IERG4210 2014-15 Term 2 Tutorial 9

Wenrui Diao
Department of Information Engineering
The Chinese University of Hong Kong

Outline

1. <u>Domain Name</u>
2. Assignment Phase 4b -- Apply SSL certificate

Domain Name

- A Level-2 domain name like storeXX.ierg4210.org has been assigned to you.
- XX → your shop ID

- Now you could assess your website via the above domain name.

Domain Name

4. Branch out **phase3b** in your repository, where TAs can checkout for inspection
   - Include a README.md file in your repo and document your application URL

- If you can not access it, the reasons:
- You didn't provide your application URL (xxxx. elasticbeanstalk.com) in your github respository. Since I don't know your application URL, I can not set DNS configuration for you.
  - Solution: Send your name, SID, application URL and Shop ID to me: dw013@ie.cuhk.edu.hk
  - Upon receiving your email, I will process it in three days.

- Your application URL (xxxx.elasticbeanstalk.com) is inaccessible.
  - Solution: Debug by yourself

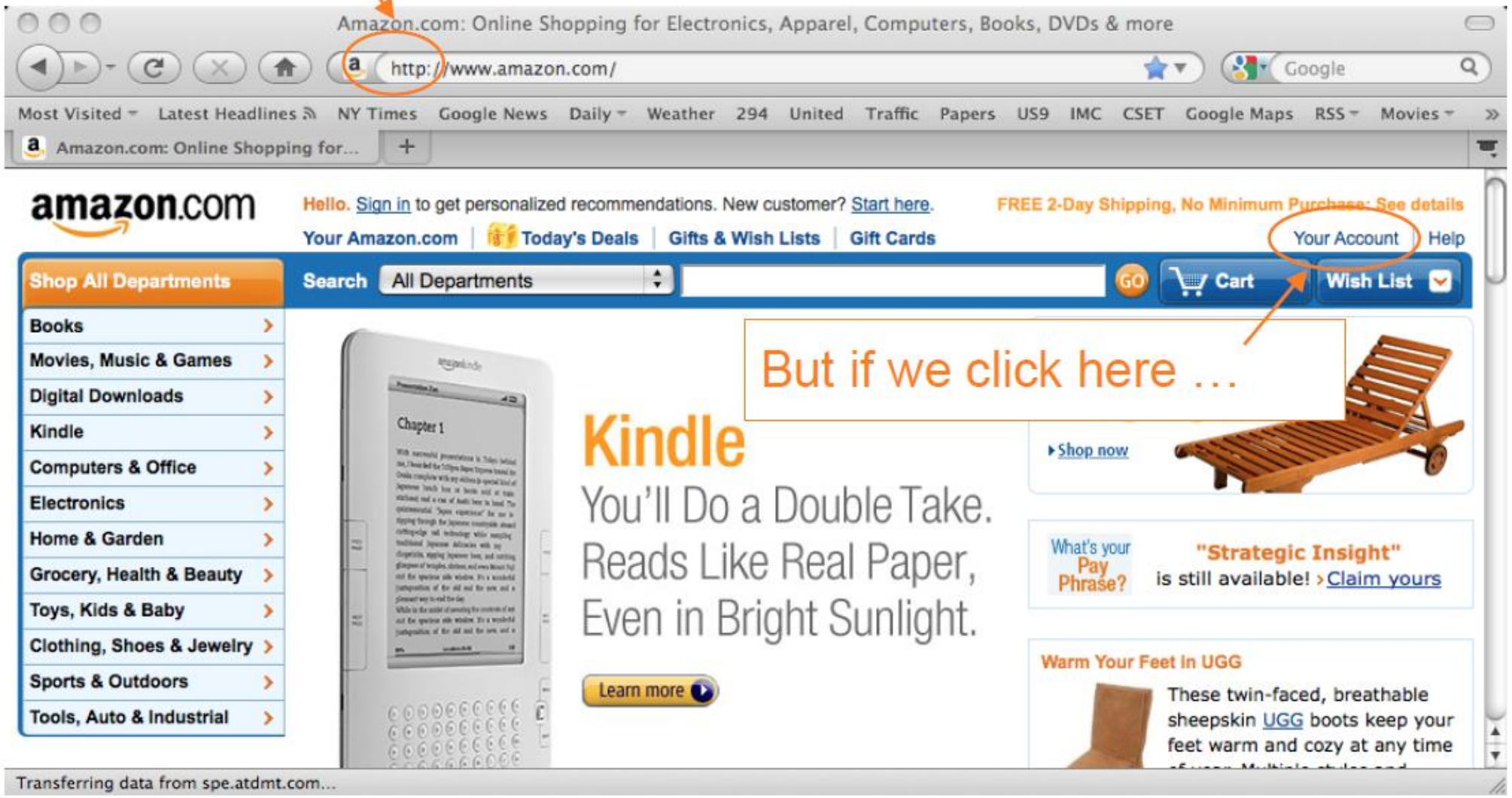
Outline

1. Domain Name
2. <u>Assignment Phase 4b -- Apply SSL certificate</u>

What is SSL / TLS?

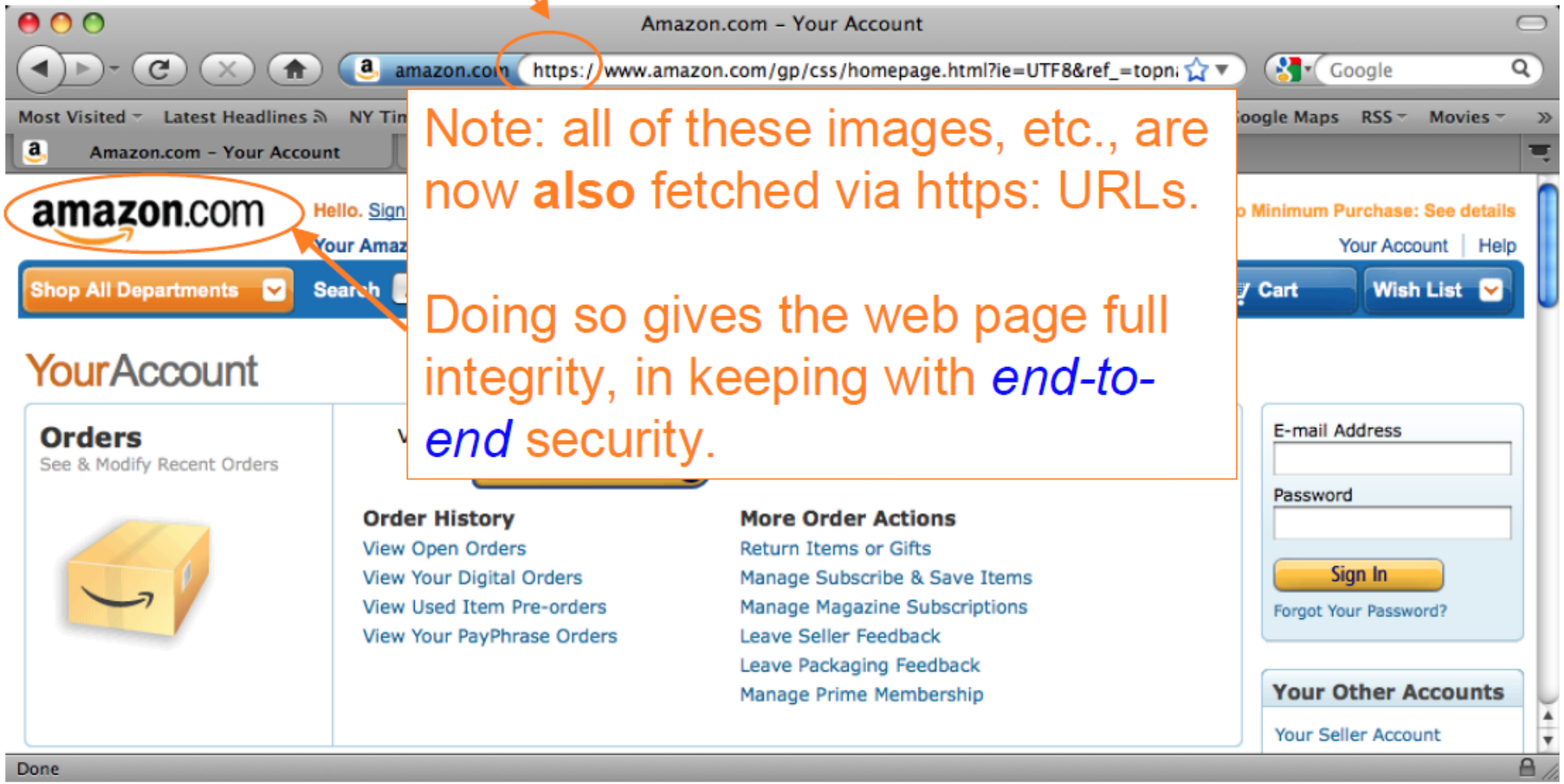
- Transport Layer Security protocol, ver 1.0
  - De facto standard for Internet security
  - “The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications”
  - In practice, used to protect information transmitted between browsers and Web servers
- Based on Secure Sockets Layers protocol, ver 3.0
  - Same protocol design, different algorithms
  - TLS 1.1, 1.2, …
- Deployed in nearly every web browser
- *More contents will be covered in the lecture.*

Regular web surfing - http: URL



But if we click here …

Web surfing with TLS/SSL - https: URL



Note: all of these images, etc., are now **also** fetched via https: URLs.

Doing so gives the web page full integrity, in keeping with *end-to-end* security.

Assignment Phase 4b -- Apply SSL certificate

- Certificate Application
  - -- Apply a 90-day free certificate from FreeSSL.su

- Certificate Installation
  - -- Elastic Beanstalk load balancer settings

- For more details, please check http://ierg4210.github.io/web/assign-spec/AssignmentMarkingChecklist4.1.pdf

Create a private key and CSR

- Openssl is preinstalled in most Linux distribution versions, like Ubuntu

- Generate the private key
- $ openssl genrsa 2048 > privatekey.pem

never upload it to github

```
diaowenrui@ubuntu:~/4210Amazon$ openssl genrsa 2048 > privatekey.pem
Generating RSA private key, 2048 bit long modulus
.....+++
.....................................................................
.......................+++
e is 65537 (0x10001)
```

Create the Certificate Signing Request (CSR)

- $ openssl req -new -key privatekey.pem -out csr.pem

```
diaowenrui@ubuntu:~/4210Amazon$ openssl req -new -key privatekey.pem -out csr.pe
m
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:HK
State or Province Name (full name) [Some-State]:Hong Kong
Locality Name (eg, city) []:Hong Kong
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CUHK
Organizational Unit Name (eg, section) []:IERG4210
Common Name (e.g. server FQDN or YOUR name) []:store97.ierg4210.org
Email Address []:diaowenrui@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

It will be shown in your certificate.

To show your CSR:

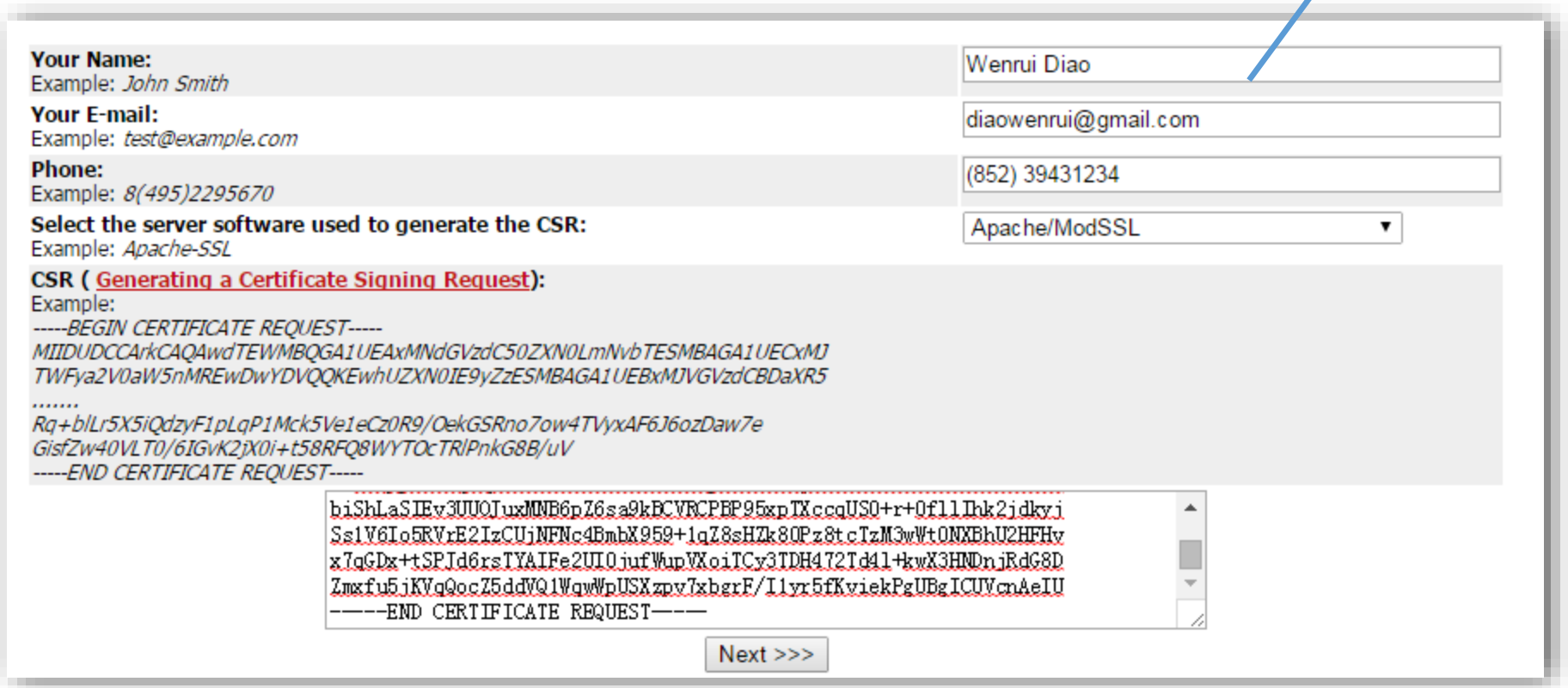
- $ cat csr.pem
- It will be used in the next step

```
(local-dev-env)diaowenrui@ubuntu:~/4210Amazon$ cat csr.pem
-----BEGIN CERTIFICATE REQUEST-----
MIICzDCCAbQCAQAwgYYxCzAJBgNVBAYTAkhLMRIwEAYDVQQIDAlIb25nIEtvbmcx
DTALBgNVBAoMBENVSEsxETAPBgNVBAsMCElFUkc0MjEwMRwwGgYDVQQDDBNzaG9w
OTcuaWVyZzQyMTAub3JnMSMwIQYJKoZIhvcNAQkBFhRkdzAxM0BpZS5jdWhrLmVk
dS5oazCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL+li/d7J6HKNUjZ
G4+Ds3W2bhDLi12n57/bUOxHn6c9yME3bkAUtAJAx1jHQrh5KUv5bdJzJp7jyDVJ
pt5Ny/hBoQiGmyYGXqe2MwD0q/HQhNqOeiEBWtrBXregLeHZlhf3x4JPxuZwef6k
civS3ZdjgQdWRrhDyY1W9FvQb4JXpvQITwWxCl3kBgsYHLQ0blKMffwOy6Mmasad
/YuMXdhzEEzIqBzF5oDzk+2g/BqZmiExCE9Z2n4CVU/o3DTTV3lVf97yzIushHqI
ZPKEmRXXljdKMIq2O1HLqe0Y6VtCzpZg2YP4hvLSnTw+Ot79nVQyiTc7qzdvR3ej
Y68fgZ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQAkRcJn0M/nZUgZa3qGAbF7
c/voxpp91Crq0qQ2AF9vImZKP2IROdXHEy67UkMcOjluASPSEZ6GAmUXBtPierev
biShLaSIEv3UUOJuxMNB6pZ6sa9kBCVRCPBP95xpTXccqUS0+r+0fllIhk2jdkyj
Ss1V6Io5RVrE2IzCUjNFNc4BmbX959+1qZ8sHZk80Pz8tcTzM3wWt0NXBhU2HFHv
x7qGDx+tSPJd6rsTYAIFe2UI0jufWupVXoiTCy3TDH472Td4l+kwX3HNDnjRdG8D
Zmxfu5jKVqQocZ5ddVQ1WqwWpUSXzpv7xbgrF/I1yr5fKviekPgUBgICUVcnAeIU
-----END CERTIFICATE REQUEST-----
```

Certificate Application

- Go to http://www.freessl.su/

Change to your own Information. This Email address will be used to receive the certificate.



Your Name:
Example: *John Smith*
Wenrui Diao

Your E-mail:
Example: *test@example.com*
diaowenrui@gmail.com

Phone:
Example: *8(495)2295670*
(852) 39431234

Select the server software used to generate the CSR:
Example: *Apache-SSL*
Apache/ModSSL

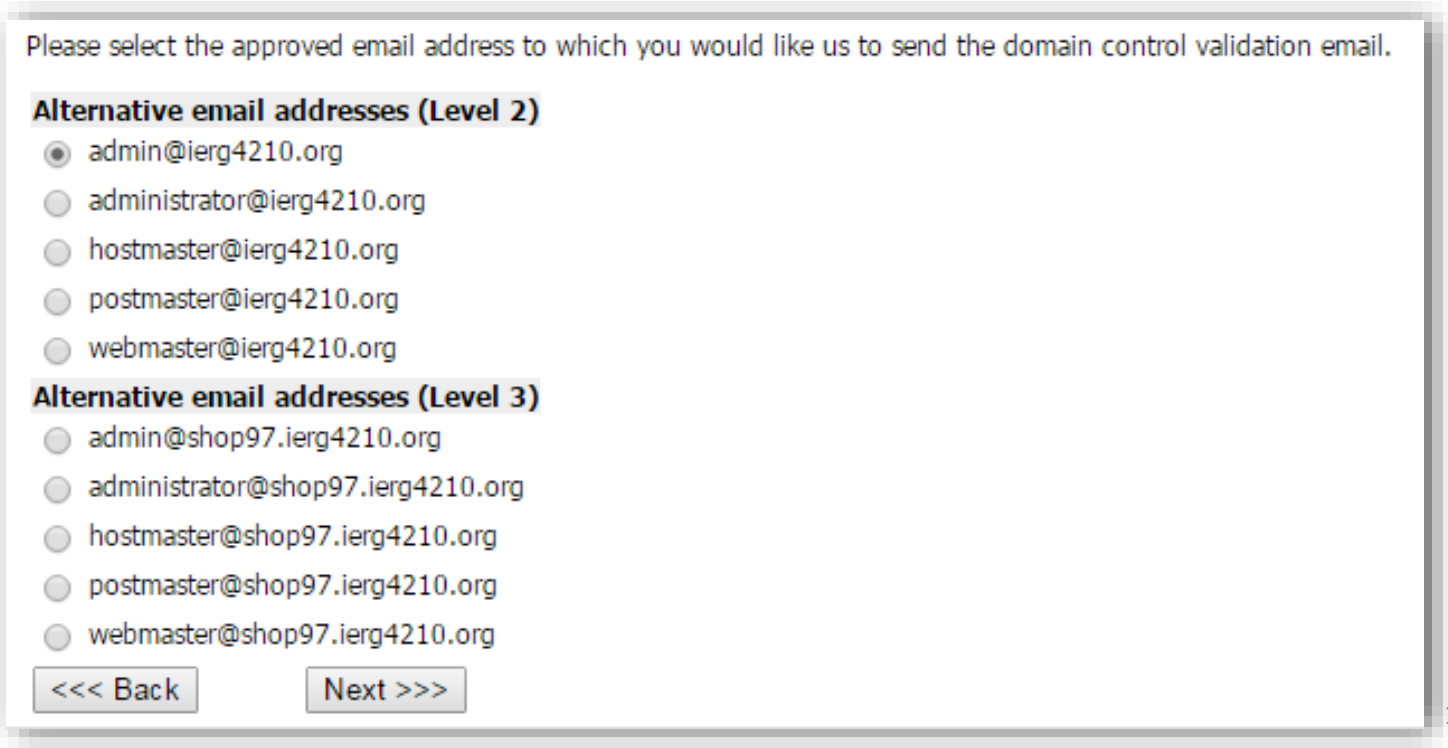
CSR (Generating a Certificate Signing Request):
Example:
-----BEGIN CERTIFICATE REQUEST-----
MIIDUDCCArkCAQAwdTEWMBQGA1UEAxMNdGVzdC50ZXN0LmNvbTESMBAGA1UECxMJ
TWFya2V0aW5nMREwDwYDVQQKEwhUZXN0IE9yZzESMBAGA1UEBxMJVGVzdCBDaXR5
.....
Rq+blLr5X5iQdzyF1pLqP1Mck5Ve1eCz0R9/OekGSRno7ow4TVyxAF6J6ozDaw7e
GisfZw40VLT0/6IGvK2jX0i+t58RFQ8WYTOcTRlPnkG8B/uV
-----END CERTIFICATE REQUEST-----


```
biShLaSIEv3UUOJuxMNB6pZ6sa9kBCVRCPBP95xpTXccqUS0+r+0fllIhk2jdkyj
Ss1V6Io5RVrE2IzCUjNFNc4BmbX959+1qZ8sHZk80Pz8tcTzM3wWt0NXBhU2HFHv
x7qGDx+tSPJd6rsTYAIFe2UI0jufWupVXoiTCy3TDH4T2Td41+kwX3HNDnjRdG8D
Zmxfu5jKVqQocZ5ddVQ1WqwWpUSXzpv7xbgrF/I1yr5fKviekPgUBgICUVcnAeIU
-----END CERTIFICATE REQUEST----
```


Next >>>

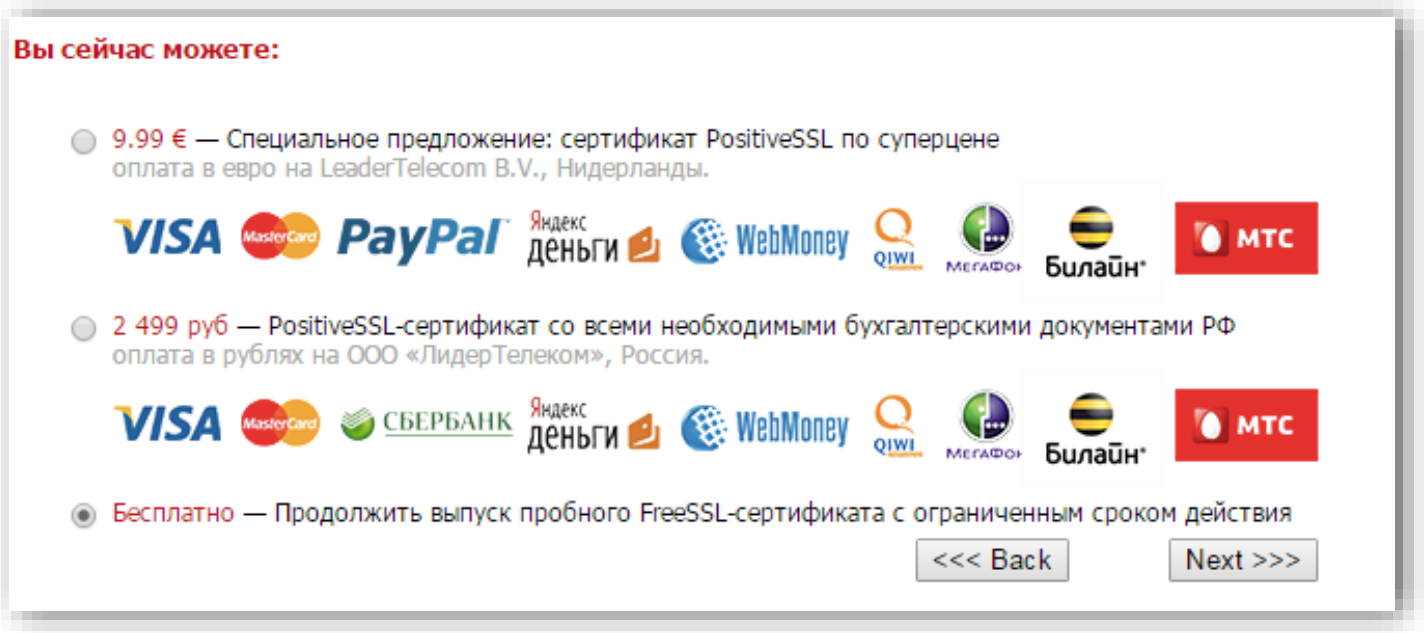
Certificate Application

- For Domain Control Validation, choose admin@ierg4210.org as the approved email address to prove domain ownership. The TA team upon receiving an email from Comodo will help you authorize such a SSL cert application.



Certificate Application

- Choose the last one.



- It then take an hour or up to 2 days to have the cert signed by Comodo and emailed to you (in an attachment ssl_certificate.zip).

Upload the private key and signed cert

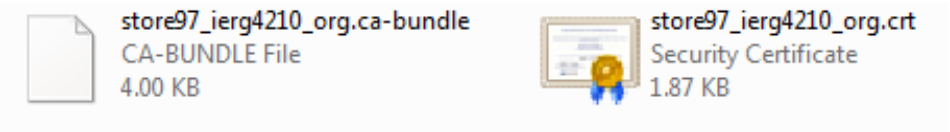
- Install the aws client
- $. local-dev-env/bin/activate
- $ pip install aws
- $ pip install awscli

- You may need to set the access key (which you got in your previous phase) if you face the permission deny problem
- $ aws configure

Upload the private key and signed cert

- $ aws iam upload-server-certificate --server-certificate-name comodo-signed-shop97-2015 --certificate-body file://~/4210Amazon/cert/store97_ierg4210_org.crt --private-key file://~/4210Amazon/cert/privatekey.pem --certificate-chain file://~/4210Amazon/cert/store97_ierg4210_org.ca-bundle

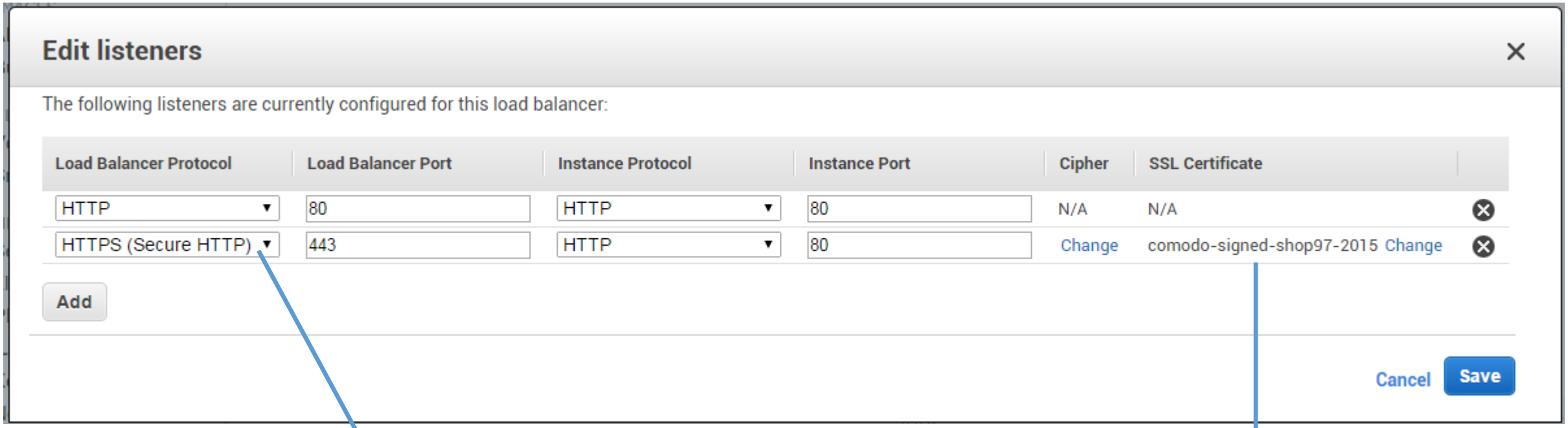
```
(local-dev-env)diaowenrui@ubuntu:~/4210Amazon/cert$ aws iam upload-server-certif
icate --server-certificate-name comodo-signed-shop97-2015 --certificate-body fil
e://~/4210Amazon/cert/store97_ierg4210_org.crt --private-key file://~/4210Amazon
/cert/privatekey.pem --certificate-chain file://~/4210Amazon/cert/store97_ierg42
10_org.ca-bundle
{
    "ServerCertificateMetadata": {
        "ServerCertificateId": "ASCAJ2MCSDGBJWT5OOG36",
        "ServerCertificateName": "comodo-signed-shop97-2015",
        "Expiration": "2015-06-12T23:59:59Z",
        "Path": "/",
        "Arn": "arn:aws:iam::096581827784:server-certificate/comodo-signed-shop9
7-2015",
        "UploadDate": "2015-03-15T03:10:14.648Z"
    }
}
```



Change them according to your received files.

Elastic Beanstalk load balancer settings

- EC2 Dashboard → Network & Security → Load Balancers → Edit listeners

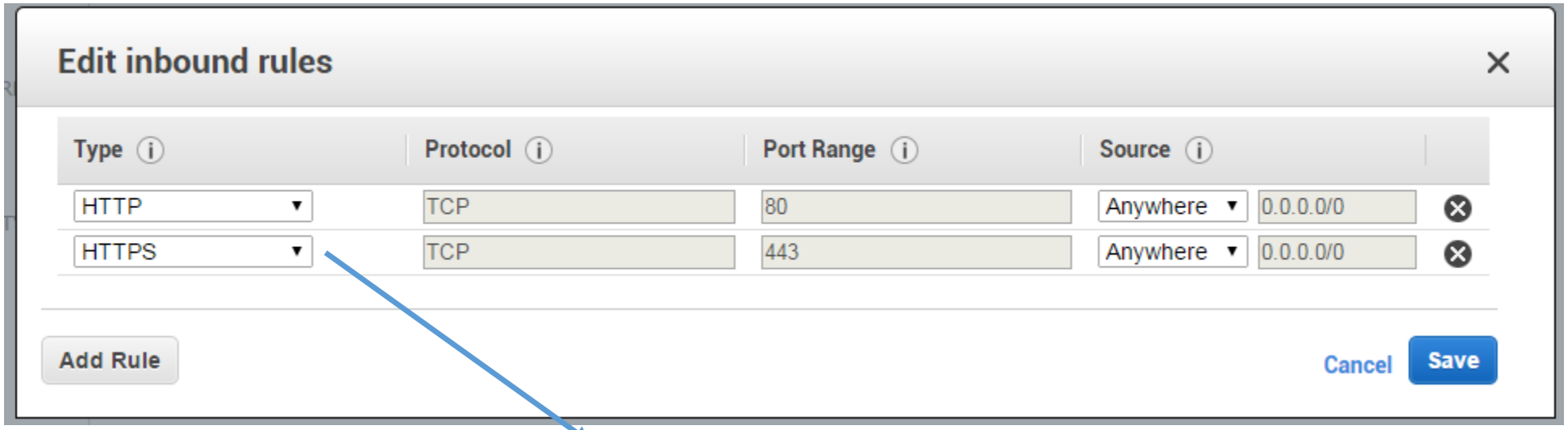


Add HTTPS Protocol

Choose the certificate you uploaded

Elastic Beanstalk load balancer settings

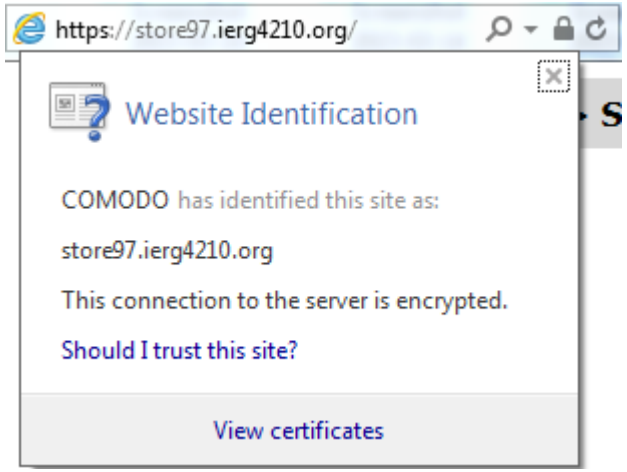
- EC2 Dashboard → Network & Security → Security Groups → Choose the one with the description “ELB created security group used when no security group is specified during ELB creation - modifications could impact traffic to future ELBs”
- Edit inbound rules

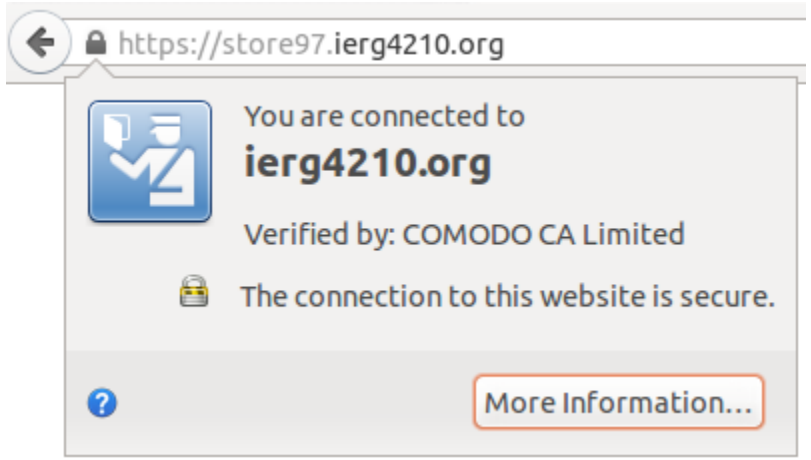


Add rules for HTTPS

Test

- After a few mins, visit your website https://shopXX.ierg4210.org to verify.





Enforce the admin panel /admin to https

```
app.use('/admin', function(req, res, next) {
  var schema = req.headers['x-forwarded-proto'];

  if (schema === 'https') {
    // Already https; don't do anything special.
    next();
  }
  else {
    // Redirect to https.
    res.redirect('https://' + req.headers.host + req.url + '/admin');
  }
});
```

Demo and Q&A

- Ref (prepared by Dr. Fung):
- https://github.com/ierg4210/shop-samples/blob/master/SETUP-CERT.md

- Some contents are borrowed from
- http://inst.eecs.berkeley.edu/~cs161/fa14/
- http://www.stanford.edu/class/cs259