Web Application

Penetration Test Report

Md Shofiur Rahman
Shofiur007@gmail.com

Scope https:// example.com/

1. Key Findings Summary

Md Shofiur Rahman performed manual and automated security tests to identify risks and provide solutions for the client. These findings represent a comprehensive assessment of the client's overall security posture for web application-related information.

OWASP Top 10 and Top 25 Programming Errors Mapping

Several security areas were reviewed during the assessment process. These areas are a focal point of the application assessment methodology. Discovered vulnerabilities are mapped to OWASP (Open Web Application Security Project) top 10 vulnerabilities and top 25 most dangerous programming errors.

The first column in Table 4 represents top 10 web application vulnerabilities as defined by the OWASP community. The top 10 vulnerabilities address the most critical security flaws present in web applications and provide a most effective method to secure them.

The second column highlights the Top 25 most dangerous programming errors (developed by SANS, MITRE's Common Weakness Enumeration (CWE) and other renowned security experts around the globe) that could lead to serious software vulnerabilities. The list represents the most common mistakes that could lead to fatal security flaws in the software and ways to mitigate them.

The list can also be used as a benchmark against which security standards of the application can be measured. The evaluation rating is one of three levels. Each level and its definition are listed below to help understand the ratings with respect to your application environment.

S. No	OWASP Top 10 Web Application Vulnerabilities	Top 25 Programming Errors	Evaluation
1.	A1 Injection	**CWE-78:** Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') **CWE-89:** Improper	**Insufficient.** **Attacker may attack the following web applications:** http://example.com/ http://example.com/

S. No	OWASP Top 10 Web Application Vulnerabilities	Top 25 Programming Errors	Evaluation
		Neutralization of Special Elements used in an SQL Command ('SQL Injection')	/sites/
2.	A2 Broken Authentication	**CWE-306:** Missing Authentication for Critical Function **CWE-307:** Improper Restriction of Excessive Authentication Attempts **CWE-798:** Use of Hard-coded Credentials	**Insufficient.** **Attacker may attack the following web applications:** http://example.com/ http://example.com/sites/
3.	A3 Sensitive Data Exposure	**CWE-311:** Missing Encryption of Sensitive Data **CWE-327:** Use of a Broken or Risky Cryptographic Algorithm **CWE-759:** Use of a One-Way Hash without a Salt	**Insufficient.** **Attacker may attack the following web applications:** http://example.com/ http://example.com /sites/
4.	A4 XML External Entities (XXE)	No Sans Top 25 mapped to this OWASP.	**Meets.** **No A4 XML External Entities (XXE) Vulnerabilities Detected.**
5.	A5 Broken Access Control	**CWE-732:** Incorrect Permission Assignment for Critical Resource **CWE-862:** Missing Authorization **CWE-863:** Incorrect Authorization	**Meets.** **No A5 Broken Access Control Vulnerabilities Detected.**
6.	A6 Security Misconfiguration	No Sans Top 25 mapped to this OWASP.	**Insufficient.** **Attacker may attack the following web applications:**

S. No	OWASP Top 10 Web Application Vulnerabilities	Top 25 Programming Errors	Evaluation
			http://example.com/ http://example.com /sites/
7.	A7 Cross Site Scripting	**CWE-79:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	**Insufficient.** **Attacker may attack the following web applications:** http://example.com/ http://example.com /sites/
8.	A8 Insecure Deserialization	**CWE-22:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	**Meets.** **No A8 Insecure Deserialization Vulnerabilities Detected.**
9.	A9 Using Components with Known Vulnerabilities	No Sans Top 25 mapped to this OWASP.	**Insufficient.** **Attacker may attack the following web applications:** http://example.com/ http://example.com /sites/
10.	A10 Insufficient Logging & Monitoring	No Sans Top 25 mapped to this OWASP.	**NA**

Table 4: OWASP top 10

The table below provides severity wise breakup of the vulnerabilities identified during vulnerability assessment.

Vulnerability	Aplication-wide
High Unique Vulnerability Count	7
Medium Unique Vulnerability Count	2
Low Unique Vulnerability Count	2

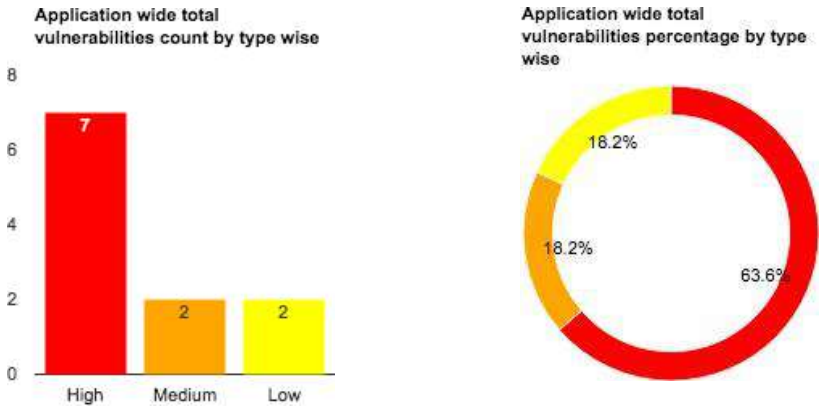


Figure 4: Unique vulnerabilities.

1.1 Vulnerability to Severity Mapping

The table below provides the mapping of the each identified vulnerability with respect to their severity and the number of instances occurred after first, second, third, and fourth rounds of assessment.

S. No	Vulnerability	Severity	
			1st
1.	SQL Injection	High	40
2.	Cross site scripting	High	150
3.	Broken Authentication & Session Management	High	1
4.	Sensitive data exposure	High	5
5.	Cross site Request Forgery	High	160
6.	Security Misconfiguration	High	3
7.	Malicious File Upload	High	8
8.	External Service Interaction (DNS/ HTTP)	Medium	2
9.	Known Vulnerabilities	Medium	4
10.	Banner Disclosure	Low	1
11.	Clickjacking	Low	1
12.	Password Autocomplete	Low	1
Total Count of Vulnerabilities			376

* Apply best practices throughout the application

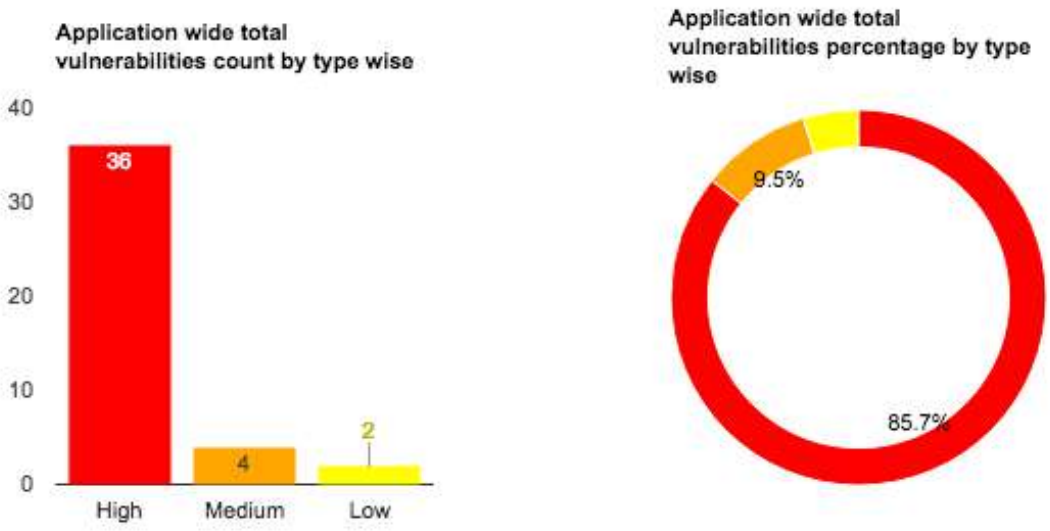


Figure 5: Total Vulnerabilities

2. Detailed Assessment Findings and Recommendations

This section provides below details of identified vulnerabilities during the assessment

- Description
- Assessment Type
- Affected Application
- Impact
- Risk Rating
- Recommendations

2.1 Assessment Findings

Below are the vulnerabilities identified during the assessment and are listed according to the risk associated with them.

4.1.1 SQL Injection

Description	A SQL injection attack exploits vulnerability in input validation to run arbitrary commands in the database. It can occur when the application uses input to construct dynamic SQL statements to access the database. It can also occur if the code uses stored procedures that are passed strings that contain raw user input. Using the SQL injection attack, an attacker can execute arbitrary commands in your database, with all the privileges granted to the process being attacked. The issue is magnified if the application uses an over-privileged account to connect to the database. In this instance it is possible to use the database server to run operating system commands and potentially compromise other servers, in addition to being able to retrieve, manipulate, and destroy data. **Note:** Some other pages that are generating the response based on the user input provided to SQL queries of the application are vulnerable to SQL injection. Implement all the SQL queries of the application with the Parameterized Class APIs.
Assessment Type	Web Application Security
Affected applications	http://example.com/ http://example.com/sites/
Impact	By exploiting SQL injection vulnerability an attacker can take control over the database.

Risk Rating	High
Recommendations	**Constrain input.** Use vigorous white-list style checking and type checking on any user input that may be used in an SQL command. Rather than escape meta-characters, it is safest to avoid adding them to your white-list. Later use of data that has been entered in the database may neglect to escape meta-characters before use. **Use Parameterized SQL statements and stored procedures.** Parameterized SQL statements will process characters that have special meaning to SQL (like single quote) without negative security implications. **Use escaping routines**. If you cannot use parameters and must use dynamic SQL, use escaping routines to handle special characters that have meaning to the database. **Do not echo database errors**. Catch exceptions on the server and return generic error messages to the client.

Proof of Concept

Figure A1: The **dept_id** parameter in get_designations.php with single quote returns SQL error.

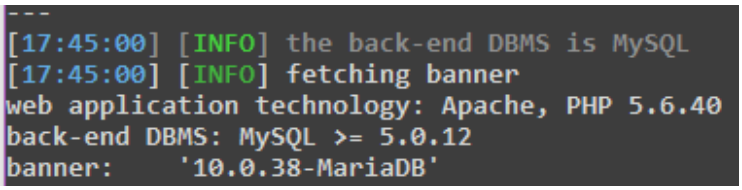


Figure A2: The application uses MySQL DBMS as database software.

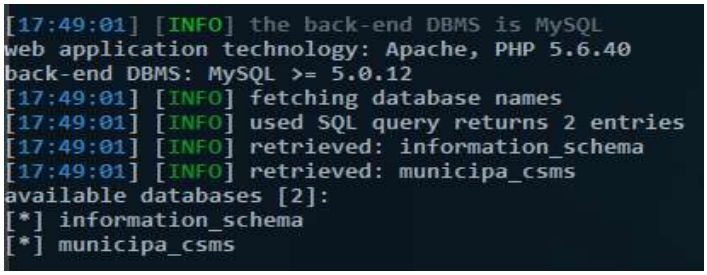


Figure A3: The available databases list in the DBMS.

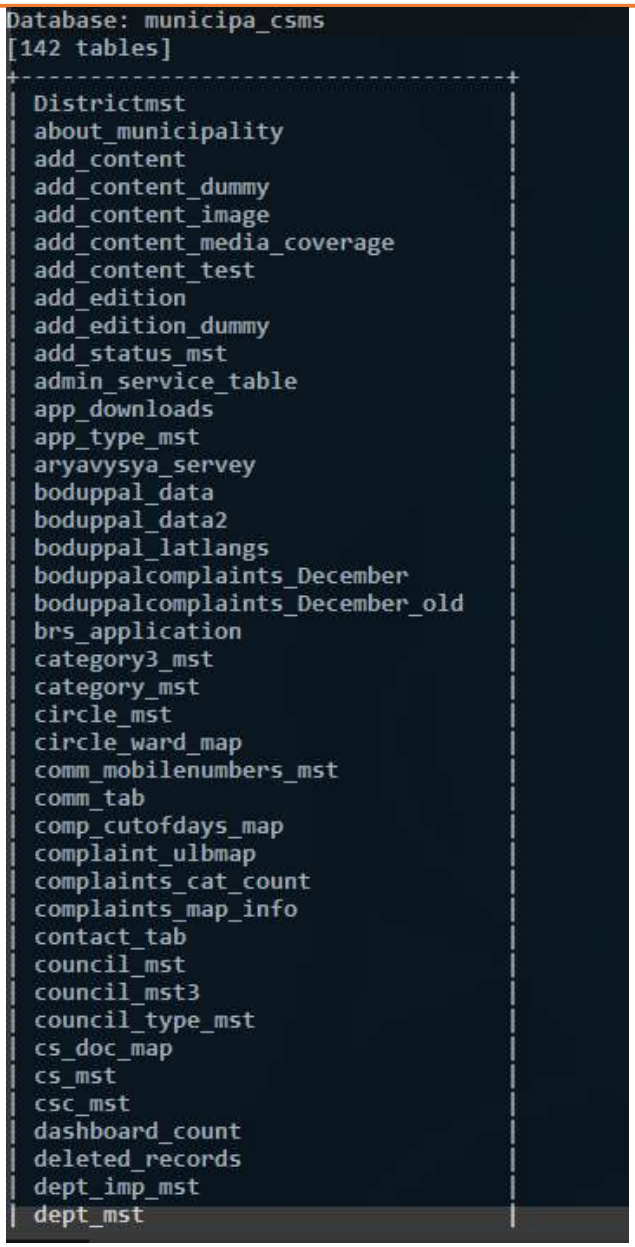


Figure A4: Availabale databases in municipa_csms database.

Note: Similarly, the following URLS and parameters are vulnerable to SQL Injection.

1. The Post request parameter **dept_id** in the URL http://example.com/get_designations.php is vulnerable to SQL Injection.
2. The Post request parameter **app_type_id, ref_no, applicant_name, mobile, ward_id, dept_id and**

cat3_id in the URL http://municipalservices.in/manage_comp.php is vulnerable to SQL Injection.

3. The Post request parameter **taker_number, name, mobile and address** in the URL http://municipalservices.in/add-tanker.php is vulnerable to SQL Injection.
4. The Post request parameter **rdmaid** in the URL http://municipalservices.in/ajax_getdists2.php is vulnerable to SQL Injection.
5. The Post request parameter **distid** in the URL http://municipalservices.in/ajax_getulbs2.php is vulnerable to SQL Injection.
6. The Post request parameter **regionid, distid and ulbid** in the URL http://municipalservices.in/app_downloads.php is vulnerable to SQL Injection.

4.1.2 Cross Site Scripting

Description	Cross Site Scripting (XSS) attack can cause arbitrary code (java script) to run in a user's browser while the browser is connected to a trusted web site. The application targets your application's users and not the application itself, but it uses your application as the vehicle for the attack.
Assessment Type	Web Application Security
Affected application	http://example.com/ http://example.com/sites/
Impact	An attacker can inject the malicious code into the vulnerable variable and exploit an application through cross site scripting (XSS) Vulnerability.
Risk Rating	High
Recommendations	Perform context sensitive encoding of entrusted input before it is echoed back to a browser by using encoding library throughout the application. Implement input validation for special characters on all the variables that are reflecting to the browser and storing in the database.
Proof of Concept	
Issue 1: Reflected Cross Site Scripting	

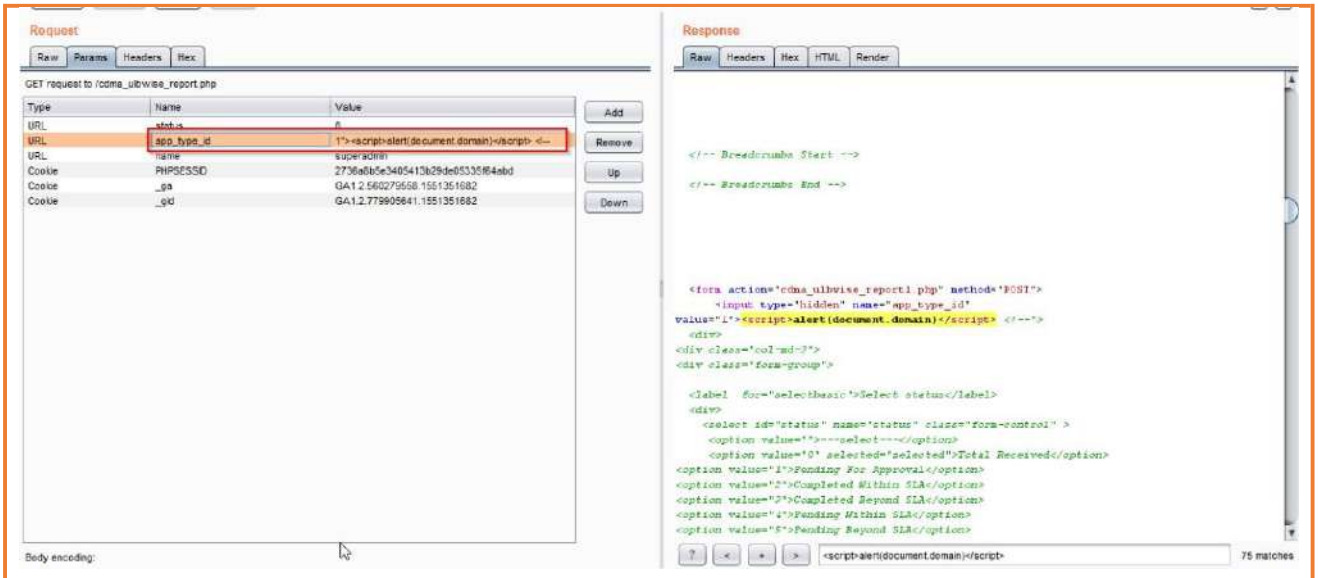


Figure B1: The app_type_id parameter with JavaScript payload in cdma_ulbwise_report page returns the payload in output HTML.

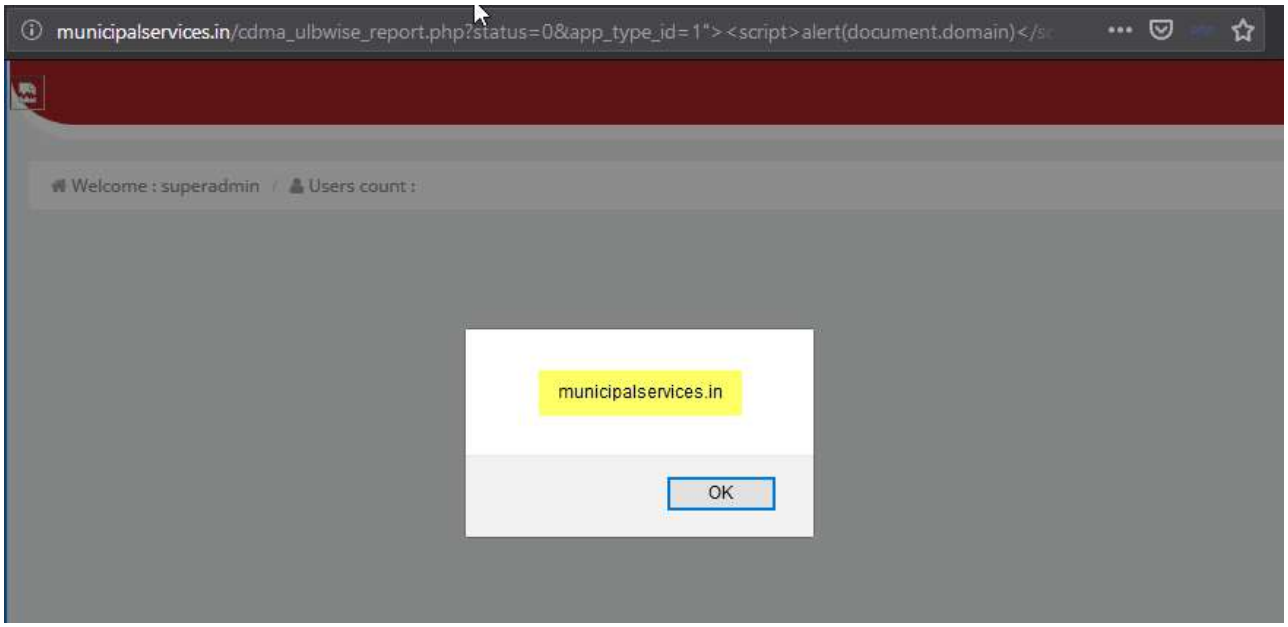


Figure B2: The JavaScript payload executes in the context of current user browser.

Issue 2: Stored Cross site scripting

Figure B3: video information update request with JavaScript payload saves into database.

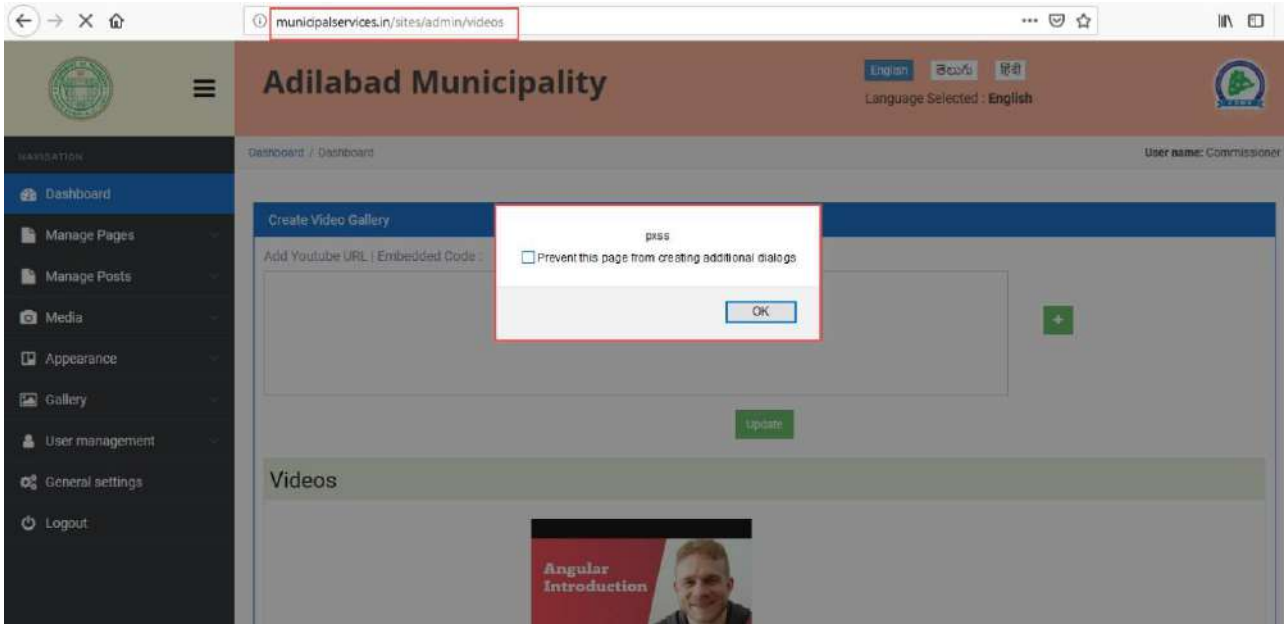


Figure B4: The JavaScript payload gets executed in the current user browser context whenever the user visits videos page.

Similarly, the following URLS and parameters are vulnerable to Cross Site Scripting.

1. The GET request parameter **status and app_type_id** in the URL

   http://example.com/cdma_ulbwise_report.php is vulnerable to cross site scripting.

2. The GET request parameter **status and app_type_id** in the URL http://municipalservices.in/ulbwise_reopened_rep.php is vulnerable to cross site scripting.
3. The GET request parameter **dept_id, emp_id, emp_id2 and emp_id3** in the URL http://municipalservices.in/ward_emp_complaint_map.php is vulnerable to cross site scripting.
4. The GET request parameter **id** in the URL http://municipalservices.in/get_complntform_04_02_2019.php is vulnerable to cross site scripting.
5. The GET request parameter **emp_name** in the URL http://municipalservices.in/update_emp.php is vulnerable to cross site scripting.

Note: Implement the best practices throughout the application.

4.1.3 Broken Authentication & Session Management

Description	The application doesn't change the session-id of the user before login and after login.
Assessment Type	Web Application Security
Affected application	http://example.com/ http://example.com/sites/
Impact	An attacker who knows the session-id of a user, can use it for compromising the user account.
Risk Rating	High
Recommendations	Please change the session-id of the user during login and logout process.
Proof of Concept	

Issue: Session Fixation

Figure C1: The PHPSESSID of the user is same before login and after login.

4.1.4 Sensitive Data Exposure

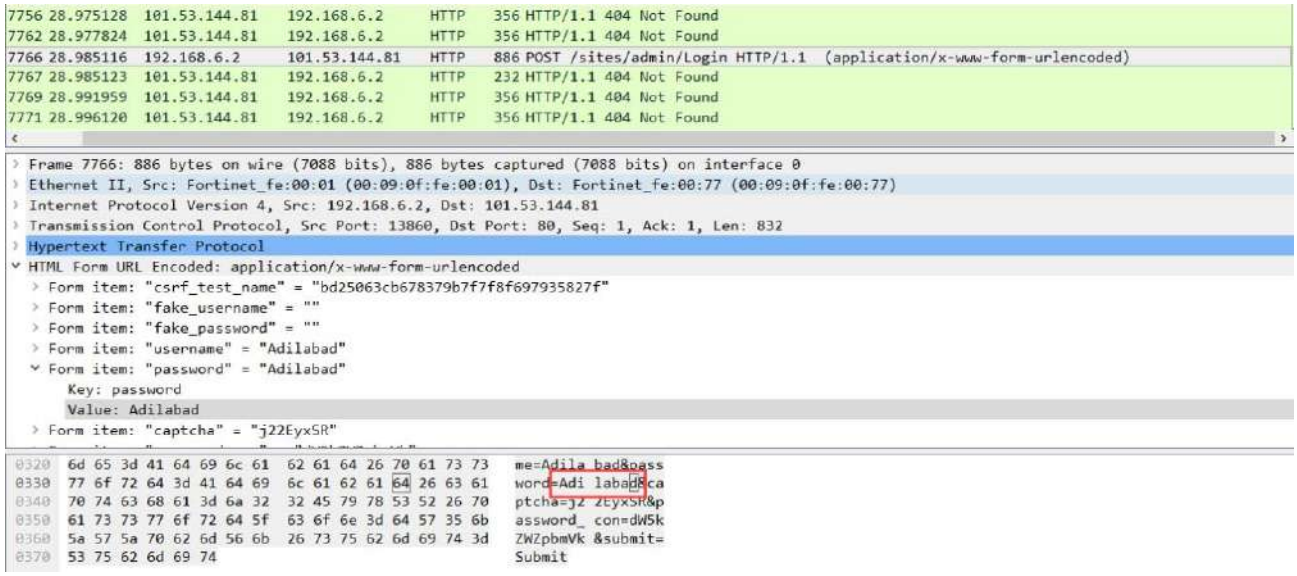
Description	The application is sending user credentials over an insecure channel. Sensitive data exposure occurs when an application does not adequately protect sensitive information. The data can vary and anything from passwords, session tokens, credit card data to private health data and more can be exposed.
Assessment Type	Web Application Security
Affected application	http://example.com/ http://example.com/sites/
Impact	Attacker can gather all the sensitive information and will launch further attacks.
Risk Rating	High
Recommendations	As the application needs authentication and authorization to grant access to the services, it is recommended to deploy it with trusted SSL certificate. The successful authentication of user should not return the password hash and salt details of the user.
Proof of Concept	

Raw | Params | Headers | Hex

POST request to /update_profile.php

Type	Name	Value
Cookie	PHPSESSID	6cacb76c5a60ab53de2f96e29633edda
Cookie	csrf_cookie_name	54af0886091af325a3f9fe8c62cb1fcb
Cookie	__atuvc	6|5
Cookie	_ga	GA1.2.2040690662.1549016111
Cookie	_gid	GA1.2.749467183.1549016111
Cookie	ci_session	223k3j624kv1drttls6mlr7r1cb92b22
Body	user_name	Administrator
Body	change_pwd	on
Body	user_email	csw@gmail.com
Body	user_pwd1	CSw123
Body	user_mobile	9703587230
Body	user_pwd2	CSw123
Body	save	Update Profile

Figure D1: The application sends user credentials in insecure channel.



```
7756 28.975128  101.53.144.81   192.168.6.2     HTTP   356 HTTP/1.1 404 Not Found
7762 28.977824  101.53.144.81   192.168.6.2     HTTP   356 HTTP/1.1 404 Not Found
7766 28.985116  192.168.6.2     101.53.144.81   HTTP   886 POST /sites/admin/Login HTTP/1.1  (application/x-www-form-urlencoded)
7767 28.985123  101.53.144.81   192.168.6.2     HTTP   232 HTTP/1.1 404 Not Found
7769 28.991959  101.53.144.81   192.168.6.2     HTTP   356 HTTP/1.1 404 Not Found
7771 28.996120  101.53.144.81   192.168.6.2     HTTP   356 HTTP/1.1 404 Not Found

> Frame 7766: 886 bytes on wire (7088 bits), 886 bytes captured (7088 bits) on interface 0
> Ethernet II, Src: Fortinet_fe:00:01 (00:09:0f:fe:00:01), Dst: Fortinet_fe:00:77 (00:09:0f:fe:00:77)
> Internet Protocol Version 4, Src: 192.168.6.2, Dst: 101.53.144.81
> Transmission Control Protocol, Src Port: 13860, Dst Port: 80, Seq: 1, Ack: 1, Len: 832
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "csrf_test_name" = "bd25063cb678379b7f7f8f697935827f"
  > Form item: "fake_username" = ""
  > Form item: "fake_password" = ""
  > Form item: "username" = "Adilabad"
  v Form item: "password" = "Adilabad"
      Key: password
      Value: Adilabad
  > Form item: "captcha" = "j22EyxSR"

0320  6d 65 3d 41 64 69 6c 61  62 61 64 26 70 61 73 73   me=Adila bad&pass
0330  77 6f 72 64 3d 41 64 69  6c 61 62 61 64 26 63 61   word=Adi labad&ca
0340  70 74 63 68 61 3d 6a 32  32 45 79 78 53 52 26 70   ptcha=j2 2EyxSR&p
0350  61 73 73 77 6f 72 64 5f  63 6f 6e 3d 64 57 35 6b   assword_ con=dW5k
0360  5a 57 5a 70 62 6d 56 6b  26 73 75 62 6d 69 74 3d   ZWZpbmVk &submit=
0370  53 75 62 6d 69 74                                 Submit
```

Figure D2: Requests to the server at network level can allow attackers to see the clear text credentials.

4.1.5 Cross-Site Request Forgery

Description	Attacker creates forged HTTP requests and tricks a victim into submitting them via image tags, XSS, or numerous other techniques. If the user is authenticated, the attack succeeds.
Assessment Type	Web Application Security

Affected application	http://example.com/ http://example.com/sites/
Impact	Attackers can cause victims to change any data the victim is allowed to change or perform any function the victim is authorized to use.
Risk Rating	High
Recommendations	To fix this, implement anti CSRF token in all the sensitive forms of the application and validate it at server end. For more information, please go through the following URL https://www.webtipblog.com/implementing-csrf-protection-in-php/

Proof of Concept

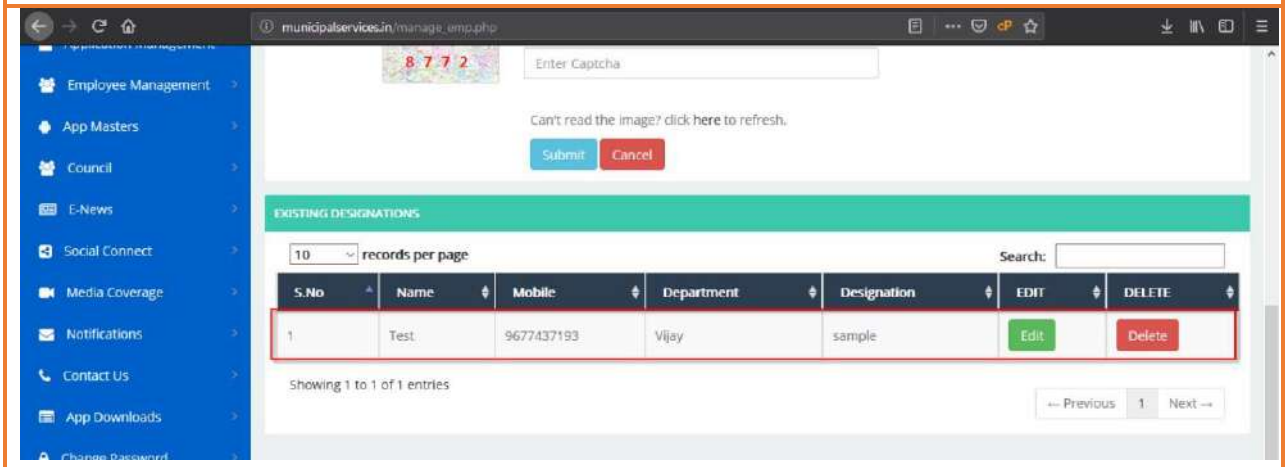


Figure E1: Update user details before performing CSRF.

CSRF HTML:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://municipalservices.in/update_emp.php" method="POST">
      <input type="hidden" name="emp&#95;id" value="2705" />
      <input type="hidden" name="dept&#95;id&#95;prev" value="745" />
      <input type="hidden" name="cnt" value="0" />
      <input type="hidden" name="emp&#95;name" value="Test CSRF" />
      <input type="hidden" name="emp&#95;mobile" value="9999999999" />
      <input type="hidden" name="emp&#95;dept" value="745" />
      <input type="hidden" name="emp&#95;desg" value="2355" />
      <input type="hidden" name="save" value="Add&#32;&#47;&#32;Update&#32;Ward" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Figure E2: HTML form of forged request to update designations

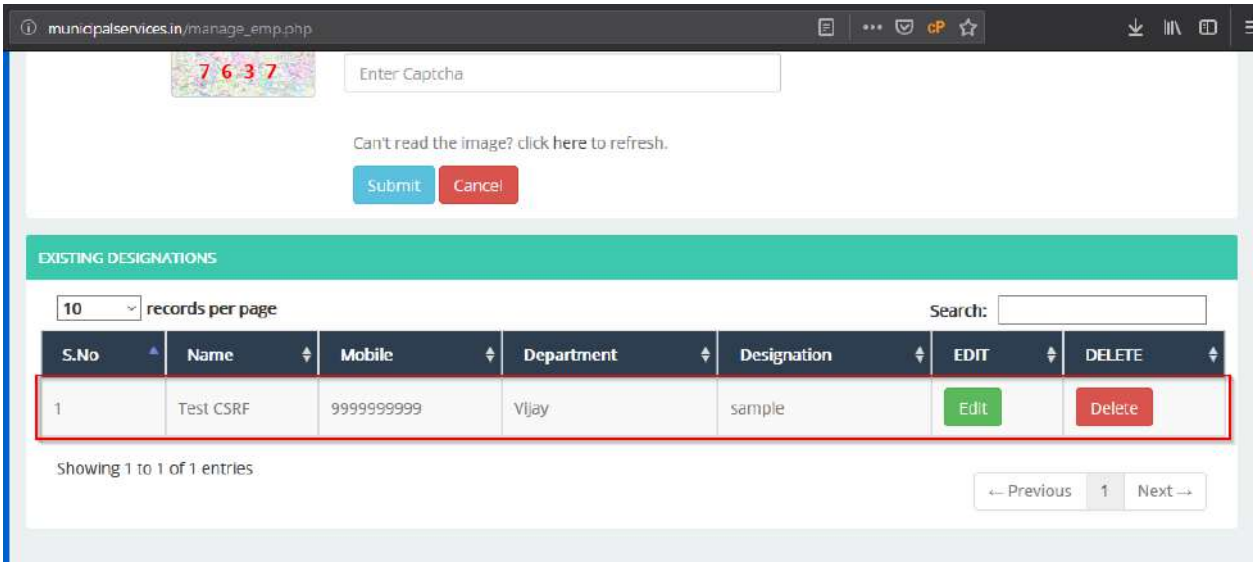


Figure E3: By clicking the link to the forged html sent by the attacker, the currently logged in user updated his user services details without his notice.

Note: Similarly, all the Forms are in the both applications URLs http://municipalservices.in/ and http://municipalservices.in/sites/ are vulnerable to CSRF.

4.1.6 Security Misconfiguration

Description	Security Misconfiguration reveals some relevant information about the server in which attackers have possibility of exploiting the application
Assessment Type	Web Application Security
Affected application	http://example.com/ http://example.com/sites/
Impact	By this vulnerability malicious users can collect information and use for launching further attacks.
Risk Rating	High
Recommendations	• Deploying all new software updates and patches in a timely manner. • Remove unwanted pages and services. • Remove the file(s) if they are not required on your website. As an additional step, it is recommended to implement a security policy within your organization to disallow creation of backup files in directories accessible from the web. • Remove or restrict access to all configuration files accessible from internet.

Proof of Concept

Issue 1: Improper Error Handling

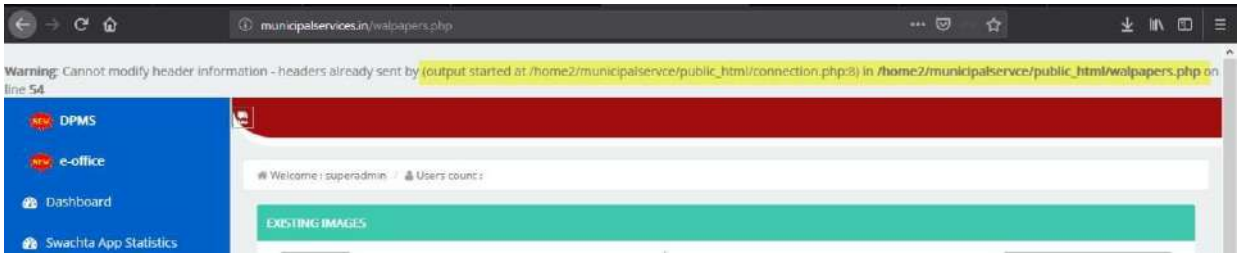


Figure F1: Application is not able to handle run time errors and discloses physical path.

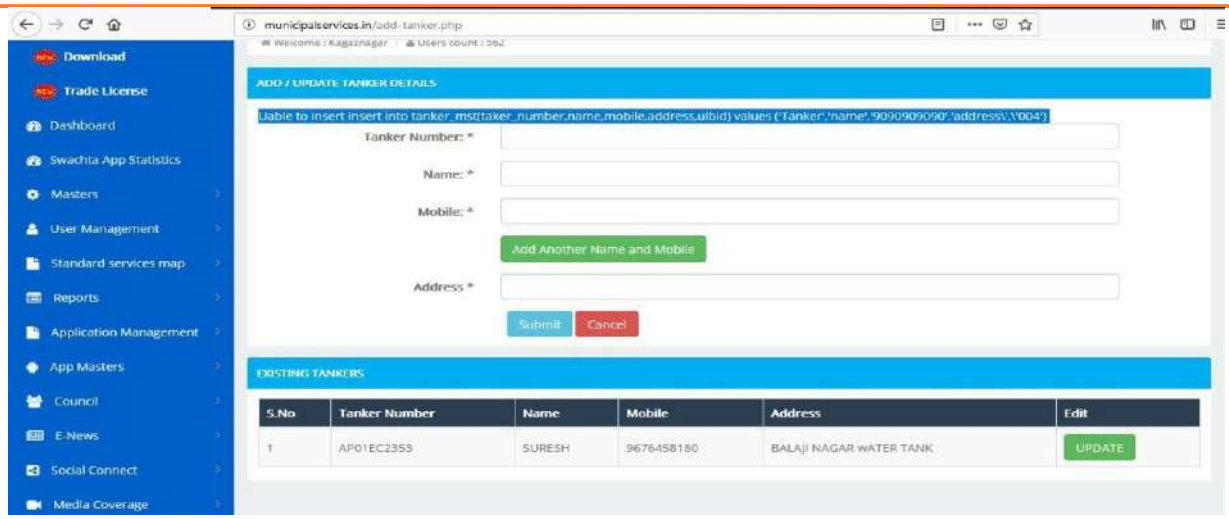


Figure F2: Application errors disclose entire SQL query

Issue 2: Old password not implemented

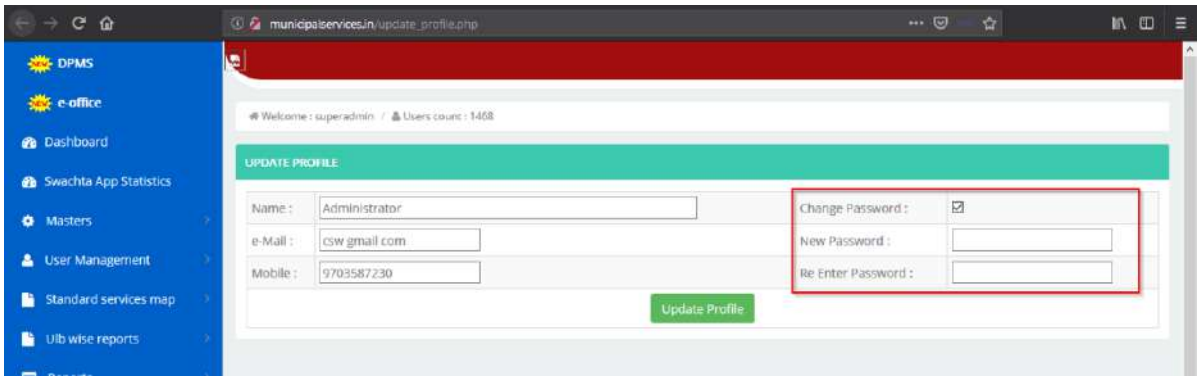


Figure F3: For admin user changing password page old password field did not implemented**.**

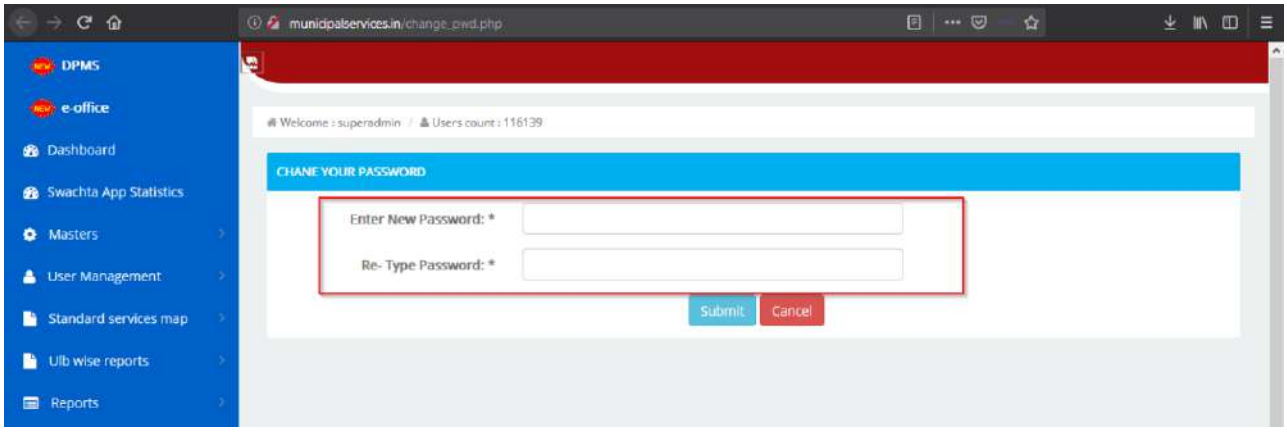


Figure F4: For ULB user changing password page old password field did not implemented.

Issue 3: Source Code disclosure

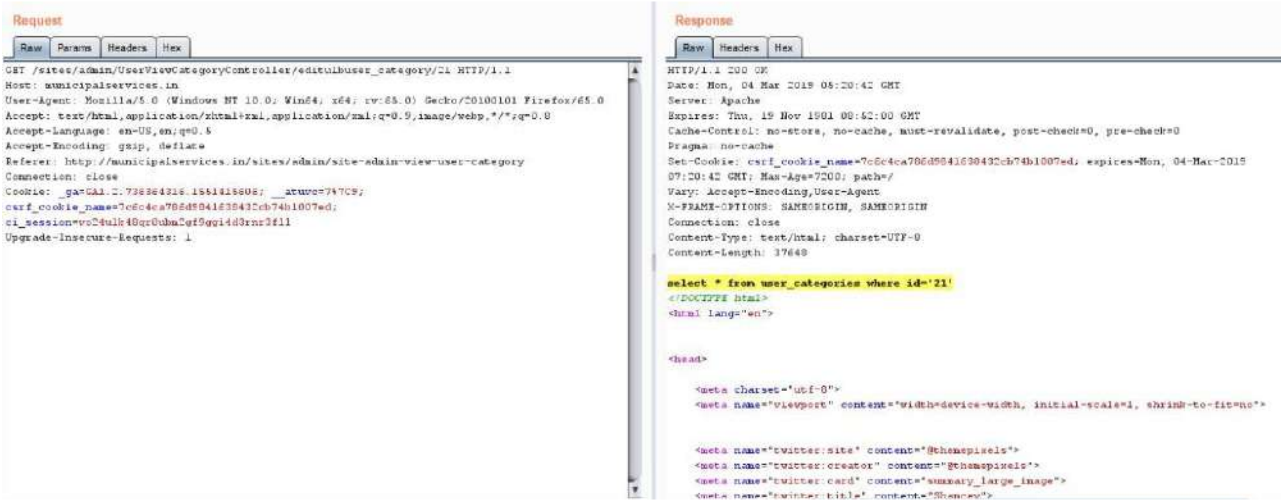


Figure F5: SQL select query code is shown in burp response body.

Issue 4: Default PHP info file found

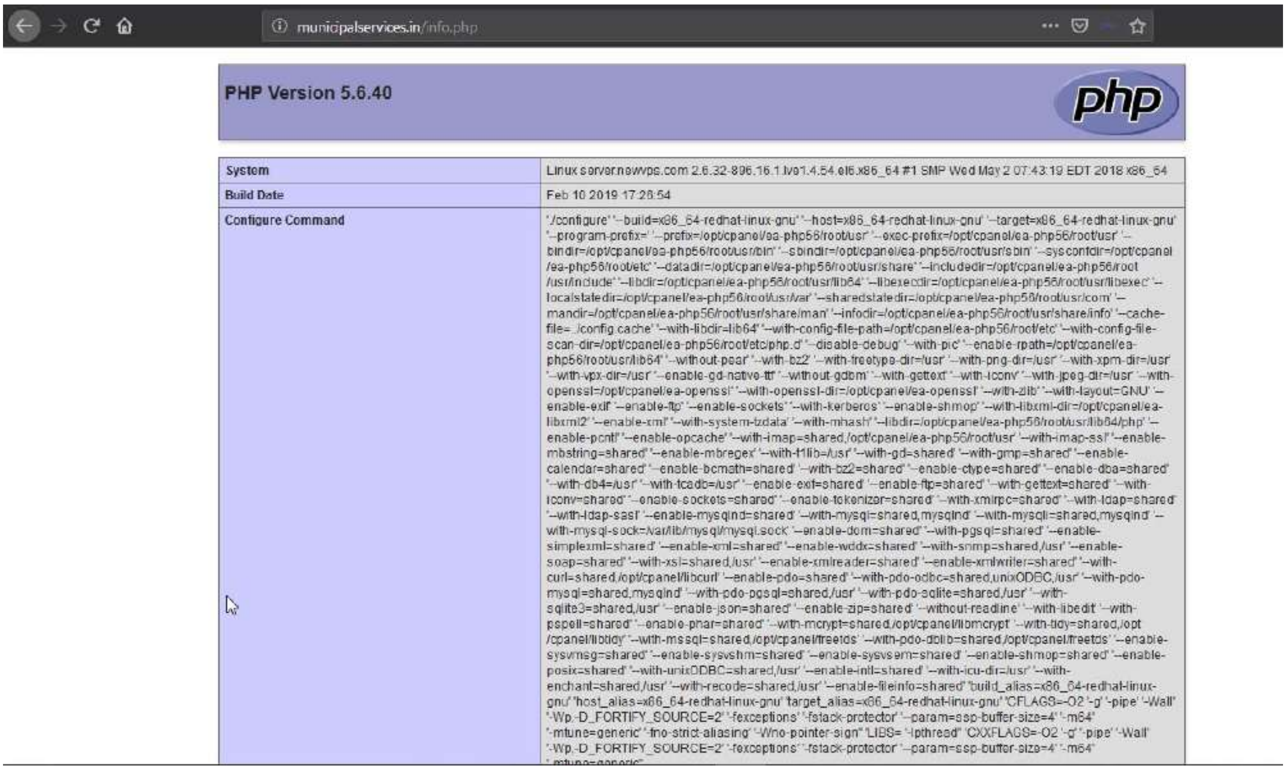


Figure F6: php info page disclosure the sensitive information of the application.

Issue 5: Cookie without HTTPOnly flag set enabled

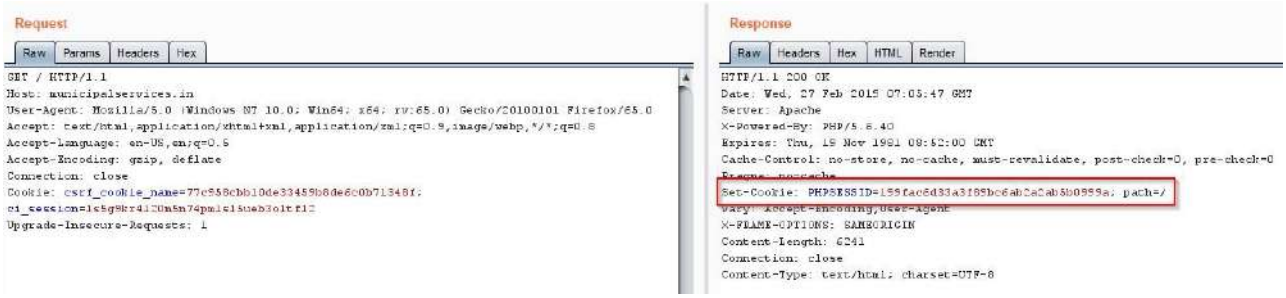


Figure F6: The application doesn't enable HTTPOnly flag on session to protect it from hijacking attacks.

4.1.7 Malicious File Upload

Description	File upload vulnerabilities allow attackers to upload malicious code. (Technically, allowing users to upload anything that the application's design doesn't account for can be considered a file upload vulnerability. In practice, real file upload vulnerabilities are those that allow attackers to upload and execute malicious code.)
Assessment Type	Web Application Security
Affected application	http://example.com/ http://example.com/sites/
Impact	File upload vulnerabilities allow attackers to execute arbitrary code with the privileges of the application server. Using this vulnerability, the attacker will usually upload a small backdoor that will give him easy access to the application server's functions, such as performing file and database operations, executing operating system commands, executing arbitrary code that is sent in HTTP requests, and executing additional exploits.
Risk Rating	High
Recommendations	To check for adequate protection against file upload vulnerabilities, • Whitelist the allowed extension of file types. • Uploaded Files Are Stored Outside of Web Root • Names of Uploaded Files Are Scrambled **Note:** We are unable to delete the shell uploaded as part of our assessment. Please remove it from the server.

Proof of Concept

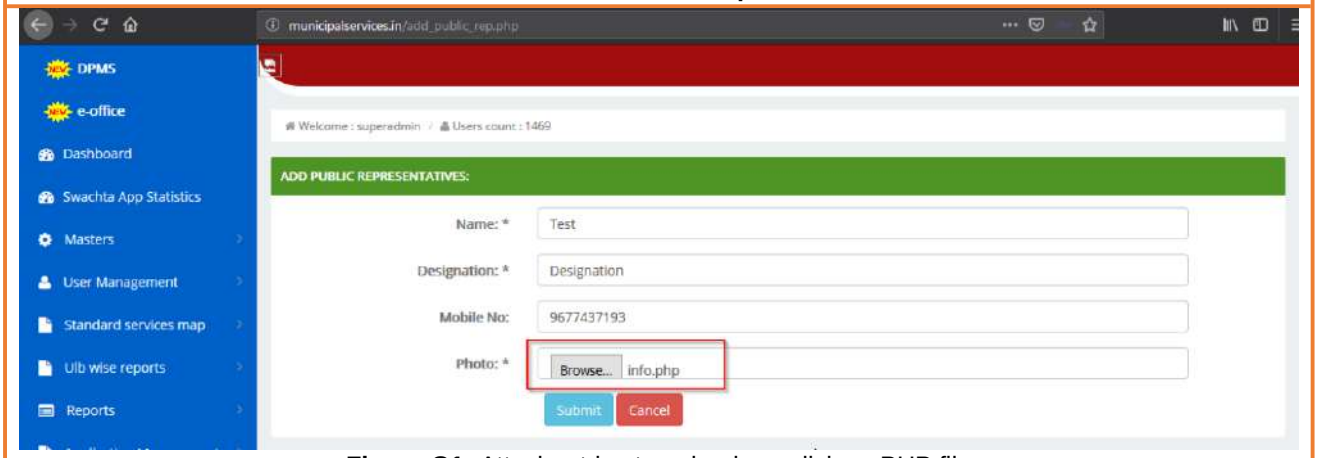


Figure G1: Attacker tries to upload a malicious PHP file

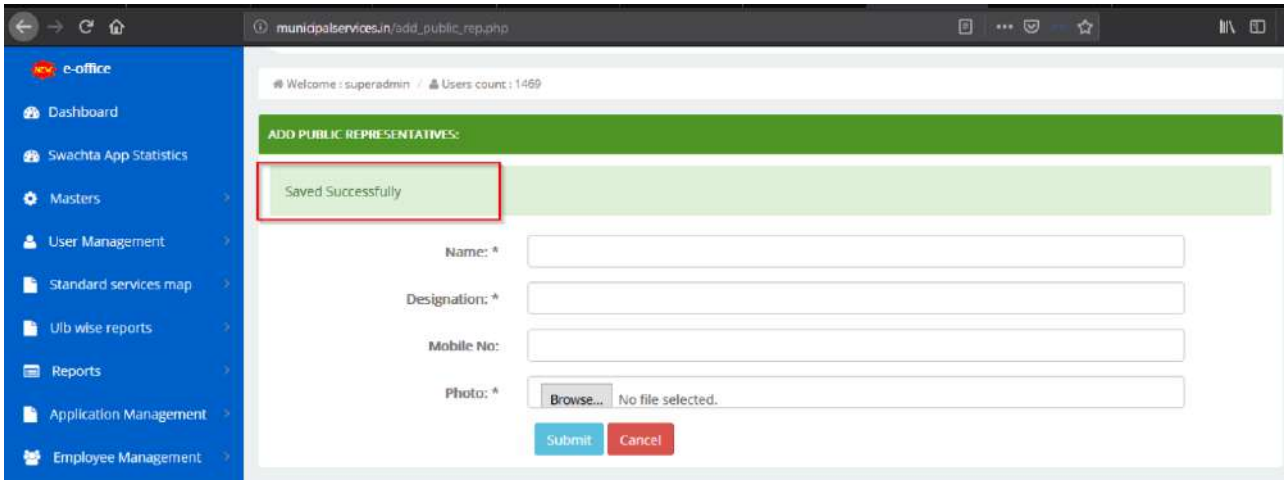


Figure G2: The application accepts the files with malicious extensions and it confirms it through success message.

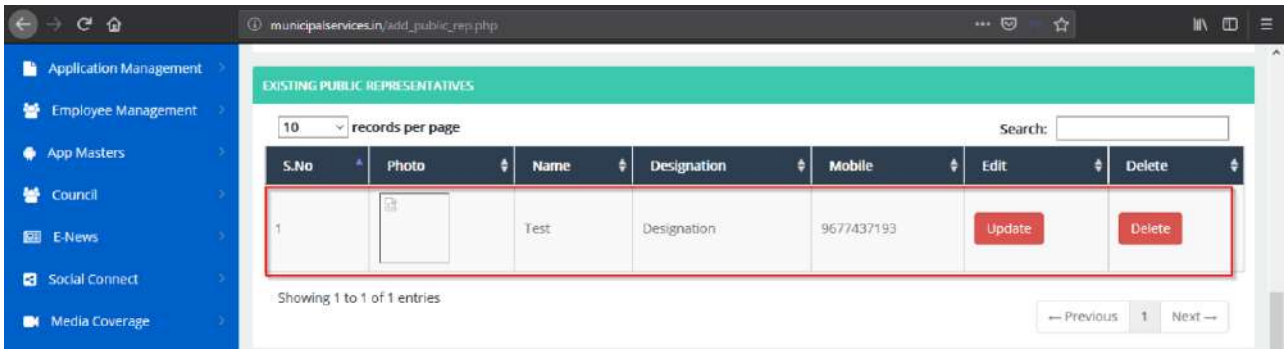


Figure G3: The broken image link in list of existing public representatives page points to the uploaded file.

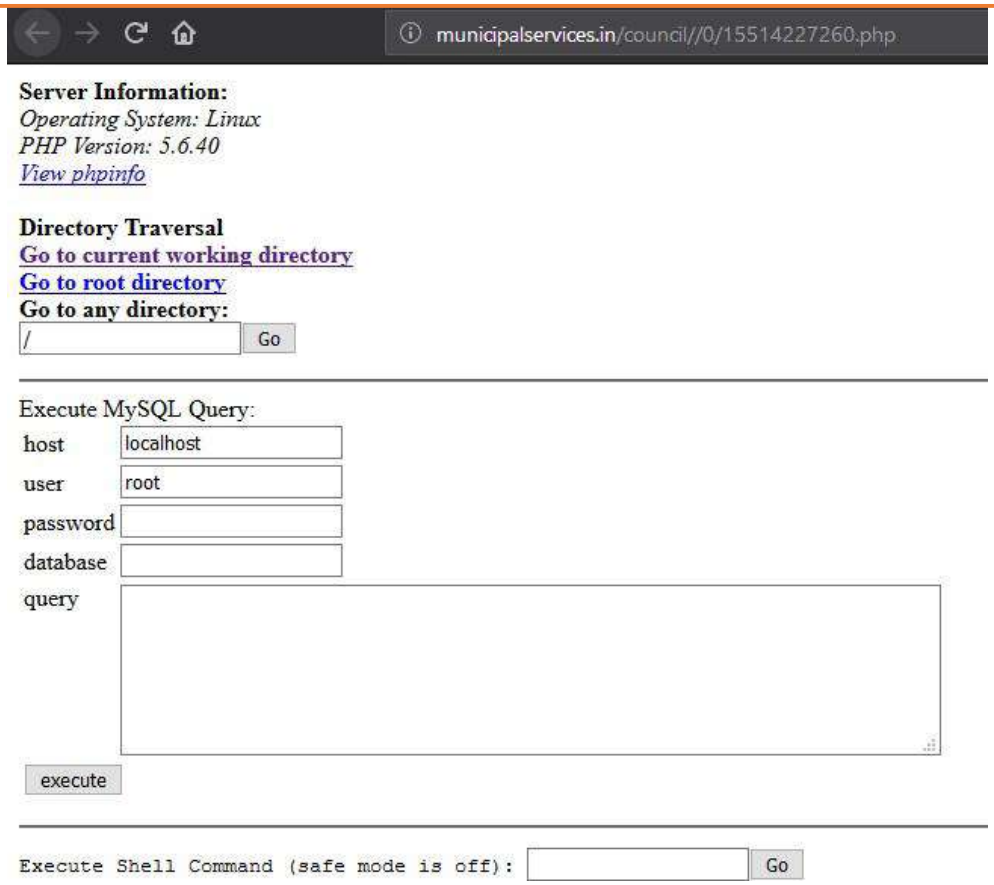


Figure G4: The URL of the uploaded PHP backdoor. This file gives access to the server.

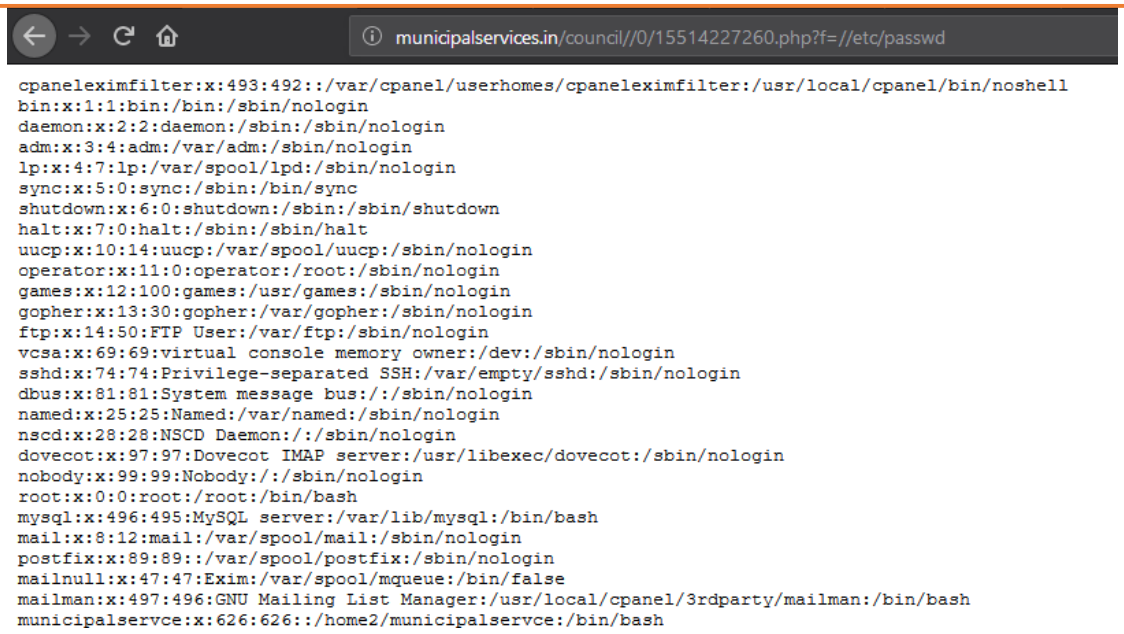


Figure G5: Fetching /etc/passwd file through PHP backdoor.

Note: Similarly, all the upload options in the application are vulnerable to malicious file upload

4.1.8 External Service Interaction

Description	External service interaction arises when it is possible to induce an application to interact with an arbitrary external service, such as a web or mail server. The ability to trigger arbitrary external service interactions does not constitute a vulnerability in its own right, and in some cases might even be the intended behavior of the application.
Assessment Type	Web Application Security
Affected application	http://example.com/ http://example.com/sites/
Impact	By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with. This may include public third-party systems, internal systems within the same organization, or services available on the local loopback adapter of the application server itself.
Risk Rating	Medium

Recommendations	The application server shouldn't accept request with random host headers. To fix this vulnerability, please go through the following URL http://niiconsulting.com/checkmate/2018/10/manipulating-host-headers-not-anymore/

Proof of Concept

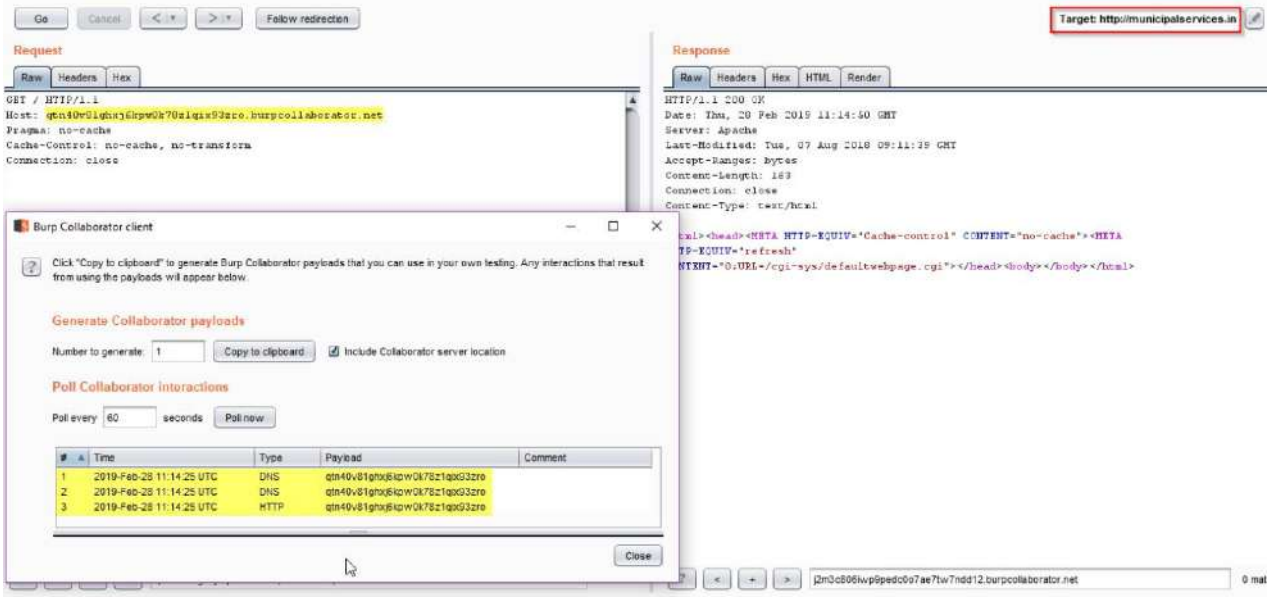


Figure H1: The server accepts requests with different domain and forward those requests to the actual domain for resolution.

4.1.9 Known Vulnerabilities

Description	Vulnerabilities in third-party libraries and software are extremely common and could be used to compromise the security of systems using the software.
Assessment Type	Web Application Security
Affected application	http://example.com/ http://example.com/sites/
Impact	The vulnerability might be affecting a feature of the library that the website is not using. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may

	undermine application defenses and enable a range of possible attacks and impacts.
Risk Rating	Medium
Recommendations	Upgrade the jQuery and Bootstrap libraries used in the application to latest version.

Proof of Concept

Issue 1: Vulnerable jQuery

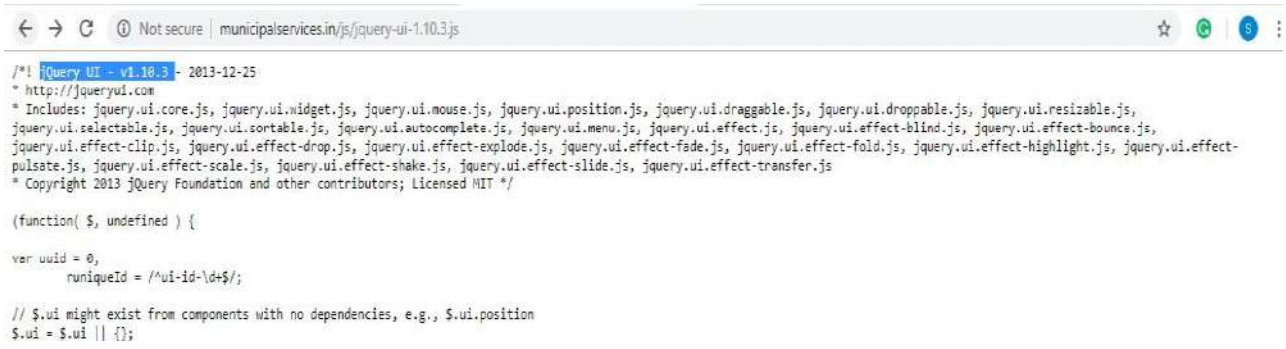


Figure I1: The application uses the jQuery libraries which have known vulnerabilities.

Similarly, the following URLs also have vulnerable components of the jQuery library.

- http://example.com/menu/js/jquery.js
- http://example.com/js/jquery.min.js

Issue 2: Vulnerable Bootstrap

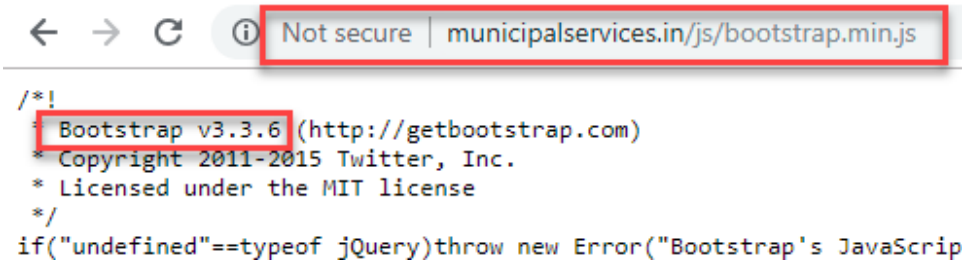


Figure I2: The Bootstrap version used for the application has publicly known vulnerabilities.

Issue 3: Vulnerable CKEditor

Figure I3: The application uses CKEDITOR version 4.4.2 which has publicly known vulnerabilities.

4.1.10 Banner disclosure

Description	The web application is disclosing server banner information along with all responses from the server.
Assessment Type	Web Application Security
Affected application	http://example.com/ http://example.com/sites/
Impact	By this vulnerability malicious users can collect information and use for launching further attacks.
Risk Rating	Low
Recommendations	Disable X-Powered-By response headers in server. For more information, please go through the following URL https://www.petefreitag.com/item/722.cfm. Also, set expose_php to off in php.ini file.
Proof of Concept	

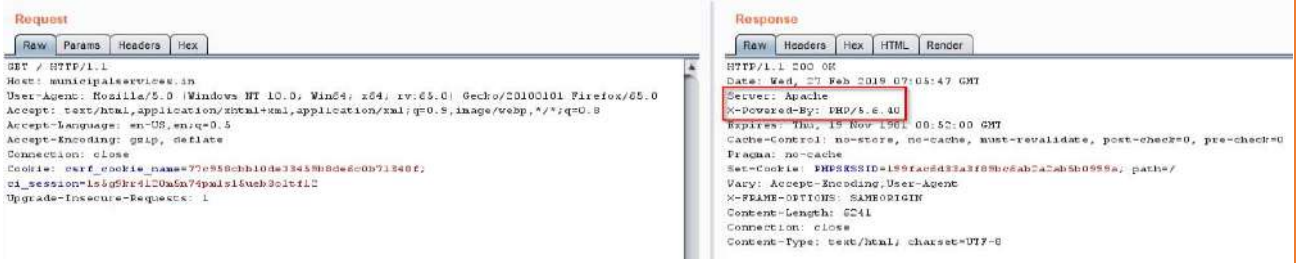


Figure J1: X-Powered-BY Response header information disclosed.

4.1.11 Password Field with Autocomplete enabled

Description	When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.
Assessment Type	Web Application Security
Affected application	http://example.com/ http://example.com/sites/
Impact	Possible sensitive information disclosure.
Risk Rating	Low
Recommendations	The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code like: <INPUT TYPE="password" AUTOCOMPLETE="off">

Proof of Concept

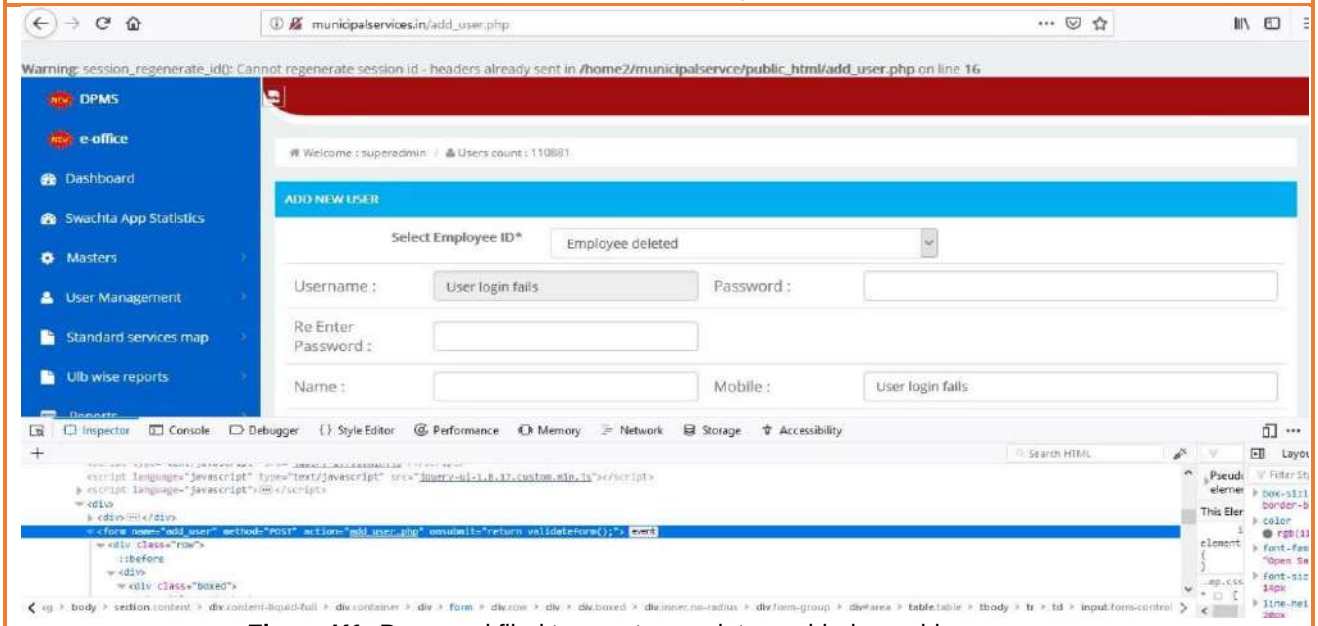


Figure K1: Password filed type autocomplete enabled on add_user page.

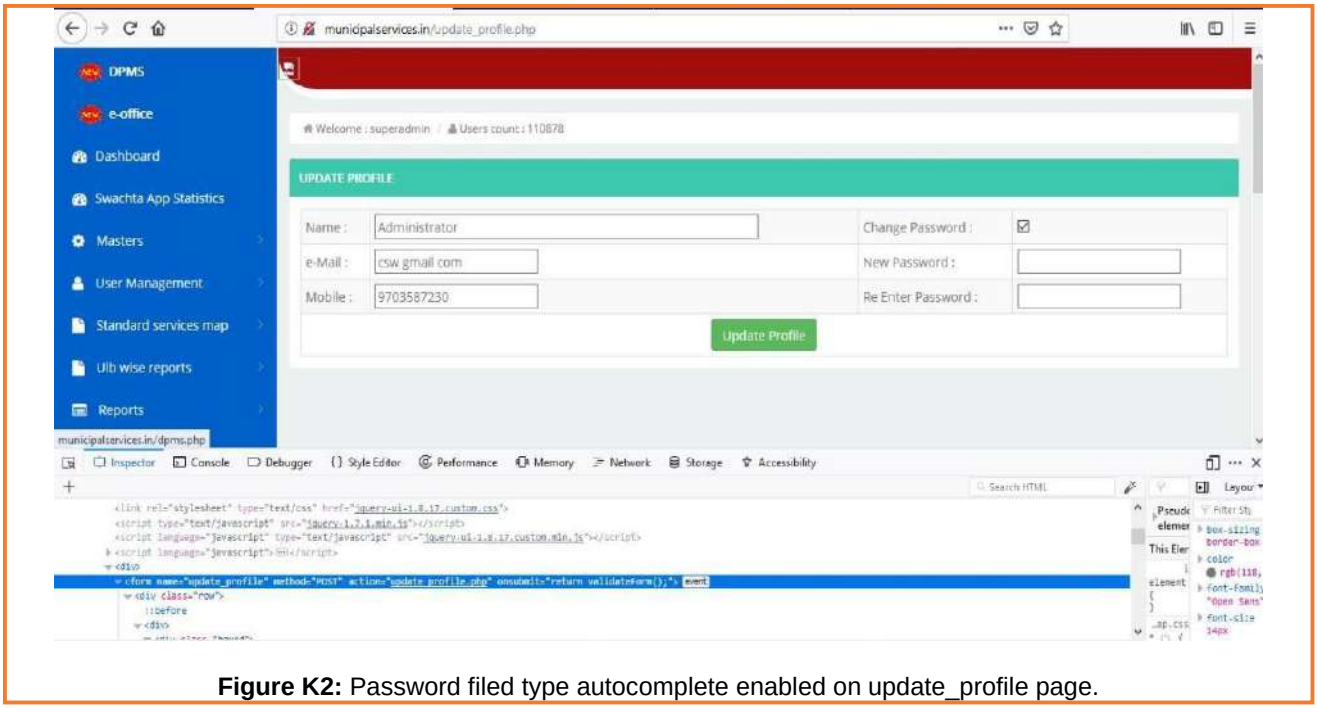


Figure K2: Password filed type autocomplete enabled on update_profile page.

3. Functional Issues:

CSW team did not check the following mentioned pages. The pages should show some data to check for-security issues.

- ✓ **Figure L1:** http://example.com/complaint_emp_map_report_street_wise.php

  Link returns 404 not found error message.

Similarly, the below URLs have the same issue,

- ✓ http://example.com/manage_sms_emp_dept.php

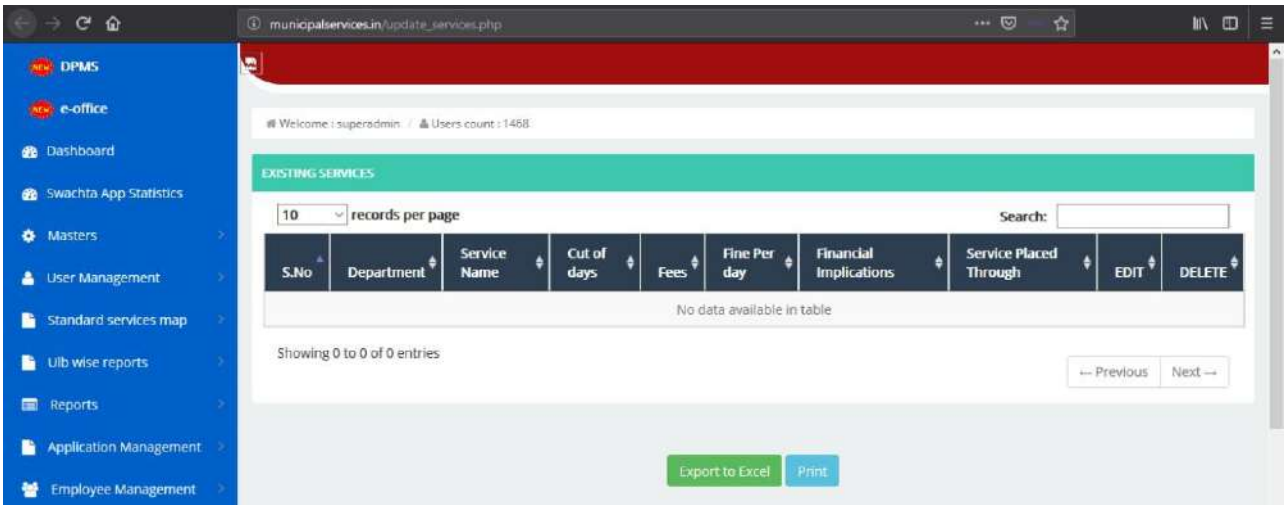


Figure L2: No Data available to check the form.

Similarly, the below URLs have same issue

- ✓ http://example.com/update_services.php
- ✓ http://example.com/view_pending_approval.php
- ✓ http://example.com/tanker_req.php
- ✓ http://example.com/update_tanker_req.php

Figure L3: On select Employee ID options username and mobile fields loading details as User login fails.

4. Appendices

4.1 Appendix A: Tested URLs

- http://example.com/
- http://example.com/about-municipality.php
- http://example.com/add-edition.php
- http://example.com/add-tanker.php
- http://example.com/add_council.php
- http://example.com/add_document.php
- http://example.com/add_notification.php
- http://example.com/add_public_rep.php
- http://example.com/add_user.php
- http://example.com/addcontent.php
- http://example.com/ajax_complaint_dashboard.php
- http://example.com/ajax_del_dept.php
- http://example.com/ajax_del_enew_content.php
- http://example.com/ajax_del_ward.php?ward_id=1
- http://example.com/ajax_delete_councillor.php
- http://example.com/ajax_delete_edition.php
- http://example.com/ajax_delete_media_coverage.php
- http://example.com/ajax_delete_media_coverage_image.php
- http://example.com/ajax_delete_public_rep.php
- http://example.com/ajax_delete_spe_off.php
- http://example.com/ajax_get_employees2.php
- http://example.com/ajax_get_search_cat3ids.php
- http://example.com/ajax_getdists2.php
- http://example.com/ajax_getstreets.php
- http://example.com/ajax_getulbs2.php
- http://example.com/ajax_mobile_check.php
- http://example.com/app_downloads.php
- http://example.com/cdma_ulbwise_report.php?status=0&app_type_id=1&name=superadmin
- http://example.com/cdma_ulbwise_report1.php
- http://example.com/check_availability.php

- http://example.com/check_comp_status.php?id=058
- http://example.com/check_login.php
- http://example.com/comp_cutoffdate_map.php
- http://example.com/complaint_emp_map_report_street_wise.php
- http://example.com/complaint_form.php?id=058
- http://example.com/contact_us.php
- http://example.com/council//0/15514227260.php?d=/home2/municipalservce/public_html/council/0
- http://example.com/council/0/15514227260.php?phpinfo=true
- http://example.com/delete_doc.php
- http://example.com/delete_holy.php
- http://example.com/delete_notification.php
- http://example.com/dept_empwise.php?app_type_id=2&dept_id=24&status=0&f_date=&t_date=
- http://example.com/deptwise_reopened.php?ulbid=001&app_type_id=1&status=13
- http://example.com/e-news/news-det.php?content_id=8348&content_no=2596
- http://example.com/e-news/view.php?ulbid=052
- http://example.com/edit_council.php?id=2139
- http://example.com/edit_media_coverage.php?content_no=859
- http://example.com/edit_public_rep.php?id=2137
- http://example.com/feedback_dept_rep.php?ulbid=001
- http://example.com/fonts/fontawesome-webfont3295-2.html?v=4.5.0
- http://example.com/fonts/fontawesome-webfont3295.woff?v=4.5.0
- http://example.com/get_complntform_04_02_2019.php
- http://example.com/get_designations.php?dept_id=24
- http://example.com/get_emps.php?dept_id=
- http://example.com/get_firstservices.php
- http://example.com/get_iframe.php
- http://example.com/get_serviceform2.php
- http://example.com/getcate3.php
- http://example.com/getdoc2.php
- http://example.com/getempcutdet.php
- http://example.com/manage_comp.php
- http://example.com/manage_dept.php
- http://example.com/manage_emp.php

- http://example.com/manage_street.php
- http://example.com/manage_wards.php
- http://example.com/map-cat.php
- http://example.com/media_coverage.php
- http://example.com/menu/admin/uploads/source/1-767x479.jpg?1530008447128
- http://example.com/menu/admin/uploads/source/Koala.jpg?1528973415944
- http://example.com/menu/album?album=test
- http://example.com/menu/fonts/fontawesome-webfont.woff?v=4.2.0
- http://example.com/pending_approval.php?grievance_status_id=1&aptid=1
- http://example.com/public_holydays.php
- http://example.com/receive_print.php?id=269288&aptid=1
- http://example.com/register_comp_helpline.php
- http://example.com/rep_comp_dept_abs.php
- http://example.com/select_edition.php
- http://example.com/service_emp_map_report_street_wise.php
- http://example.com/services.php?aptid=1&status=0&user_type={$user_type}&sla=0
- http://example.com/services1.php?aptid=1&status=3&sla=1&user_type={$user_type}
- http://example.com/sites/052/https:/www.google.com/maps/embed?pb=!1m18!1m12!1m3!1d60561.20714141589!2d79.09812845618879!3d18.43488326744133!2m3!1f0!2f0!3f0!3m2!1i1024!2i768!4f13.1!3m3!1m2!1s0x3bccd93d3d7fe1ad%3A0xb78df26ce7aa3d9f!2sMunicipal+Corporation!5e0!3m2!1sen!2sin!4v1536639522996
- http://example.com/sites/058/https:/www.google.com/maps/place/Public%2bToilets%2b@PetrolBunk%2bnear%2bRailwayGate%2bKothurGP/@17.2095471,80.1532549,17z/data=!4m12!1m6!3m5!1s0x0:0x20e8024fb76f7111!2sPublic%2bToilets%2b@PetrolBunk%2bnear%2bRailwayGate%2bKothurGP!8m2!3d17.2095471!4d80.1554436!3m4!1s0x0:0x20e8024fb76f7111!8m2!3d17.2095471!4d80.1554436?hl=en-IN
- http://example.com/sites/058/https:/www.google.com/maps/place/Public%2bToilets%2b@Railwaygate/@17.2458944,80.1372992,17z/data=!3m1!4b1!4m5!3m4!1s0x0:0x413730926b3732d4!8m2!3d17.2458944!4d80.1394879?hl=en-IN
- http://example.com/sites/058/https:/www.google.com/maps/place/Public%2bToilets@BabuRaoPetrolBunk/@17.250584,80.1426863,17z/data=!4m12!1m6!3m5!1s0x0:0xc0f77c3d3f848ae3!2sPublic%2bToilets@BabuRaoPetrolBunk!8m2!3d17.250584!4d80.144875!3m4!1s0x0:0xc0f77c3d3f848ae3!8m2!3d17.250584!4d80.144875?hl=en-IN
- http://example.com/sites/058/https:/www.google.com/maps/place/Public%2bToilets@HpPetrolBunk%2bRotary%2bNagar/@17.2461631,80.1669942,17z/data=!4m12!1m6!3m5!1s0x0:0x7f53040e78de35e8!2

sPublic%2bToilets@HpPetrolBunk%2bRotary%2bNagar!8m2!3d17.2461631!4d80.1691829!3m4!1s0x0:0x7f53040e78de35e8!8m2!3d17.2461631!4d80.1691829?hl=en-IN

- http://example.com/sites/058/https:/www.google.com/maps/place/Public%2bToilets@HpPetrolBunk%2bSri%2bSri%2bCircle/@17.2452554,80.1766152,17z/data=!4m12!1m6!3m5!1s0x0:0x33d6d3336182d0a4!2sPublic%2bToilets@HpPetrolBunk%2bSri%2bSri%2bCircle!8m2!3d17.2452554!4d80.1788039!3m4!1s0x0:0x33d6d3336182d0a4!8m2!3d17.2452554!4d80.1788039?hl=en-IN
- http://example.com/sites/058/https:/www.google.com/maps/place/Public%2bToilets@grain%2bmarket/@17.2381143,80.1313118,17z/data=!4m12!1m6!3m5!1s0x0:0xd2f37af6f7e3bc39!2sPublic%2bToilets@grain%2bmarket!8m2!3d17.2381143!4d80.1335005!3m4!1s0x0:0xd2f37af6f7e3bc39!8m2!3d17.2381143!4d80.1335005?hl=en-IN
- http://example.com/sites/058/https:/www.google.com/maps/place/Public%2btoilet@%2bRailwaystation/@17.248741,80.1369864,17z/data=!4m12!1m6!3m5!1s0x0:0x3d6e58395e48e758!2sPublic%2btoilet@%2bRailwaystation!8m2!3d17.248741!4d80.1391751!3m4!1s0x0:0x3d6e58395e48e758!8m2!3d17.248741!4d80.1391751?hl=en-IN
- http://example.com/sites/058/https:/www.google.com/maps/place/Public%2btoilet@indianOilbunk%2bMustafanagar/@17.2285866,80.1475204,17z/data=!4m12!1m6!3m5!1s0x0:0x65d43a21851fe40e!2sPublic%2btoilet@indianOilbunk%2bMustafanagar!8m2!3d17.2285866!4d80.1497091!3m4!1s0x0:0x65d43a21851fe40e!8m2!3d17.2285866!4d80.1497091?hl=en-IN
- http://example.com/sites/058/https:/www.google.com/maps/place/Public%2btoilets%2b@barath%2bpetrolbunk/@17.2512446,80.1545193,17z/data=!4m12!1m6!3m5!1s0x0:0xe760763641ec17bc!2sPublic%2btoilets%2b@barath%2bpetrolbunk!8m2!3d17.2512446!4d80.156708!3m4!1s0x0:0xe760763641ec17bc!8m2!3d17.2512446!4d80.156708?hl=en-IN
- http://example.com/sites/058/https:/www.google.com/maps/place/Public%2btoilets%2b@bustand/@17.2504482,80.1403924,17z/data=!3m1!4b1!4m5!3m4!1s0x0:0xf191489fb53b6c0b!8m2!3d17.2504482!4d80.1425811?hl=en-IN
- http://example.com/sites/058/https:/www.google.com/maps/place/PublicToilets@pavilionground/@17.2533722,80.1400055,17z/data=!4m12!1m6!3m5!1s0x0:0x482a25e7dfc65a51!2sPublicToilets@pavilionground!8m2!3d17.2533722!4d80.1421942!3m4!1s0x0:0x482a25e7dfc65a51!8m2!3d17.2533722!4d80.1421942?hl=en-IN
- http://example.com/sites/058/search
- http://example.com/sites/082/https:/example.com/complaint_form.php?id=082
- http://example.com/sites/082/https:/tools.wmflabs.org/geohack/geohack.php?pagename=Siddipet&params=18.1_N_78.85_E_

- http://example.com/sites/207/https:/www.google.com/maps/embed?pb=!1m14!1m8!1m3!1d15227.29 9583085407!2d78.5846889!3d17.420189!3m2!1i1024!2i768!4f13.1!3m3!1m2!1s0x0%3A0x6e701a3a716a9 b99!2sBoduppal+Municipal+Office!5e0!3m2!1sen!2sin!4v1538219817018
- http://example.com/sites/CustomePageController/add_feedback
- http://example.com/sites/admin/CreateMediaController/deleteContent
- http://example.com/sites/admin/CreateMediaController/getContent
- http://example.com/sites/admin/GeneralSettingsController/ulbLogoUpdate
- http://example.com/sites/admin/GeneralSettingsController/uploadfile
- http://example.com/sites/admin/Login
- http://example.com/sites/admin/PostCategoryController/add_cat
- http://example.com/sites/admin/PostCategoryController/checkingcatInfo
- http://example.com/sites/admin/PostCategoryController/deletecatInfo
- http://example.com/sites/admin/UpdateprofileController/update_userprofile
- http://example.com/sites/admin/UploadMediaController/deleteContent
- http://example.com/sites/admin/UploadMediaController/exportDatatomedialibrary
- http://example.com/sites/admin/UploadMediaController/imageUploadPost
- http://example.com/sites/admin/UserViewCategoryController/update_user_category/21
- http://example.com/sites/admin/ViewAlbumsController/checkingAlbumName
- http://example.com/sites/admin/ViewAlbumsController/getAlbumList
- http://example.com/sites/admin/ViewUlbUserController/update_user/CDMA
- http://example.com/sites/admin/general-settings
- http://example.com/sites/admin/user-categories
- http://example.com/sites/admin/videos
- http://example.com/sites/assets/cdma/font/fontawesome-webfont3e6e.html?v=4.7.0
- http://example.com/sites/assets/cdma/font/theme-corea727.ttf?g49o0u
- http://example.com/sites/http:/125.18.179.57:8080/CDMA_TS_Dashboard/dashboard/sroUlbWise.do ?ULBCode=1105
- http://example.com/sites/http:/epaycdma.telangana.gov.in:8081/Tradeapplication/tradeReportAll.do? ulb_id=1105
- http://example.com/sites/http:/epaycdma.telangana.gov.in:8082/CDMA_Water/waterTaxReportAll.do ?ulb_id=1105
- http://example.com/social_connect.php
- http://example.com/statistics.php?cs_type_id=2&code=0

- http://example.com/swapp_dashboard.php?ulbid=001
- http://example.com/swapp_details.php?cs_id=22&ulbid=
- http://example.com/tanker-available-status.php
- http://example.com/ulb_cat_wise.php?ulbid=001&status=1&app_type_id=1
- http://example.com/ulb_cat_wise1.php?ulbid=001&status=1
- http://example.com/ulb_dept_wise.php?ulbid=001&status=0&app_type_id=1
- http://example.com/ulbwise_reopened_rep.php?app_type_id=1&status=13&name=superadmin
- http://example.com/update-enew-content.php?id=8362
- http://example.com/update_emp.php
- http://example.com/update_notification.php?id=763
- http://example.com/update_service_doc_map.php
- http://example.com/update_tankers.php
- http://example.com/update_user.php?user_id=CDMA
- http://example.com/update_user_services.php?user_id=superadmin
- http://example.com/walpapers.php?content_no=859
- http://example.com/ward_emp_complaint_map.php
- http://example.com/Events/
- http://example.com/Events/check_login.php
- http://example.com/Events/dashboard.php
- http://example.com/Online_Advertisement.php
- http://example.com/Property_tax_calculator.php
- http://example.com/Property_tax_self_assessment.php
- http://example.com/ajax_dashboard.php
- http://example.com/api/
- http://example.com/change_pwd.php
- http://example.com/co_option_members.php
- http://example.com/comm_address/1551444212.php
- http://example.com/config1.php
- http://example.com/controlpanel/
- http://example.com/council//0/15514226240.php
- http://example.com/council//2216/15514301652216.php
- http://example.com/council//2216/15514302032216.php
- http://example.com/council_desg_map.php

- http://example.com/cpanel/
- http://example.com/csc.php
- http://example.com/dashboard.php
- http://example.com/dept_login.php
- http://example.com/dpms.php
- http://example.com/e-news/error/404.php
- http://example.com/e-office1.php
- http://example.com/ediotr_plugins/
- http://example.com/employee_map.php
- http://example.com/entry_app_downloads.php
- http://example.com/feedback/
- http://example.com/feedbackrep.php
- http://example.com/index.php
- http://example.com/info.php
- http://example.com/logout.php
- http://example.com/manage_comp_sel.php
- http://example.com/manage_desg.php
- http://example.com/manage_desg_del.php
- http://example.com/menu/
- http://example.com/menu/-
- http://example.com/menu/-aaa
- http://example.com/menu/-aaa'%2520AND%25203*2*1=6%2520AND%2520'000jTNO'='000jTNO
- http://example.com/menu/-chart
- http://example.com/menu/-comissioner
- http://example.com/menu/-councile
- http://example.com/menu/-mayorcontact
- http://example.com/menu/-ms
- http://example.com/menu/-propertytaxcalculator
- http://example.com/menu/-testreddy
- http://example.com/menu/-ttt
- http://example.com/menu/-urb
- http://example.com/menu/GovernmentInitiatives
- http://example.com/menu/admin/budgets/21.pdf

- http://example.com/menu/admin/budgets/EOI%20for%20DPR%20of%20Slaughter%20House.pdf
- http://example.com/menu/admin/budgets/EOI 2.PDF
- http://example.com/menu/admin/tenders/EOI_Busbay_11.05.2018.pdf
- http://example.com/menu/budgets
- http://example.com/menu/fonts/glyphicons-halflings-regular.woff
- http://example.com/menu/gallery
- http://example.com/menu/index
- http://example.com/menu/index.php
- http://example.com/menu/tenders
- http://example.com/menu/videos
- http://example.com/save_comp.php
- http://example.com/select_page.php
- http://example.com/services_disable.php
- http://example.com/sites/001/a123
- http://example.com/sites/001/ab1234567890
- http://example.com/sites/001/about-sircilla
- http://example.com/sites/001/about-us
- http://example.com/sites/001/accessibility
- http://example.com/sites/001/adilabad-municipality
- http://example.com/sites/001/adilabad-municipality1536662934
- http://example.com/sites/001/advertisement-tax
- http://example.com/sites/001/annual-audit-account
- http://example.com/sites/001/b123
- http://example.com/sites/001/basic-information
- http://example.com/sites/001/beneficiaries-detail
- http://example.com/sites/001/beneficiaries-list
- http://example.com/sites/001/budgets
- http://example.com/sites/001/building-permission
- http://example.com/sites/001/category-posts/001/
- http://example.com/sites/001/category-posts/Slider
- http://example.com/sites/001/category-posts/Slider%20images
- http://example.com/sites/001/chairman-contact
- http://example.com/sites/001/commissioner-contact

- http://example.com/sites/001/contact-us
- http://example.com/sites/001/copyright-policy
- http://example.com/sites/001/council
- http://example.com/sites/001/demand-collection-de
- http://example.com/sites/001/details-of-assigned-
- http://example.com/sites/001/details-of-grants-re
- http://example.com/sites/001/details-of-plan-and-
- http://example.com/sites/001/details-of-taxes-and
- http://example.com/sites/001/directory-of-staff
- http://example.com/sites/001/disclaimer
- http://example.com/sites/001/district-web-directory
- http://example.com/sites/001/engineering-section
- http://example.com/sites/001/engineering-section1531283450
- http://example.com/sites/001/engineering-services
- http://example.com/sites/001/engineering-staff
- http://example.com/sites/001/fdfds
- http://example.com/sites/001/feedback
- http://example.com/sites/001/financial-statements
- http://example.com/sites/001/general-administration
- http://example.com/sites/001/grievance-redressal
- http://example.com/sites/001/health-related-services
- http://example.com/sites/001/health-section
- http://example.com/sites/001/health-section1531283132
- http://example.com/sites/001/health-section1536726099
- http://example.com/sites/001/help
- http://example.com/sites/001/home-page
- http://example.com/sites/001/hyperlinking-policy
- http://example.com/sites/001/income-expenditure-details
- http://example.com/sites/001/income-generated-for
- http://example.com/sites/001/kk
- http://example.com/sites/001/latest-digitised-records
- http://example.com/sites/001/list-of-defaulters-f
- http://example.com/sites/001/list-of-layout-open-spaces

- http://example.com/sites/001/mandatory-documents
- http://example.com/sites/001/mandatory-documents1532321957
- http://example.com/sites/001/master-plan-details
- http://example.com/sites/001/municipal-assets
- http://example.com/sites/001/mutations
- http://example.com/sites/001/ram
- http://example.com/sites/001/related-links
- http://example.com/sites/001/related-links1531285487
- http://example.com/sites/001/renewal-of-tradelicense
- http://example.com/sites/001/revenue-section
- http://example.com/sites/001/revenue-section1531283934
- http://example.com/sites/001/road-cutting-permission
- http://example.com/sites/001/rti-act-2005-telugu
- http://example.com/sites/001/rti-brief
- http://example.com/sites/001/rti-contacts
- http://example.com/sites/001/sanitation
- http://example.com/sites/001/sanitation-status-as
- http://example.com/sites/001/screen-reader
- http://example.com/sites/001/screen-reader-access

- http://example.com/sites/001/socio-economic-activities
- http://example.com/sites/001/speech-recognition-support
- http://example.com/sites/001/srinivas1234
- http://example.com/sites/001/staff-login
- http://example.com/sites/001/state-web-directory
- http://example.com/sites/001/subsidy-programmes
- http://example.com/sites/001/swacch-survekshan
- http://example.com/sites/001/terms-conditions
- http://example.com/sites/001/terms-of-use
- http://example.com/sites/001/test
- http://example.com/sites/001/test1549020749
- http://example.com/sites/001/town-planning-sectio1531284745
- http://example.com/sites/001/town-planning-section
- http://example.com/sites/001/town-planning-staff
- http://example.com/sites/001/urban-community-deve1531282812
- http://example.com/sites/001/urban-community-development
- http://example.com/sites/001/urban-poverty
- http://example.com/sites/001/vacant-land-tax
- http://example.com/sites/001/viewing-information-in-various-file-formats
- http://example.com/sites/001/water-tap-connection

4.2 Appendix B: OWASP Top 10 Web Application Vulnerabilities

OWASP	Description
A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

OWASP	Description
A2-Broken Authentication	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3-Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A4-XML External Entities (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal SMB file shares on unpatched Windows servers, internal port scanning, remote code execution, and denial of service attacks, such as the Billion Laughs attack.
A5-Broken Access Control	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests to access functionality without proper authorization.
A6-Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
A7-Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A8-Insecure Deserialization	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A9-Using Components with	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate

OWASP	Description
Known Vulnerabilities	serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
A10-Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.