Боловсруулсан багш: Н.Анхбаяр
И-мэйл хаяг: ankhbayar.n@gmail.com,
Өрөө: 312

Бие даалт-2 ОНОО-5 (III/5-III/19 18:00 цаг)

- Форм баталгаажуулалт
- SQL injection, XSS халдагаас хамгаалах

Зорилго: Тус бие даалтийг хийж гүйцэтгэхдээ заавал лаборатори хичээл 3-р үүсгэсэн өгөгдлийн санг ашиглан (Өгөгдлийн сан: IT301, Хүснэгт: employee, Талбар: employeeid int autoincrement PK, name varchar(20), email varchar(50), pass char(32) ӨС-гийн sql – г Сургалтын системээс татан авна уу) хэрэглэгчийн нэвтрэлтийг удирдах, сэтгэгдэл үлдээх дараах шаардлагуудыг хангасан програмыг хийж гүйцэтгэнэ.
Илгээх: оюутныкод_login.php, description.php 2 файлыг шахалгүйгээр илгээнэ. Файлуудын нэрийг багшийн зүгээс засаж солихгүйгээр ажиллуулах боломжоор хангаж өгнө. ӨС-нг илгээхгүй. Тайлангийн оронд кодон дунд хангалттай тайлбар хийж явуулна уу. Амжилт хүсье

Шаардлага:

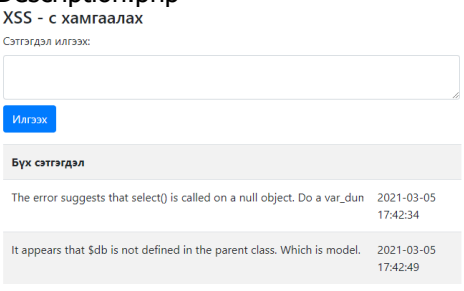
1. Хэрэглэгч системд өөрийн и-мэйл(email) хаяг, нууц үгээр(pass) нэвтрэнэ.
2. Нууц үг нь md5() ашиглан үүсгэгдсэн байна. Лаборатори-3 шаардлагын хүрээнд
3. Нэвтрэх хуудсанд клиент талын баталгаажуулалтыг хийж өгнө. (JavaScript ашиглан нэвтрэх нэр оруулсан эсэхийг шалгах, Нэвтрэх нэр и-мэйл зөв форматтай эсэхийг шалгах, нууц үг оруулсан эсэхийг шалгах.) Хөтөч дээр JS идэвхгүй болгож формыг submit хийж үзэх.
4. Нэвтрэх хуудсанд сервер талын баталгаажуулалтыг хийж өгөх. дээрх шаардлагатай ижил.
5. SQL injection ашиглан өөрийн үүсгэсэн хуудсанд нэвтэрч үзэх, Үүний дараа SQL injection – с хамгаалах. Үүнд: mysql_real_escape_string(), mysqli_stmt_bind_param() хоёланг нь ашиглах.
6. Баталгаажуулалтын алдааны мэдэгдэл харгалзах оролтын контролын ард эсвэл доод талд нь гарах. Үүнд: Хэрэглэгчийн нэр оруулна уу!, Нууц үг оруулна уу!, И-мэйл хаяг буруу байна. Нэвтрэх эрхгүй хэрэглэгч гэсэн 4 алдааг харгалзах үйлдэлд нь харуулна.
7. Намайг сана хэсгийг оруулж өгөх. Хэрэв намайг сана талбарыг зөвөлбөл яг 7 хоногийн хугацаанд хэрэглэгчийн нэвтрэх нэрийг cookie ашиглан хадгалах ба дараагийн удаа нэвтрэх хуудсаар ороход Хэрэглэгчийн нэр бөглөгдсөн байна. Компьютерийн огноог өөрчилж cookie устаж байгаа эсэхийг шалгах.

Дээрх хэсгийг гүйцэтгэхдээ дараах зүйлсийг ашиглана.

1. Сургалтын системийн Лекц 6-р ороход тухайн лекц дээр үзсэн жишээг татан авч үргэлжлүүлэх.
2. mysql_real_escape_string(),mysqli_stmt_bind_param()
3. $_SESSION, $_COOKIE, setcookie ()

8. Нэвтэрсэн хэрэглэгч сэтгэгдэл бичих хэсэг description.php хуудас руу шууд шилжинэ.
9. Хэрэглэгч description.php хуудсанд нэвтрээгүй хандсан тохиолдолд Нэвтрэх хуудас руу шилжүүлнэ.
10. Сэтгэгдэл бичих хуудас нь IT301 өгөгдлийн сангийн comment хүснэгттэй ажиллана. (sql файлыг татах)
11. Сэтгэгдэл бичих хуудас нь Нийт сэтгэгдлүүдийг харах өөрөө сэтгэгдэл оруулах хэсэгтэй байна.
12. Сэтгэгдэл бичих хэсгээр дамжуулан хортой код оруулж үзэх.
13. description.php хуудсанд XSS халдлагаас хамгаалсан кодыг бичиж өгнө.

Description.php



Description.php хуудсанд дараах зүйлсийг ашиглана.

1. document.cookie()
2. htmlspecialchars()
3. window.location
4. $_SESSION
5. Now() сэтгэгдэл бичсэн огноог авах