**ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ**

**Мэдээлэл, холбооны технологийн сургууль**



**БИЕ ДААЛТЫН АЖИЛ 2**

**Вэб систем ба технологи(F.IT301)**

**2020-2021 оны хичээлийн жилийн хавар**

**Шалгасан багш:** Н. Анхбаяр

**Лабораторыг гүйцэтгэсэн:** Т. Дөлгөөн / B180910062

**Улаанбаатар хот**

**2021 он**

Энэхүү бие даалтын ажлаар бид лабораторын ажил 3 дээр хийсэн зүйлээ дэлгэрүүлж түүнийгээ SQL injection-оос хамгаалсан нэвтрэх формоор нэвтрэн орж XSS-ээс хамгаалсан comment бичих хэсгийг хийсэн билээ.

# Ашигласан функц элементүүд

md5()– Тэмдэгт мөрийг md5 аргаар encrypt хийж нууцлах функц

mysqli\_real\_escape\_string()– MySQL-д аюулгүй утга оруулахын тулд зарим нэг тэмдэгтүүдийн урд нь backslash-\ -ийг залгаж өгнө.

mysqli\_stmt\_bind\_param()– ашиглавал шууд query-гээ execute хийгээд өгөгдлийн сан луу явуулалгүй эхлээд prepare хийж дараа нь параметрүүдээ execute хийлгүйгээр bind хийж хадгалан эцэст нь execute хийхэд өөр протоколоор дамжуулж байгаа тул SQL injection гарах боломжгүй болох юм.

setcookie() – cookie үүсгэх функц cookie-гийн нэр, утга, амьдрах хугацаа, зам гэх мэт параметрүүд авна.

$\_COOKIE – дээрх функцээр үүсгэсэн функцэд хандахдаа энэ утгаар нэрээр нь хандана.

htmlspecialchars() – &, <, >, ‘, “ гэх мэт тэмдэгтүүдийг html –ийн форматаар &amp, &quot, &lt гэх мэт болгоно. Ингэснээр XSS халдлагаас сэргийлж болох юм.

var re = new RegExp() – Regular Expression буюу формат шалгах формат үүсгэнэ.

re.test() – дээр үүсгэсэн форматаар ямар нэгэн зүйл шалгахад ашиглана. Формат алдаатай бол False –ийг буцаана.

date("Y-m-d H:i:s")- яг одоогийн огноог 2000-01-01 20:20:20 форматаар хадгална.

# XSS халдлагын төрлүүд

**Reflected XSS** – хортой скрипт нь HTTP хүсэлтээр ирэх халдлага

**Stored XSS** – хортой скрипт нь тухайн вэб хуудсын өгөгдлийн санаас ирэх халдлага

**DOM-based XSS** – сервер талаас биш хэрэглэгчийн талын кодонд хортой скрипт нь байх халдлага

# Дүгнэлт

Энэхүү бие даалтын ажлыг хийснээр