**Section 1**

1. First hash

A screenshot of a computer

Description automatically generated

i. 55/73

ii. file name: **x0\_q.exe**, size: 726.00KB

A screenshot of a computer

Description automatically generated

iii. 2024-11-17 17:25:38 UTC

iv.

A screenshot of a computer

Description automatically generated



1. **Platform:** Windows
2. **File Type:** Win32 EXE
3. **Programming Language:** .NET executable

v.

A screenshot of a computer

Description automatically generated

**Domains Related:**

1. api.ipify.org
2. api4.ipify.org
3. crt.sectigo.com
4. ipify.org
5. mail.quartieri97italy.com.ng
6. microsoft.com
7. quartieri97italy.com.ng
8. sectigo.com
9. tse1.mm.bing.net
10. [www.microsoft.com](http://www.microsoft.com)

**IP Addresses Related:**

1. 104.18.14.101
2. 104.194.10.93
3. 104.237.62.212
4. 104.26.12.205
5. 104.26.13.205
6. 13.107.21.200
7. 172.67.74.152
8. 173.231.16.77
9. 192.168.0.26
10. 192.168.0.27

vi.

A screenshot of a computer

Description automatically generated

1. **Zenbox**

2. **C2AE**

3. **VMRay**

4. **Yomi Hunter**

5. **CAPE Sandbox**

vii.

2) Second hash A screenshot of a computer

Description automatically generated

i. 65/72

ii. a58b87f315fd77116edce2744.exe, 403.00 KB

A screenshot of a computer

Description automatically generated

iii. 2024-10-09 14:01:51 UTC.

iv.

A screenshot of a computer

Description automatically generated



A screenshot of a computer

Description automatically generated

1. Platform: Windows.
2. File type: Win32 EXE (PE32 executable GUI).

3. Programming language: C++.

v.

A screenshot of a computer

Description automatically generated

1. **Domains:**

* crt.sectigo.com
* gstatic-node.io
* sectigo.com

2. **IP Addresses:**

* 104.18.14.101
* 104.21.37.53
* 172.67.204.199
* 192.229.211.108
* 20.99.184.37
* 20.99.186.246
* 23.216.147.64

vi.

* VMRay
* C2AE
* Yomi Hunter

vii.

MAITRE ATTA%CK

**Section 2**

Part-A

a.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

b.

A close up of a computer screen

Description automatically generated

A screen shot of a computer program

Description automatically generated

c.

gcc delete.c

./a.out

d.

target.txt deleted

Part-B

a.



b.

A close up of a computer screen

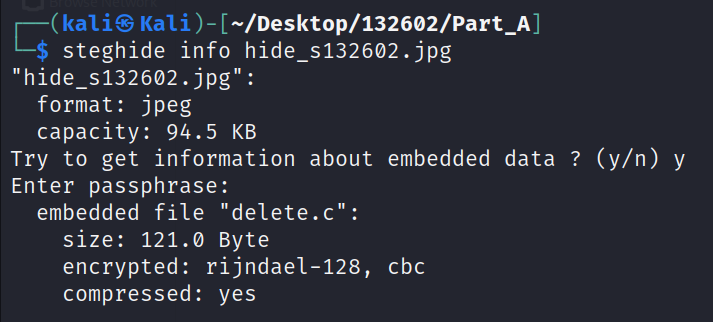
Description automatically generated

c.

A computer screen shot of white text

Description automatically generated

d.

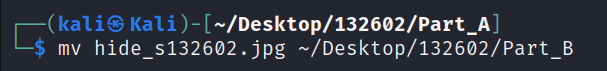


Part-C

a.

A screenshot of a computer

Description automatically generated



c.

A close up of a computer screen

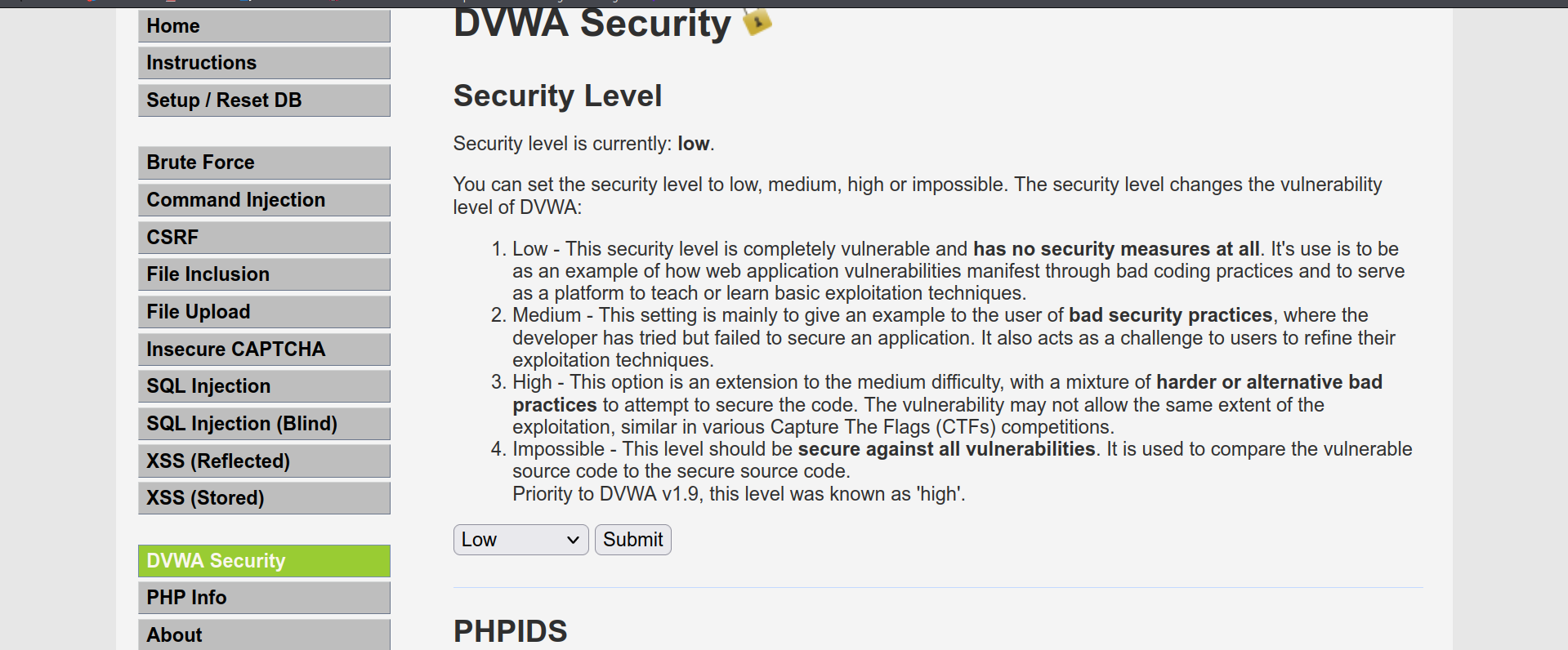
Description automatically generatedA computer screen shot of a computer screen

Description automatically generated

**Section 3**

Step 1:

Done



Step 2:

a.

A screenshot of a computer

Description automatically generated

b. <script> window.location = "http://malicious-site.com"; </script>

c. A screenshot of a computer

Description automatically generated

d.

- the victim redirected to phishing website the design to steal data or personal information.

- the victim device my download or execute malicious software without a consent

- stealing tokens, authentication and cookies

- the malicious site may exploit a vulnerability

e.

- input validation and ensuring they don’t have a malicious scripts

- Implement CSP headers to restrict the execution of unauthorized scripts.

- Avoid Reflected Data and Minimize the use of user-supplied data in response outputs unless properly sanitized.

- Educate Users and Raise awareness to prevent clicking on suspicious links