بسمه‌تعالی

جمع‌بندی جلسه اول دوره آموزش تست نفوذ وب

مقدمه

- این دوره بدون هیچ‌گونه پیش‌نیازی برگزار می‌شود.
- دوره کاربردی است و از ذکر مطالب کلی و بنیادی اجتناب خواهد شد. تلاش می‌شود اصول اولیه‌ی مورد نیاز برای افراد ارائه گردد و شروعی برای یک مسیر طولانی باشد.
- البته مبانی ضروری آموزش داده می‌شود؛ گاهی در برخی از همکاران مشاهده می‌شود که به دلیل مسلط نبودن به مفاهیم ضروری از جمله مفاهیم وب یا مفاهیم رمزنگاری، برداشت‌های بسیار غلطی از برخی موضوعات دارند.
- در طی جلسات، باهم تمرین می‌کنیم و ممکن است بخش عمده‌ای از جلسات سکوت باشد و همه در حال فکر کردن یا انجام یک تمرین باشند.
- بازار داخلی و بین‌المللی در حوزه امنیت نیازمندی جدی در این بخش دارد و این نیازمندی به نیروی انسانی متخصص با گسترش جنبه‌ها و کاربردهای فناوری اطلاعات در زندگی روزمره بیشتر می‌شود.

مفاهیم وب (۱)

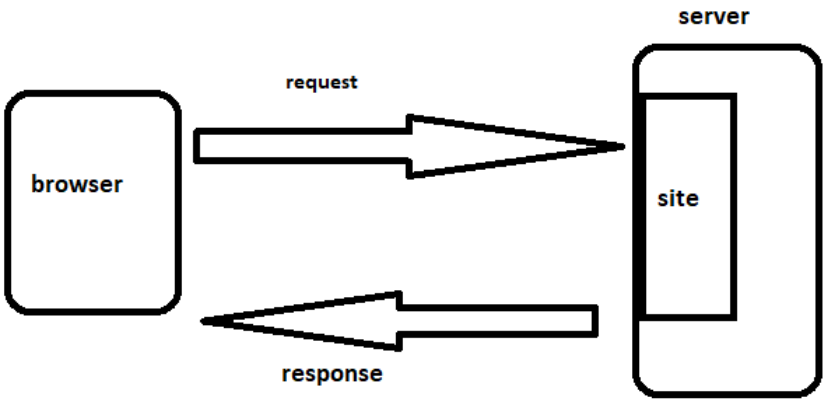
- وب‌سایت (سایت) یک نرم‌افزار است که از طریق مرورگر (browser) قابل دسترسی است.
- وب زیرمجموعه‌ای از اینترنت است که شامل صفحاتی است که از طریق مرورگر(browser) می‌توان مشاهده کرد.
- مرورگر (browser) نرم‌افزاری است که از طریق آن می‌توان صفحات وب (وب‌سایت‌ها) را مشاهده کرد.
- نرم‌افزارهای مرورگر زیادی وجود دارد که بسته به نوع سیستم عامل روی آن نصب می‌شوند: Google chrome, Mozilla Firefox, Microsoft Edge , Microsoft Internet Explorer
- کلمه وب‌سایت (website) یا سایت (site) به جای هم استفاده می‌شوند و فرقی باهم ندارند.
- www (world wide web) که در ابتدای نام سایت‌ها دیده می‌شود به معنای این است که این صفحه، یک web site است.
- دامنه (domain) یک آدرس یکتا برای هر سایت است. مثلا دامنه سایت دیجی‌کالا برابر است با digikala.com
- هر دامنه از دو بخش تشکیل شده است، بخش ابتدایی که یک نام است و بخش دوم (... , .ir ,.com) که مربوط به نوع دامنه است.
- تصویر زیر نشان دهنده مدل ارتباط در یک وب‌سایت است.

یک رستوران را تصور کنید که مشتری، غذا سفارش می‌دهد. سفارش به آشپزخانه می‌رود، پردازش می‌شود و سپس تحویل داده می‌شود. هنگامی که مرورگر را باز می‌کنید، در واقع به رستوران رفته‌اید، هنگامی که در بخش آدرس مرورگر، دامنه مورد نظرتان را تایپ می‌کنید، غذا سفارش داده‌اید و هنگامی که آیکون مرورگر در حال چرخش

است، سفارش شما در آشپزخانه (سرور) در حال آماده‌شدن است. در نهایت غذا (پاسخ سرور) برای شما ارسال می‌شود.

کلمه server از کلمه serve به معنای ارائه کردن می‌آید.

Server یعنی بخشی که درخواست (request) شما را پردازش می‌کند.



- سرور (server) در واقع چیزی نیست به جز یک کامپیوتر که احتمالا قدرت پردازش بیشتری دارد و می‌تواند درخواست‌ها را پردازش و به آنها پاسخ بدهد.
- هر کامپیوتری را می‌توان با نصب نرم‌افزارهای خاصی به سرور تبدیل کرد. این کامپیوتر پس از این، در حال ارائه سرویس (service) یا سرویس‌های مشخصی است. مثلا می‌توان یک کامپیوتر را با نصب نرم‌افزار خاصی به فایل سرور (file server) تبدیل کرد. فایل‌سرور (file server) یعنی ارائه دهنده خدمات فایل؛ همین کامپیوتر می‌تواند همزمان وب‌سرور (web server) نیز باشد؛ وب سرور یعنی ارائه دهنده خدمات وب؛ یعنی سروری که می‌تواند درخواست‌های از جنس وب کاربران را پردازش و پاسخ دهد.
- طبق شکل بالا، مرورگر و سرور مستمرا باهم در تعامل و ارتباط هستند. این ارتباط از طریق ارسال و دریافت request و response است.
- با هر کلیکی که روی یک سایت انجام می‌شود یا هر عبارتی که در فیلدهای سایت وارد می‌شود، در واقع یک درخواست به سمت سرور ارسال می‌شود و سرور آن درخواست را پردازش و سپس پاسخ مناسب را به مرورگر باز می‌گرداند.
- ارتباط و تعامل client (همان مرورگر) و server با یک زبان مشترکی انجام می‌گیرد که قابل فهم و پردازش برای هردو طرف است. به این زبان مشترک protocol ارتباطی می‌گویند.
- در وب‌سایت‌ها، پروتکل ارتباطی بین کلاینت (مرورگر) و سرور از نوع http یا https است.
- https همان http است که داده‌های بین کلاینت و سرور، رمز شده‌اند. Secure http
- پاسخ‌هایی که از سمت سرور به مرورگر تحویل می‌شود به صورت یک سری کدهای خاصی به نام html است.

- **تمرین: یک سایت را در مرورگر خود باز کنید و با کلیک روی inpect element کدهای html مربوط به این سایت را ببینید.**
- مرورگر (browser) این کدهای html را به صورت فیلد و متن و تصویر و .... ترجمه می‌کند.

- **تمرین: کدهای زیر را روی یک فایل txt کپی کنید، سپس پسوند این فایل را از txt. به .html تغییر بدهید.**

```
<html>
<body>
<h1>Hello Html </h1>
</body>
</html>
```

این فایل را با browserخود اجرا کنید.

- **تمرین: با استفاده از inspect element در browser خود، یک نوشته روی سایتی که در مرورگر خود باز کرده‌اید را تغییر دهید.**

- **تمرین: inspect element در مرورگرها چیست و چه کاربردهایی دارد؟**

- **تمرین: چند پروتکل ارتباطی دیگر به جز http یا https را نام ببرید؟ در هرکدام مشخص کنید چه کاربردی دارند؟**

- **تمرین: فرق بین سیستم عامل (operating system)، سرور (server)، وب‌سرور (web server)، فایل سرور (file server) و ایمیل سرور (email server) را شرح دهید.**