TU Wien
Institut für Information Systems Engineering
Forschungsgruppe Industrial Software
Arbeitsgruppe ESSE
https://establishing-security.at/

Abgabedokument Lab1

Einführung in Security

194.157 – 2024 W

17. Dezember 2024

Team 44

Name	**MatrNr.**
Kevin Csele	12122544
Clemens Schneider	MATRIKELNUMMER
Luka Twaroch	MATRIKELNUMMER
Wen Long Zhou	MATRIKELNUMMER
Ramin Shaikh	12123657

Inhaltsverzeichnis

1 Der Service war auch schon besser ...

1.1 Achtung! Streng geheim!

Um diese Aufgabe zu lösen, hat es genügt, das besagte PDF im Browser zu öffnen. Der “streng geheime“ String befand sich im Titel des Tabs.

1.2 Eine schräge Nummer

Die Rechnungsnummer wurde zwar von einem schwarzen Rechteck verdeckt, ließ sich jedoch ganz einfach kopieren, indem man die betroffene Stelle markiert -> Strg + C

1.3 Was letzte Preis?

Selbes Spiel, auch der Preis ließ sich ganz simpel herauskopieren.

1.4 IBANs sollte man verbannen!

Um den IBAN aufzudecken, habe ich PDF-XChange verwendet, um das schwarze Rechteck mit dem Objektbearbeitungswerkzeug zu entfernen.

2 Wireless Time Travel

2.1 Vier zukunftssichere Handschläge

Nicht gelöst.

2.2 Code der Zukunft

Nicht gelöst.

2.3 Ungewöhnlich verschlüsselte Botschaft

Nicht gelöst.

2.4 Geheimnisvoller Zugang: superboss

Nicht gelöst.

2.5 Unbrauchbarer Schlüssel

Nicht gelöst.

2.6 Einen Schlüssel für einen Schlüssel! Echt jetzt?!

Nicht gelöst.

2.7 Verborgenes Protokoll

Nicht gelöst.

3 Bot Bot Bot Bot

3.1 I keep you my little secret ...

Nicht gelöst.

4 Cäsars Schlüsselbund

4.1 Schlüssel. Knacken.

Nicht gelöst.

4.2 Passwörter Retten.

Nicht gelöst.

5 Paranoider Mozart

5.1 MozART.

Nicht gelöst.

6 Zertifiziertes Durcheinander

6.1 Zertifizieren ist schwer

Um den Certificate Signing Request zu erstellen habe ich den folgenden Befehl verwendet: `openssl req -newkey rsa:4096 -sha512 -config openssl.cnf -out csr.csr -subj "/CN=12123657-Intermediate-CA-WS2024/OU=ESSE-Lab1-Exercise"`
`req` ist der Befehl um einen CSR zu erstellen;
`-newkey rsa:4096` spezifiziert, dass ein neuer Key (4096-Bit RSA) erstellt werden soll;
`-sha512` gibt an, dass sha512WithRSAEncription als Signaturalgorithmus verwendet werden soll;
mit `-config` wird angegeben, welches config file zu verwenden ist;
`-out` bestimmt das output-file und
`-subj "/CN=12123657-Intermediate-CA-WS2024/OU=ESSE-Lab1-Exercise"` definiert die gewünschten Namens-Parameter im CSR.

Das config file dient dazu, die nötigen X509v3 Parameter zu setzen und sieht aus wie folgt:

```
[ req ]
default_bits            = 4096
default_md              = sha512
default_keyfile         = privkey.pem
distinguished_name      = req_distinguished_name
req_extensions           = v3_req

[ req_distinguished_name ]

[ v3_req ]
subjectKeyIdentifier = hash
basicConstraints = critical, CA:true, pathlen:0
keyUsage = critical, Certificate Sign, CRL Sign
```

Listing 1: openssl.cnf

Nach Ausführung des oben genannten Befehls, wird der CSR in der Datei csr.csr gespeichert, diese wurde im Abgabetool eingereicht.

7 Zeitreise durch das World Wide Web

7.1 Wieder Elvis

Nicht gelöst.

7.2 CäsarMussWeg! MussCäsarWeg?

Nicht gelöst.

7.3 dackboor.

Nicht gelöst.

7.4 Schlechtes Timing (Time Travel Edition)

Nicht gelöst.

7.5 Sorcerer ... ?

Nicht gelöst.

8 Seitlich fließend

8.1 Newton und Co KG.

Nicht gelöst.

9 Antike Mobile Security

9.1 iTimeTravel

Nicht gelöst.

9.2 AND(roid)ERS

Nicht gelöst.

10 Babycam Espionage

10.1 The Rise of the HuManoiD5

Nicht gelöst.

10.2 ETA

Nicht gelöst.

11 Das Social Media der Zukunft

11.1 Der vergiftete Passwort Reset

Nicht gelöst.

11.2 Accountübernahme

Nicht gelöst.

12 Hidden Timelines

12.1 Phantom Domain

Nicht gelöst.

13 Vault Voyage

13.1 That's all your vault!

Nicht gelöst.

14 Wikinger Overflow

14.1 Überlauf. Hand drauf.

Nicht gelöst.

14.2 Typisch Typing ... Stufe 1

Nicht gelöst.

14.3 Typisch Typing ... Stufe 2

Nicht gelöst.

14.4 Typisch Typing ... Stufe 3

Nicht gelöst.

15 Tap to the Future

15.1 Tick Tock Tap

Nicht gelöst.

16 So viele

16.1 Das Device ist heiß

Nicht gelöst.

16.2 Persona non grata

Nicht gelöst.

16.3 Eine Frage der Kommunikation

Nicht gelöst.

16.4 Treffpunkt

Nicht gelöst.

16.5 Alles dokumentiert!

Nicht gelöst.

16.6 Es geht immer um Inhalte

Nicht gelöst.

17 Web of Treats

Nicht gelöst.

17.1 Mitgliedschaftsnr.

Nicht gelöst.

17.2 Geheimer Artikel

Nicht gelöst.

17.3 Überfüllt

Nicht gelöst.

17.4 A shell in the forest?

Nicht gelöst.

17.5 Elvis

Nicht gelöst.

18 Das. Beste. Text. Adventure. Aller. Zeiten.

18.1 Time to travel!

Nicht gelöst.

18.2 Mein Name?

Nicht gelöst.

18.3 Ein PIN!

Nicht gelöst.

18.4 Ach ... ein Schlüssel

Nicht gelöst.

18.5 Flag!

Nicht gelöst.

19 Passwörter werden wir auch nie los, oder?!

19.1 Gute Idee, um ein Passwort zu verstecken?!

Nicht gelöst.

19.2 Call Julius ... äh. John.

Nicht gelöst.

19.3 Nicht nur Ziffern, sonder auch ...?

Nicht gelöst.

19.4 /etc/ANTIK?

Nicht gelöst.

19.5 Sicher sicher?

Nicht gelöst.

19.6 Zeitlose Liste

Nicht gelöst.

19.7 (Image)magic(k)

Nicht gelöst.

19.8 Auch in Zukunft ein schweres Passwort?

Nicht gelöst.

20 Franz Joseph und die Kommandozeile

20.1 Stage

Nicht gelöst.

20.2 Stagee

Nicht gelöst.

20.3 Stageee

Nicht gelöst.

20.4 Stageeee

Nicht gelöst.

20.5 Stageeeee

Nicht gelöst.

20.6 Stageeeeee

Nicht gelöst.

20.7 Stageeeeeee

Nicht gelöst.

20.8 Stageeeeeeee

Nicht gelöst.

20.9 Stageeeeeeeee

Nicht gelöst.

20.10 Stageeeeeeeeee

Nicht gelöst.

20.11 Stageeeeeeeeeee

Nicht gelöst.

20.12 Stageeeeeeeeeeee

Nicht gelöst.

21 Ueberschrift 1

21.1 Hinweise

Hinweise:

- Verwenden Sie entweder diese deutsche Version oder die englische Version in `protocol.tex`.
- Setzen Sie alle Variablen nach *FOR STUDENTS* in der .tex Datei.
- Ersetzen Sie die Platzhalter für Ihre Namen und MatNr.
- Löschen Sie diese Sektion über Hinweise und die folgenden Beispiel-Kapitel.
- Achten Sie auf geforderte Formate und Anforderungen an die Dateinamen.
- Führen Sie `pdflatex` mindestens zweimal aus, damit die Referenzen und Seitenzahlen richtig im PDF dargestellt werden.
- Sie können dazu auch das Makefile verwenden: `make de`.

22 Beispiele

22.1 Source Code formatieren

Es folgen einige Beispiele wie Sourcecode in diesem Dokument formatiert und referenziert werden kann (siehe Listing 2 auf Seite 17 und siehe Listing 3 auf Seite 16).

Ebenso können kurzer Code oder kurze Befehle direkt in der Zeile in einem `lstinline Block` mit typengleicher Schrift formatiert werden.

```
#!/bin/bash
echo "Bash version ${BASH_VERSION}..."
for i in {0..10..2}
  do
     echo "Welcome $i times"
 done

echo "some very very very very very very very very very very
   very very very very very very very very very very very very
   long string"

exit 0;
```

Listing 3: Example bash script

22.2 Bilder

Es folgen einige Beispiele wie Bilder in diesem Dokument eingefuegt werden koennen (siehe Abbildung 1 auf Seite 16).

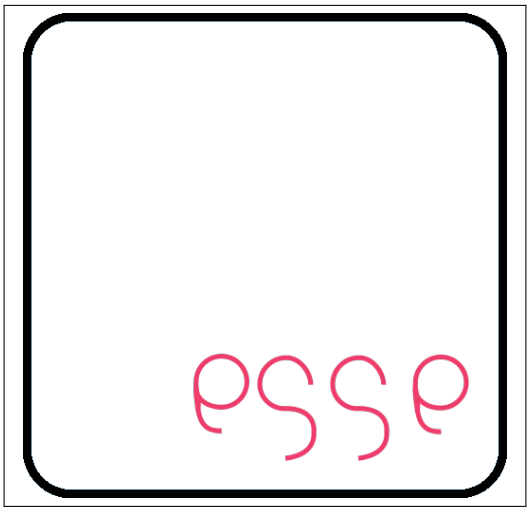

Abbildung 1: ESSE Logo

```c
/*
 * Just an example C-file.
 */

#include <stdio.h>

int global_variable = 1;
#ifdef DEBUG
int another_global_variable = 1;
#endif

/*
 * Some comment
 */
int main(void)
{
  temp_variable = 4711;
  another_variable = 0815;

  printf("foo bar baz %02d", temp_variable);

  return 1;
}
```

Listing 2: Example C/C++ file