# Развој безбедног софтвера

# Садржај

# Увод

- Назив предмета: Развој безбедног софтвера
- Година: 1, семестар: 2
- Фонд часова: 2 + 2 + 1
- Број ЕСПБ бодова: 6
- Предуслов: одслушани предмети Заштита података, Пројектовање софтвера, Програмирање интернет апликација

# Наставници

- **Предавања: др Жарко Станисављевић**
  zarko@etf.rs
  Консултације сваке недеље путем MSTeams платформе
- **Вежбе: маст. инж. Данко Миладиновић**
  danko@etf.bg.ac.rs
  Канцеларија 26а
  Часови удаљено коришћењем MSTeams платформе

# Сарадници из привреде

- **Вежбе: маст. инж. Владимир Томић**

  vladimir.tomic@zuehlke.com
  Часови удаљено коришћењем MSTeams платформе
- **Вежбе: маст. инж. Петар Вуковић**

  petar.vukovic@zuehlke.com
  Часови удаљено коришћењем MSTeams платформе

# Циљ предмета

- Упознавање студената са облашћу развоја безбедног софтвера. Обука студената за примену добрих пракси у развоју безбедног софтвера. Разумевање претњи и начина за детекцију и отклањање претњи у постојећим софтверским решењима. Упознавање студената са методологијама сигурносне ревизије програмског кода.

# Исход предмета

- Студенти ће стећи знања о методама развоја безбедног софтвера, као и о методама проналажења и отклањања сигурносних пропуста у постојећим софтверским решењима.

# Програм предмета

- Методологија процеса развоја безбедног софтвера. Анализа сигурносних захтева. Архитектура и дизајн безбедног софтвера. Моделовање претњи и правци напада. Процена ризика. Сигурносни пропусти интернет апликација, скрипт језика, API-а и програмских језика. Сигурносна ревизија програмског кода. Сигурносно тестирање софтверских решења. Преглед и анализа најзаступљенијих сигурносних пропуста.

# Лабораторијске вежбе

- Раде се на лицу места, одмах након термина вежби.
- Преглед вежби:
  - SQL Injection
  - Cross Site Scripting (XSS)
  - Alati za statičku i dinamičku analizu
  - Cross Site Request Forgery (CSRF)
  - Sigurna implementacija autentifikacije
  - Autorizacioni modeli
  - Logging, auditing, rukovanje izuzecima i monitoring
- **Не оцењују се**
- **Припрема за израду пројекта**

# Семинарски рад

- Носи **20 поена**
- **Нема надокнаде**
- **Важи годину дана**
- Одабрати један рад са листе понуђених на Moodle курсу или један пропуст за који ћете направити примере
- Написати кратак извештај на максимално 3 стране
- Презентација+питања мах. 10 минута (уочи испита у јануарском року или у терминима током семестра)
- Сваки студент ће имати различиту тему. Списак одабраних тема ће бити објављен на Moodle курсу.

# Пројекат

- Носи **40 поена**
- **Нема надокнаде**
- **Важи годину дана**
- Теме које су практично рађене кроз вежбе и лаб. вежбе повезане у једну целину.
- Термин: уочи испита у јануарском и јулском року.

# Предиспитне обавезе студената

- **Лабораторијске вежбе**
  - Не оцењују се
- **Семинарски рад**
  - укупно 20 поена
  - Важи за текућу школску годину
- **Пројекат**
  - укупно 40 поена
  - Важи за текућу школску годину
- **Присуство настави**
  - Не оцењује се

# Начин полагања испита

- **Испит – 40 поена**
  - Градиво са предавања

# Начин полагања испита

Коначна оцена се формира на основу броја бодова на следећи начин:

- 91 <= X < 100 – оцена 10
- 81 <= X < 91 – оцена 9
- 71 <= X < 81 – оцена 8
- 61 <= X < 71 – оцена 7
- 51 <= X < 61 – оцена 6
- 0 <= X < 51 – студент није положио испит

# Литература

- Материјали за предавања
- Материјали за вежбе

# Комуникација

- Сајт предмета: https://rti.etf.bg.ac.rs/rti/ms1rbs/
- Moodle курс: https://elearning.rcub.bg.ac.rs/moodle/course/view.php?id=1156
- MSTeams: https://teams.microsoft.com/l/team/19%3aKfbo4YF0nq6Mn3RjCaIUS9g-jI87vSFspcya0NnWDOg1%40thread.tacv2/conversations?groupId=f0443fc2-b40b-4b1d-b249-6a802daa6c65&tenantId=1774ef2e-9c62-478a-8d3a-fd2a495547ba
- Мејл листа предмета: https://lists.etf.bg.ac.rs/wws/info/13m111rbs

# ОБАВЕШТЕЊЕ ЗА СТУДЕНТЕ

- Настава на предмету Развој безбедног софтвера подразумева изучавање различитих механизама којима се нарушава информациона безбедност и врше напади на интернет апликације и софтверске системе.
- Примена ових механизама када се извршавају према системима физичких и правних лица која нису упозната и сагласна са активностима на провери рањивости и тестирању упада у њихове системе је кажњива према Кривичном законику Републике Србије (Чланови 298 до 304а).
- Студенти на предмету Развој безбедног софтвера могу ове методе за потребе изучавања да користе искључиво у оквиру затвореног лабораторијског окружења које је обезбеђено за наставу на предмету Развој безбедног софтвера.
- Студенти не могу да подразумевају да су на било који начин охрабрени од стране наставника или да им се препоручује да користе ове методе који се изучавају према другим апликацијама Електротехничког факултета или апликацијама било ког трећег правног или физичког лица.
- Свака евентуална активност коју би предузео неки студент коришћењем ових метода и механизама према апликацијама које нису у оквиру лабораторије на предмету искључива је одговорност студента.

# Питања?

Електротехнички Факултет

Универзитет у Београду