امنیت تجارت الکترونیک

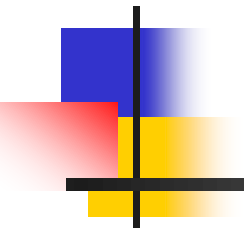
فصل پانزدهم:
پروتکل HTTP

تهیه و تنظیم: دکتر آرش حبیبی لشکری
منبع: کتاب "اصول امنیت برای تجارت الکترونیکی"

اولین نسخه: دی 1393
بروزرسانی: فروردین 1396

فهرست:

- مقدمه
- پروتکل انتقال ابر متن
- پیامهای HTTP
- سربارها اطلاعات حساس را فاش میکنند
- مسائل امنیتی حافظه گش پروتکل HTTP
- احراز هویت سرویس گیرنده HTTP
- احراز هویت خلاصه
- ایجاد تونل SSL
- امنیت تراکنش وب



پروتکل HTTP

مقدمه

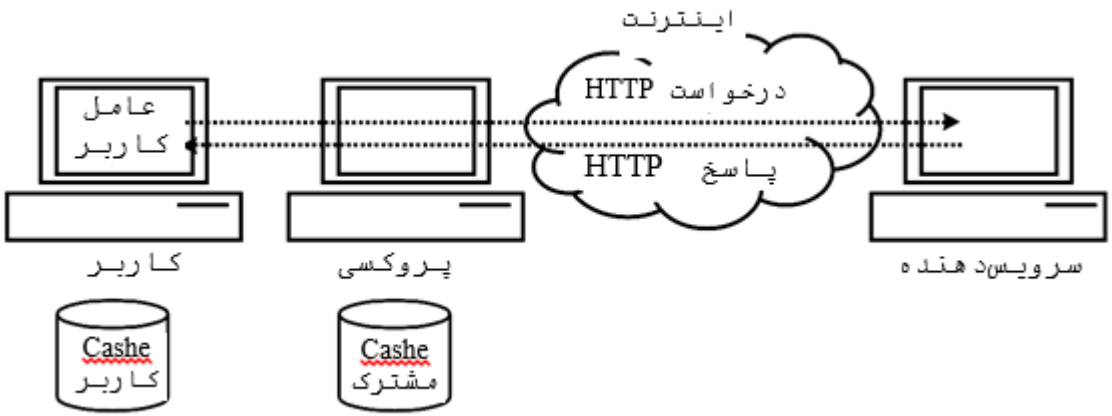
وب یک سیستم اطلاعات توزیع شده است که شامل موارد زیر است:

- سرویس‌دهنده‌هایی که منابع اطلاعاتی را ذخیره می‌کنند؛
- سرویس گیرندگانی که این اطلاعات را می‌توانند بازیابی کنند؛
- پروتکلی که سرویس‌دهنده‌ها و سرویس‌گیرنده‌ها برای برقراری ارتباط استفاده می‌کنند؛
- یک قرارداد نام گذاری برای شناسایی منابع اطلاعاتی؛
- یک تعریف از قالب‌های داده که قابل مبادله هستند؛

زبان اصلی برای ایجاد اسناد وب زبان نشانه گذاری ابرمتن است (HTML).
در برابر
زبان نشانه گذاری توسعه پذیر (XML) که امکان تعریف برچسب‌های جدید را می‌دهد.

پروتکل انتقال ابر متن (HTTP)

HTTP یک پروتکل سرویس‌گیرنده- سرویس‌دهنده (درخواست-پاسخ) برای سیستم‌های اطلاعاتی توزیع شده، مشترک و ابر می‌باشد که توسط درخواستهای جدید از طریق تعریف روش‌ها و سربارهای جدید قابل توسعه است.



HTTP و HTTP امن

پروکسی

تفاوت بین حافظه کَش اشتراکی و غیر اشتراکی

پیامهای HTTP

پیام‌های HTTP شامل درخواست‌ها از سرویس گیرندگان به سرویس‌دهنده‌ها، و پاسخ‌ها از سرویس‌دهنده‌ها به سرویس گیرندگان است. در کل، یک پیام HTTP شامل یک خط شروع، بدون سربار یا با چند سربار، و یک بدنه پیام انتخابی است. یک سربار همیشه حاوی یک نام فیلد، یک دو نقطه، و یک مقدار فیلد، برای مثال: From: somebody@something.com

درخواست واقعی سرویس‌گیرنده: روش، یک URL، و ویرایش HTTPای که سرویس‌گیرنده استفاده می‌کند.

انواع روش ها : خود توان و غیر خود توان

سربارها اطلاعات حساس را فاش میکنند

همه سربارهای HTTP حامل اطلاعات یک سرویس‌گیرنده یا یک سرویس‌دهنده اصلی هستند که خطرهای امنیتی بالقوه محصوب می‌شون:

سربار پاسخ server به ویرایش نرم افزار سرویس‌دهنده اصلی اشاره می‌کند (مانند " CERN/3.0 libwww/2.17")، که اگر ویرایش نرم افزار به داشتن حفره‌های امنیتی معروف باشد، می‌تواند سرویس-دهنده را در مقابل حملات آسیب پذیر نماید.

سربار خواست User-Agent ویرایش نرم‌افزار سرویس‌گیرنده را فاش می‌کند (مانند "CERN-LineMode/2.15libwww/2.17b3").

سربار درخواست From، حاوی یک آدرس ایمیل یا اینترنت از کاربر است. البته اگر کاربر ترجیح دهد که گمنام باقی بماند، این سربار نباید در درخواست ارسال شود.

سایر سربارها و مشکلات امنیتی

مسائل امنیتی حافظه کَش پروتکل HTTP

یک حافظه کَش یک حافظه محلی است که ممکن است توسط یک سرویس‌گیرنده، یک پروکسی، یا یک دروازه ساخته و نگهداری شود.

برای ذخیره پاسخ‌ها از سرویس‌دهنده‌های اصلی به جهت بهبود کارایی و کاهش ترافیک شبکه

سربارهای :

Authentication ،***cachable*** ،**cache-control**

از آنجا که پروکسی‌ها به اطلاعات شخصی، اختصاصی، و مربوط به امنیت دسترسی دارند، یک پروکسی غیر معتمد موقعیتهای زیادی برای حمله و ایجاد اختلالات حریم خصوصی دارد.

حملات محرومیت – از - خدمات

احراز هویت سرویس‌گیرنده HTTP

پروتکل HTTP دو مکانیزم انتخابی چالش-پاسخ احراز هویت سرویس‌گیرنده برپایه – رمزعبور را مهیا می‌نماید: احراز هویت اساسی و احراز هویت خلاصه

احراز هویت پایه:

- سرویس‌گیرنده:

```
GET http://www.some.org/pub/WWW/TheProject.html HTTP/1.1
User-Agent: Mozilla/4.0
```

- سرویس‌دهنده:

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Basic realm."Users".
```

- سرویس‌گیرنده:

```
GET http://www.some.org/pub/WWW/TheProject.html HTTP/1.1
User-Agent: Mozilla/4.0
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ
```

احراز هویت خلاصه

سرویس‌گیرنده:

- WWW-Authenticate: Digest
- realm="testrealm@host.com",
- qop="auth,auth-int",
- nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
- algorithm=MD5

سرویس‌گیرنده:

- authorization: Digest
- username="Mufasa",
- realm="testrealm@host.com",
- nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
- uri="/dir/index.html",
- qop=auth,
- nc=00000001,
- cnonce="0a4f113b",
- response="6629fae49393a05397450978507c4ef1"

ایجاد تونلSSL

- سرویس‌گیرنده:

CONNECT home.some.com:443 HTTP/1.1
User-agent: Mozilla/4.0
...SSL data...

- پروکسی:

HTTP/1.1 407 Proxy Authentication Required
Proxy-Authenticate: Basic realm ."Users".
...SSL data...

- سرویس‌گیرنده:

CONNECT home.some.com:443 HTTP/1.1
User-Agent: Mozilla/4.0
Proxy-Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ
...SSL data...

امنیت تراکنش وب

نیازمندی‌های کلی امنیتی برای پیام‌های HTTP:

- احراز هویت مبدا پیام؛
- یکپارچگی پیام ؛
- محرمانگی پیام؛
- عدم انکار مبدا پیام؛
- تازگی پیام

سرویس‌های امنیتی ممکن است بطور کلی فراهم شده باشند:

- به عنوان پروتکل امنیتی اساسی که یک کانال امن را فراهم می‌کند (از قبیل SSL یا TLS)؛
- به عنوان یک پروتکل امنیتی کپسوله سازی که در موجودیتها در بدنه پیام HTTP به کار گرفته شده است؛
- به عنوان یک بخش الحاقی برای HTTP (از قبیل S-HTTP یا PEP).

کانال امن و امضای دیجیتال

فواید و مضرات کانال امن

خلاصه: پروتکل انتقال ابر متن، پیامهای HTTP، سربارها اطلاعات حساس را فاش میکنند، مسائل امنیتی حافظه کَش پروتکل HTTP، احراز هویت سرویس گیرنده HTTP، احراز هویت خلاصه، ایجاد تونل SSL، امنیت تراکنش وب

جلسه بعدی: امنیت سرویس دهنده وب

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.