



IE2062 [2023/JUL]- Web Security

Web Security BB Assignment

Report 07 – Smart Pension


Lecturer in charge – Ms. Chethana Liyanapathirana

IT21826368 – Nanayakkara Y.D.T.D

Contents

| | |
|--|----|
| 1. Smart Pension/Smart Pension VDP/Detail..... | 3 |
| 1.1. Overview | 3 |
| 1.2. Scope | 4 |
| 1.3. Out of Scope..... | 5 |
| 1.4. Selected Domains | 6 |
| 2. Information Gathering | 7 |
| 2.1. Using Amass | 7 |
| 2.2. Using Knockpy..... | 7 |
| 2.3. Using Dmitry..... | 7 |
| 3. Scanning Vulnerability | 9 |
| 3.1. Using Nmap..... | 9 |
| 3.2. Using Nikto | 9 |
| 3.3. Using Rapid Scan | 10 |
| 4. Vulnerability description | 12 |
| 5. Affected components..... | 13 |
| 6. Impact assessment | 13 |
| 7. Steps to reproduce. | 14 |
| 8. Proof of concept (if applicable) | 14 |
| 9. Proposed mitigation or fix | 14 |
| 10. Summary | 14 |

1. Smart Pension/Smart Pension VDP/Detail



Registered

Open

Smart Pension/Smart Pension VDP/Detail

1.1.Overview

Description

We want to transform retirement, savings and financial wellbeing across all generations, around the world.

We do this by blending the financial expertise and tech innovation that our founders, Will and Andrew, brought together in 2014. We create tech-driven financial products, whilst remaining responsible, trustworthy and compliant.

Smart is committed to maintaining a robust set of security standards and really appreciate the help of the security researcher community to achieve this.

Bounties ⓘ

This is a responsible disclosure program without bounties.

1.2.Scope

In scope

Introduction

We are happy to announce our program! We've done our best to clean up our known issues and now would like to request your help to spot the ones we missed!

This program is currently not offering rewards however we will launch a private Bug Bounty Program for selected assets soon.

Types of vulnerabilities to report

We are specifically interested in OWASP Top 10 vulnerability categories and to learn about any potential vulnerability that could impact the security and privacy of our systems. This includes:

- Leaking of personal data
- Horizontal / Vertical privilege escalation
- SQLi

Avoiding impact to our systems

- Please be careful with your tests and avoid any impact to customers and/or services. If you suspect that your tests caused any damage to our systems, please report the first steps and request permission to continue
- Limit all requests to 5 requests per second
- Do not modify any information or code
- It is prohibited to access, extract or download adviser, employers, employees, or any confidential information. If you accidentally access any of these, please stop and report the finding immediately

Feedback

Would you like to help us improve our program or have some feedback to share, please send your anonymous feedback here:

[Program feedback link](#)

Please note this form will be checked periodically and **should not** be used for submission or support queries.

1.3.Out of Scope

Out of scope

Domains

- Any domain that is not listed in the Domains section, is out of scope for this program



Application

- Wordpress usernames disclosure
- Pre-Auth Account takeover/OAuth squatting
- Self-XSS that can't be used to exploit other users
- Verbose messages/files/directory listings without disclosing any sensitive information
- CORS misconfiguration on non-sensitive endpoints
- Missing cookie flags
- Missing security headers
- Cross-site Request Forgery with no or low impact
- Presence of autocomplete attribute on web forms
- Reverse tabnabbing
- Bypassing rate-limits or the non-existence of rate-limits.
- Best practices violations (password complexity, expiration, re-use, etc.)
- Clickjacking without proven impact/unrealistic user interaction
- CSV Injection
- Sessions not being invalidated (logout, enabling 2FA, etc.)
- Tokens leaked to third parties
- Anything related to email spoofing, SPF, DMARC or DKIM
- Content injection without being able to modify the HTML

General

- In case that a reported vulnerability was already known to the company from their own tests, it will be flagged as a duplicate
- Theoretical security issues with no realistic exploit scenario(s) or attack surfaces, or issues that would require complex end user interactions to be exploited
- Spam, social engineering and physical intrusion
- DoS/DDoS attacks or brute force attacks
- Vulnerabilities that only work on software that no longer receive security updates
- Attacks requiring physical access to a victim's computer/device, man in the middle or compromised user accounts
- Recently discovered zero-day vulnerabilities found in in-scope assets within 14 days after the public release of a patch or mitigation may be reported, but are usually not eligible for a bounty
- Reports that state that software is out of date/vulnerable without a proof-of-concept

1.4.Selected Domains

| | | |
|--|--------|-----|
| id.sandbox.autoenrolment.co.uk/user/sign-in  | Tier 1 | URL |
| Web portal used by an accountant, IFA or Payroll Bureau to manage their clients. Adviser portal provides the functionality to add a new company, maintain and view company and member details. | | |
| Hide description ^ | | |
|  View changes | | |

URL: Id.sandbox.autoenrolment.co.uk/user/sign-in used in the report.

2. Information Gathering

2.1.Using Amass

```
(user@user)-[~]
$ sudo amass enum -d id.sandbox.autoenrolment.co.uk
id.sandbox.autoenrolment.co.uk

OWASP Amass v3.23.2 https://github.com/owasp-amass/amass
1 names discovered - dns: 1

ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.
104.16.0.0/14 2 Subdomain Name(s)

The enumeration has finished
Discoveries are being migrated into the local database
```

2.2.Using Knockpy

```

[user@user]~$ sudo knockpy id.sandbox.autoenrolment.co.uk
[sudo] password for user:

v6.1.0
Knockpy
Python 3.9.6
Github: https://github.com/g0tmilk/knockpy

local: 10757 | remote: 1

Wordlist: 10758 | Target: id.sandbox.autoenrolment.co.uk | Ip: 104.18.16.152

20:43:54

Ip address      Code  Subdomain      Server      Real hostname
-----
(ctrl+c) | 20.4% | db8.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 20.4% | db9.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 20.5% | dba.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 20.5% | dbadmin.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 20.5% | dbase.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 20.5% | dbm.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 20.5% | dbs.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 20.5% | dc01.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 20.5% | dc.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 20.5% | dbtest.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 20.5% | dbserver.id.sandbox.autoenrolment.co.uk

(ctrl+c) | 65.0% | plt.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 65.1% | plugin.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 65.1% | plugins.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 65.1% | plum.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 65.1% | plus.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 65.1% | pluto.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 65.1% | pluton.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 65.1% | pm.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 65.1% | pm1.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 65.1% | pm2.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 65.1% | pma.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 65.1% | pm2.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 65.2% | pmail.id.sandbox.autoenrolment.co.uk
(ctrl+c) | 65.2% | pmb.id.sandbox.autoenrolment.co.uk

21:05:15

Ip address: 0 | Subdomain: 0 | elapsed time: 00:21:21

```

2.3.Using Dmitry

```
(user@user)-[~]
$ sudo dmitry id.sandbox.autoenrolment.co.uk/user/sign-in
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host IP addr. for id.sandbox.autoenrolment.co.uk/user/sign-in
Continuing with limited modules
HostIP:
HostName:id.sandbox.autoenrolment.co.uk/user/sign-in

Gathered Inic-whois information for id.sandbox.autoenrolment.co.uk/user/sign-in
Error: Unable to connect - Invalid Host
ERROR: Connection to InicWhois Server uk/user/sign-in.whois-servers.net failed

Gathered Netcraft information for id.sandbox.autoenrolment.co.uk/user/sign-in

Retrieving Netcraft.com information for id.sandbox.autoenrolment.co.uk/user/sign-in
Netcraft.com Information gathered

Gathered Subdomain information for id.sandbox.autoenrolment.co.uk/user/sign-in

Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 possible subdomain(s) for host id.sandbox.autoenrolment.co.uk/user/sign-in, Searched 0 pages containing 0 results

Gathered E-Mail information for id.sandbox.autoenrolment.co.uk/user/sign-in

Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host id.sandbox.autoenrolment.co.uk/user/sign-in, Searched 0 pages containing 0 results

All scans completed, exiting
```


3. Scanning Vulnerability

3.1.Using Nmap

```
L$ sudo nmap -sS 104.16.0.0
[sudo] password for user:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 13:41 PDT
Nmap scan report for 104.16.0.0
Host is up (0.012s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.74 seconds
```

3.2.Using Nikto

```
L$ sudo nikto -h id.sandbox.autoenrolment.co.uk
- Nikto v2.5.0

+ Multiple IPs found: 104.18.17.152, 104.18.16.152
+ Target IP: 104.18.17.152
+ Target Hostname: id.sandbox.autoenrolment.co.uk
+ Target Port: 80
+ Start Time: 2023-10-31 13:42:46 (GMT-7)

+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://id.sandbox.autoenrolment.co.uk/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
+ 8218 requests: 4 error(s) and 4 item(s) reported on remote host
+ End Time: 2023-10-31 13:51:33 (GMT-7) (527 seconds)

+ 1 host(s) tested
```

- The anti-clickjacking X Frame Options Headers is not present.
- Retrieved Access control- allow – origin header.
- Cloudflare trace CGI found which can leak Information.

3.3.Using Rapid Scan



- Found Subdomains With fierce and amass

```
Vulnerability Threat Level
[medium] Found Subdomains with Fierce.
Vulnerability Definition
Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even chances for the attacker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.
Vulnerability Remediation
It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
```

```
Vulnerability Threat Level
[medium] Found Subdomains with AMass
Vulnerability Definition
Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even chances for the attacker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.
Vulnerability Remediation
It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
```

- XSS Protection is not present, and filter disabled.

```
Vulnerability Threat Level
[medium] X-XSS Protection is not Present
Vulnerability Definition
As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.
Vulnerability Remediation
Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.
```

```
Vulnerability Threat Level
[medium] XSS Protection Filter is Disabled.
Vulnerability Definition
As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.
Vulnerability Remediation
Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.
```

- Secure Client Initiated Renegotiation is supported

```
Vulnerability Threat Level
[medium] Secure Client Initiated Renegotiation is supported.
Vulnerability Definition
This is a known as PlainText Injection attack, which allows MITM attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context.
Vulnerability Remediation
Detailed steps of remediation can be found from these resources. https://securingtomorrow.mcafee.com/technical-how-to/tips-securing-ssl-renegotiation/ https://www.digicert.com/news/2011-06-03-ssl-renego/
```

- SNMP service Detected

```
Vulnerability Threat Level
[medium] SNMP Service Detected.
Vulnerability Definition
Hackers will be able to read community strings through the service and enumerate quite a bit of information from the target. Also, there are multiple Remote Code Execution and Denial of Service vulnerabilities related to SNMP service.
Vulnerability Remediation
Use a firewall to block the ports from the outside world. The following article gives wide insight on locking down SNMP service. https://www.techrepublic.com/article/lock-it-down-dont-allow-snmp-to-compromise-network-security/
```

- Open Directories Found with DirB

```
Vulnerability Threat Level
  medium Open Directories Found with DirB.
Vulnerability Definition
  Attackers may find considerable amount of information from these directories. There are even chances attackers may get access to critical information from these directories.
Vulnerability Remediation
  It is recommended to block or restrict access to these directories unless necessary.
```

- RDP server detected over UDP

```
Vulnerability Threat Level
  high RDP Server Detected over UDP.
Vulnerability Definition
  Attackers may launch remote exploits to either crash the service or tools like ncrack to try brute-forcing the password on the target.
Vulnerability Remediation
  It is recommended to block the service to outside world and made the service accessible only through the a set of allowed IPs only really neccessary. The following resource provides insights on the risks and as well as the steps to block the service. https://www.perspectiverisk.com/remote-desktop-service-vulnerabilities/
```

```
[ Report Generation Phase Initiated. ]
Complete Vulnerability Report for id.sandbox.autoenrolment.co.uk named rs.vul.id.sandbox.autoenrolment.co.uk
Total Number of Vulnerability Checks           : 80
Total Number of Vulnerability Checks Skipped: 21
Total Number of Vulnerabilities Detected       : 11
Total Time Elapsed for the Scan                : 1h 37m 46s
```

4. Vulnerability description

- **Found Subdomains with Fierce and Amass:**
 - Subdomains were discovered using the tools Fierce and Amass, which could potentially widen the attack surface, exposing additional points of vulnerability and unauthorized access.
 -
- **XSS Protection is Not Present, and Filter Disabled:**
 - The absence of XSS protection headers and filters indicates a vulnerability to cross-site scripting (XSS) attacks, where attackers can inject malicious scripts into web pages to compromise user data and security.
 -
- **Secure Client-Initiated Renegotiation Supported:**
 - The support for Secure Client-Initiated Renegotiation may introduce security risks if not configured correctly, potentially facilitating man-in-the-middle attacks.
 -
- **SNMP Service Detected:**
 - The presence of the Simple Network Management Protocol (SNMP) service may expose sensitive information and configuration details, potentially posing a security risk if not adequately secure.
 -
- **Open Directories Found with DirB:**
 - The discovery of open directories using DirB reveals potentially sensitive or unprotected files and resources that can be accessed by unauthorized individuals, raising security concerns.
 -
- **RDP Server Detected Over UDP:**
 - Detecting an RDP (Remote Desktop Protocol) server operating over UDP (User Datagram Protocol) may present security concerns, as it might expose the server to various security risks if not properly configured.

5. Affected components.

- **Found Subdomains with Fierce and Amass:**
 - Impacts the subdomains and their associated services and content.
 -
- **XSS Protection is Not Present, and Filter Disabled:**
 - Affects the entire website, potentially exposing user data to XSS attacks.
 -
- **Secure Client-Initiated Renegotiation Supported:**
 - Impacts the server's SSL/TLS configuration and security.
 -
- **SNMP Service Detected:**
 - Impacts the server or network infrastructure and potentially exposes sensitive information.
 -
- **Open Directories Found with DirB:**
 - Affects the security and integrity of the identified directories.
 -
- **RDP Server Detected Over UDP:**
 - Affects the security and configuration of the RDP server.

6. Impact assessment

- **Found Subdomains with Fierce and Amass:**
 - Moderate risk: The discovery of subdomains widens the attack surface and requires scrutiny for potential vulnerabilities.
 -
- **XSS Protection is Not Present, and Filter Disabled:**
 - Moderate risk: The absence of XSS protection headers increases the risk of successful XSS attacks, compromising user data and security.
 -
- **Secure Client-Initiated Renegotiation Supported:**
 - Moderate risk: If not properly configured, it could lead to SSL/TLS vulnerabilities.
 -
- **SNMP Service Detected:**
 - Moderate risk: SNMP services may expose sensitive information, necessitating proper security configurations.
 -
- **Open Directories Found with DirB:**
 - Low to moderate risk: Open directories may expose sensitive files and require proper access controls.
 -
- **RDP Server Detected Over UDP:**
 - Moderate risk: RDP server configurations over UDP should be scrutinized to prevent potential security issues.

7. Steps to reproduce.

- None

8. Proof of concept (if applicable)

- None

9. Proposed mitigation or fix

- securing subdomains
- enabling XSS protection
- configuring Secure Client-Initiated Renegotiation securely
- securing SNMP services
- securing open directories
- reviewing RDP server configurations over UDP.

10. Summary

- The assessment has uncovered various vulnerabilities and security concerns, including the discovery of subdomains, the absence of XSS protection, support for Secure Client-Initiated Renegotiation, SNMP services, open directories, and RDP server configurations over UDP.