بسمه تعالی

تمرین اول **مهندسی اینترنت** **نیم‌سال اول ۹۷-۹۸**

بخش اول: به سوالات زیر به‌صورت مختصر پاسخ دهید.

۱- برنامه‌نویسان وب، در رابطه با سناریوهای post و get از الگویی تحت عنوان post/redirect/get و یا به اختصار PRG، تبعیت می‌کنند. اهمیت این الگو به ویژه در هنگام مدیریت form ها دیده می‌شود. در رابطه با این الگوی طراحی و دلیل استفاده آن تحقیق کرده و به اختصار توضیح دهید.

۲- در رابطه با پراکسی سرورها به دو سوال زیر پاسخ دهید:

الف : معمولا پراکسی سرورها را در دو دسته forward-proxy و reverse-proxy دسته‌بندی می‌کنند. تفاوت این دو دسته‌بندی در چیست؟

ب: خدماتی که پراکسی سرورها ارائه می‌دهند را توضیح دهید (حداقل به دو مورد از وظایف اشاره کنید).

۳- با توجه به request message زیر به سوالات پاسخ دهید. (در پاسخ به هر سوال اشاره کنید که به کدام بخش از هدِر استناد می‌کنید):

GET / HTTP/1.1

Host: server.com

Connection: keep-alive

User-Agent : Mozilla/5.0 (Windows NT 6.1; WOW64) Chrome/16.0.912.75 Safari/535.7

Accept: text/html, application/xhtml+xml, application/xml; q=0.9,*/*; q=0.8

Referrer: http://www.google.com/url?&q=broccoli

Accept-Encoding: gzip, deflate, sdch

Accept-Lnaguage: en-US, en , q=0.8

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*q=0.3

الف : منظور از connection : keep-alive چیست؟

ب: از کدام وب‌سایت (یا موتور جست‌وجو) به این صفحه هدایت شده‌ایم؟

ج: آیا سرور در هنگام ارسال منابع، می‌تواند آن‌ها را فشرده سازی کند؟

د: منظور از پارامتر q چیست و مقادیری که به آن نسبت داده می‌شود چه معنایی دارند؟ (راهنمایی: نام این پارامتر relative quality value است و در بعضی منابع نیز به آن degree of preference گفته می‌شود).

۴- با توجه به response message زیر به سوالات مطرح شده پاسخ دهید:

HTTP/1.1 200 ok

Content-Type: image/png

Last-Modified: Tue, 23 Aug 2011 13:28:21 GMT

Cache-Control : private, max-age=31536000

الف: منظور از private بودن cache-control چیست؟

ب: اگر cache-control به public تغییر کند ، فرآیند کَش چه تغییری خواهد کرد؟

ج: هدف از قرار داشتن last-modified در این پیغام چیست؟

د: هدف از قراردادن max-age چیست؟ واحد آن چیست؟

بخش دوم: پیاده‌سازی پراکسی سرور

همان‌طور که می‌دانیم پروتکل HTTP رمزنگاری نشده است و نسبت به حملاتی از قبیل حمله مرد میانی[1] و استراق سمع[2] بسیار آسیب پذیر بوده و به هکرها اجازه دسترسی به اطلاعات کاربری و حیاتی یک سایت را می‌دهد. از این رو یک سرور امنیتی برای جلوگیری از لو رفتن اطلاعات، فقط با متد post و به‌صورت رمزنگاری شده[3]کار می‌کند. کلاینت‌ها برای کار با این سرور باید تمام درخواست‌های[4]خود را تبدیل به post کنند و داده‌های مربوط به درخواست خود را رمزنگاری کرده و به این سرور ارسال کنند. هدف از این تمرین پیاده‌سازی یک پراکسی[5] می‌باشد که این تبدیل را برای کلاینت انجام دهد.

روال کار این پراکسی به این شرح است که کاربر پراکسی مرورگر خود را به آدرس این پراکسی تغییر می‌دهد. از این رو تمام درخواست‌های مرورگر به این پراکسی داده می‌شود. پراکسی مورد نظر، تمام درخواست‌ها اعم از get، put، trace، delete، head و option را می‌تواند دریافت کند. توجه داشته باشید که فقط درخواست‌های get از سمت مرورگر به پراکسی می‌تواند ارسال شود. برای بقیه‌ی درخواست‌ها از postman استفاده کنید. برای دانلود می‌توانید به این لینک مراجعه کنید. پراکسی پس از دریافت درخواست، آن را تبدیل به post کرده و تمام داده‌های مربوط به درخواست را رمزنگاری کرده و سپس به سرور مورد نظر می‌فرستد و پس از دریافت پاسخ[6] از سرور، پاسخ بازگردانده شده را به کاربر ارسال می‌کند.

---

[1] Man in the Middle
[2] Eavesdropping
[3] Encrypted
[4] Request
[5] Proxy Server
[6] Response

نکات پیاده‌سازی

۱- نحوه‌ی رمزنگاری درخواست‌ها بر عهده‌ی خود شماست.

۲- با توجه به این‌که کاربر چندین درخواست موازی را خواهد داشت (چندین tab را باز کرده و درخواست خواهد زد)، برای سادگی کار پیشنهاد می‌شود، از multi-threading استفاده کنید. این پراکسی به یک پورت گوش می‌دهد، پس از ایجاد یک ارتباط TCP، یک thread برای آن می‌سازد. این thread مسئول پاسخ‌گوئی به آن دسته از درخواست‌هایی است که از آن ارتباط TCP می‌رسد.

۳- استفاده از هر زبان برنامه‌نویسی و هر کتابخانه socket programming آزاد است.

۴- **امتیازی ۱**: سرور امنیتی مورد نظر را پیاده‌سازی کنید. نحوه‌ی کار سرور به این‌صورت است که همواره در حال شنود برای درخواست است و با رسیدن آن، درخواست را رمزگشایی[7]کرده و به آن پاسخ می‌دهد.

پاسخ‌های سرور نیاز به پیچیدگی بالایی ندارد و همان بدنه‌ی درخواست را در قالب یک html در پاسخ، به همراه کد پاسخ صحیح (برای مثال در پاسخ put، پاسخ با مضمون created، دارای کد ۲۰۱ است) بازگرداند.

۵- **امتیازی ۲:** رمزنگاری طوری باشد که به هیچ وجه بدون داشتن کلید، قابل رمزگشایی نباشد (برای این کار می‌توانید از الگوریتم‌های موجود استفاده کنید).

[7] Decrypt

نحوه تحویل تمرین

۱- تمرین به‌صورت تک نفره انجام می‌شود (برای تمرینات کار گروهی نداریم).

۲- تمرین را در قالب یک فایل zip با اسم شماره دانشجویی (zip.*****۹) حداکثر تا ساعت ۲۳:۵۵ روز ۴ آبان در مودل آپلود کنید. هر فایلی که در این قالب نباشد تصحیح نخواهد شد.

۳- تمریناتی که بعد از تاریخ مد نظر ارسال گردند هر روز ۱۵٪ جریمه می‌شوند. بنابراین به تمریناتی که بعد از یک هفته ارسال شود نمره‌ای تعلق نمی‌گیرد.

موفق باشید