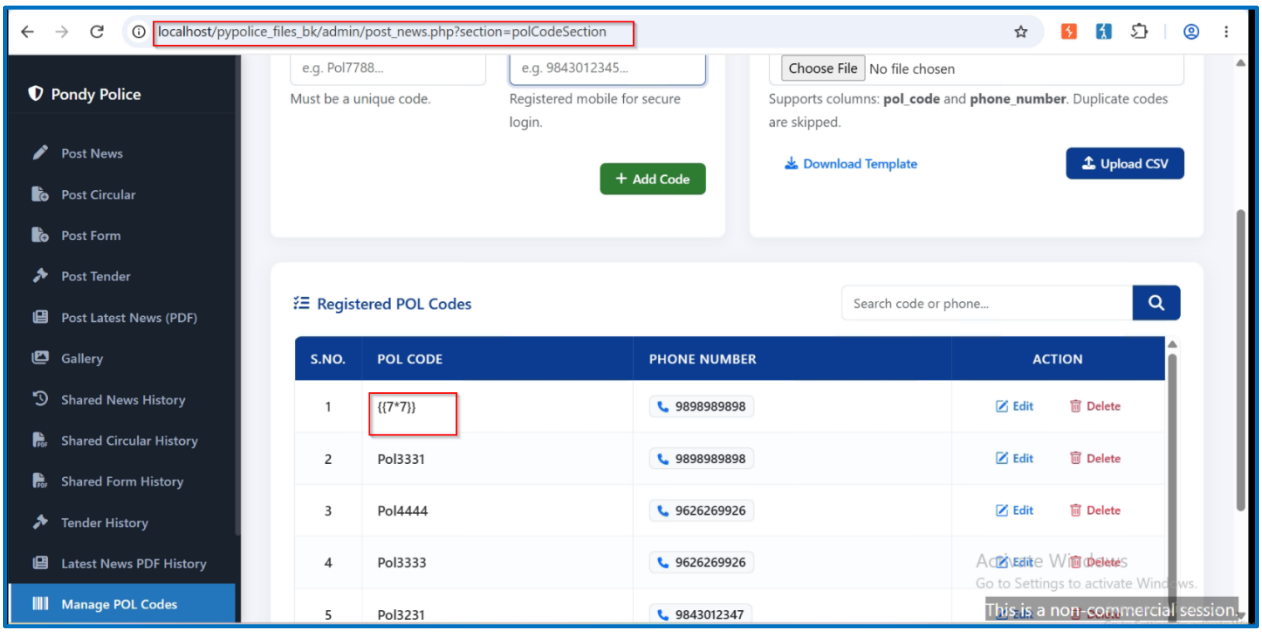



Post News & Add Station
localhost/pypolice_files_bk/admin/station_post.php
Pondy Police
Add Station Info
Shared Station History
Latest Achievements
Logout
Post News & Add Station
Station details submitted successfully for
Station_admin Panel - testst
Add Police Station Details
Police Station
ARIANKUPPAM
Officer Name
Contact Number
Email
About Station
Brief about this police station...
Activate Windows
Go to Settings to activate Windows.
This is a non-commercial session.
31°C
Partly sunny
Search
ENG
US
12:10
22-09-2026


Post News & Add Station
localhost/pypolice_files_bk/admin/station_post.php#
Pondy Police
Add Station Info
Shared Station History
Latest Achievements
Logout
Post News & Add Station
Station_admin Panel - testst
Shared Station History
OFFICER NAME
CONTACT
EMAIL
ABOUT
PHOTO
SUBMITTED
STATUS
{{7*7}}
<h1>sdfdf</h1>
{{7*7}}@gmail.com
N/A
PENDING
{{7*7}}
{{7*7}}
{{7*7}}@gmail.com
N/A
PENDING
<h1>sdfdf</h1>
<h1>sdfdf</h1>
{{7*7}}@gmail.com
N/A
PENDING
{{7*7}}
{{7*7}}
{{7*7}}@gmail.com
N/A
PENDING
Activate Windows
Go to Settings to activate Windows.
This is a non-commercial session.
31°C
Partly sunny
Search
ENG
US
12:11
22-09-2026

Scenario 2:


Admin Dashboard
localhost/pypolice_files_bk/admin/post_news.php?section=polCodeSection
Pondy Police
Post News
Post Circular
Post Form
Post Tender
Post Latest News (PDF)
Gallery
Shared News History
Shared Circular History
Shared Form History
Tender History
Latest News PDF History
Admin Dashboard
Admin Panel - tes123
POL Code added successfully!
Manually Add POL Code
POL Code
{{7*7}}
Must be a unique code.
Phone Number
9898989898
Registered mobile for secure login.
+ Add Code
Upload POL Codes via CSV
Choose CSV File
Choose File
No file chosen
Supports columns: pol_code and phone_number. Duplicate codes are skipped.
Download Template
Upload CSV
Registered POL Codes
Search code or phone...
PHONE NUMBER
ACTION
This is a non-commercial session.


localhost/pypolice_files_bk/admin/post_news.php?section=polCodeSection
Pondy Police
Post News
Post Circular
Post Form
Post Tender
Post Latest News (PDF)
Gallery
Shared News History
Shared Circular History
Shared Form History
Tender History
Latest News PDF History
Manage POL Codes
e.g. Pol7788...
Must be a unique code.
e.g. 9843012345...
Registered mobile for secure login.
+ Add Code
Choose File
No file chosen
Supports columns: pol_code and phone_number. Duplicate codes are skipped.
Download Template
Upload CSV
Registered POL Codes
Search code or phone...
S.NO.
POL CODE
PHONE NUMBER
ACTION
1
{{7*7}}
9898989898
Edit
Delete
2
Pol3331
9898989898
3
Pol4444
9626269926
4
Pol3333
9626269926
5
Pol3231
9843012347
This is a non-commercial session.

Impact:

- **Data Integrity Compromise:** Fields with a defined expected format (e.g., police code, email, phone number) accept arbitrary or malformed values, including special characters, leading to corrupt or inconsistent data being stored and processed by the application.
- **Injection Attack Surface:** Unrestricted acceptance of special characters in input fields increases the risk of downstream injection attacks (e.g., SQL Injection, Cross-Site Scripting, CSV/Formula Injection) if the unvalidated data is later used in queries, rendered in the UI, or exported without proper handling.
- **Security Misconfiguration Risk:** The absence of consistent, centralized input validation across form fields indicates a broader weakness in input handling standards, increasing the likelihood that this issue can be chained with other vulnerabilities in the application.

Affected Hosts:

HOST	PROOF
http://localhost/pypolice_files_bk/admin/post_news.php http://localhost/pypolice_files_bk/station_post.php	Available

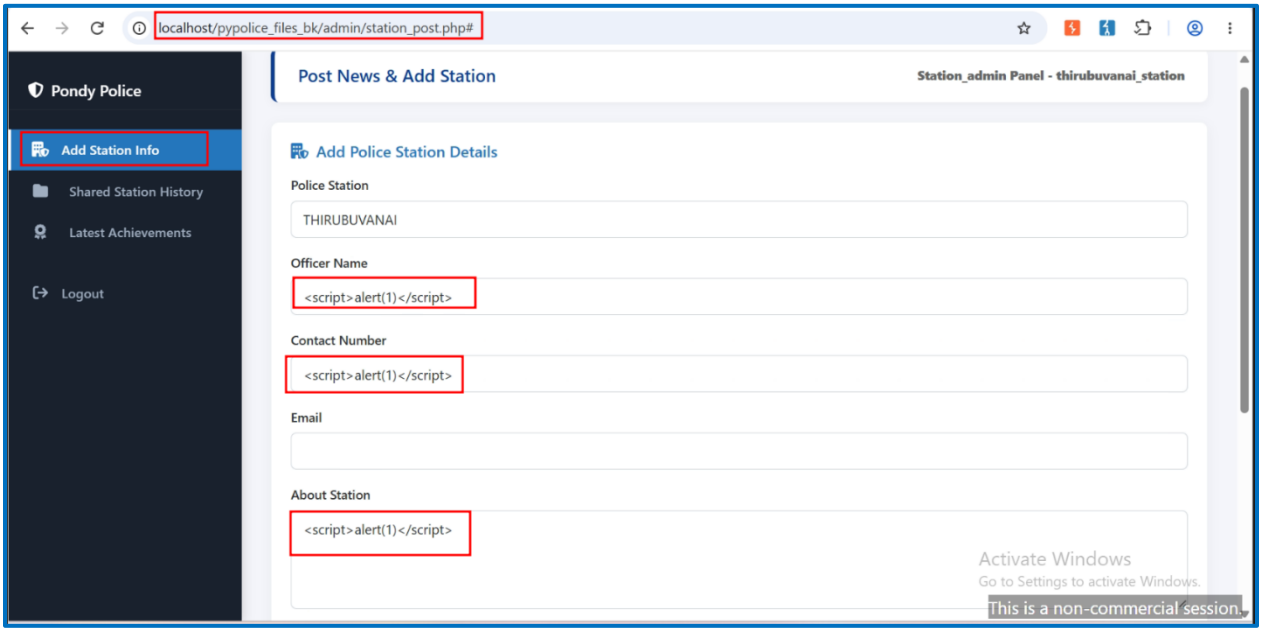
Recommendation:

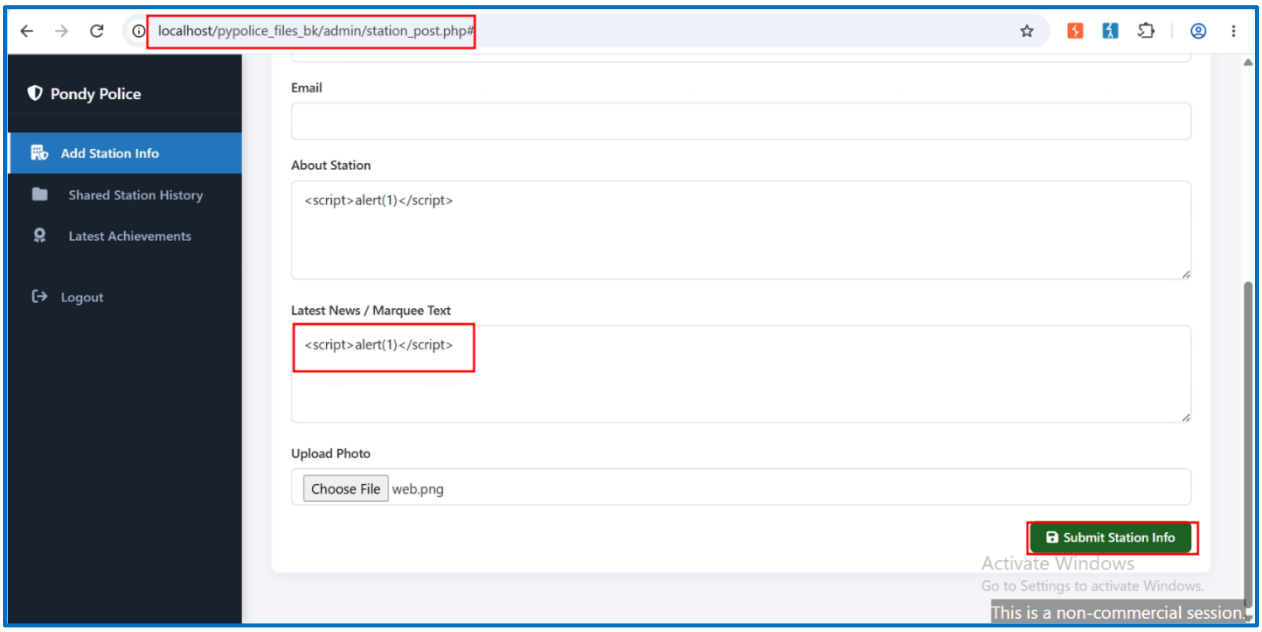
- **Enforce Server-Side Input Validation:** Implement strict, allow-list-based validation for all structured input fields; do not rely solely on client-side (JavaScript) validation.
- **Sanitize Data**: Any data input that might be used in queries or commands should be sanitized to remove potentially dangerous characters or code (e.g., special characters in SQL queries).
- **Use Whitelisting Over Blacklisting**: Instead of only filtering known malicious inputs (blacklisting), use whitelisting to define exactly what valid inputs should look like, allowing only expected values.

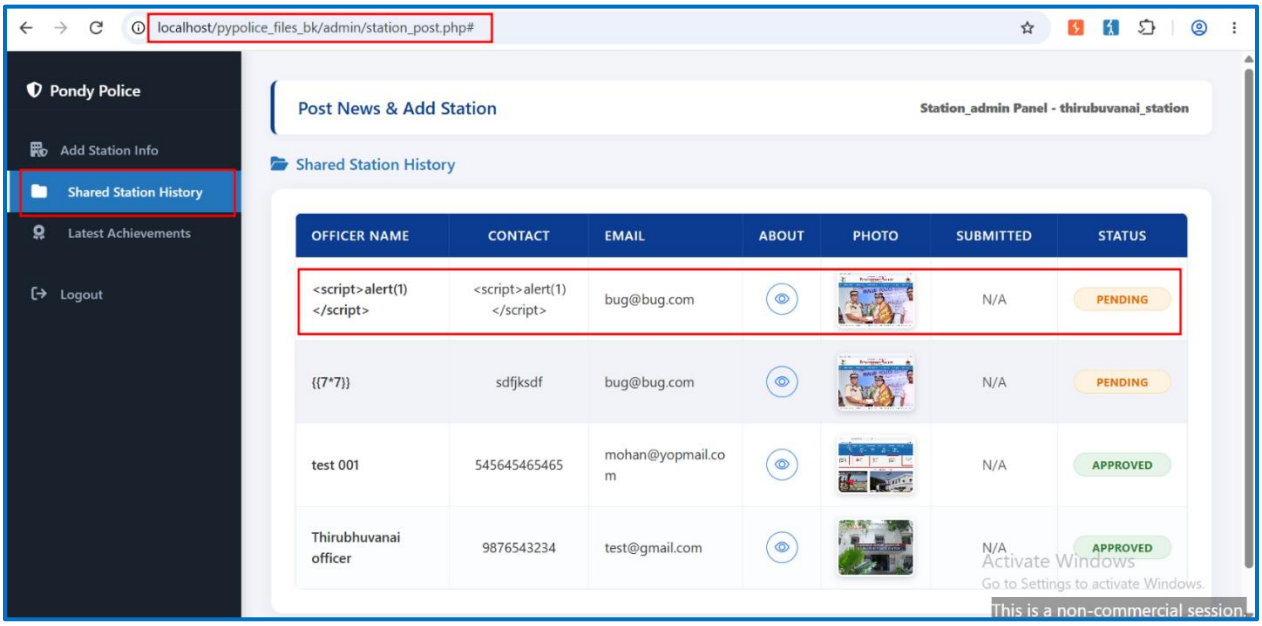
Retest Observation: Open

During the reassessment, we observe that application is vulnerable to Improper Input Validation.

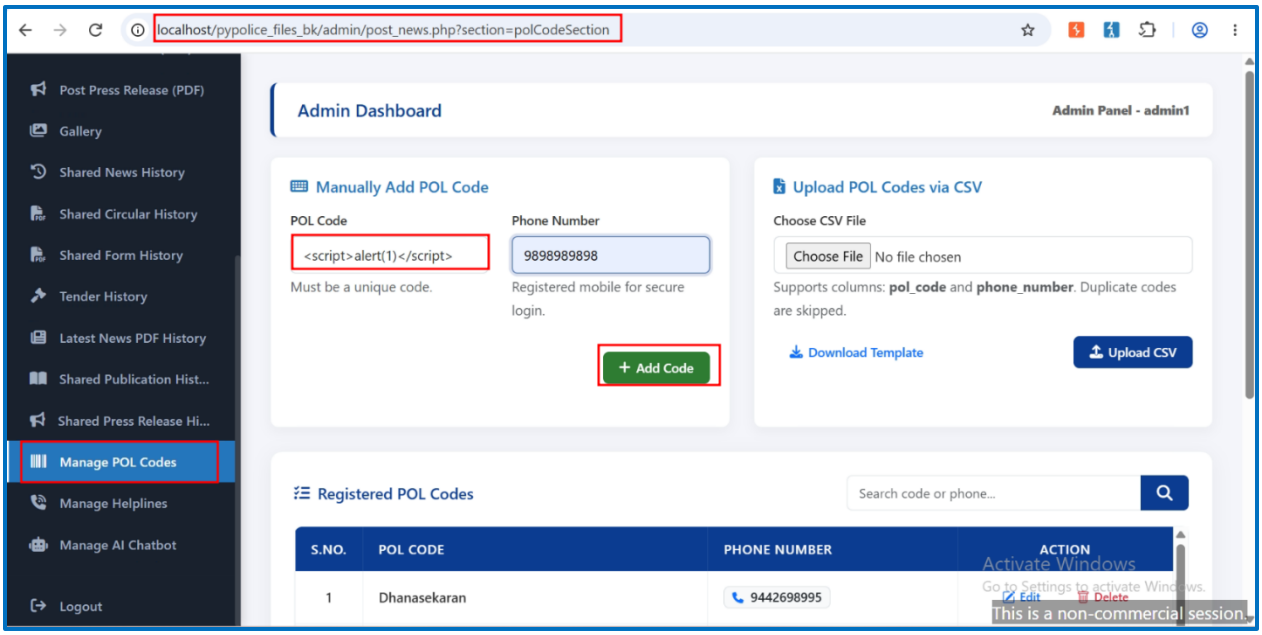
Scenario 1:

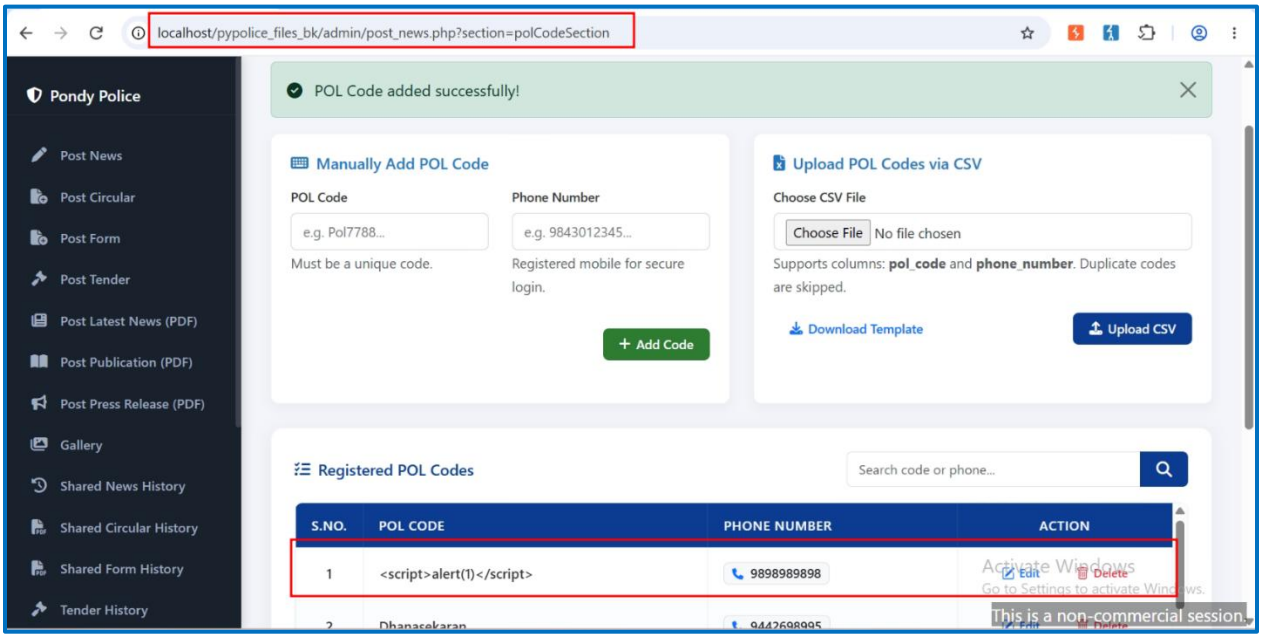





localhost/pypolice_files_bk/admin/station_post.php#
Pondy Police
Add Station Info
Shared Station History
Latest Achievements
Logout
Post News & Add Station
Station_admin Panel - thirubuvanai_station
Shared Station History
OFFICER NAME
CONTACT
EMAIL
ABOUT
PHOTO
SUBMITTED
STATUS
<script>alert(1) </script>
<script>alert(1) </script>
bug@bug.com
N/A
PENDING
{{7*7}}
sdfjksdf
bug@bug.com
N/A
PENDING
test 001
545645465465
mohan@yopmail.com
N/A
APPROVED
Thirubhuvanai officer
9876543234
test@gmail.com
N/A
APPROVED
Activate Windows
Go to Settings to activate Windows.
This is a non-commercial session.

Scenario 2:


localhost/pypolice_files_bk/admin/post_news.php?section=polCodeSection
Post Press Release (PDF)
Gallery
Shared News History
Shared Circular History
Shared Form History
Tender History
Latest News PDF History
Shared Publication Hist...
Shared Press Release Hi...
Manage POL Codes
Manage Helplines
Manage AI Chatbot
Logout
Admin Dashboard
Admin Panel - admin1
Manually Add POL Code
POL Code
<script>alert(1)</script>
Must be a unique code.
Phone Number
9898989898
Registered mobile for secure login.
+ Add Code
Upload POL Codes via CSV
Choose CSV File
Choose File
No file chosen
Supports columns: pol_code and phone_number. Duplicate codes are skipped.
Download Template
Upload CSV
Registered POL Codes
Search code or phone...
S.NO.
POL CODE
PHONE NUMBER
ACTION
1
Dhanasekaran
9442698995
Edit
Delete
Activate Windows
Go to Settings to activate Windows.
This is a non-commercial session.


localhost/pypolice_files_bk/admin/post_news.php?section=polCodeSection
Pondy Police
Post News
Post Circular
Post Form
Post Tender
Post Latest News (PDF)
Post Publication (PDF)
Post Press Release (PDF)
Gallery
Shared News History
Shared Circular History
Shared Form History
Tender History
POL Code added successfully!
Manually Add POL Code
POL Code
e.g. Pol7788...
Must be a unique code.
Phone Number
e.g. 9843012345...
Registered mobile for secure login.
+ Add Code
Upload POL Codes via CSV
Choose CSV File
Choose File No file chosen
Supports columns: pol_code and phone_number. Duplicate codes are skipped.
Download Template
Upload CSV
Registered POL Codes
Search code or phone...
S.NO.
POL CODE
PHONE NUMBER
ACTION
1
<script>alert(1)</script>
9898989898
Edit
Delete
Activate Windows
Go to Settings to activate Windows.
This is a non-commercial session.