Vertix
it je naše starost

Co-funded by the
Erasmus+ Programme
of the European Union

How to secure web server

Ing. Jan Budina, System Engineer

What is webserver?

Web server is an information technology that processes request via HTTP protocol, which is used to distribute information on the world wide web.

Most common types

- Apache web server
- Microsoft Internet Information Service (IIS)
- Nginx web server

How to make basic security

- install security patches regularly
- deploy SSL certificate
- allow only safe ciphers
- avoid SQL injection attack
- avoid DoS attack

Security patches

- necessary for basic security
- better to test new patches on laboratory environment
- Microsoft reveals updates every month
- Linux are more flexible for updates
- read about new attacks and vulnerabilities in web server technologies

Using SSL (HTTPS)

WHY?

- somebody can fake information between computer <-> web server
- somebody can steal your login and password
- all communication is unencrypted visible for everybody

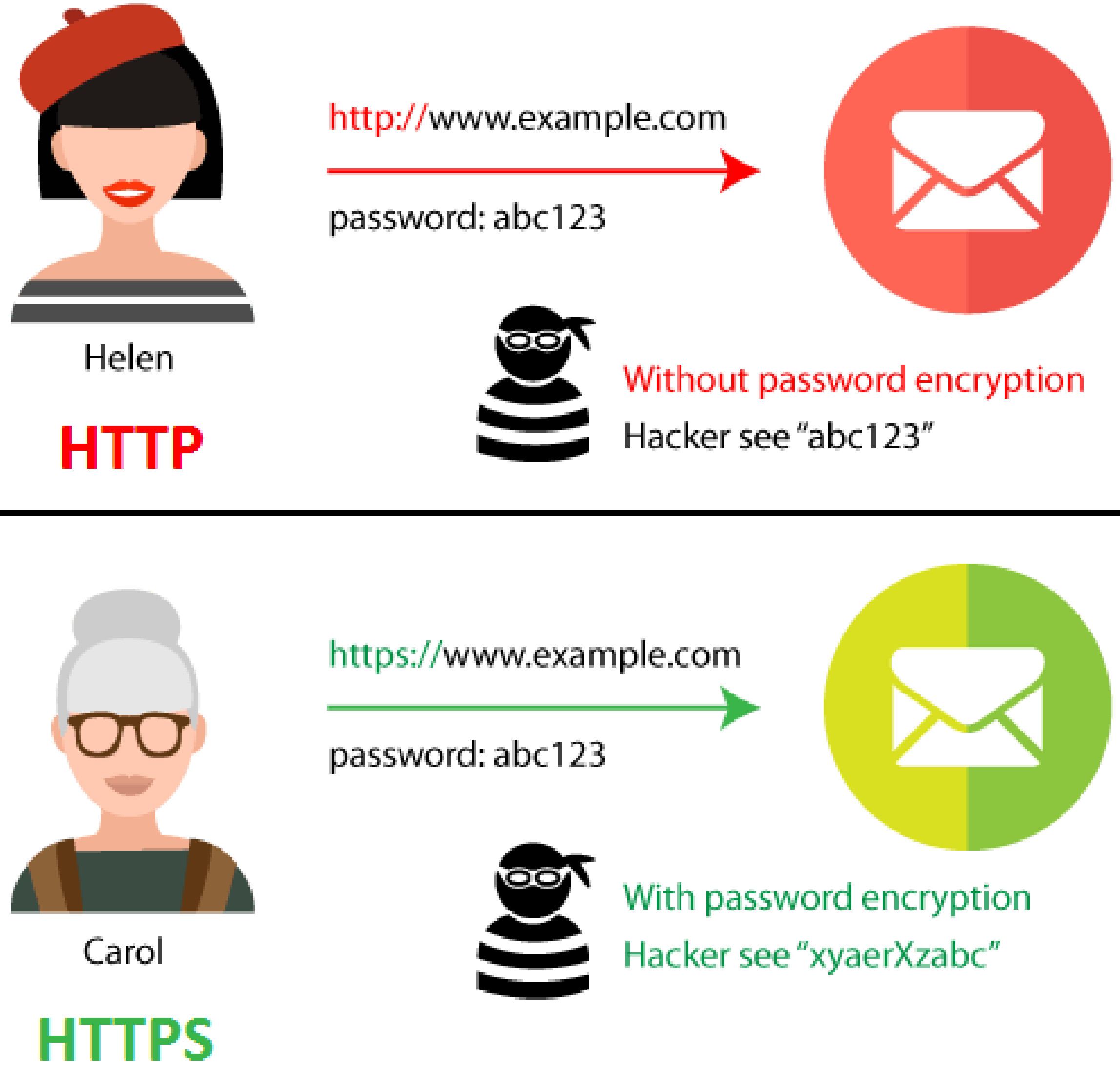
SSL provides two important functions

- **SSL Encryption** – allow user to transmit data over internet securely
- **Identity validation** – verifies whether the server is legitimate or not

SSL provides two important functions

- **SSL Encryption** – allow user to transmit data over internet securely
- **Identity validation** – verifies whether the server is legitimate or not

How to secure web serever



Helen

HTTP

http://www.example.com

password: abc123

Without password encryption

Hacker see "abc123"

Carol

HTTPS

https://www.example.com

password: abc123

With password encryption

Hacker see "xyaerXzabc"

How to secure web serever

What you need to enable HTTPS?

- get an SSL Certificate
- generate CSR (Certificate Signing Request) and Private key
- validate your domain and business
- install your certificate on your server

Most common certificate authorities

- GeoTrust
- RapidSSL
- thawte
- Comodo

Installation on web server

- many tutorials on certificate authorities webpage
- also videos on youtube

Installation on web server

That is all?

Installation on web server

NO

Define allowed ciphers

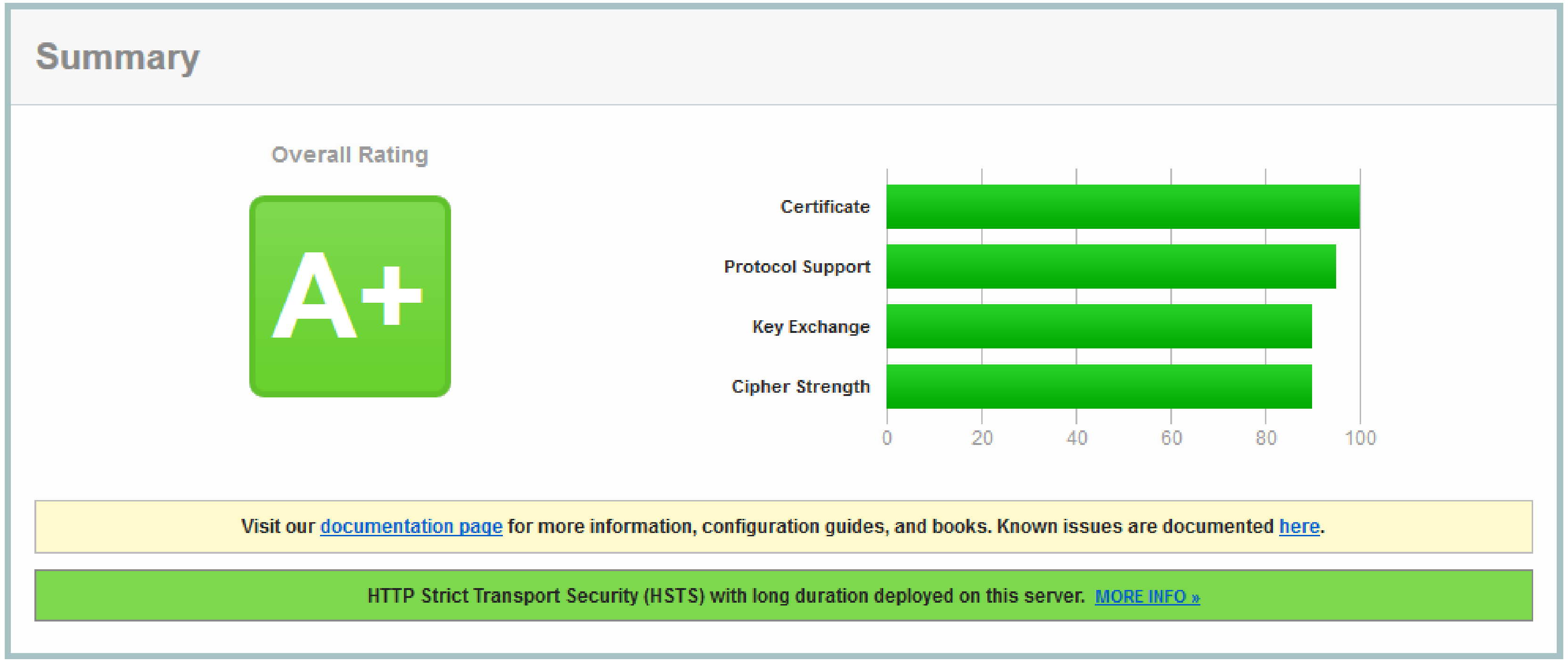
- many ciphers are allowed by default
- need to find which one is old or unsecure
- basicly these are not secure:
  - SSL 2.0, SSL 3.0, TLS 1.0 with compression, TLS 1.2 and many others

Example for Apache web server

```
SSLProtocol all -SSLv2 -SSLv3
SSLHonorCipherOrder on
SSLCipherSuite
ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:ECDH+3DES:DH+3DES:RSA+AESGCM:RSA+AES:RSA+3DES:!aNULL:!MD5:!DSS
```

How to test my SSL settings?

- test on SSL labs for free
- https://www.ssllabs.com/ssltest/



Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Vertix

it je naše starost

Hacking Windows Active Directory

Ing. Jan Budina, System Engineer

Are you using Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016?

You are hack able

You will see it right now

It is not a tutorial how to hack Windows Server!

Vertix

it je naše starost

VERTIX s.r.o.
Štrossova 291
530 03 Pardubice

www.vertix.cz