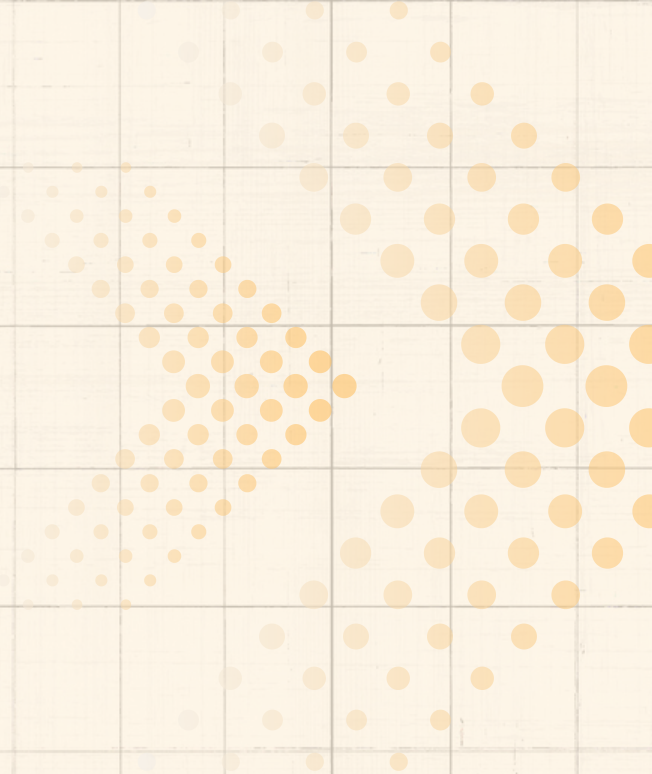
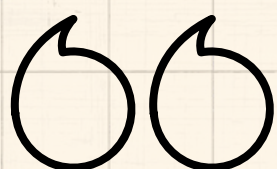
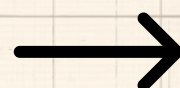




۷ حمله نرم افزاری

که هر توسعه دهنده‌ای
باید بدونه!



XSS (Cross-Site Scripting)

◆ چی هست؟

توی XSS مهاجم میاد کدی مثل **جاوااسکریپت** رو جایی تزریق می‌کنه (مثلاً داخل فرم یا فیلدی که توی سایت نمایش داده میشه) و اون کد روی مرورگر کاربر قربانی اجرا میشه. یعنی بدون اینکه خود کاربر بفهمه، مرورگرش دستورات **مخرب** رو اجرا می‌کنه.

◆ اثر حمله:

- سرقت **کوکی** / توکن **سشن** و جا زدن به جای کاربر
- تغییر محتوای صفحه، تزریق فرم‌های **فیشینگ**، اجرای عمل ناخواسته
- دور زدن محدودیت‌های **ال** و **فریب** کاربر

◆ راهکارها:

- **Escape** و فیلتر کردن همه ورودی‌ها قبل از نمایش.
- استفاده از قالب‌ها و فریم‌ورک‌های امن.
- فعال‌سازی **Content Security Policy (CSP)**.

Phishing

♦ چی هست؟

فیشینگ یعنی جعل یه **ایمیل** یا **وبسایت** شبیه سرویس معتبر (مثلاً بانک یا شبکه اجتماعی) تا کاربر خودش اطلاعات **حساسش** مثل **پسورد** یا **کارت بانکی** رو وارد کنه.

♦ اثر حمله:

- سرقت رمز عبور یا اطلاعات **مالی**.
- جعل هویت کاربر در سرویس‌های مختلف.
- ایجاد دسترسی **غیرمجاز** به حساب‌ها.

♦ راهکارها:

- آموزش کاربران برای شناسایی **لینک‌ها** و **ایمیل‌های** مشکوک.
- بررسی دامنه و **SSL** قبل از وارد کردن اطلاعات.
- استفاده از احراز هویت دومرحله‌ای (**2FA**).

Session Hijacking

◆ چی هست؟

توی این حمله، مهاجم **کوکی** یا توکن سشن کاربر رو به دست میاره (مثلاً از طریق **XSS** یا **شنود** شبکه) و خودش رو جای اون کاربر **جا** می‌زنه.

◆ اثر حمله:

- دسترسی کامل به حساب کاربر بدون نیاز به **رمز**.
- سرقت داده‌های **حساس** و **شخصی**.
- نقض امنیت **سازمان** و **کاربران**.

◆ راهکارها:

- استفاده از **HTTPS** برای رمزنگاری ترافیک.
- تغییر توکن سشن بعد از **لاگین** یا عملیات **حساس**.
- کوتاه کردن مدت زمان **اعتبار** سشن.



CSRF

(Cross-Site Request Forgery)

♦ چی هست؟

CSRF وقتی رخ می‌ده که کاربر وارد حسابشه و مهاجم یه درخواست جعلی از طرفش می‌فرسته. مرورگر کوکی سشن رو همراه درخواست می‌فرسته و سرور فکر می‌کنه این درخواست واقعی بوده.

♦ اثر حمله:

- تغییر ناخواسته اطلاعات کاربر (مثلاً تغییر ایمیل یا رمز).
- ارسال تراکنش یا عملیات حساس بدون اطلاع کاربر.
- سوءاستفاده از اعتبار کاربر برای حملات بعدی.

♦ راهکارها:

- استفاده از CSRF Token در همه فرم‌ها.
- بررسی هدر Origin یا Referer.
- محدود کردن اعتبار کوکی‌ها و سشن.



DoS / DDoS

◆ چی هست؟

DoS یعنی پر کردن سرور با حجم زیادی از درخواست‌ها تا منابعش اشباع بشه.
DDoS هم همینه، فقط با هزاران سیستم آلوده (Botnet) همزمان اجرا می‌شه، پس خیلی شدیدتره.

◆ اثر حمله:

- از دسترس خارج شدن کامل سرویس.
- کاهش سرعت و کیفیت خدمات برای کاربران واقعی.
- خسارت مالی و ضربه به اعتبار برند.

◆ راهکارها:

- استفاده از فایروال و WAF برای فیلتر ترافیک.
- توزیع بار با Load Balancer و CDN.
- شناسایی و مسدود کردن IP یا ترافیک مشکوک.



Brute Force Attack

♦ چی هست؟

Brute Force یعنی تلاش مداوم برای شکستن رمز عبور با امتحان کردن ترکیب‌های مختلف.
این کار یا با استفاده از یک لیست آماده پسوردهای **لو رفته** (Dictionary Attack) انجام می‌شه، یا با تست همه حالت‌های ممکن کاراکترها (**Pure Brute Force**) که خیلی زمان‌بره.

♦ اثر حمله:

- دسترسی **غیرمجاز** به حساب کاربر.
- خطر نشت اطلاعات **شخصی** یا **سازمانی**.
- قفل شدن یا از دسترس خارج شدن حساب‌ها به خاطر تلاش‌های **متعدد**.

♦ راهکارها:

- محدود کردن تعداد تلاش‌های ورود (**Rate Limiting**).
- استفاده از **Captcha** یا **reCaptcha**.
- اجبار به رمزهای **پیچیده** و **غیرتکراری**.
- فعال‌سازی احراز هویت **دومرحله‌ای** (2FA).



Malware

♦ چی هست؟

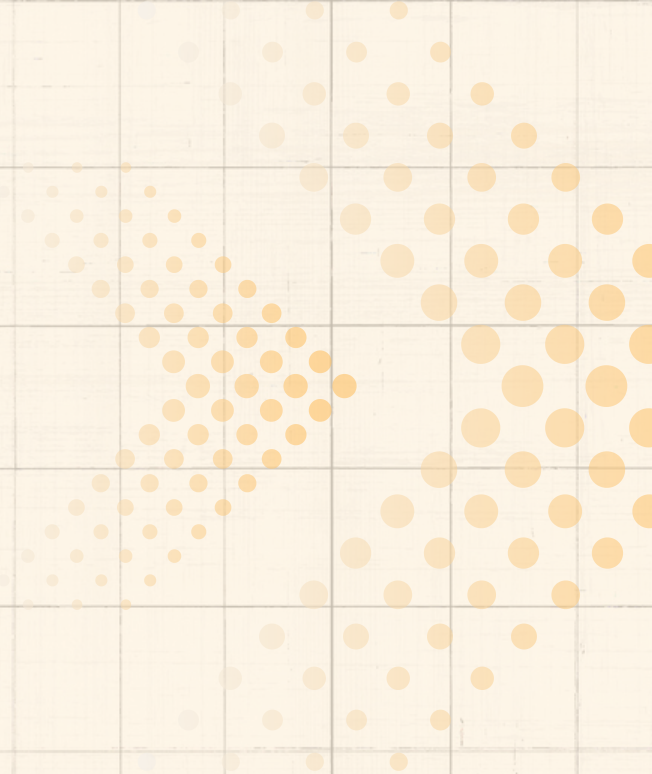
- Malware یا همون «بدافزار» به هر نرم‌افزاری می‌گن که هدفش خرابکاری، سرقت یا اخاذیه. این می‌تونه شکل‌های **مختلف** داشته باشه:
- **Virus** (ویروس): کدی که به فایل‌ها یا برنامه‌ها **می‌چسبه** و پخش می‌شه.
 - **Trojan** (تروجان): وانمود می‌کنه برنامه‌ی سالمه، ولی پشت‌پرده **مخربه**.
 - **Ransomware** (باج‌افزار): فایل‌های کاربر رو قفل می‌کنه و برای آزاد کردنش **پول** می‌خواد.

♦ اثر حمله:

- دسترسی کامل به حساب کاربر بدون نیاز به **رمز**.
- سرقت داده‌های **حساس** و **شخصی**.
- نقض امنیت **سازمان** و **کاربران**.

♦ راهکارها:

- استفاده از **آنتی‌ویروس** و به‌روزرسانی **مداوم** سیستم‌ها.
- دانلود نرم‌افزار فقط از منابع **معتبر**.
- محدود کردن دسترسی‌های **غیرضروری** در سیستم.



اگر مفید بود

**با دوستانات به
اشتراک بزار
یه فیدبک و لایکم
هدیه به من بده (:**

