

PET Fragensammlung

NOTE: Keine Garantie auf Richtigkeit!!

[2022-01-13 exam questions.pdf](#)

(a)

3pts) The Top Level Domain ".dev" is currently in the HSTS preload list.
What does that mean for your new web project that runs at "pets-exam.dev"?

HSTS (from google):

The HSTS (HTTP Strict Transport Security) protocol is a policy / mechanism that forces a web connection over a secure HTTPS channel. In other words: without a valid SSL certificate, such a website will not load in your browser.

In our case for "pets-exam.dev":

If .dev is in the preload, this means that for your web project you have to use HTTPS as well because all sites using .dev top-level-domain must only be over HTTPS.

Source:

<https://comodossstore.com/blog/google-launches-app-top-level-domain-with-hsts-as-a-default.html>

(b)

3pts) Your DNS resolver gives you the following record. What does that mean?

```
$ dig CAA pets-exam.dev
[...]
;; ANSWER SECTION:
pets-exam.dev.      3580    IN      CAA     128 issue "letsencrypt.org"
pets-exam.dev.      3580    IN      CAA     128 issue "globalsign.com"
[...]
```

What kind of CA can issue certificates for pets-exam.dev

In this case only "letsencrypt.org" and "globalsign.com" can issue certificates for this site.

(c)

4pts) You configured the TLS settings of your project only with the most modern version TLS1.3 to ensure maximum security.
What are possible problems with this configuration?

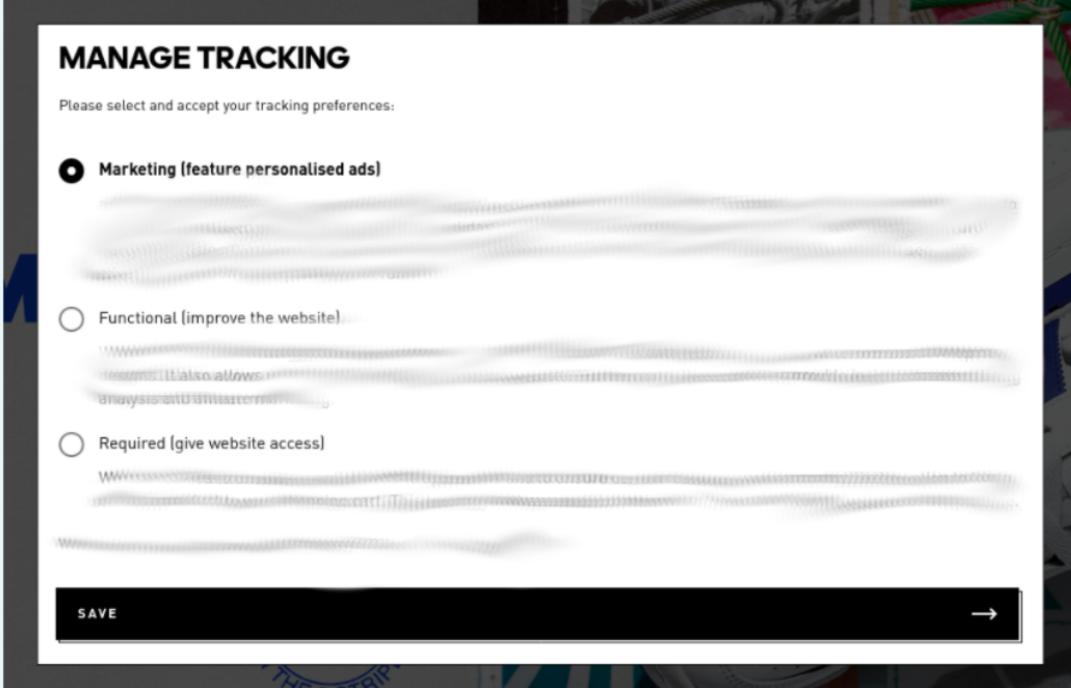
Version intolerance, some middlebox implementations can just speak TLS 1.2 and might have compatibility issues with the project.

Google:

Not all servers and clients support TLS 1.3 yet, so it may not be possible to use it in all cases.

Additionally, some older systems or devices may not be compatible with TLS 1.3, so it is important to verify compatibility before attempting to use it.

The ongoing pandemic led to an increase in new online shops. One of these new online shops sparks your interest. Before you start using the online shop you want to verify how they use online tracking. Below you see a screenshot of the online shop's tracking consent dialog.



1) (3 pt) Provide examples of services commonly used for "Marketing", "Functional" and "Required" tracking.

2) (4 pt) Describe how to verify if the tracking consent settings have an effect?

3) (3 pt) Describe the overall risks of relying on opt-out dialogs.

a. Marketing = Personalized Advertisements

Functional = Statistic Analysis for the company

Required = Shopping Cart tracking, so to know what the user put in the basket

b. If the ads are not personalized for marketing, other than that it is not possible?

c. Trust issues, you cannot be sure how the company is handle your data

You are a reporter who is publishing sensitive information about a company.

The websites containing the information are hosted at national hosting providers in foreign countries.

1) (3pts) The company wants to block access to that information for their employees. Name exactly two technical methods which are possible to censor this information. Describe why the entity would choose these methods and how employees could circumvent them.

1. Blocking IP-Addresses: is very simple for the company - use TOR or VPN

2. DNS-Filtering: also rather simple for the company as they can block the domain or redirect them - change DNS or use DoH
3. URL Filter: the company could also block URL, more flexible in comparison to DNS filter (which blocks whole domains, but with URL filter you can only block a website) - use TOR or VPN

2) (3pts)

You also published the information over .onion services. An employee of the company has problems connecting to Onion services via Tor. What is an explanation for this blocked Tor access, and how could the employee still connect to the Onion service?

Company could also blocked tor or the .onion domain, the employee could use bridges or use pluggable transport (snowflakes) to get access to the Onion service.

3) (4pts) You expected censorship problems. How would you publish the information to make censorship more difficult?

Make use of overblocking, use domains e.g. google which are too costly to block (maybe with domain fronting over a legitimate host)

Provide information over onion services

Use DoH, looks like a normal https form the outside

(4pt) Describe **in your own words** how Tor works. How many relays are involved in a regular Tor connection? What would be different if there were more, or less relays?

The Tor Browser hides your IP address and browsing activity by redirecting web traffic through a series of different routers known as nodes.

A regular Tor connection uses three relays.

It would not make difference if there were more except that it would slow down speed, if you use less relays your path could be tracked: One would be pointless, since whoever operates that node you chose will see everything. Two is dangerous, because the entry and exit nodes would then be directly connected.

(3pt) How many Tor relays are there right now, and what are the top-3 countries hosting them? Where can you look this information up?

There are approx. 6000 24/7 Tor relays world-wide probably on Tor (metrics)?

(3pt) What does the usage of Tor protect against, what does it NOT protect against?

The use of Tor decouples you from your IP address and protect against tracking, it does not protect against a global adversary who can see everything (like a low latency systems) and Man In the Middle attacks on encrypted exit relay traffic.

Your company (Evil Corp) announced a new IT policy: employees must exclusively use Evil Corp's DNS System on all their devices (smartphones, laptops, etc.).

The change is required for "IT-security" protection and Evil Corp is also asking employees to change the DNS settings on their private devices.

Analyse the impact of this new DNS policy in the following.

1) (3 pt) Which information does Evil Corp receive if you use their DNS system?

DNS monitoring can discover and track IP addresses of DNS requests and log every website viewed by a device connected to your network. This helps your network team find out which websites your employees are visiting and how long it takes to complete the DNS request.

2) (3 pt) Would only using websites with HTTPS protect your privacy?

No, the hostname is still visible in the initial TLS handshake

<https://shop.com/offers/feber/mediacation>

HTTPS ensure that the data you send and receive on the website is encrypted and secure.

However, HTTPS only protects the data in transit between your browser and the website, not the data on either end.

3) (4 pt) Briefly describe to your co-worker why he/she should be concerned with a short "nothing to hide" counter example

Everyone still needs privacy, if he/she is looking at a new job on any on his/her devices the company will know that

(4pt) Explain **in your own words** how Tor Onion (Hidden) services work. How many Tor relays are involved per connection?

Tor Onion/ Hidden services in general: no geolocation based on IP is possible

-> only reachable through the TOR network

-> two connection are needed

-> one to protect ip address of user and one to protect ip address of server

How to:

- setup hidden service locally
- server (Bob) chooses tor relays as introduction points IP and build circuits to them
- server advertises his hidden service xyz.onion to the database (by sending service descriptor (= public key, introduction points, etc just info))
- client has to know .onion address and request more info from the database

- client chooses rendezvous point RP
- client writes message listing RP and one time secret and asks IP to deliver it to server
- server connects to client's RP and provides one time secret
- client and server have a normal tor circuit over RP as normal

In a hidden service 7 relays are needed (3 for connection for each side + RP)

(2pt) What is the difference between v2 and v3 Tor Onion services? Why are Onion Services v3 better than v2?

- V3: Longer names that encode the actual ed25519 key of the onion service into the name
-> better cryptography
- V2: Shorter names that are a hash of the RSA public key of the onion service
- result: 56 characters instead of 16 (before: 2-7 and a-z)
-> makes it even harder to brute force
- and cleaner code base

(2pt) Is it useful to have a TLS certificate for your Onion services? What are the benefits, if any?

- to help the user verify that the .onion address is indeed the site you are hosting
- some services work with protocols, frameworks, and other infrastructure that has HTTPS connection as a requirement
- the last hop from the exit node to the server can be encrypted in clear!
Use TLS / HTTPS to encrypt this traffic (ONLY FOR TOR NOT ONION SERVICES!)

(2pt) How do you get a onion domain like "facebookcorewwwi.onion"? Other domains look random compared to this. So, how does this work and why?

Addresses are generated automatically, and usually they are an unreadable set of characters, almost impossible to remember.

You cannot customly create a .onion domain name, but you can create a large number of random names and choose the appropriate ones from them. With the help of **special programs** you can automate and speed up this process by using gpu or cpu. It looks for domain addresses that match one of the entered regular expressions

The ongoing pandemic led to a surge of online projects from publishing houses.

You signed a contract with a well established Austrian newspaper to develop "AnoUp" - a whistle blower platform for submitting sensitive documents without exposing your identity.

Part foolishness, part excess budget - they want you to develop this system from scratch.

1) (5 pt) Sender IP Anonymity

Describe how you would protect the IP of the whistle blowers.

ChatGPT:

- Implement Onion Services: Onion Services, also known as Tor hidden services, allow users to connect to your platform without revealing their IP address. By using an onion service, users can access your platform anonymously and securely. However, you will need to ensure that your platform is designed to work well with onion services, as there are some limitations and considerations to keep in mind.
- Use a Proxy Server: A proxy server can act as an intermediary between your users and your platform, and can help to hide their IP addresses. By routing traffic through a proxy server, the IP addresses of your users will be masked, and their activities will be more difficult to monitor.
- Implement IP address anonymization: Implement IP address anonymization techniques, such as hashing or truncation, to ensure that user IP addresses cannot be traced back to their specific device or location.

2) (5 pt) Automated removal of identifying information from uploaded documents

The system should allow two file types: pdf, jpg. Describe which information needs to be removed for these file types and suggest how this could be done automatically.

ChatGPT:

- Remove metadata: PDF and JPG files can contain metadata such as author name, date created, and location.
- Remove embedded fonts: PDF files can also contain embedded fonts that may be unique to a particular device or user.
- Remove file properties: JPG files can contain file properties such as camera make and model, which can be used to identify the user.
- Remove personal information: PDF files can contain personal information such as names and contact details.

The first three can be done via a self written program, but for the last one needs some more training as it might be hard to recognize what 'personal' information is.

There is this new shiny messenger app. It calls itself "Titanic" and promises to support military-grade encryption. Military-grade encryption sounds good, so many people think it's secure.

1) (4pts)

While examining the application, you observe that it is using TLS. That is good, but you can perform MITM attacks from your local WIFI.

Why is that possible? What could Titanic do to prevent this?

My guess: CA was not trustworthy and got hacked, similar to DigiNotar -> MITM issued certificates and because all certificates are trusted the same, no one noticed

ChatGPT:

It is possible if the attacker has access to the network traffic, such as through a compromised WiFi

network. This is because the attacker can intercept the traffic between the app and the server and then decrypt and read the traffic.

To prevent MITM attacks, the app can take the following steps:

1. Certificate Pinning: Use certificate pinning to ensure that the app only accepts certificates from trusted sources. This prevents attackers from using fake or self-signed certificates to intercept traffic.
2. Strict Transport Security (HSTS): Implement HSTS to ensure that the app only communicates over HTTPS and not HTTP. This prevents attackers from downgrading the connection to HTTP and intercepting traffic.
3. Certificate Transparency: Use certificate transparency to ensure that any new certificates issued for the domain are publicly logged. This allows for quick detection of any fraudulent certificates issued for the domain.

2) (4pts)

There is also this cool One-Time-Photo feature. It is perfect to share your "holiday photos" because you can only look at these photos once. After some time, you spot your "holiday photos" on some websites in the Internet. Your original recipient was trustworthy and did not screenshot your message, so how could that happen?

ChatGPT

1. App vulnerabilities: The app itself may have a vulnerability that allows photos to be saved or accessed after they are supposed to be deleted. This could be due to a coding error or security flaw in the app.
2. Provider can read all messages: Provider could have sold pictures to third parties
3. Man-in-the-middle (MITM) attacks: An attacker may have intercepted the traffic between the app and the server, allowing them to access and save the photo before it was deleted.

3) (2pts)

In an additional security mode of the app, the messages are end-to-end encrypted. Do you think that this extra mode is good or bad for privacy, and why?

Good because the provider is unable to read messages and only clients can decrypt messages. It protects against eavesdropping and reduces data break because even if messages are intercepted, they cannot be read without a decryption key.

You want to protect your DNS queries from the snooping eyes of your Internet Services Provider.

In addition, you want to hide your request IP from alternative encrypted DNS services.

Discuss how to implement your DNS privacy goals.

1) (3 pt) Which options do you have for private DNS queries. (You are only concerned about your Internet Service Provider and not alternative DNS service providers)

Use VPN, using a VPN encrypted the sites you used and in this way the web sites cannot be decrypted. VPN creates a secure, encrypted connection between the user's device and the VPN server, which can prevent DNS queries from being intercepted or monitored.

Or use private DNS providers, they ensure private DNS queries.

2) (3 pt) Which DNS privacy protocol would you prefer if you are also concerned about potential censorship (blocking of encrypted DNS services)?

You can use DoH, for provider it looks like a standard encrypted web browsing HTTPS

3) (4 pt) Discuss which methods exist to protect the client IP of DNS query from leaking to DNS service providers?

Use Proxies, proxy servers can act as an intermediary between the client and DNS service providers, masking the client IP address from DNS service providers.