

Security Audit Report

DEENDAYAL UPADHYAYA GRAM JYOTI YOJANA

Highly Confidential



All rights reserved to Sandrock eSecurities Pvt. Ltd., 2019

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Sandrock eSecurities.

Table of Contents

1	INTRODUCTION	3
1.1	TESTING METHODOLOGY	3
1.1.1	OSSTMM.....	3
1.1.2	OWASP.....	3
1.2	REPORT AND COMPLIANCE	4
2	EXECUTIVE SUMMARY	5
2.1	SCOPE OF ACTIVITY	5
2.2	OUT-OF-SCOPE	5
2.3	VULNERABILITIES' CRITICALITY SUMMARY	5
2.4	VULNERABILITIES' TECHNICAL SUMMARY	5
2.5	TEST CASE' ARTIFACTS/SCREENSHOTS	6
2.5.1	<i>Server Misconfiguration</i>	<i>6</i>
2.5.1.1	Encrypted Communication Channel: SSL to be implemented on Production.....	6
2.5.1.2	Server Version Disclosure: Passed	6
2.5.1.3	Application Framework Version Disclosure: Passed	6
2.5.1.4	Clickjacking (X-Frame-Options): Passed	7
2.5.1.5	XSS Protection: Passed	7
2.5.1.6	MIME Sniffing: Passed.....	8
2.5.1.7	Cache Poisoning: Passed	8
2.5.1.8	Cross Origin Resource Sharing: Passed	9
2.5.1.9	Allowed HTTP Methods: Passed	9
2.5.1.10	Directory Listing: Passed	10
2.5.2	<i>User Authentication</i>	<i>10</i>
2.5.2.1	Default or Guessable User Login Credentials: Passed	10
2.5.2.2	CAPTCHA on Login: Passed	11
2.5.2.3	Strong Authentication Method: Passed	11
2.5.2.4	Password Encryption Algorithms: Passed	12
2.5.2.5	Password Autocomplete Off: Failed	12
2.5.2.6	Credentials Submission in POST Method: Passed	13
2.5.2.7	Logout Option: Passed	14
2.5.2.8	Change Password Option: Passed	14
2.5.2.9	Change Password Requires Old Password: Passed	15
2.5.2.10	Strong Password Policy: Failed	15
2.5.3	<i>Session Management.....</i>	<i>17</i>
2.5.3.1	Strong Session Management: Passed	17
2.5.3.2	Unpredictable Session ID: Passed.....	17
2.5.3.3	Session Timeout: Passed	18
2.5.3.4	Insecure Session Cookie Parameters: Passed	18
2.5.3.5	Session Fixation: Passed	18
2.5.3.6	Session Expiry on Logout: Passed.....	20
2.5.3.7	Cross Site Request Forgery: Passed	21
2.5.4	<i>Access Control.....</i>	<i>22</i>
2.5.4.1	Bypass Authentication – Admin Functionality: Passed	22
2.5.4.2	Bypass Access Control: Failed	23
2.5.5	<i>Input Data Validation</i>	<i>24</i>
2.5.5.1	Cross Site Scripting (XSS): Passed	24
2.5.5.2	SQL Injection: Passed	26
2.5.5.3	Malicious File Upload: Passed	27
2.5.6	<i>Information Disclosure.....</i>	<i>30</i>
2.5.6.1	Password Disclosure: Passed	30
2.5.6.2	Information Disclosure in HTML Source Code Comments: Passed	30
2.5.6.3	Information Disclosure in Cookie: Passed	30
2.5.6.4	Errors and Exceptions: Failed.....	30

1 Introduction

A security vulnerability assessment identifies and reports noted vulnerabilities in the web application, followed by a penetration test which attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible.

1.1 Testing Methodology

Security penetration testing and exploitation can never be an exact science where a complete list of all possible issues that should be tested can be defined. Indeed, penetration testing is only an appropriate technique for testing the security of network based resources under certain circumstances. The goal is to collect all the possible testing techniques, explain them and keep the guide updated.

When conducting a penetration testing assignment, Sandrock adopts a strong technology and process based approach supported by a well-documented methodology to identify potential security flaws in the network resources and underlying environment.

1.1.1 OSSTMM

Fact does not come from the grand leaps of discovery but rather from the small, careful steps of verification.

Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed manual of security testing and analysis which result in verified facts which provide actionable information that can measurably improve your operational security. OSSTMM is the formal methodology using which security analysis is done thoroughly, efficiently, and accurately. By undergoing OSSTMM followed testing you no longer have to rely on general best practices, anecdotal evidence, or superstitions because you will have verified information specific to your needs on which to base your security decisions.



This project is maintained by the Institute for Security and Open Methodologies (ISECOM). ISECOM is a registered non-profit organization and established in New York, USA and in Catalonia, Spain.

1.1.2 OWASP

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Their mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.



OWASP Testing Guide describes in details both the general Testing Framework and the techniques required to implement the framework in practice.

This guide helps organizations test their web applications in order to build reliable and secure software, rather than simply highlighting areas of weakness, although the latter is certainly a byproduct of many of OWASP's guides and checklists.

Adherence to industry standards such as OWASP, customized tests based on technology and business logic, skilled and certified security engineers, risk assessment on the vulnerabilities found, scoring system based on CVSS (Common Vulnerability Scoring System) make us different from the other vendors in this space.

Sandrock eSecurities was tasked with following methodical approach in obtaining access to the objective goals.

1. Information Gathering

- Looking for information on publicly available resources
- Inserting technical information provided by the organization
- Non-intrusive scan to determine systems, servers and services

2. Planning and Analysis

- Analyzing the possible risks and vulnerabilities
- Planning for a High Level Intense Penetration Test
- Designing the overall testing approach

3. **Vulnerability Detection and Identification**
 - Searching for vulnerabilities on the resources
 - Enumerating known flaws, loopholes and mis-configurations
 - Manually probing the target, looking for vulnerabilities
4. **Attack or Active Penetration**
 - Customizing and using readymade exploits for a few known vulnerabilities
 - Building exploits for uncommon specific security loophole
 - Testing the exploits against vulnerabilities
 - Escalating the privileges to exploit higher roles, systems and services
5. **Reporting**
 - Executive Report for Top Management
 - Comprehensive Technical Report for Technical Personnel with solutions

1.2 Report and Compliance

The penetration testing report includes the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, etc
- Any additional items that were not included

This report can be used to support the regulatory and compliance requirements of:

- CERT-IN
- ISO 27001 ISMS
- PCI-DSS
- HIPAA
- GLBA

2 Executive Summary

Sandrock eSecurities performed a security audit on the in-scope web application.

Date of Penetration Test: 3rd June to 17th June 2019

Number of Technical Personnel Involved: 1

2.1 Scope of Activity

- Black box security audit of DEENDAYAL UPADHYAYA GRAM JYOTI YOJANA website hosted at <http://49.50.107.91/ddugjy/> and the custom CMS <http://49.50.107.91/ddugjy/admin>

2.2 Out-of-scope

- Security audit of the application's hosting infrastructure (servers, network, database, etc).
- Security audit of the source code of the application.

2.3 Vulnerabilities' Criticality Summary

Total	Critical	High	Medium	Low	Remarks
13	1	5	7	0	NA

2.4 Vulnerabilities' Technical Summary

S#	Vulnerability	Rating	Status
1	Strong Password Policy	Medium	Failed
2	Default or Guessable User Login Credentials	High	Fixed
3	Password Autocomplete Off	Medium	Failed
4	Change Password Option	Medium	Fixed
5	Change Password Requires Old Password	Medium	Fixed
6	Insecure Session Cookie Parameters	Medium	Fixed
7	Session Fixation	Medium	Fixed
8	Session Expiry on Logout	Medium	Fixed
9	Cross Site Request Forgery	High	Fixed
10	Bypass Access Control	High	Failed
11	Cross Site Scripting (XSS)	High	Fixed
12	Malicious File Upload	High	Fixed
13	Errors and Exceptions	Medium	Failed

2.5 Test Case' Artifacts/Screenshots

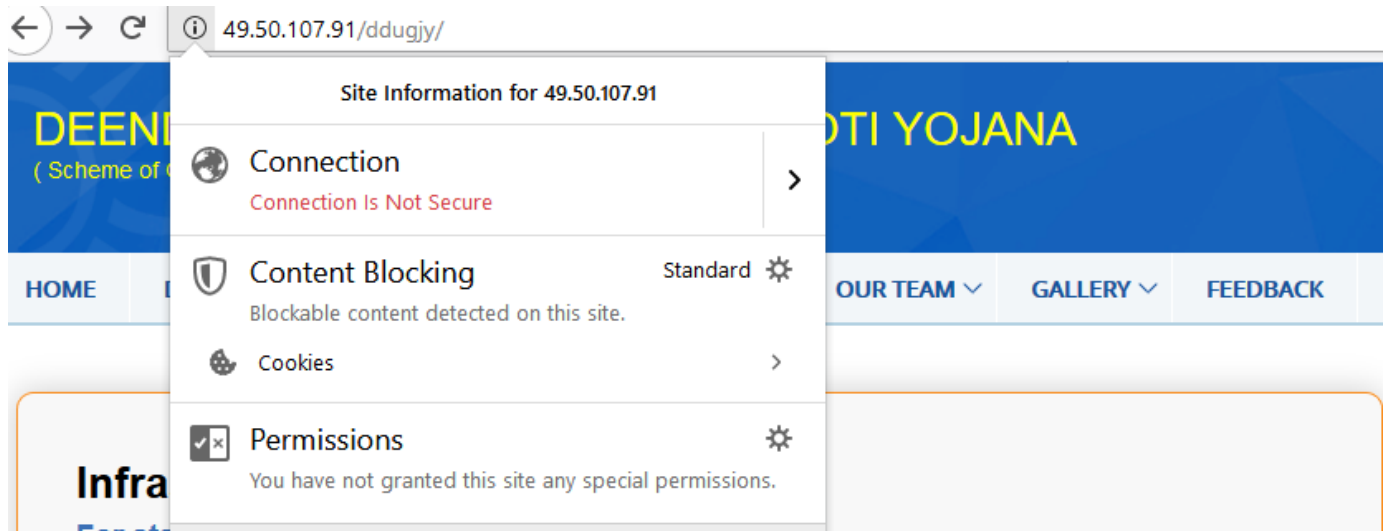
2.5.1 Server Misconfiguration

2.5.1.1 Encrypted Communication Channel: **SSL to be implemented on Production**

Scan Round 1

Application does not use a valid SSL/TLS certificate.

Fix: Kindly implement a valid SSL certificate.



2.5.1.2 Server Version Disclosure: **Passed**

Scan Round 1

Server does not disclose the web server version information.

Host	Method	URL	Params	Status
http://49.50.107.91	GET	/ddugjy/		200

Request	Response
---------	----------

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------


```
HTTP/1.1 200 OK
Date: Mon, 03 Jun 2019 14:13:25 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46349
```

2.5.1.3 Application Framework Version Disclosure: **Passed**

Scan Round 1

Application does not disclose the application framework information. This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of technology used.

Host	Method	URL	Params	Status
http://49.50.107.91	GET	/ddugjy/		200

Request	Response
---------	----------

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------


```

HTTP/1.1 200 OK
Date: Mon, 03 Jun 2019 14:13:25 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46349

```

2.5.1.4 Clickjacking (X-Frame-Options): Passed

Scan Round 1

Server responds with "X-Frame-Options: SAMEORIGIN" header.

Host	Method	URL	Params	Status
http://49.50.107.91	GET	/ddugjy/		200

Request	Response
---------	----------

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------


```

HTTP/1.1 200 OK
Date: Mon, 03 Jun 2019 14:13:25 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46349

```

2.5.1.5 XSS Protection: Passed

Scan Round 1

Server responds with "X-XSS-Protection" response header.

Host	Method	URL	Params	Status
http://49.50.107.91	GET	/ddugjy/		200

Request	Response
---------	----------

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------


```

HTTP/1.1 200 OK
Date: Mon, 03 Jun 2019 14:13:25 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46349

```

2.5.1.6 MIME Sniffing: Passed

Scan Round 1

Server responds with "X-Content-Type-Options: nosniff" header.

Host	Method	URL	Params	Status
http://49.50.107.91	GET	/ddugjy/		200

Request	Response
---------	----------

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------


```

HTTP/1.1 200 OK
Date: Mon, 03 Jun 2019 14:13:25 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46349

```

2.5.1.7 Cache Poisoning: Passed

Scan Round 1

Server does not respond with "Cache-Control: max-age=0, must-revalidate, no-cache, no-store" header.

Host	Method	URL	Params	Status
http://49.50.107.91	GET	/ddugjy/		200

Request	Response
---------	----------

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------


```

HTTP/1.1 200 OK
Date: Mon, 03 Jun 2019 14:13:25 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46349

```

2.5.1.8 Cross Origin Resource Sharing: **Passed**

Scan Round 1

Application does not allow all origins for resource sharing.

Host	Method	URL	Params	Status
http://49.50.107.91	GET	/ddugjy/		200

Request	Response
---------	----------

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------


```

HTTP/1.1 200 OK
Date: Mon, 03 Jun 2019 14:13:25 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46349

```

2.5.1.9 Allowed HTTP Methods: **Passed**

Scan Round 1

HTTP OPTIONS method is not enabled on this web server. The OPTIONS method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI. The OPTIONS method may expose sensitive information that may help malicious user to prepare more advanced attacks.

Request

Raw

Params

Headers

Hex

```

OPTIONS /ddugjy/ HTTP/1.1
Host: 49.50.107.91
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0)
Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=5rk0h8gmaggit5v5jj3846hrv71
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

Response

Raw

Headers

Hex

HTML

Render

```

HTTP/1.1 405 Method Not Allowed
Date: Mon, 03 Jun 2019 14:19:41 GMT
Server: Apache
Allow:
Content-Length: 232
Connection: close
Content-Type: text/html; charset=iso-8859-1

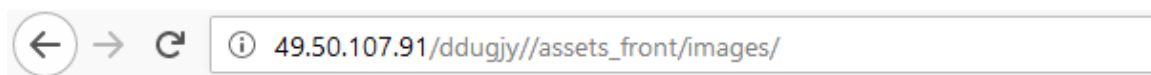
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>405 Method Not Allowed</title>
</head><body>
<h1>Method Not Allowed</h1>
<p>The requested method OPTIONS is not allowed for the URL /ddugjy/.</p>
</body></html>

```

2.5.1.10 Directory Listing: Passed

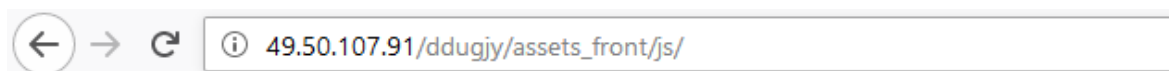
Scan Round 1

Directory listing is restricted. Application gives error when tried to access directories directly.



Forbidden

You don't have permission to access /ddugjy//assets_front/images/ on this server.



Forbidden

You don't have permission to access /ddugjy/assets_front/js/ on this server.

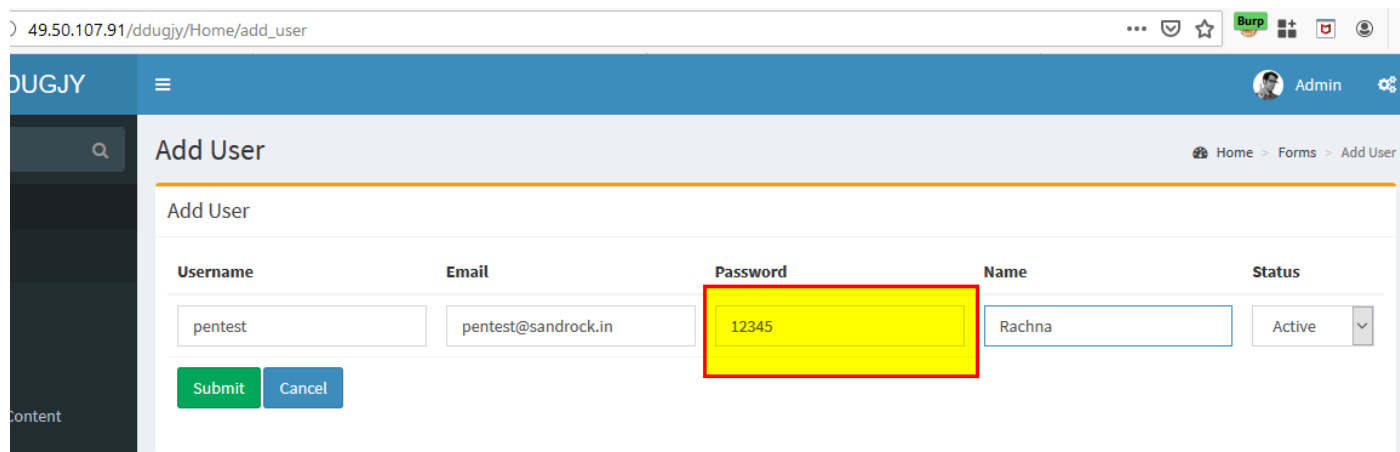
2.5.2 User Authentication

2.5.2.1 Default or Guessable User Login Credentials: Passed

Scan Round 1

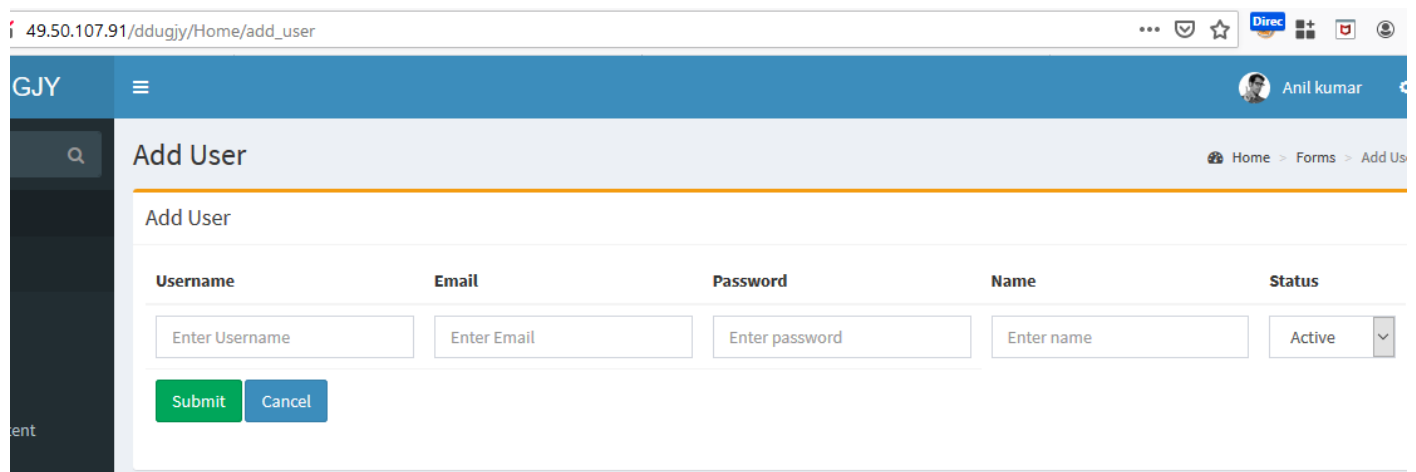
Application sets same default password that is "12345" for multiple users.

Fix: Do not set default password for users. Ask user to change the password during first login or send them email to reset their password.



Scan Round 1

Application does not set any default password while creating user.
Admin needs to enter strong password while creating new user.



The screenshot shows a web browser window with the URL `49.50.107.91/ddugjy/Home/add_user`. The page has a blue header with the logo 'GJY' and a user profile 'Anil kumar'. The main content area is titled 'Add User' and contains a form with the following fields:

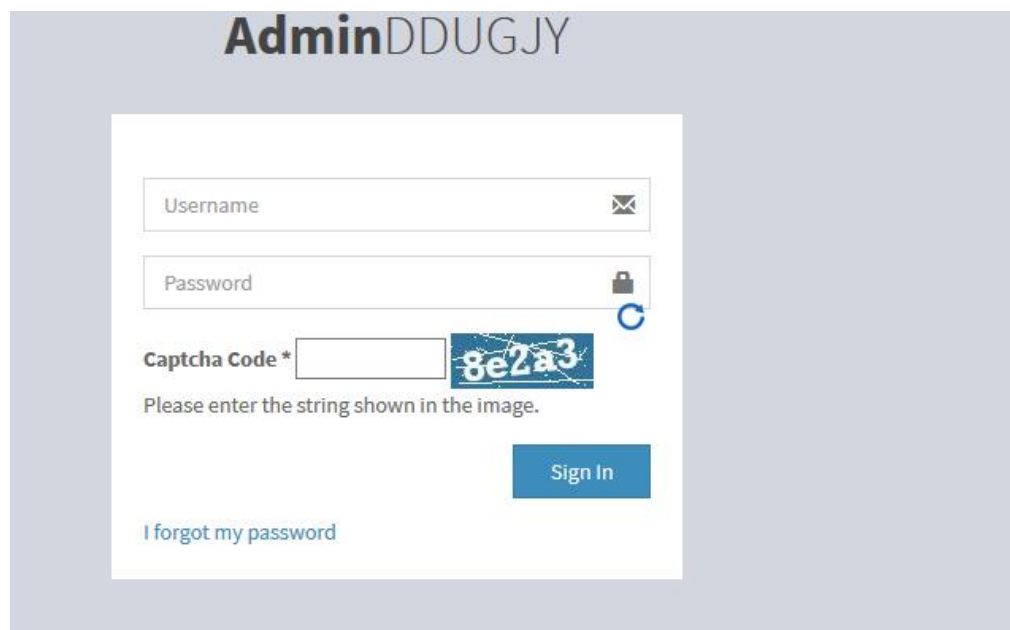
Username	Email	Password	Name	Status
<input type="text" value="Enter Username"/>	<input type="text" value="Enter Email"/>	<input type="text" value="Enter password"/>	<input type="text" value="Enter name"/>	<input type="text" value="Active"/>

Below the form are two buttons: 'Submit' (green) and 'Cancel' (blue).

2.5.2.2 CAPTCHA on Login: **Passed**

Scan Round 1

Application enforces CAPTCHA on user login form.



The screenshot shows the 'AdminDDUGJY' login page. The form includes the following fields:

- Username (with an envelope icon)
- Password (with a lock icon)
- Captcha Code * (with a refresh icon)

The CAPTCHA image displays the string '8e2a3'. Below the CAPTCHA field, there is a text prompt: 'Please enter the string shown in the image.' A 'Sign In' button is located at the bottom right of the form. A link 'I forgot my password' is at the bottom left.

2.5.2.3 Strong Authentication Method: **Passed**

Scan Round 1

Application uses form-based authentication for login form.

2.5.2.4 Password Encryption Algorithms: **Passed**

Scan Round 1

Application does not use MD5 hashing algorithm without salting to store passwords.
It uses strong password encryption algorithm with dynamic salting to store the passwords.

324	http://49.50.107.91	POST	/ddugjy/Login/process	✓	303	1025	HTM
-----	---------------------	------	-----------------------	---	-----	------	-----

Request

Response

Raw

Params

Headers

Hex

```

POST /ddugjy/Login/process HTTP/1.1
Host: 49.50.107.91
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://49.50.107.91/ddugjy/admin
Content-Type: application/x-www-form-urlencoded
Content-Length: 102
Connection: close
Cookie: PHPSESSID=5rk0h8gmqgit5v5jj3846hrv71; ci_session=0ba71bm19n9e6t45chs3eltdvk
Upgrade-Insecure-Requests: 1

username=admin&password=7676aaafb027c825bd9abab78b234070e702752f625b752e55e55b48e607e358&captcha=8e2a3

```

2.5.2.5 Password Autocomplete Off: **Failed**

Scan Round 1

Autocomplete is not set to OFF on password fields of Change Password and Login Forms.

Fix: Set "autocomplete=OFF" on all form password fields including login forms and change password forms.

```

</head>
<body class="hold-transition login-page">
  <div class="login-box">
    <div class="login-logo"></div>
    <!--/.login-logo-->
    <div class="login-box-body">
      <p class="login-box-msg"></p>
      <form id="myform" class="email" action="http://49.50.107.91/ddugjy/Login/process" method="post" accept-charset="utf-8">
        <div class="form-group has-feedback"></div>
        <div class="form-group has-feedback">
          <input id="password" class="form-control" type="password" name="password" value="" placeholder="Password">
          <span class="glyphicon glyphicon-lock form-control-feedback"></span>
        </div>
        <div class="form-group has-feedback"></div>
        <div class="row"></div>
      </form>
    </div>
  </body>

```

Scan Round 2

Autocomplete is set to OFF on password fields of Login Forms but on the password fields of Change Password or Reset Password or Add User forms.

Fix: Please add Autocomplete OFF for all password fields.

The screenshot displays the AdminDDUGJY login interface. It includes a Username field, a Password field, and a Captcha Code field with a visual captcha image showing the string '29bae'. Below the interface, the browser's DOM inspector is open, showing the HTML structure. The password input field is selected, and its attributes are visible, including 'autocomplete="off"', which is highlighted with a red box.

2.5.2.6 Credentials Submission in POST Method: Passed

Scan Round 1

Application submits the user login credentials in POST.

319	http://beekp.idaminfra.com	POST	/Admin	✓	302	557	HTML
-----	----------------------------	------	--------	---	-----	-----	------

Request

Response

Raw

Params

Headers

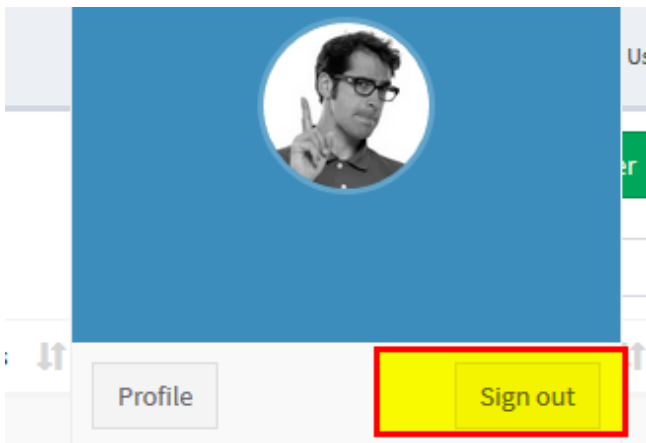
Hex

POST /Admin HTTP/1.1
Host: beekp.idaminfra.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://beekp.idaminfra.com/Admin
Content-Type: application/x-www-form-urlencoded
Content-Length: 617
Connection: close
Cookie: ASP.NET_SessionId=avsxonyqjlpgrlex2rgcbur2;
__RequestVerificationToken=c104YqBvyp0h0hETBFY3sfe2EhKpZitLcu9fNqWq5AriUNjrQy4UcDtEypCW7m07ffXyPmmXlvRKw89KvjKavGa_ts5tcWF
AntiFixationCookie=ad192472-274c-4a92-95c9-71aa28726bb5
Upgrade-Insecure-Requests: 1

2.5.2.7 Logout Option: **Passed**

Scan Round 1

Application provides logout option to user.



2.5.2.8 Change Password Option: **Passed**

Scan Round 1

Application does not provide change password option to user.

Fix: Implement Change Password for Admin/Users.

Scan Round 2

Application implements change password option to user.

DDUGJY

49.50.107.91/ddugjy/Home/reserpassword

User 1

Rachna

Home > Forms > Add

Add User

Reset Password
Note:(Password should be alphanumeric , 8 characters long)

Username	Old Password	Password	Confirm Password
pentest	Enter Old password	Enter password	Enter password

Submit Cancel

2.5.2.9 Change Password Requires Old Password: **Passed**

Scan Round 1

Application does not provide change password option to user.

Fix: Implement Change Password for Admin/Users which confirms user's existing password before setting the new password.

Scan Round 2

Application implements change password option for Admin/Users which confirms user's existing password before setting the new password.

DDUGJY

49.50.107.91/ddugjy/Home/reserpassword

User 1

Rachna

Home > Forms > Add

Add User

Reset Password
Note:(Password should be alphanumeric , 8 characters long)

Username	Old Password	Password	Confirm Password
pentest	Enter Old password	Enter password	Enter password

Submit Cancel

2.5.2.10 Strong Password Policy: **Failed**

Scan Round 1

Application does not provide change password option to user. So we cant test Strong Password Implementation.

Scan Round 2

Application provide change password option to user where strong Password is implemented at server side. Strong password is also implemented at Reset Password form. But strong password is not implemented at Add User Form.

Fix: Implement Strong password at Add User Form also.

Reset Password

49.50.107.91/ddugjy/Home/reserpassword/2

User 2

DDUGJY

Add User

Home > Forms > Add Us

✓ Password should be alphanumeric , 8 characters long !

Reset Password
Note:(Password should be alphanumeric , 8 characters long)

Username	Password	Confirm Password
admin1	Enter password	Enter password

Submit Cancel

Change Password

49.50.107.91/ddugjy/Home/reserpassword/4

User 1

DDUGJY

Add User

Home > Forms > Add User

✓ Password should be alphanumeric , 8 characters long !

Reset Password
Note:(Password should be alphanumeric , 8 characters long)

Username	Old Password	Password	Confirm Password
pentest	Enter Old password	Enter password	Enter password

Submit Cancel

Tried to intercept the request and changed the new password to "123" from "admin123456". The request was not processed successfully. We got the response as below.

1321 http://49.50.107.91 POST /ddugjy/Home/updatepassword

Original request Edited request Response

Raw Params Headers Hex

POST request to /ddugjy/Home/updatepassword

Type	Name	Value
Cookie	PHPSESSID	mfilmbid72dojmukqg9kage2u
Cookie	csrf_cookie_name	49e41ebf6ec5f659a3072f93ed42e908
Body	csrf_test_name	49e41ebf6ec5f659a3072f93ed42e908
Body	user_id	4
Body	username	pentest
Body	old_password	admin12345
Body	password	123
Body	confirmpassword	123
Body	submit	Submit

1321 http://49.50.107.91 POST /ddugjy/Home/updatepassword ✓

Original request Edited request Response

Raw Headers Hex

HTTP/1.1 303 See Other

Date: Mon, 17 Jun 2019 07:08:44 GMT

Server: Apache

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Set-Cookie: PHPSESSID=8dijsvfkroprdre2dcj7cjqqbjr; path=/
Set-Cookie: csrf_cookie_name=24278a714ef3d58ca19fe947ea84e6b8; expires=Mon, 1
Set-Cookie: ci_session=6nkfd2jqm6vsp2nmh81ebb8a0; expires=Mon, 17-Jun-2019 0
Location: http://49.50.107.91/ddugjy/Home/reserpassword/4

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

X-Frame-Options: DENY

Content-Length: 3

Connection: close

Content-Type: text/html; charset=UTF-8

2.5.3 Session Management

2.5.3.1 Strong Session Management: Passed

Scan Round 1

Application uses cookie-based session management.

GET request to /ddugjy/Login

Type	Name	Value
Cookie	PHPSESSID	3g9vna4jb0uau393n6froaejfl

2.5.3.2 Unpredictable Session ID: Passed

Scan Round 1

Application generates unpredictable session cookies.

GET request to /ddugjy/Login		
Type	Name	Value
Cookie	PHPSESSID	3g9vna4jb0uau393n6froaejfl

2.5.3.3 Session Timeout: **Passed**

Scan Round 1

Application expires the session from the server side, the previous session was not active after 24 hours of user inactivity.

2.5.3.4 Insecure Session Cookie Parameters: **Passed**

Scan Round 1

Application has not set the HTTPOnly flag and the SECURE parameter to TRUE on session cookies.
Fix: Set HTTPOnly and SECURE parameter to TRUE.

```

▼ PHPSESSID: "3g9vna4jb0uau393n6froaejfl"
  CreationTime: "Mon, 03 Jun 2019 14:31:56 GMT"
  Domain: "49.50.107.91"
  Expires: "Session"
  HostOnly: true
  HttpOnly: false
  LastAccessed: "Mon, 03 Jun 2019 14:34:05 GMT"
  Path: "/"
  Secure: false
  sameSite: "Unset"

```

Scan Round 2

Application has set the HTTPOnly flag to TRUE. Please make sure to set the SECURE parameter to TRUE on session cookies once application is deployed on production server with SSL implementation.

```

▼ ci_session: "bvtvd5o6qq6b17o63i9drjnti"
  CreationTime: "Mon, 17 Jun 2019 07:15:38 GMT"
  Domain: "49.50.107.91"
  Expires: "Mon, 17 Jun 2019 09:15:38 GMT"
  HostOnly: true
  HttpOnly: true
  LastAccessed: "Mon, 17 Jun 2019 07:17:39 GMT"
  Path: "/"
  Secure: false
  sameSite: "Unset"

```

2.5.3.5 Session Fixation: **Passed**

Scan Round 1

Application neither creates any additional session token as Authentication token nor regenerate the default phpsessionid on successful login.

Fix: Application should either create an additional token or regenerate the default session id on successful login.

Pre – Login

```

GET /ddugjy/Login HTTP/1.1
Host: 49.50.107.91
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://49.50.107.91/ddugjy/Home/mngusers
Connection: close
Cookie: PHPSESSID=3g9vna4jb0uau393n6froaejfl
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

Post Login

```

GET /ddugjy/Home/mngusers HTTP/1.1
Host: 49.50.107.91
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://49.50.107.91/ddugjy/Home
Connection: close
Cookie: PHPSESSID=3g9vna4jb0uau393n6froaejfl
Upgrade-Insecure-Requests: 1

```

Scan Round 2

Application regenerate the default phpsessionid on successful login.

Pre – Login

1377	http://49.50.107.91	GET	/ddugjy/Login	200	5695
------	---------------------	-----	---------------	-----	------

Request

Response

Raw

Headers

Hex

HTML

Render

```

HTTP/1.1 200 OK
Date: Mon, 17 Jun 2019 07:17:23 GMT
Server: Apache
Set-Cookie: PHPSESSID=3tnllpdp4epiqbp6gljcd9r3m; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=r3jpb8bmluqb4ue6mr0f685i9tpi; path=/
Set-Cookie: csrf_cookie_name=a4aefc8df1597113414653e91edeb2c9; expires=Mon, 17-Jun-2019 09:17:23 GMT;
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Content-Length: 5093
Connection: close
Content-Type: text/html; charset=UTF-8

```

Post – Login

Raw	Params	Headers	Hex
<pre> GET /ddugjy/Home HTTP/1.1 Host: 49.50.107.91 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://49.50.107.91/ddugjy/Login Connection: close Cookie: PHPSESSID=c69ian5e4msugbgpj49h0tibpl; csrf_cookie_name=5182242e5e34bff095981736ba0e5399 Upgrade-Insecure-Requests: 1 </pre>			

2.5.3.6 Session Expiry on Logout: **Passed**

Scan Round 1

Application does not remove the session data from the server-side on logout. The session cookie is also changed after logout.

Fix: Session data should be changed after logout.

Pre-Logout

```

GET /ddugjy/Home/mngusers HTTP/1.1
Host: 49.50.107.91
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://49.50.107.91/ddugjy/Home
Connection: close
Cookie: PHPSESSID=3g9vna4jb0uau393n6froaejfl
Upgrade-Insecure-Requests: 1

```

Post-Logout

```

GET /ddugjy/Login HTTP/1.1
Host: 49.50.107.91
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://49.50.107.91/ddugjy/Home
Connection: close
Cookie: PHPSESSID=3g9vna4jb0uau393n6froaejfl
Upgrade-Insecure-Requests: 1

```

Scan Round 2

Application regenerate the session data from the server-side on logout. The session cookie is also changed after logout.

Pre-Logout

```
GET /ddugjy/Login/logout HTTP/1.1
Host: 49.50.107.91
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://49.50.107.91/ddugjy/Home/mngpage
Connection: close
Cookie: PHPSESSID=0k7g63mqt37ess4976lsjbnqc6; csrf_cookie_name=5182242e5e34bfff095981736ba0e5399
Upgrade-Insecure-Requests: 1
```

Post-Logout

```
GET /ddugjy/Login HTTP/1.1
Host: 49.50.107.91
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://49.50.107.91/ddugjy/Home/mngpage
Connection: close
Cookie: PHPSESSID=incs23b38ssrf4o0pt84d0q06h; csrf_cookie_name=5182242e5e34bfff095981736ba0e5399
Upgrade-Insecure-Requests: 1
```

2.5.3.7 Cross Site Request Forgery: Passed

Scan Round 1

Application does not use hidden CSRF tokens to protect from CSRF attacks.

Fix: Implement hidden CSRF token to protect from CSRF attacks for each request.

POST request to /ddugjy/Home/insert_user

Type	Name	Value
Cookie	PHPSESSID	djlellss31gqpdb6j3ugdb9jah
Body	user_id	1
Body	username	admin
Body	email	anil.kumar@cyfuture.com
Body	name	Admin
Body	status	1
Body	submit	Submit

POST request to /ddugjy/Home/insert_topMenu

Type	Name	Value
Cookie	PHPSESSID	djlellss31gqpdb6j3ugdb9jah
Body	menu_id	1
Body	menu_ename	Home1
Body	menu_section	1
Body	menu	1
Body	menutype	1
Body	url	ss
Body	status	1
Body	submit	Submit

Scan Round 2

Application implements and validates CSRF tokens for each request to protect from CSRF attacks.

Request

Raw Params Headers Hex

POST request to /ddugjy/Home/insert_topMenu

Type	Name	Value
Cookie	PHPSESSID	4kjf5ln1jcb771a11218f6b
Cookie	csrf_cookie_name	3b2eeaaaa5f851d37b70d52142c1c201
Body	csrf_test_name	3b2eeaaaa5f851d37b70d52142c1c20111
Body	menu_id	1
Body	menu_ename	Home1
Body	menu_section	1
Body	menu	1
Body	menutype	1
Body	url	ss
Body	status	1
Body	submit	Submit

Response

Raw Headers Hex HTML Render

HTTP/1.1 403 Forbidden

Date: Mon, 17 Jun 2019 07:24:38 GMT

Server: Apache

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Set-Cookie: PHPSESSID=1918j5k28hangqrblimdc7k8; path=/

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

X-Frame-Options: DENY

Content-Length: 1131

Connection: close

Content-Type: text/html; charset=UTF-8

```
<!DOCTYPE html>
<html lang="en">
<head>
```

Changed the csrf token. Got forbidden message

Request

Raw Params Headers Hex

POST request to /ddugjy/Home/insert_user

Type	Name	Value
Cookie	PHPSESSID	9j33deid49mslv99gm4b62jfu6
Cookie	csrf_cookie_name	5/5777f189aa77f80d80122ebd4b30b1
Body	csrf_test_name	575777f189aa77f80d80122ebd4b30b1111
Body	user_id	1
Body	username	admin
Body	email	anilkumar@cyfuture.com
Body	name	Anil kumar
Body	status	1
Body	submit	Submit

Response

Raw Headers Hex HTML Render

HTTP/1.1 403 Forbidden

Date: Mon, 17 Jun 2019 07:26:21 GMT

Server: Apache

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Set-Cookie: PHPSESSID=6pd832oad0ag9tpjibin4s6g0c; path=/

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

X-Frame-Options: DENY

Content-Length: 1131

Connection: close

Content-Type: text/html; charset=UTF-8

```
<!DOCTYPE html>
```

2.5.4 Access Control

2.5.4.1 Bypass Authentication - Admin Functionality: Passed

Scan Round 1

Application sends 302 Found Object Moved when trying to access admin user's internal pages without login.

Intercepted the request and changed the session Id.

Request

Raw Params Headers Hex

GET /ddugjy/Home/topmenu HTTP/1.1

Host: 49.50.107.91

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://49.50.107.91/ddugjy/Home/mngusers

Connection: close

Cookie: PHPSESSID=4j1e1lss3lgqpdb6j3ugdb6jal

Upgrade-Insecure-Requests: 1

Response

Raw Headers Hex

HTTP/1.1 307 Temporary Redirect

Date: Tue, 04 Jun 2019 05:23:54 GMT

Server: Apache

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Location: http://49.50.107.91/ddugjy/Login

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

X-Frame-Options: DENY

Content-Length: 3

Connection: close

Content-Type: text/html; charset=UTF-8

Changed the session id from the logged in one

Request	Response
<div>Raw Params Headers Hex</div> <pre> GET /ddugjy/Home/mngusers HTTP/1.1 Host: 49.50.107.91 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://49.50.107.91/ddugjy/Home/add_user/1 Connection: close Cookie: PHPSESSID=djle1lss3lqgqdb6j3ugdb9jal Upgrade-Insecure-Requests: 1 </pre>	<div>Raw Headers Hex</div> <pre> HTTP/1.1 307 Temporary Redirect Date: Tue, 04 Jun 2019 05:25:03 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Location: http://49.50.107.91/ddugjy/Login X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Frame-Options: DENY Content-Length: 3 Connection: close Content-Type: text/html; charset=UTF-8 </pre>

2.5.4.2 Bypass Access Control: **Failed**

Scan Round 1

Application allows users to access information and perform actions outside their designated roles.
Fix: Please check access control at each request.

Example 1

Logged in with user "Pentest". User "Pentest" do not have the permission to view "Manage User" Page. is not allowed to change the email address and password for User "Admin". But on entering the Manage User URL directly in the browser, Pentest is able to access the user details. "Pentest" is also able to change password for any other admin.

On entering the Manage User URL directly, Rachna is able to access the page and also can change the password for all other admin user.

Rachna does not access to Menu "Manage User". There is no such menu present.

Sr No.	Username	Name	Email	Login time	status	Action
1	admin	Admin	anil.kumar@cyfuture.com	2019-06-04 10:49:51	Active	Edit Set Permission Reset Password
2	admin1	admin1	anil.kumar10020@gmail.com	2019-03-18 16:40:26	Active	Edit Set Permission Reset Password
3	User1	user1	user@gmail.com	2019-03-18 16:52:00	Active	Edit Set Permission Reset Password
4	pentest	Rachna	pentest@sandrock.in	2019-06-04 11:01:03	Active	Edit Set Permission Reset Password

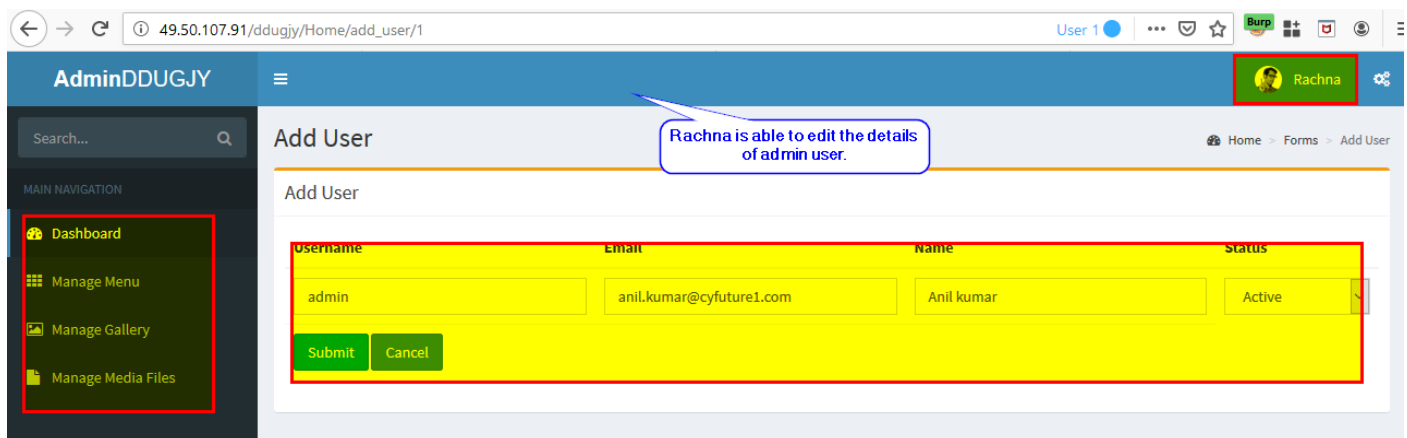
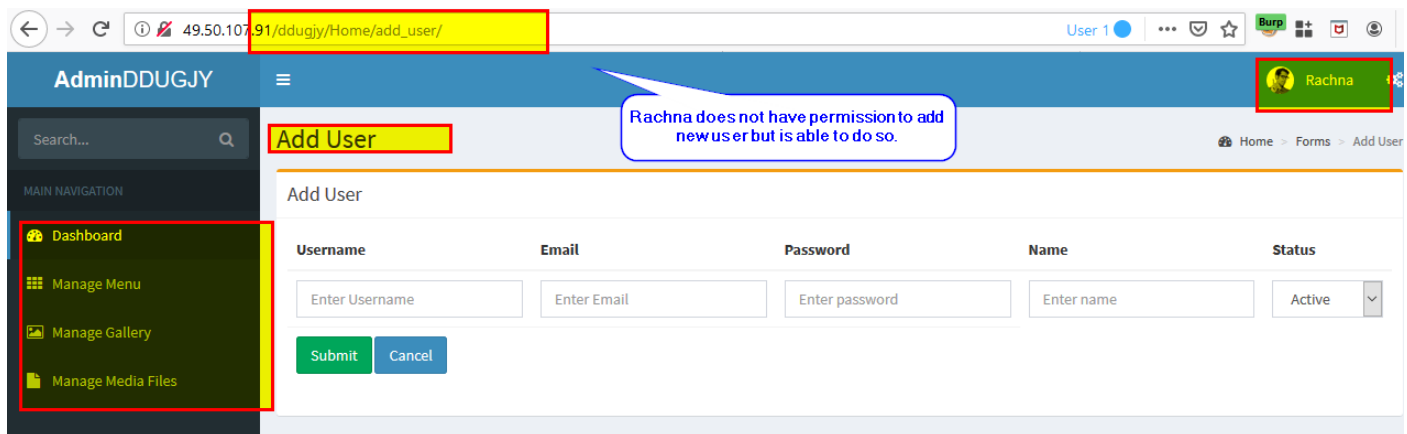
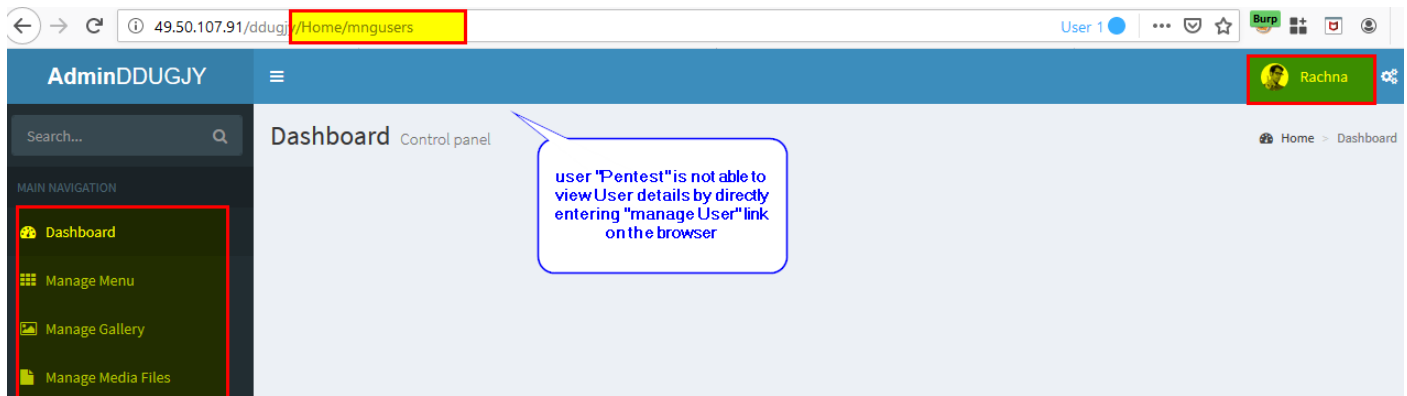
Showing 1 to 4 of 4 entries

Scan Round 2

Application allows users to access information and perform actions outside their designated roles.

Example 1

Logged in with user "Pentest". User "Pentest" do not have the permission to view "Manage User" Page and add new user or edit/update details/password for other users or Admin. On entering the Manage User URL directly in the browser, Pentest is not able to access the user details. But on entering add user or edit user or reset password for other users link directly in the browser, "Pentest" is able to perform all these actions.



2.5.5 Input Data Validation

2.5.5.1 Cross Site Scripting (XSS): **Passed**

Scan Round 1

Application does not validate input data or encode output data to protect from XSS attacks.

Fix: Validate input data or encode output data to protect from XSS attacks as per Codeigniter

49.50.107.91/ddugjy/Home/add_team/MTk=

DDUGJY Admin

Update Team

Update Team

Team Category*
REC (Nodal Agency)

Twitter Handle
https://twitter.com/RameshPV2010

Name (English)
Mr. P.V. Ramesh, (IAS) **<script>alert(123)</script>**

Designation Name (English)
Chairman & Managing Director, REC Ltd.

Image
Browse... No file selected.

Description(English)*

49.50.107.91/ddugjy/Home/mngourteam

DDUGJY

Manage Team list Team

Team Member Updated Successfully

Team List

Sr No.	Team Type	Designation	Image	Twiter	Status
1	REC (Nodal Agency)				

123

OK

Scan Round 2

Application validates input data or encode output data to protect from XSS attacks.

49.50.107.91/ddugjy/Home/add_team/MjM=

DDUGJY User 2

Update Team

Update Team

Team Category*
Ministry of Power

Twitter Handle
test

Name (English)
<script>alert(123)</script>

Designation Name (English)
test

Image
Browse... No file select

49.50.107.91/ddugjy/Home/add_team/MjM= User 2

DDUGJY

Update Team

Update Team

Team Category* Ministry of Power

Twitter Handle test

Name (English) [removed]alert(123)[removed]

Designation Name (English) test

Image Browse... No file selected.

Description(English)*

Rich text editor toolbar: Bold, Italic, Underline, Text Color, Background Color, Bulleted List, Numbered List, Indent, Outdent, Link, Unlink, Source, Styles, Format, Help.

2.5.5.2 SQL Injection: Passed

Scan Round 1

Application validates input data to protect from SQL injection attacks.

Request

Raw Params Headers Hex

POST request to /ddugjy/Home/insert_user

Type	Name	Value
Cookie	PHPSESSID	djellss31gqpd63u...
Cookie	ci_session	oe5nejcud4144iej89...
Body	user_id	1
Body	username	admin
Body	email	anil.kumar@cyfutur...
Body	name	Admin
Body	status	1
Body	submit	Submit

Response

Raw Headers Hex

HTTP/1.1 303 See Other

Date: Tue, 04 Jun 2019 08:49:44 GMT

Server: Apache

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Location: http://49.50.107.91/ddugjy/Home/mngusers

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

X-Frame-Options: DENY

Content-Length: 3

Connection: close

Content-Type: text/html; charset=UTF-8

AdminDDUGJY

Captcha Code * a9e58

Please enter the string shown in the image.

Sign In

[I forgot my password](#)

2.5.5.3 Malicious File Upload: **Passed**

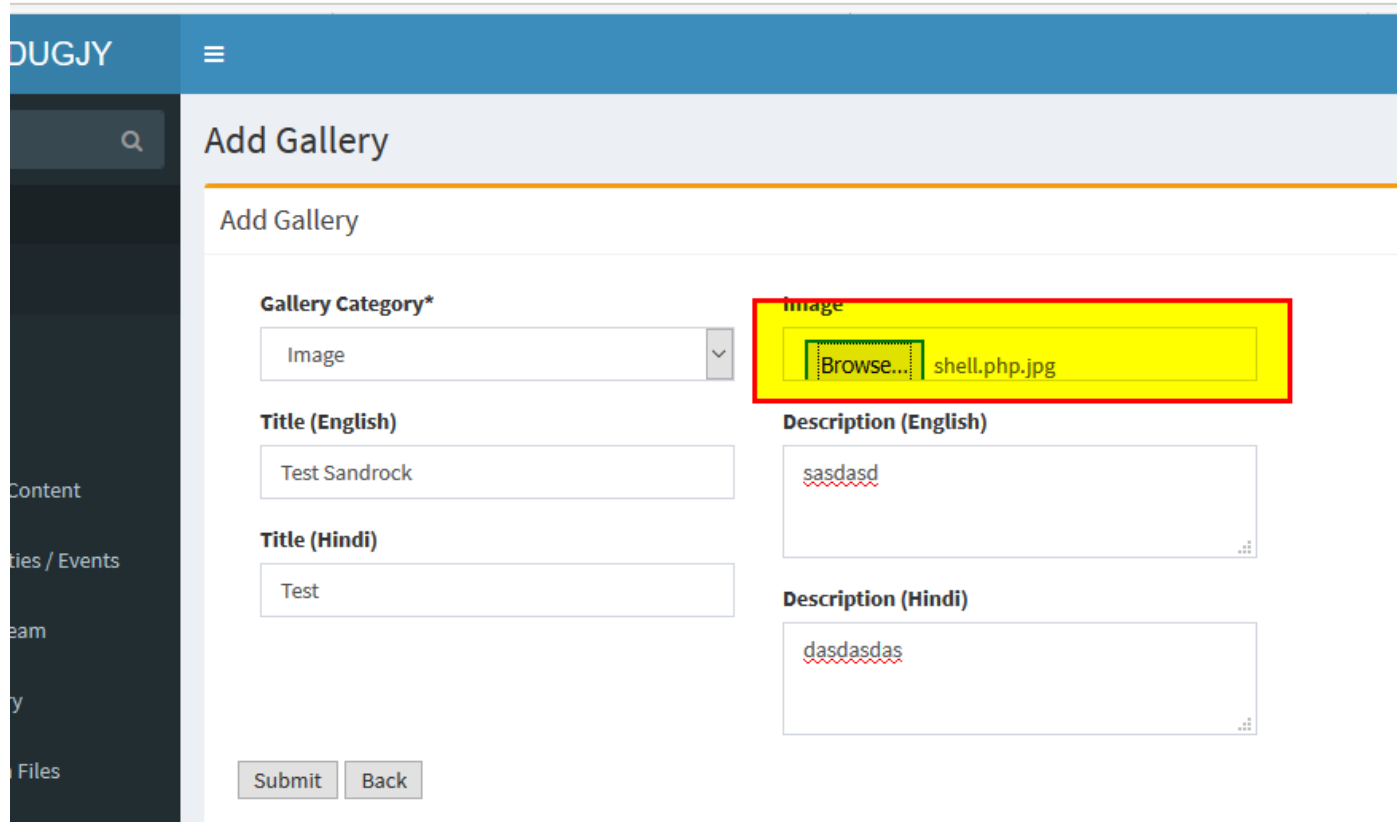
Scan Round 1

Application does not validate file input data and allows malicious files to be uploaded.

Fix: Validate the input data file before uploading to the application server.

Trying to upload a php file by changing the extension to jpg.

49.50.107.91/ddugjy/Home/add_gallery



Changed the extension of the file back to php by intercepting the request.

```
POST /ddugjy/Home/insert_gallery HTTP/1.1
Host: 49.50.107.91
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://49.50.107.91/ddugjy/Home/add_gallery
Content-Type: multipart/form-data; boundary=-----167041816121086
Content-Length: 7790
Connection: close
Cookie: PHPSESSID=djle1lss3lgqpd6j3ugdb9jah; ci_session=oe5nejcud4l44iej89lv8fvu3t
Upgrade-Insecure-Requests: 1

-----167041816121086
Content-Disposition: form-data; name="gallery_id"

-----167041816121086
Content-Disposition: form-data; name="gallery_type"

1
-----167041816121086
Content-Disposition: form-data; name="file"; filename="shell.jpg.php"
Content-Type: image/jpeg
```

Changed the file
extension to php

Application allows the malicious file to be uploaded.

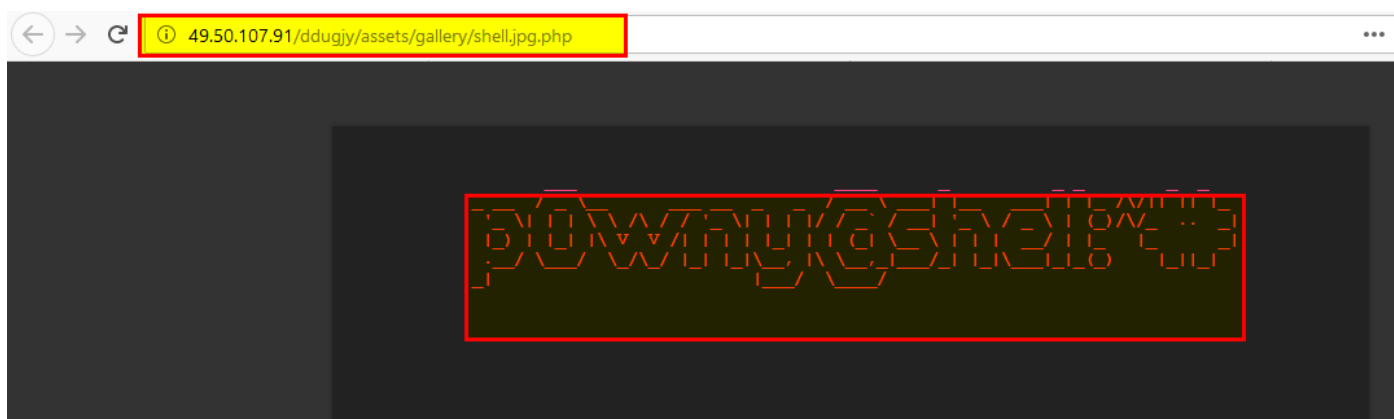
Name	Value
GET	/ddugjy/assets/gallery/shell.jpg.php HTTP/1.1
Host	49.50.107.91
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Referer	http://49.50.107.91/ddugjy/Home/mnngallery
Connection	close
Cookie	PHPSESSID=djlelss31gqpdb6j3ugdb9jah; ci_session=oe5nejcud4144iej891v8fvu3t
Upgrade-Insecure-Requests	1

Shell was executed successfully on the server.

49.50.107.91/ddugjy/Home/mnngallery

...

	6	image	image			Active	Delete
	7	Image	Test Sandrock		<input type="checkbox"/>	Active	Delete



Scan Round 2

Application validates file input data and allows malicious files to be uploaded.

Trying to upload a php file by changing the extension to jpg.

49.50.107.91/ddugjy/Home/add_gallery

DDUGJY

Add Gallery

Add Gallery

Gallery Category*

Image

Image

Browse... shell.php.jpg

Title (English)

Name

Title (Hindi)

Name

Description (English)

Description

Description (Hindi)

Description

Submit Back

Changed the extension of the file back to php by intercepting the request.

```
POST /ddugjy/Home/insert_gallery HTTP/1.1
Host: 49.50.107.91
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://49.50.107.91/ddugjy/Home/add_gallery
Content-Type: multipart/form-data; boundary=-----57052814523281
Content-Length: 7899
Connection: close
Cookie: PHPSESSID=vdisd9ntvqmc64dm8esg7gmkrvv; csrf_cookie_name=fb2776b78ec3d960bd57a599b83a8bc3; ci_session=sqrt35dvflujboil2vto3g9983
Upgrade-Insecure-Requests: 1

-----57052814523281
Content-Disposition: form-data; name="csrf_test_name"

fb2776b78ec3d960bd57a599b83a8bc3
-----57052814523281
Content-Disposition: form-data; name="gallery_id"

-----57052814523281
Content-Disposition: form-data; name="gallery_type"

1
-----57052814523281
Content-Disposition: form-data; name="file"; filename="shell.jpg.php"
Content-Type: image/jpeg

<?php

function featureShell($cmd, $cwd) {
    $stdout = array();
```

The application does not uploaded the malicious file. Error was thrown on doing so.

49.50.107.91/ddugjy/Home/add_gallery

nDDUGJY

Add Gallery

Add Gallery

Some error occurred, please try again

Gallery Category*

Image

Image

Browse... No file selected.

Title (English)

Name

Description (English)

Description

2.5.6 Information Disclosure

2.5.6.1 Password Disclosure: **Passed**

Scan Round 1

Application does not disclose user login passwords in any format.

2.5.6.2 Information Disclosure in HTML Source Code Comments: **Passed**

Scan Round 1

Application does not disclose unreferenced/backup pages in the HTML source code comments.

2.5.6.3 Information Disclosure in Cookie: **Passed**

Scan Round 1

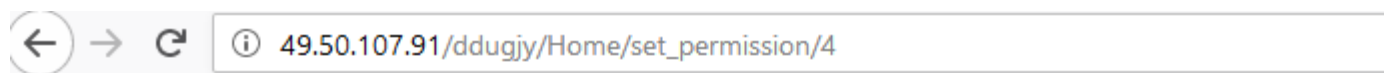
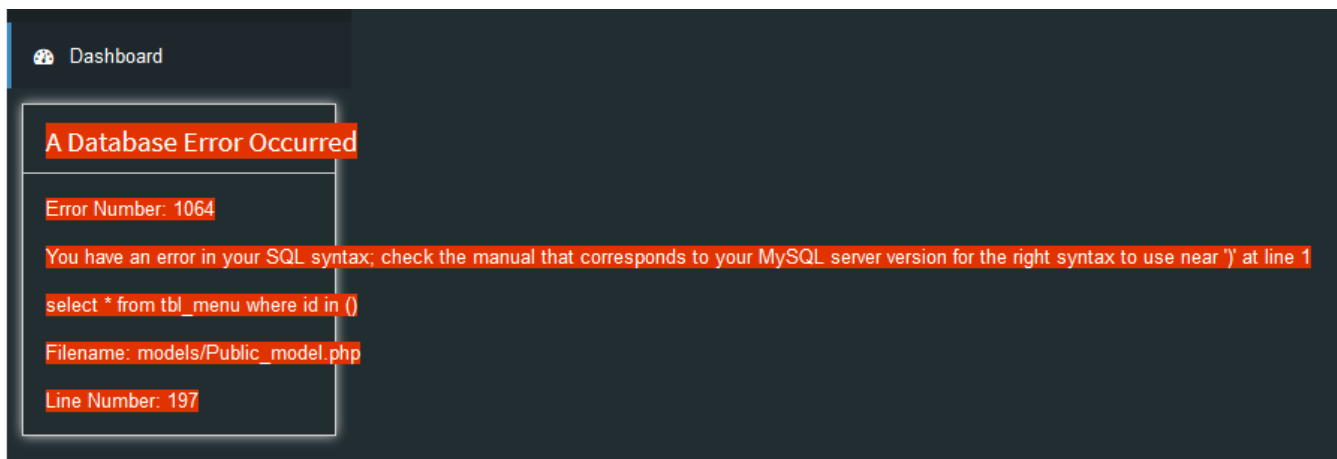
Application does not disclose session information in the web browsers local storage.

2.5.6.4 Errors and Exceptions: **Failed**

Scan Round 1

Application discloses server/application's internal information in the error messages.

Fix: Show generic error messages to users.



A PHP Error was encountered

Severity: Notice

Message: Undefined offset: 0

Filename: controllers/Home.php

Line Number: 444

Backtrace:

File: /var/www/html/ddugjy/application/modules/Home/controllers/Home.php

Line: 444

Function: _error_handler

File: /var/www/html/ddugjy/index.php

Line: 300

Function: require_once

Scan Round 2

Application discloses server/application's internal information in the error messages.

Fix: Show generic error messages to users.

AdminDDUGJY

Rachna

Search...

MAIN NAVIGATION

Dashboard

A Database Error Occurred

Error Number: 1064

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ')' at line 1

select * from tbl_menu where id in ()

Filename: models/Public_model.php

Line Number: 208