

PRESENTATION ON VULNERABILITY ASSESSMENT (VA) AND PENETRATION TESTING (PT) ON SRD ONLINE SYSTEM ADMINISTERED AND MANAGED BY THE SOUTH AFRICAN SOCIAL SECURITY AGENCY (SASSA)

PORTFOLIO COMMITTEE

27 NOVEMBER 2024

Building a Caring Society Together.

www.dsd.gov.za



PRESENTATION OUTLINE

1. Contextual Overview
2. Establishment of the Task Team to Oversee the Implementation of Parliament's Recommendations
 - 2.1 Appointment of Co-ordinator(s) to Oversee the Investigation
 - 2.2 Roles of the Task Team
3. Process Followed in Appointing a Service Provider
 - 3.1 Process for Selecting the Successful Service Provider
 - 3.2 Assessment of the Bid Proposal
4. Independent Audit Report
 - 4.1 Executive Summary
 - 4.2 Methodology/Approach Followed
 - 4.3 Key Findings
 - 4.4 Audit Recommendations
5. Conclusion

1. CONTEXTUAL OVERVIEW

- ❖ Two first year students from the University of Stellenbosch alleged that the application system of SASSA is vulnerable. They made these allegations in various media platforms including a presentation made on 23 October 2024 to the Portfolio Committee.
- ❖ In response to these allegations, **Parliament** recommended a comprehensive investigation of the SRD system and all other **grant systems administered by SASSA**. Parliament's directive reflects concerns over the integrity and security of SASSA's digital systems across various grant types, including but not limited to **Child Support, Disability, Old Age Pension, and Foster Child grants**.
- ❖ The Parliament made a recommendation that the Investigation should be finalised within thirty (30) days and this recommendation was supported by the Minister of Social Development. The Parliament subsequently invited the DSD to table the investigation report and also outline a clear guidance on the focus points of the Presentation to Parliament.
- ❖ As a result, the Minister of Social Development has committed to a thorough review of its entire grant infrastructure, focusing on identifying and mitigating potential vulnerabilities, ensuring the security of beneficiary data, and safeguarding public resources.

2. ESTABLISHMENT OF THE TASK TEAM TO OVERSEE THE IMPLEMENTATION OF PARLIAMENT'S RECOMMENDATIONS

2.1 Appointment of Co-ordinator(s) to Oversee the Investigation

- ❖ Members raised a concern about the perceived interference in the process to appoint a Forensic Investigator into alleged weaknesses and fraud in the application and payment system of social grants.
- ❖ In response to Parliament's concern regarding the perceived interference with the appointment of an independent investigator and overseeing the investigation by SASSA and DSD management, the Executive Authority, who is the Minister of Social Development established a task team, which comprised of assurance providers who are not functionally involved in the daily activities of SASSA and DSD.
- ❖ The task team consists of the following role players
 - Chief Audit Executive (CAE) of DSD (Head of Internal Audit) and support staff.
 - Chief Director: Fraud and Investigation (Head of Anti-Fraud and Investigation: Inspectorate)

2. ESTABLISHMENT OF THE TASK TEAM TO OVERSEE THE IMPLEMENTATION OF PARLIAMENT'S RECOMMENDATIONS (CONT...)

2.2 Functions/Roles of the task team

- ❖ The task team assessed the deliverables that are expected by Parliament as per the letter dated 28 October 2024 against the scope of work that is required to be completed and the timeframe for delivering a comprehensive investigation report.
- ❖ The assessment indicated certain areas that can be achieved within the given timelines after taking into consideration the processes involved such as:-
 - a) Drafting the investigation scope / Terms of Reference (TOR);
 - b) Process of appointing a service provider;
 - c) Conducting the investigation; and
 - d) Drafting of an investigation report.

2.2 FUNCTIONS/ROLES OF THE TASK TEAM (CONT..)

- ❖ In light of the timeframes and the magnitude of the work that is required to be performed per the letter from Parliament, the task advised the following :
 - a) That a preliminary investigation be conducted limited to the Vulnerability Assessment (VA) and Penetration Test (PT) on the SRD online system which is feasible to be completed and presented by completed by 27 November 2024.
 - b) The Vulnerability Assessment (VA) and Penetration Test (PT) on the SOCPEN system will be conducted during the second (2nd) phase that will also include a comprehensive investigation which will cover the entire aspects of the Parliamentary recommendations.
 - c) The outcome of the preliminary investigation on the VA and PT will determine the scope of the second (2nd) phase and the comprehensive investigation as well as the required budget.
 - d) That progress on the investigation be reported on a regular basis to Parliament.

3. PROCESS FOLLOWED IN APPOINTING A SERVICE PROVIDER

3.1 Process for selecting the successful Service Provider

- ❖ In May 2023, the Department took a decision to appoint a Panel to complement the Internal Audit staff which comprised of the following:-
 - a) Internal Audit Service Providers and
 - b) Forensic Investigators.
- ❖ The above panel is appointed for a fixed period of three (3) years and this is the first year that the Panel is in place.
- ❖ The Companies appointed on the Panel of Service Providers comprises of a mixture of
 - a) Large / Established Accounting and Audit Firms
 - b) Medium Sized Accounting Firms and
 - c) Micro Enterprises (Emerging Accounting Firms)

3.1 PROCESS FOR SELECTING THE SUCCESSFUL SERVICE PROVIDER (CONT...)

- ❖ Five (05) service providers were selected from the approved panel and the following was considered during the selection process:-
 - a) The experience demonstrated by the Prospective Service Providers;
 - b) The reputation of the Prospective Service Providers; and
 - c) The Qualifications of the Prospective Service Providers' employees;
- ❖ The following service providers were invited:-
 - ✓ Price Water House Coopers;
 - ✓ Entsika Consultants;
 - ✓ Sizwe Ntsaluba Grant Thornton advisory services (Pty) Ltd;
 - ✓ Masegare and Associates incorporated;
 - ✓ Molefi business experts consulting (Pty) Ltd.

3.1 PROCESS FOR SELECTING THE SUCCESSFUL SERVICE PROVIDER (CONT...)

- ❖ A briefing session of potential service providers was held whereby the following was highlighted amongst others:
 - a) The scope of work as outlined in the Terms of Reference
 - b) Expectations of the project and expected deliverables; and
 - c) Project timelines as informed by the timelines set by Parliament.
- ❖ Out of the five (05) service providers that were invited to submit proposals, only one (01) service provider responded to the request for proposals and the reasons advanced for failing to respond by other service providers in the main were the tight/limited timelines for completing the work and reporting to Parliament.

Assessment of the proposal

- ❖ The team led by the CAE assessed the bid proposal against the following:
 - a) The Terms of Reference for the project;
 - b) The methodology outlined in the proposal;
 - c) Staff complement (human resources) and staff profiles provided for the project; and
 - d) The Software (tools) proposed to be utilised for the project.
- ❖ The Service Provider Masegare and Associates Incorporated was appointed to conduct the project.

4. INDEPENDENT AUDIT REPORT

Masegare & Associates Inc.

4.1. EXECUTIVE SUMMARY (Covered in Slide 1 above)

4.1.1. SUMMARY OF STUDENT'S FINDINGS ON THE SASSA SRD SYSTEM

The students' investigation on SASSA's SRD system uncovered several alleged vulnerabilities using a combination of randomly generated South African identification (ID) numbers and public access to SASSA's Application Programming Interface (API). They reported the following issues among others:-

a)API Vulnerabilities:

- No Rate Limiting: The API allowed an unlimited number of requests, which the students exploited to check the application status of thousands of ID numbers without restriction.

b)Data Exposure:

- The students claimed that the API exposed sensitive details, such as whether a person had applied for an SRD grant or not.

c)Anomalous Application Rates:

- The students identified unusually high application rates for individuals born in certain years, particularly those born in February 2005 and from 2003 to 2006, suggesting possible fraud or identity misuse.

d)Potential Payments to Non-Beneficiaries:

- The students observed that SRD grants appeared linked to applications with their own ID numbers, despite never having applied. This raised concerns about unauthorized applications and potential misallocation of funds.

4.1.2. SUMMARY OF STUDENT'S FINDINGS ON THE SASSA SRD SYSTEM

1. The students said that their study was prompted by issues with their own Social Relief of Distress (SRD) grant applications, which were rejected because their (IDs) were already in use. The presentation covered their research methodology, including interviews with fellow students to assess the scope of the problem. They demonstrated how they generated numerous identification numbers using algorithms, detailing the legal framework and presenting their findings and recommendations for SASSA.
2. The Parliamentary Committee engaged in a critical discussion about allegations raised by students regarding fraud and inefficiencies within SASSA's SRD grant system. Members of Parliament (MPs) welcomed the students' presentation but emphasized the need for a detailed technical report and thorough investigations. Concerns centred on systemic corruption, inefficiencies, and the vulnerability of grant recipients. The students highlighted identity theft and systemic flaws, citing the lack of effective verification mechanisms and a dysfunctional SASSA hotline. Members called for urgent action, stressing adherence to the Protection of Personal Information Act (POPIA) and proposing a 30-day timeline for the Department of Social Development (DSD) to report back with actionable solutions.

4.1.3. SCOPE OF WORK

Background

Masegare and Associates Incorporated (Masegare) was appointed on 11 November 2024 by the Department of Social Development (DSD) to conduct a Vulnerability Assessment (VA) and Penetration Testing (PT) on the SRD Online System, managed and administered by the South African Social Security Agency (SASSA). This assignment, referenced under RFQ SD02/2023/01, aimed to enhance the security and resilience of the SRD online system and its associated platforms.

Assignment Overview

The scope included a comprehensive analysis of the SRD online system to identify and address vulnerabilities that could compromise its security. Key focus areas included system architecture, authentication processes, and access controls. The assessment also extended to associated websites, namely:

- <https://srd.sassa.gov.za/said>
- <https://srd.sassa.gov.za/>
- <https://srd-sassa.org.za/>

Simulated attacks were conducted to assess the system's resilience against potential cyber threats.

Building a Caring Society. Together.

www.dsd.gov.za

4.1.4 BACKGROUND AND SCOPE OF WORK

The assignment included the following deliverables:

Vulnerability Assessment

Identify existing vulnerabilities across the system's network infrastructure, applications, databases, and APIs, with a focus on the SRD system.

Penetration Testing

- i. Conduct internal and external penetration tests to assess the system's defenses against cyber threats.
- ii. Simulate real-world attack scenarios to evaluate system robustness and the effectiveness of security controls.

Investigation

- i. Analyze system logs, error reports, and anomalies to detect unauthorized access, data exfiltration, or the presence of malicious code.
- ii. Assess third-party management of the SRD system, including contractual terms, application hosting, data storage, ownership, SASSA's access rights, and system specifications.

Risk Evaluation

- i. Assess the operational and beneficiary-related risks posed by identified vulnerabilities.
- ii. Evaluate risks related to data privacy and regulatory compliance, particularly compliance with the Protection of Personal Information Act (POPIA).

Recommendations Deliver a detailed report with actionable recommendations to address identified vulnerabilities, strengthen security measures, and mitigate future risks

4.2. METHODOLOGY.

Cybersecurity Testing Methodology

Vulnerability Assessment (VA)

- The Vulnerability Assessment was conducted to identify and evaluate security weaknesses in the SRD online system. The steps included:
 1. **Information Gathering:** Collected data on the system's architecture, network configurations, and application details to create a testing baseline.
 2. **Automated Scanning:** Used reliable tools to scan for vulnerabilities, such as outdated software, misconfigurations, and known weaknesses.
 3. **Manual Validation:** Verified scan results to remove false positives and ensure accurate findings.
 4. **Classification of Vulnerabilities:** Organized vulnerabilities by severity and potential impact using the Common Vulnerability Scoring System (CVSS).
 5. **Documentation:** Compiled findings into a detailed report, categorizing risks as critical, high, medium, or low.

4.2. METHODOLOGY (CONT...)

Cybersecurity Testing Methodology

Penetration Testing (PT)

- Penetration Testing simulated real-world cyberattacks to evaluate the system's resilience. The process included:
 1. **Planning and Reconnaissance:** Defined testing scope and objectives. Collected information about the system and its infrastructure.
 2. **Threat Modelling:** Identified potential attack paths based on known vulnerabilities and system functions.
 3. **Exploitation:** Tested vulnerabilities by safely attempting to exploit them, demonstrating potential risks.
 4. **Post-Exploitation Analysis:** Assessed the extent of breaches, including unauthorized access to sensitive data or functionalities.
 5. **Reporting:** Prepared a report detailing exploited vulnerabilities, their impacts, and recommended mitigations.

4.2. METHODOLOGY. (CONT..)

Digital Forensic Investigation

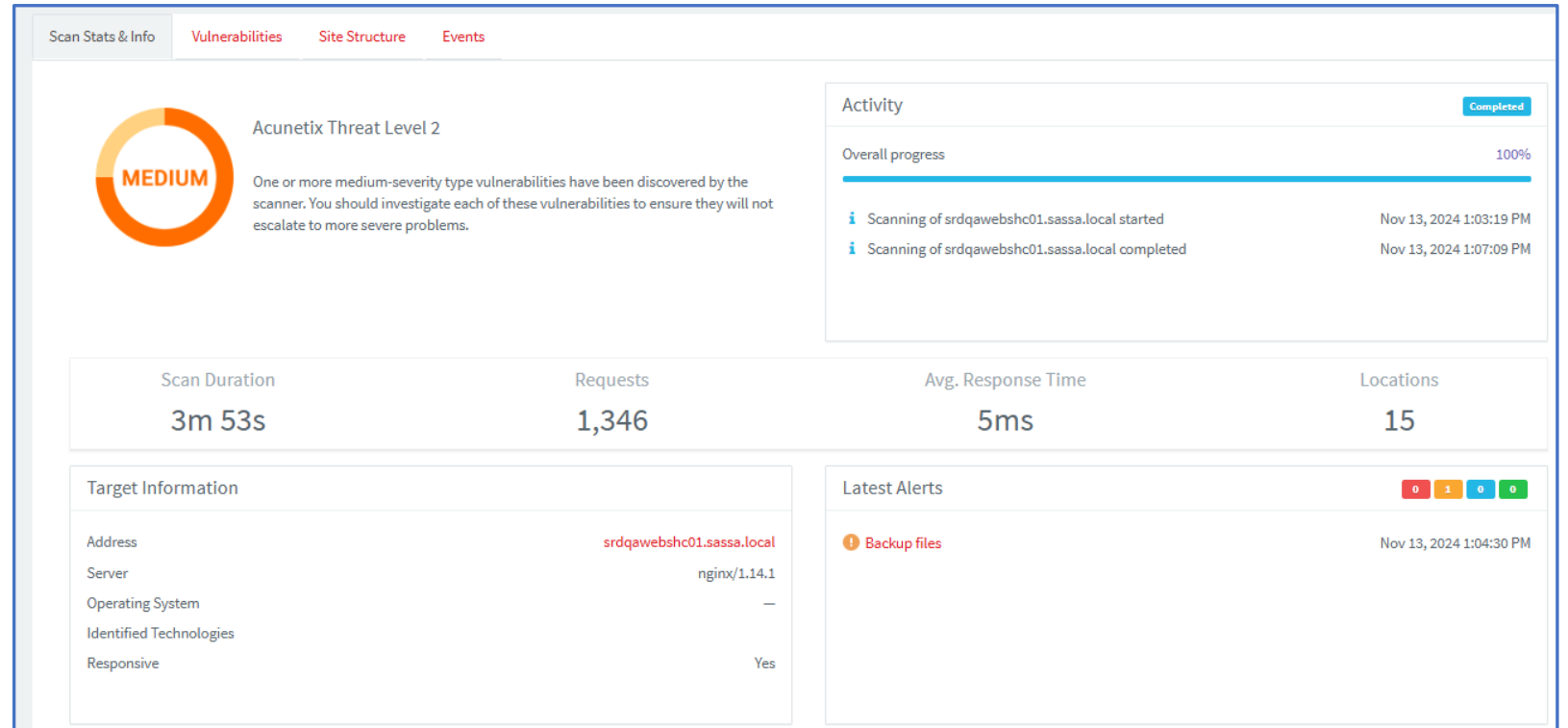
- The Digital Forensic Investigation examined anomalies to identify their sources while preserving evidence integrity. Steps included:

1. **Identification:** Defined the scope by pinpointing activities or incidents requiring analysis.
2. **Preservation:** Secured system logs and files by creating forensic copies to ensure tamper-proof evidence.
3. **Analysis:** Reviewed logs, metadata, and digital artifacts to trace the origin and impact of anomalies.
4. **Correlation:** Linked findings to vulnerabilities and potential attackers, constructing a timeline and context for events.
5. **Reporting:** Created a forensic report summarizing findings, conclusions, and actionable recommendations to prevent recurrence.

4.3. KEY FINDINGS

System Threat Level Evaluation

- Overview:** The results from the web assessment tool (Acunetix) indicate that the overall threat level for the system is classified as **Threat Level 2 (Medium)**. This classification is based on an evaluation of various vulnerabilities, misconfigurations, and potential risks that could affect the security and integrity of the platform. The medium threat level indicates a moderate risk of exploitation, meaning that while the system is not highly vulnerable, it is still susceptible to certain types of attacks that could compromise security if left unaddressed.



4.3. KEY FINDINGS Cont

- **Vulnerabilities Identified:** The system assessment revealed several vulnerabilities, including potential issues with authentication mechanisms, server configurations, data encryption, and missing security headers. These vulnerabilities create opportunities for attackers to exploit weak points in the system.
- **Risk Exposure:** Despite being classified as medium risk, there are significant threats that could potentially lead to unauthorized access, data breaches, service disruptions, or reputational damage if the vulnerabilities are exploited. Key areas of concern include the lack of encryption, unprotected backup files, and weak authentication policies.
- **Severity of Threats:** The medium threat level indicates that the likelihood of an attack is moderate, but the consequences of a successful exploit could still be impactful, especially regarding data exposure or manipulation. Certain vulnerabilities may be easier for attackers to exploit if not mitigated effectively.
- The medium threat level classification indicates that while the system is not at high risk, there are still important vulnerabilities that need to be addressed to ensure its security. Taking the recommended actions will help to reduce the threat level and protect the system from potential attacks, safeguarding sensitive data and preserving the integrity of the platform.

4.3.1. THE WALKTHROUGH OF THE SRD PLATFORM

SASSA SRD System Overview and Identified Gaps

The SASSA SRD system is a vital platform designed to assist individuals aged 18–59 who were financially affected by the Covid-19 pandemic. With a focus on accessibility, it allows clients to apply for the grant through USSD, WhatsApp, and an online portal. The system processes approximately 17 million applications monthly and verifies applicants' ID and banking details before payments are made. Despite its efficiency and stability, a thorough review has identified several potential gaps and areas for improvement to enhance its security and operational integrity.

Key Features of the SRD System

- **Application Channels:** Clients can apply using multiple channels, including USSD, WhatsApp, and an online portal, making the process convenient and inclusive.
- **Security Measures:** The system employs OTP-based authentication, user session tokens, and biometric verification in cases of suspected fraud.
- **Verification and Payments:** ID and banking details are verified for all applicants. For unbanked users, mobile money services like Cash Send are available.
- **System Infrastructure:** Hosted internally at SASSA's Data Centre, the system operates independently of other grant types and ensures high uptime.

4.3.2 THE SRD PLATFORM - GAPS

1. Multiple Applicants per Cell phone Number

- **Risk:** Allowing multiple applications with the same number increases the chances of impersonation and fraudulent claims.
- **Recommendation:** Strengthen the link between applicant IDs and unique phone numbers or limit the number of registrations per number unless verified exceptions are provided.

2. OTP-Based Authentication

- **Risk:** OTP reliance makes the system vulnerable to SIM swap fraud, where attackers gain control of victims' numbers and intercept OTPs. Lack of OTPs is even a greater risk to the platform.
- **Recommendation:** Always enforce OTP requirements, and introduce multi-factor authentication (MFA), such as combining OTPs with biometrics or secure tokens, for enhanced security.

3. Mobile Money and Cash Send

- **Risk:** Fraudulent beneficiaries could exploit weak verification processes to divert funds via mobile money or Cash Send.
- **Recommendation:** Strengthen account verification, conduct regular audits, and implement real-time fraud monitoring.

4. Biometric Verification

- **Risk:** Limited use of biometrics, only in suspected fraud cases, could allow low-profile fraudulent claims to go undetected.
- **Recommendation:** Expand biometric checks to a broader range of applications or introduce random verifications to deter fraud.

4.3.2 THE SRD PLATFORM - GAPS Cont

1. Server Location and Access Control

- **Risk:** Hosting the system on an internal server reduces external risks but remains vulnerable to insider threats and advanced persistent threats (APTs).
- **Recommendation:** Enforce strict access controls, conduct regular security audits, and implement real-time monitoring to detect unusual activity.

2. Cell phone Ownership Validation

- **Risk:** The system may not detect cases of shared or reassigned cell phone numbers, leading to disputes or misuse.
- **Recommendation:** Periodically revalidate cell phone ownership and notify users of any new applications tied to their numbers.

3. Data Encryption

- **Risk:** A lack of clear encryption protocols for sensitive data like IDs, permits, or banking details increases the risk of data breaches.
- **Recommendation:** Implement end-to-end encryptions for all sensitive data, both in transit and at rest, to align with best practices and data protection regulations.

4.3.3. VULNERABILITY ASSESSMENT AND PENETRATION TEST

Our assessment of the SASSA SRD web application revealed vulnerabilities that could compromise the security and functionality of the system. These issues include weaknesses in protecting user information, securing system components, and ensuring compliance with modern security standards. Below is a summary of the key concerns:

- **Login Security:** The login page is vulnerable to automated attacks where hackers can repeatedly guess passwords to access sensitive accounts. This can lead to unauthorized access to user data and administrative controls.
- **Server Configuration Risks:** Misconfigurations in the server allow unauthorized access to internal systems. This could expose critical data and make the system a target for malicious activities.
- **Weak Content Security Policies (CSP):** The system does not properly restrict untrusted scripts from running, making it susceptible to harmful code execution. Additionally, errors in the security settings weaken protection against certain attacks.
- **Exposed System Directories:** Certain directories on the server are accessible to the public. This increases the risk of exposing sensitive files, such as system configurations or database credentials.
- **Missing Security Headers:** Important security controls that protect users' information during web browsing are not implemented, increasing the likelihood of data leakage and misuse.

4.3.3. VULNERABILITY ASSESSMENT AND PENETRATION TEST ... Cont

- **Weak Encryption Standards:** The website's encryption configuration does not meet the highest security standards, leaving communications vulnerable to interception or manipulation.
- **Unprotected Backups:** Backup files containing sensitive information are stored in unsecured locations, making them easy targets for attackers.
- **Unencrypted Communications:** Communication between the website and its users is not adequately encrypted, exposing sensitive data to potential interception.
- **Impact**
 - The issues identified pose significant risks, including unauthorized access to sensitive information, system disruption, and potential non-compliance with data protection laws. These vulnerabilities also expose SASSA to reputational damage and loss of public trust.
- **Recommendations**
 - To address these risks, we recommend implementing stronger password protection, improving server configurations, encrypting all communications, and securing sensitive files. Adopting industry-standard security practices will strengthen the system's defences and ensure better protection for user data and system functionality.

4.4. SRD SYSTEM RECOMMENDATIONS

1. Strengthen Multi-Factor Authentication (MFA):

- **Issue:** The current OTP-based authentication is vulnerable to SIM swap fraud, where attackers can intercept OTPs by gaining control of the victim's phone number. Lack of OTPs in some instances further worsens the security of the system.
- **Recommendation:** Implement multi-factor authentication (MFA) by combining OTPs with biometric verification or other secure authentication methods (e.g., secure tokens). This will provide an additional layer of security, reducing the risk of unauthorized access.

2. Limit Multiple Applicants per Cell phone Number:

- **Issue:** Allowing multiple applicants to register using the same cell phone number increases the risk of impersonation and fraudulent claims.
- **Recommendation:** Enforce stricter controls by linking each applicant's ID to a unique phone number and limit the number of registrations per phone number unless verified exceptions are presented. This will reduce the potential for fraud and identity manipulation.

3. Enhance Mobile Money and Cash Send Verification:

- **Issue:** Mobile money services and Cash Send mechanisms may be vulnerable to unauthorized access and fraud if account verification is weak.
- **Recommendation:** Strengthen account verification processes for mobile money and Cash Send disbursements. Implement regular audits and real-time fraud detection monitoring to detect and prevent fraudulent transactions. This will ensure that only verified beneficiaries receive funds.

4. Expand Biometric Verification:

- **Issue:** Biometric verification is currently only used in cases of suspected fraud, leaving some fraudulent claims unchecked.
- **Recommendation:** Implement biometric verification for a broader range of transactions or at random intervals. This will improve fraud detection capabilities and make it harder for fraudsters to bypass security measures.

4.4. SRD SYSTEM RECOMMENDATIONS Cont

1. Improve Call Centre Security:

- **Issue:** Contact information changes via call centre assistance could be exploited through social engineering attacks, where fraudsters impersonate legitimate users to manipulate agents.
- **Recommendation:** Strengthen call centre protocols by implementing stricter identity verification procedures before updating contact details. Additionally, conduct regular training for call centre agents to recognize and respond appropriately to social engineering tactics.

2. Implement Strict Access Controls and Insider Threat Mitigation:

- **Issue:** Hosting the SRD system on an internal server exposes it to potential insider threats or compromised credentials.
- **Recommendation:** Implement strict access controls, including the principle of least privilege, to limit internal access to the system. Conduct regular security audits, real-time monitoring for unusual activities, and provide insider threat training to employees. Additionally, adopt a zero-trust security model to further minimize the risk of internal threats.

3. Periodic Revalidation of Cell phone Ownership:

- **Issue:** Cell phone numbers may be reassigned or shared within households, which could lead to misuse and disputes.
- **Recommendation:** Implement periodic revalidation of cell phone ownership, especially for long-term users. Send user alerts when new applications are tied to their phone numbers to enhance tracking and prevent fraudulent use.

4.4. SRD SYSTEM RECOMMENDATIONS Cont

1. Implement Data Encryption:

- **Issue:** There is currently no mention of encryption for sensitive data such as IDs, permits, or banking details, increasing the risk of data breaches.
- **Recommendation:** Implement end-to-end encryptions for all sensitive data, both in transit and at rest. This will ensure compliance with best practices and data protection regulations, safeguarding beneficiary information from unauthorized access and breaches.

2. Regular Security Audits and Penetration Testing:

- **Issue:** The system may be vulnerable to undetected attacks or exploits if not regularly tested for security weaknesses.
 - **Recommendation:** Conduct regular security audits and penetration testing to identify potential vulnerabilities and proactively address them. This will help maintain a strong security posture and ensure the SRD system is resilient against emerging threats.
- By implementing these recommendations, SASSA can significantly enhance the security of the SRD system, ensuring it continues to function efficiently and securely while minimizing the risk of fraud and data breaches. These measures will protect beneficiaries, safeguard sensitive information, and maintain public trust in the system's integrity.

4.4. SRD WEB APPLICATION RECOMMENDATIONS Cont

To ensure the security and integrity of the SRD system, it is essential that the identified vulnerabilities be addressed promptly. The following recommendations are made to mitigate the risks and improve the system's overall security posture:

1. Enhance Login Security:

- Implement CAPTCHA or similar mechanisms to prevent automated login attempts and mitigate brute-force attacks.
- Introduce a limit on failed login attempts, with automatic account lockout and alerts for administrators when this threshold is reached.
- Enforce strong password policies, ensuring users select complex passwords to reduce the likelihood of credential-stuffing attacks.
- Monitor login attempts for unusual activity and set up IP-based restrictions to block suspicious login attempts.

2. Strengthen Proxy Security:

- Conduct an audit of the Apache mod_proxy configuration to identify and disable unused proxy modules.
- Restrict proxy access to trusted domains and IP addresses, preventing unauthorized access to internal systems.
- Regularly update Apache servers with the latest security patches and apply best practices, such as disabling Proxy Requests and using explicit allowlists for proxied content.

3. Improve Content Security Policies:

- Define a strict Content Security Policy (CSP) that limits trusted sources for scripts, images, and other resources.
- Use nonce or hash-based CSP policies to prevent the execution of malicious or unauthorized inline scripts.
- Regularly review and update CSP configurations to ensure they align with the latest security standards and protect against cross-site scripting (XSS) attacks.

4.4. RECOMMENDATIONS Cont

1. Implement Critical HTTP Security Headers:

- Add and properly configure HTTP headers such as Referrer-Policy and Permissions-Policy to prevent the sharing of sensitive information and reduce the risk of browser feature exploitation.
- Use automated security testing tools to verify the presence and correct configuration of all recommended security headers.

2. Upgrade SSL/TLS Security:

- Update the server configuration to support strong encryption protocols, such as TLS 1.2 and TLS 1.3, while disabling outdated protocols like TLS 1.0 and 1.1.
- Conduct regular SSL/TLS assessments to ensure that the encryption settings meet modern security standards and are free from vulnerabilities.

3. Secure Database Backup Files:

- Store database backups in secure locations with restricted access to prevent unauthorized access.
- Encrypt all database backups to protect sensitive information and ensure confidentiality.
- Implement strict retention policies to delete outdated backups and reduce the risk of data exposure.

4. Enforce Encrypted Communications:

- Enforce HTTPS across the entire website to ensure all communications are encrypted, protecting user data from interception.
 - Automatically redirect all HTTP traffic to HTTPS to ensure secure communication.
 - Regularly audit encryption practices and configurations to ensure compliance with the latest security standards and protect data in transit.
- By implementing these recommendations, SASSA can significantly improve the security of the SRD system, protect sensitive user data, and enhance the overall trust and reliability of the platform. Continuous monitoring, regular security audits, and prompt response to emerging threats are essential to maintaining a secure and resilient system.

5. SCOPE OF WORK YET TO BE FINALISED

1. Comprehensive Server Assessment

- We still need to conduct a full evaluation of the server hosting the SRD Online System. This will include:
 - Analysing its performance under high user volumes.
 - Identifying potential vulnerabilities, outdated software, or hardware risks.
 - Verifying compliance with SASSA's IT and security standards.

2. Completion of Interviews with Students (SUN)

- We still need to interview the students involved in the SRD Online System operations. This will help us gather:
 - What the students discovered at the time of their assessments.

3. Review of Service Level Agreements (SLAs)


- We still need to complete a detailed review of the two SLAs related to the SRD system. This will involve:
 - Confirming service provider obligations, including uptime guarantees and issue resolution timelines.
 - Evaluating whether current performance meets the agreed-upon standards.
 - Identifying gaps or areas where the SLAs need to be updated or enforced more effectively.

5.1. SCOPE OF WORK YET TO BE FINALISED

- Analysis of the SRD Server:

ANALYZE EVIDENCE



SOURCES TO PROCESS

Type	Image - location name	Evidence number	Search type	Start date/time - local time	End date/time - local time	Duration	Status
 ▾	Partition 2 (exFAT, 9.1 TB) Seagate Hub [D:\]	PhysicalDrive1 Seagate One To	Files & folders	11/22/2024 9:38:07 PM		10:19:49	Searching - 76%

SEARCH IN PROGRESS

Time Elapsed: 10:20:03

CURRENT SEARCH LOCATION

 Partition 2 (exFAT, 9.1 TB) Seagate Hub [D:\] Searching - Partition 2 (exFAT, 9.1 TB) Seagate Hub [D:\] 

^ Search Definitions:

- ^ Partition 2 (exFAT, 9.1 TB) Seagate Hub [D:\] - SASSA_SRD_Server_01 - Nov 19 2024 203208\remote-20241119-204644009\3fhoiu1x.5lk
User Selected Searching - 76% - (10:19:49)
Nested containers found: 0

▾ Thread Details:

5. CHALLENGES

- Limited time to address all the scope items
- High volumes of Data than anticipated
- The SRD site has been unreachable at some point leading to delayed assessment:

```
by Ben "epi" Risher ver: 2.11.0
Target Url      https://srd.sassa.gov.za
Threads        50
Wordlist        /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
Status Codes    All Status Codes
Timeout (secs)  7
User-Agent      ferobxbuster/2.11.0
Config File     /etc/ferobxbuster/ferox-config.toml
Extract Links   true
HTTP methods    [GET]
Recursion Depth 2

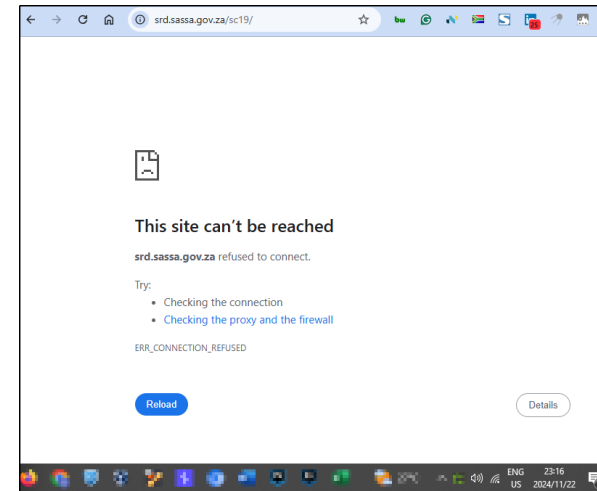
Press [ENTER] to use the Scan Management Menu™

Could not connect to https://srd.sassa.gov.za, skipping...
=> error sending request for url (https://srd.sassa.gov.za/)
ERROR: Could not connect to any target provided

WPSecScan
WordPress Security Scanner by the WPSec Team
Version 3.8.27
@_WPSecScan, @ethicalhack3r, @erwan_lr, @firefart

[!] Updating the Database ...
[!] Update completed.

Scan Aborted: The url supplied 'https://srd.sassa.gov.za/' seems to be down (Could not connect to server)
```



4. CONCLUSION

The SRD System

- The vulnerability assessment of the SASSA SRD system highlights several areas of concern that must be addressed to enhance security and maintain the integrity of its operations. While the SRD system operates effectively overall, there are key vulnerabilities—such as weaknesses in the OTP-based authentication, the allowance for multiple applicants per cell phone number, and the use of mobile money services—that expose the platform to potential fraud and misuse. The lack of robust data encryption and limited scope of biometric verification also present significant risks to the system’s security.
- To mitigate these risks, SASSA should implement targeted security improvements. These include adopting multi-factor authentication, enhancing verification protocols, expanding biometric checks, and enforcing end-to-end encryption for sensitive data. These measures will reduce the likelihood of fraudulent activities and ensure the secure handling of beneficiary information, further safeguarding the integrity of the SRD system.
- By addressing the security gaps, SASSA can continue to ensure safe and accurate disbursement of grants, enhancing user trust and maintaining operational integrity. Strengthening the system's security will also reinforce its resilience against future threats, ensuring the long-term protection of both beneficiaries and the system itself.
- In conclusion, while the SRD system is well-designed, addressing the identified security vulnerabilities will significantly improve its overall security posture, prevent fraud, and protect sensitive client data. With these enhancements, SASSA can further solidify its reputation for efficiently and securely serving vulnerable individuals, ensuring continued public confidence in the system.

4. CONCLUSION Cont

- **SRD Web Application Vulnerabilities:**
 - The vulnerabilities identified in the SRD system present significant risks to both the security of the platform and the trust of its users. Addressing these vulnerabilities is crucial to ensure the integrity of user data, safeguard sensitive information, and protect the system from potential exploits.
1. **Login Page Credential-Guessing Attack:** The lack of adequate protection against brute-force and credential-stuffing attacks leaves user accounts vulnerable to unauthorized access. Implementing stronger authentication measures such as CAPTCHA, login attempt limits, and promoting complex password policies is necessary to secure user accounts.
 2. **Apache mod_proxy Reverse Proxy Security Bypass:** Misconfigurations in the reverse proxy expose internal systems to unauthorized access and malicious activity. Auditing the server configuration, restricting proxy access, and applying security patches are vital steps to mitigate these risks.
 3. **Content Security Policy (CSP) Issues:** Weak or improperly configured CSPs make the system susceptible to script injection and data theft. Defining strict CSP rules, testing for effectiveness, and correcting any syntax errors will bolster protection against these types of attacks.
 4. **Directory Enumeration:** The exposure of sensitive files via directory listings increases the likelihood of data leakage and exploitation. Disabling directory listings and enforcing strict access controls will significantly reduce the chances of sensitive data being compromised.

4. CONCLUSION Cont

SRD Web Application Vulnerabilities:

1. **Missing HTTP Security Headers:** The absence of critical security headers such as Referrer-Policy and Permissions-Policy exposes the system to potential data leaks and malicious use of browser features. Implementing these headers will reduce the risk of information being inadvertently shared or exploited.
 2. **SSL/TLS Configuration:** The current "B" grade for SSL/TLS indicates that the encryption protocols are not up to modern standards, leaving data vulnerable to interception. Updating server configurations to support stronger encryption protocols and disabling outdated ones will improve the security of data in transit.
 3. **Unprotected Database Backup Files:** The lack of security for database backups puts sensitive information at risk of exposure. Encrypting backups and storing them in secure locations will help protect critical data from being accessed or exploited.
 4. **Unencrypted Communications:** Unencrypted communications expose sensitive information, such as login credentials, to interception. Enforcing HTTPS across the entire website and ensuring all communications are encrypted will safeguard user data from eavesdropping and man-in-the-middle attacks.
- In conclusion, the SRD system, while robust in design, requires several critical security improvements to mitigate potential threats and vulnerabilities. By addressing these issues through the recommended remediation steps, SASSA can strengthen the system's security posture, protect user data, and ensure the continued trust and safety of its beneficiaries.

5. RECOMMENDATIONS

It is recommended that the Portfolio committee on Social Development

- To take note of the process followed by DSD in appointing the Service Provider and the Progress made by the appointed Service Provider in the assessment of the SASSA SRD online systems for its vulnerabilities and penetration .

