Семинарски рад 2023/2024.

Потребно је да се студенти мастер студија који су пријављени за праћење предмета Развој безбедног софтвера (13М111РБС) и који су заинтересовани за израду семинарског рада пријаве за тему коју желе да обраде, најкасније до петка 24.11.2023. до 20:00, у оквиру форме за пријаву на *Moodle* страници курса. Семинарски рад се ради у групи од 4 члана. Студенти могу самостално формирати групу. Потребно је да се сви студенти једне групе пријаве за исту тему у форми за пријаву.

Одбране семинарских радова биће организоване током семестра (на почетку часова предавања за студенте који се благовремено пријаве), као и у јануарском испитном року. Сажетак се шаље у .docx или .pdf формату, а презентација у .pptx или .pdf формату, путем електронске поште два дана пре одбране семинарског рада на zarko@etf.rs, а најкасније до 30.12.2023. Имена фајлова морају да буду у формату: рб_име_презиме_с и рб_име_презиме_п за сажетак и презентацију репективно, где је рб редни број теме из доњег списка, а име и презиме су име и презиме студента који шаље као представник групе (у поруци навести ко је све учествовао у изради, за случај да се нешто промени од тренутка пријаве). Студенти могу предложити и тему која није на списку, а која припада области развоја безбедног софтвера, али за тему морају добити одобрење наставника.

За све нејасноће писати на zarko@etf.rs.

Постоје две варијанте израде семинарског рада.

Варијанта 1. Семинарски рад подразумева да студенти направе преглед 10 новијих радова за одговарајућу тему, да на основу тих радова напишу кратак извод максималне дужине пет А4 страна на српском језику који објашњава суштину прочитаних радова, да направе презентацију од максимално 10 слајдова и да презентују суштину прочитаних радова у максималном трајању од 20 минута.
Приликом претраге радова, на сајту scholar.google.com укуцати предложене кључне речи и ограничити претрагу на период од 2010 до данас. Одабрати 10 радова који су објављени у часописима или саопштени на конференцијама, а којима је могуће приступити. За радове који су раније објављени критеријум селекције може бити број цитата. За радове који су скорије објављени критеријум може бити ранг часописа/конференције у/на којима су објављени/саопштени. За сваки одабрани рад написати по један пасус у сажетку. На крају сажетка дати закључак.

Р. бр.	Тема	Кључне речи за претрагу
1.	Тајност, интегритет и доступност софтвера	confidentiality integrity availability in software
2.	Методологије сигурносне анализе ризика	security risk analysis methods
3.	Методологије развоја безбедног софтвера	secure software development methodologies
4.	Моделовање сигурносних захтева	security requirements modeling
5.	Методологије моделовања претњи	threat modeling methodologies
6.	Сигурносни лоши обрасци	security antipatterns
7.	Контрола приступа	access control
8.	Сигурносни дијаграми тока података	security data flow diagram
9.	Успостављање безбедности коришћењем језика Rust	rust language security
10.	Рањивости WebAssembly-а	wasm vulnerabilities
11.	Рањивости језика C#	C# language vulnerabilities
12.	Рањивости језика Scala	Scala language vulnerabilities
13.	Рањивости језика C++	C++ language vulnerabilities
14.	Рањивости језика PHP	PHP language vulnerabilities
15.	Алати за статичко тестирање сигурности апликација	static application security testing tools
16.	Примена вештачке интелигенције у тестирању сигурности	ai security testing
17.	Тестирање сигурности у облаку	cloud security testing
18.	Тестирање сигурности веб апликација	web application security testing
19.	Сигурносно тестирање	security testing
20.	Пенетрационо сигурносно тестирање	penetration security testing

Варијанта 2. Семинарски рад подразумева да студенти прочитају објашњење пропуста који је наведен за одговарајућу тему, да на основу тог објашњења осмисле 10 изазова типа *Capture the flag*, да изазове имплементирају или у оквиру постојећег *open source* система који пронађу или у оквиру сопственог система, да напишу кратко упутство са објашњењем имплементираних изазова максималне дужине пет А4 страна на српском језику, да направе презентацију од максимално 10 слајдова и да презентују суштину обрађеног пропуста у максималном трајању од 20 минута. Уколико за одабрани пропуст студенти не могу да смисле 10 изазова, дозвољено је проширити тему са пропустима који су повезани са одабраним пропустом. За сваки осмишљени изазов написати по један пасус у сажетку. На крају сажетка дати закључак.

Р. бр.	**Ознака пропуста**	**Линк**
21.	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	https://cwe.mitre.org/data/definitions/22.html
22.	CWE-476: NULL Pointer Dereference	https://cwe.mitre.org/data/definitions/476.html
23.	CWE-287: Improper Authentication	https://cwe.mitre.org/data/definitions/287.html
24.	CWE-918: Server-Side Request Forgery (SSRF)	https://cwe.mitre.org/data/definitions/918.html
25.	CWE-94: Improper Control of Generation of Code ('Code Injection')	https://cwe.mitre.org/data/definitions/94.html
26.	CWE-601: URL Redirection to Untrusted Site ('Open Redirect')	https://cwe.mitre.org/data/definitions/601.html
27.	CWE-640: Weak Password Recovery Mechanism for Forgotten Password	https://cwe.mitre.org/data/definitions/640.html
28.	CWE-117: Improper Output Neutralization for Logs	https://cwe.mitre.org/data/definitions/117.html

29.	CWE-209: Generation of Error Message Containing Sensitive Information	https://cwe.mitre.org/data/definitions/209.html
30.	CWE-276: Incorrect Default Permissions	https://cwe.mitre.org/data/definitions/276.html
31.	CWE-290: Authentication Bypass by Spoofing	https://cwe.mitre.org/data/definitions/290.html
32.	CWE-294: Authentication Bypass by Capture-replay	https://cwe.mitre.org/data/definitions/294.html
33.	CWE-296: Improper Following of a Certificate's Chain of Trust	https://cwe.mitre.org/data/definitions/296.html
34.	CWE-307: Improper Restriction of Excessive Authentication Attempts	https://cwe.mitre.org/data/definitions/307.html
35.	CWE-321: Use of Hard-coded Cryptographic Key	https://cwe.mitre.org/data/definitions/321.html
36.	CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG)	https://cwe.mitre.org/data/definitions/337.html
37.	CWE-756: Missing Custom Error Page	https://cwe.mitre.org/data/definitions/756.html
38.	CWE-73: External Control of File Name or Path	https://cwe.mitre.org/data/definitions/73.html

39.	CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key	https://cwe.mitre.org/data/definitions/566.html
40.	CWE-425: Direct Request ('Forced Browsing')	https://cwe.mitre.org/data/definitions/425.html
41.	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer	https://cwe.mitre.org/data/definitions/119.html
42.	CWE-434: Unrestricted Upload of File with Dangerous Type	https://cwe.mitre.org/data/definitions/434.html
43.	CWE-441: Unintended Proxy or Intermediary ('Confused Deputy')	https://cwe.mitre.org/data/definitions/441.html
44.	CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	https://cwe.mitre.org/data/definitions/444.html
45.	CWE-522: Insufficiently Protected Credentials	https://cwe.mitre.org/data/definitions/522.html