AZƏRBAYCAN RESPUBLİKASI
ELM VƏ TƏHSİL NAZİRLİYİ

Azərbaycan Kibertəhlükəsizlik
Təşkilatları Assosiasiyası

Veb təhlükəsizlik

fənni üzrə sillabus

Adil Əliyev, Fərid Əhmədli

Bu vəsait Azərbaycan Respublikasının Elm və Təhsil Nazirliyinin maliyyə dəstəyi ilə həyata keçirilən "İnformasiya təhlükəsizliyi ixtisası üzrə elmi-metodiki tədris (çap və onlayn) vəsaitlərinin hazırlanması" layihəsi çərçivəsində hazırlanmışdır.

Nəşrin məzmununa görə donor məsuliyyət daşımır.

Adil Əliyev, Fərid Əhmədli
Veb təhlükəsizlik

Bakı – 2024.
Redaktor: Adil Əliyev

İnformasiya Təhlükəsizliyi sahəsində kadr potensialının gücləndirilməsi məqsədilə 2022-ci ildə Elm və Təhsil Nazirliyi və Dövlət Təhlükəsizliyi Xidmətinin birgə təşəbbüsü ilə ölkənin aparıcı ali təhsil müəssisələrinin və müxtəlif dövlət qurumlarının nümayəndələri ilə yanaşı, dünyanın nüfuzlu universitet və şirkətlərində çalışan azərbaycanlı mütəxəssislər, o cümlədən AKTA sədri Elvin Balacanov, "ÖzünÖyrən" platformasının həmtəsisçisi Adil Əliyevin iştirakı ilə hazırlanmış təhsil proqramı elm və təhsil nazirinin 2022-ci il 28 iyul əmri ilə təsdiqlənmişdir.

Universitetlər tərəfindən adıçəkilən təhsil proqramının effektiv tətbiq olunmasına, proqramda öz əksini tapmış bəzi fənlərin tədrisinin sənayenin müasir tələblərinə uyğun hazırlanmasına dəstək vermək məqsədilə AKTA və "ÖzünÖyrən" əməkdaşları nümunəvi fənn sillabusları hazırlanmasına təşəbbüs göstərmişlər.

Bu nümunəvi fənn sillabusu həmin təşəbbüsün nəticəsi olaraq ərsəyə gəlmişdir.

1 | Veb təhlükəsizlik

Fənn barədə

Veb təhlükəsizlik fənni veb tətbiqlərin çalışma prinsiplərini, onların brauzer proqramları tərəfindən vizuallaşdırılması məntiqini (ing. rendering), serverlə əlaqə mexanizmlərini öyrədir. Daha sonra veb tətbiqlər və veb xidmətlərdəki təhlükəsizlik boşluqlarının necə və haradan qaynaqalandığını, həmçinin o boşluqların/zəifliklərin necə aradan qaldırılmasına dair praktiki biliklər aşılanır. Bununla yanaşı, veb tətbiqlərdə təhlükəsizliyin təmin olunmasına dair qabaqcıl təcrübələr, geniş yayılmış boşluqlar/zəifliklər, həmçinin boşluqların/zəifliklərin istismarına dair üsul və vasitələr öyrədilir.

Ümumilikdə bu kurs veb təhlükəsizliyinin fərqli aspektlərinə ümumi baxış xarakteri daşıyır. Kursun məqsədi ən geniş yayılmış veb hücumları və onlara göstərilməli olan əks tədbirlər haqqında anlayışları aşılamaqdır. Bəhs edilən boşluqlar nə qədər geniş yayılmış olsa da hələ də onlara mütəmadi rast gəlinir. Ona görə də proqramçılar və sistem mühəndisləri üçün veb təhlükəsizliyi başa düşmək çox vacibdir. Kursdakı laboratoriya işləri nümunə veb saytları sındırmaq, sistemlərə nüfuz etmək və onların müdafiəsini təşkil etmək kimi praktiki tapşırıqlardan ibarətdir.

Kurs bu mövzuları əhatə edir: Veb təhlükəsizliyinin prinsipləri, hücumlar və onlara qarşı əks tədbirlər, veb brauzerin təhlükəsizlik modeli, veb tətbiqlərdəki zəifliklər, SQL inyeksiya, xidmətdən imtina(DOS), TLS/SSK hücumları, XSS, autentifikasiya, JavaScript təhlükəsizliyi və təhlükəsiz kod yazmaq üçün üsullar.

İlkin şərtlər

Mütləq:

- Kompüterdən sərbəst şəkildə istifadə etməyi bacarmaq.
- HTML və JavaScript-i ilkin səviyyədə bilmək.
- İngilis dilini texniki ədəbiyyatı başa düşəcək səviyyədə bilmək.

Arzuolunan:

- Linux əməliyyat sistemi ilə tanışlıq.
- HTTP protokolu barədə ilkin anlayışlar.

Tövsiyə edilən ədəbiyyat

1. Hoffman, Andrew. Web Application Security: Exploitation and Countermeasures for Modern Web Applications. N.p., O'Reilly Media, 2020.
2. Tomas Kormen. Alqoritmlərin Sirri (Azərbaycan). Altun Kitab, 2022.
3. Elie Saad, Rick Mitchell. OWASP Web Security Testing Guide, version 4.2. 2020
4. OWASP Top Ten (https://owasp.org/www-project-top-ten/)
5. Pinto, Marcus, and Stuttard, Dafydd. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. United Kingdom, Wiley, 2011.

Dərs saatları

Dərsin növü	Mühazirə
Saatların miqdarı	30 saat
Laboratoriya işi	30 saat
Yekun	60 saat
Kreditlərin miq-darı	6
Həftəlik dərs yükü	4 saat

Hədəf auditoriya

Bakalavriat dərəcəsinin 050615 - "İnformasiya təhlükəsizliyi"ixtisası üzrə təhsil alan tə-ləbələr.

2 | Fənndən gözlənilən nəticələr

Əsas: Azərbaycan Respublikası Təhsil Nazirinin 28 İyul 2022-ci il tarixli, F-463 saylı əmri ilə təsdiqlənmiş, Bakalavriat səviyyəsinin "İnformasiya təhlükəsizliyi"ixtisası üzrə təhsil proqramı.

"Veb təhlükəsizlik" fənni üzrə təlim nəticələri (FTN)	
FTN 1	Veb brauzerlərin iş prinsiplərini, veb tətbiqlərin layihələndirilməsi, yaradılması və istismarı qaydalarını bilməlidir.
FTN 2	Müasir texnologiyalardan istifadə edərək təhlükəsiz veb səhifələr hazırlamağı bacarır. HTML, CSS, JavaScript kimi texnologiyaları bilməlidir.
FTN 3	HTTP protokolunun necə çalışdığını bilir. SSL sertifikatlarının necə çalışdığını və veb səhifələrin təhlükəsizliyini necə qoruduğunu bilir.
FTN 4	Veb saytlarda hücumların təbiəti haqqında məlumatlıdır.
FTN 5	REST və GraphQL kimi veb xidmətlərin necə çalışdığını bilir.
FTN 6	OWASP Top 10 - təhlükəsizlik zəiflikləri ilə tanışdır, o siyahıları müəyyənləşdirməyi, onların qarşısının alınması mexanizmlərini bacarır.

3 | Mövzular

Mühazirə 1

1. Giriş
    - Fənnin məqsədi.
    - Etika kodeksi.
    - Veb təhlükəsizlik nədir?
2. Veb təhlükəsizlik kursunun strukturu
    - Kursun strukturu barədə.
    - Praktiki tapşırıqlar barədə
3. Alətlər
    - Local infrastrukturun hazırlanması.
    - Visual Studio Code
    - Ubuntu for Windows
    - Kali Linux
    - Firefox/Chrome/Edge

Mühazirə 2

1. İnternet
    - İnternet nədir?
    - Brauzerdə URL yazdıqdan sonra nə baş verir?
2. Protokollar
    - İP ünvan
    - DNS
    - HTTP
3. Təcrübə
    - DNS-in ələ keçirilməsi

Mühazirə 3

1. Veb sayt nədir?
    - Veb saytlar
    - Veb texnologiyalar. Veb tətbiqlər.
2. URL
    - URL nədir. Onun quruluşu.
3. Brauzer
    - Brauzerlər haqqında.
    - Brauzer necə çalışır?

Mühazirə 4

1. HTML
    - HTML nədir?
    - HTML-də elementlər.
    - HTML elementlərin atributları
2. Elementlər
    - Başlıq elementləri
    - Paraqraf elementi
    - “Span” elementi
    - Siyahılar
    - Div, header və footer elementləri
    - Img elementi
    - Keçid elementi
    - Br və Hr elementləri
3. HTML formlar
    - HTML-də form nə üçündür?
    - İnput elementi
4. CSS
    - CSS nədir?
    - CSS-in HTML-də istifadəsi
    - Geniş istifadə edilən atributlar

Mühazirə 5

1. JavaScript nədir?
    - JavaScriptdə “Salam dünya” proqramı.
    - HTML-də JavaScriptin istifadə yolları.
2. JavaScriptin sintaksisi
    - Dəyişənlər
    - If operatoru
    - Dövrlər
    - Funksiyalar
    - Massivlər
    - JavaScriptdə HashMap
3. DOM
    - DOM nədir?
    - Window obyekti
    - Document obyekti
4. Regex
    - Regex nədir?
    - Regex ilə nümunələr

5. Digər mövzular
    - AJAX
    - NodeJS. JavaScript ilə server proqramlaşdırması

Mühazirə 6

1. Kurs üçün lazımlı alətlər
    - Kurs üçün lazımlı alətlər
2. DevTools
    - Firefox DevTools/Chrome DevTools
    - Console
    - Network
    - Storage
3. Terminal ilə çalışan alətlər
    - Curl
    - Nslookup
    - Tracert
    - ping
4. Sniffer
    - Wireshark
5. Postman
    - Postman

Mühazirə 7

1. Sessiyalar
    - İstifadəçi sessiyaları haqqında ümumi anlayış.
    - Sessiyalar və Kukilər
2. Kukilər
    - Kukilərin server və klient arasında ötürülməsi.
    - Local storage
3. Sessiyaların təhlükəsizliyi
    - Same origin policy
    - SameSite
    - Cross-Site Request Forgery
    - Kuki təhlükəsizlik boşluqlarının qarşısının alınması.

Mühazirə 8

1. Kod inyeksiyası (Code İnjection)
    - Kod inyeksiyası (Code İnjection) nədir?
    - Command injection

2. Cross-Site Scripting (XSS)
    - XSS nədir?
    - XSS-dən müdafiə
3. Digər mövzular
    - Content Security Policy (CSP)
    - strict-dynamic

Mühazirə 9

1. DoS (Denial of Service)
    - DoS (Denial of Service) nədir?
    - DDoS (Distributed Denial of Service)
2. Botnetlər
    - Botnet nədir?
3. Tətbiqlərin load test olunması
    - Load test nədir?
    - Load test necə edilir?
4. DDoS-dan müdafiə
    - DDoS-dan müdafiə mümkündürmü?
    - CDN sistemlər

Mühazirə 10

1. Fişing
    - Fişinq nədir?
    - Fişingin növləri.
2. İDN
    - İDN nədir?
    - Punnycode
    - IDN homograph attack
3. Fişinqdən müdafiə.
    - Fişinqdən müdafiə üsulları

Mühazirə 11

1. SQL
    - İlkin anlayışlar
    - Cədvəllər və sütunlar
2. MySQL
    - MySQL-in quraşdırılması
    - Verilənlər bazasının yaradılması
3. SQL ilə bəzi əmrlər

- SELECT əmri
- DROP əmri
- DELETE əmri
- UPDATE əmri

Mühazirə 12

1. SQL Injection
    - SQL injection nədir?
    - SQL injection ilə nümunələr
    - SQL injection prevention

Mühazirə 13

1. Kriptoqrafiya
    - Kriptoqrafiya barədə qısa məlumat.
    - Əvəzetmə şifrləri
    - Simmetrik və assimmetrik şifrələmə
    - Xeş funksiyalar. MD5, SHA1.
2. SSL
    - HTTP-nin problemləri
    - HTTPS necə çalışır?
    - İnanılmış (Trusted) sertifikat mərkəzləri
    - HTTPS tam təhlükəsizdir?

Mühazirə 14

1. Autentifikasiya
    - Autentifikasiya nədir?
    - Autentifikasiyanın növləri.
2. Şifrələrin etibarlılığı
    - Şifrələrin sındırılması.
    - Şifrələrin etibarlılığı
    - Şifrələrin qorunması
3. Avtorizasiya
    - Avtorizasiya nədir?

Mühazirə 15

1. Müasir problemlər
    - Müasir dünyada veb təhlükəsizlik.
    - Sosial mühəndislik

- Mobil təhlükəsizlik
- İoT təhlükəsizliyi
- Blokçeyn. Kriptovalyutalar

2. Süni intellekt
    - ChatGPT
    - Saxta xəbərlər. Clickbait.
    - Özügedən maşınlar
3. İzlənmə/izləmə
    - İzlənmə/izləmə nədir?
    - Tövsiyyə alqoritmləri
    - İzləmə taktikaları

4 | Müəlliflər barədə

Adil Əliyev

Adil Əliyev hazırda Samsung Electronics şirkətinin Vankuver ofisində mobil cihazların təhlükəsizlik sistemlərinin yaradılması ilə məşğul olur. 2019-2022-ci illərdə Amazon şirkətinin Kanada ofisində proqram təminatı üzrə mühəndis olaraq çalışmışdır. Ayrı-ayrı vaxtlarda Bakı Dövlət Universiteti, ADA Universiteti, Azərbaycan Texniki Universitetində müəllim olaraq fəaliyyət göstərib.

Fərid Əhmədli

Fərid Əhmədli hazırda Kanadanın Vankuver şəhərində, Microsoft şirkətində proqram təminatı üzrə mühəndisdir. 2022-ci ilə qədər Amazon şirkətində proqram təminatı üzrə mühəndis olaraq süni intellekt sistemlərində verilənlərin təhlükəsizliyi istiqamətində çalışmışdır. 2016-2021-ci illərdə ADA Universitetində Kompüter Elmləri üzrə müəllimlik edib.