1ai) B

ii) B

iii) C?

1bi) A) RUNNING

B) SUPPORT

C) RUNNING

D) CHAT

I think we discount the prev screen each time:

A. Running

B. Home → Health

C. Activities → Cycling

D. Home → Health → Stress (→ day1 or Day2)

1ci) It’s Ross (get hacked m8)

ii) We can use a confused deputy attack where we use the browser, who has the internet access permission, to open an url for us with some post params to be sent to the server

Iii) The technique essentially works by doing a succession of set intersection with people from the same place and at the same time. The smaller those sets, the more likely we are to end up with our target. Thus, the larger the cities, the more data we need.

2ai) A

ii) D

iii) D? I think he wants to flex his app

2bi) 2 possible answers?

* The song must actually get played by the user in the first place, so phishing is needed.
* Hard to target multiple voice assistants and it’s quite easy to see the attack due to a majority of people hearing the added noise and seeing the voice assistant react.

ii) todo

2c) NOT SURE THIS IS CORRECT, idk I've never used SELinux. Please add stuff as you see fit

// Admin can do anything

Allow admin\_r:camera{record stop}

Allow admin\_r:door{lock unlock}

Allow admin\_r:light{turn\_on turn\_off}

// Make sure no one else can access the camera

Neverallow member\_r:camera

Neverallow guest\_r:camera

// Members can access doors + lights

Allow member\_r:door{lock unlock}

Allow member\_r:light{turn\_on turn\_off}

// Guests can only access lights

Allow guest\_r:light{turn\_on turn\_off}

3ai) CSP can help reduce the chances of XSS by explicitly specifying which origins we are allows to execute code from. As such, any untrusted source such as 3rd party iframes or origins needed only to deliver content (for blog posts, images, videos etc) can be excluded from running JS. As such imagine someone injected JS into our blog post from our content server, the browser will refer to the CSP to know it shouldn’t run it.

It might be inconvenient or restrictive because in order to be truly effective, the developer should split the content between different origins depending on the type. <-- IS THIS CORRECT?

3aii)

CORS can mitigate DoS attacks by allowing only controlled origins to access the API.

It however cannot mitigate DDoS since here we can use a large collection of bots with the correct origin to flood the API?

3aiii)

<http://bbc.co.uk/news> (last one)

3aiv) Authorization

Confidentiality (could make the iframe reveal sensitive information)

3av) For isolation purposes. The global object gives access to sensitive information and functionalities such as the window object.

3avi)

3bi) Gas fees have to be paid for every instruction run. This therefore prevents people from running infinite loops or other expensive operations on the EVM as this will make them go broke.

3bii) There is no central server, everything is done though distributed consensus backed by Proof of Work or proof of stake (or other) depending on the blockchain.

Which blockchains are they referring to in the questions? >> ETH vs BTC

Proof of stake tends to be more decentralised since it’s more accessible and more people can join in.

3ci)

O