Web Application Security Consortium Glossary
Language: Persian
Soroush Dalili – Soroush.secproject.com – April 2008

واژه نامه امنیت وب:

این واژه نامه به صورت الفبایی از واژگان و اصطلاحات رایج امنیت وب با توجه به **کنسرسیوم امنیت برنامه های کاربردی تحت وب**[1] تهیه شده است:

(لطفا نواقص را به مترجم، سروش دلیلی به آدرس ایمیل irsdl در yahoo.com ارجاع دهید.)

Abuse of Functionality:

یک تکنیک حمله است که از خصیصه ها و کارایی یک وب سایت در جهت خراب کردن، کلاه برداری و یا غلبه بر کنترل های دسترسی استفاده می کند.

ActiveX Controls:

برنامه ای که control نامیده می شود با استفاده از تکنولوژی های Activex Controls توسعه داده می شود. کنترل های Activx می توانند به وسیله مرورگر های وبی که این تکنولوژی را فعال کرده باشند download و اجرا شوند. کنترل های ActiveX مجموعه ای از قوانین هستند که چگونگی به اشتراک گذاری اطلاعات بین برنامه های کاربردی را معلوم می کنند. این کنترل ها می توانند با زبان های C,C++,Visual Basic و Java نوشته شوند.

AJAX:

AJAX به کلمات JavaScript و XML برمیگردد. این تکنولوژی که بر پایه مرورگر است به یک وب سایت اجازه می دهد تا بدون باز تازه کردن صفحه برای کاربر، به وسیله شی XMLHttpRequest در JavaScript درخواست های اضافی کاربران را به منابع یک وب سایت انجام دهد.

[1] http://www.webappsec.org/ → http://www.webappsec.org/projects/glossary/v1/wasc_glossary_02262004.pdf

Anti-Automation:

یک اقدام امنیتی است که با اجرای یک تست تورینگ (Turing Test) فقط اجازه عبور انسان (و نه ماشین) را می دهد؛ و با این کار برنامه های خودکاری را که از قابلیت های سایت استفاده می کنند متوقف می کنند.

Application Server:

یک سرویس دهنده نرم افزاری، که معمولا از HTTP استفاده می کند و توانایی اجرای صفحات پویای برنامه های کاربردی تحت وب را دارد. در اینجا میان افزارهایی (middleware) نیز وجود دارند که این قطعه های نرم افزاری نزدیک یا روی سرویس دهنده وب نصب می شوند و در موقع نیاز فراخوانی می شوند.

Authentication:

فرایند بررسی هویت یا مکان یک کاربر، یک سرویس یا یک برنامه کاربردی را Authentication گویند. تایید اعتبار از طریق حداقل سه مکانیسم صورت می گیرد: 1- چیزی که ما داریم (نظیر یک سخت افزار یا یک کارت) 2- چیزی که ما می دانیم (نظیر یک پسورد) 3- چیزی که ما هستیم (مانند اثر انگشت). برنامه تایید اعتبار ممکن است سرویس های متفاوتی را به بنا به مکان، نحوه دسترسی، زمان روز و مانند آن ارائه دهد.

Authorization:

تعیین اینکه یک کاربر، یک سرویس و یا یک برنامه به چه منابعی مجوز دسترسی دارد را Authorization گویند. منابع قابل دسترس می توانند URLها، فایلها، پوشه ها، servletها، پایگاه های داده، مسیرهای اجرایی و مانند آن باشند.

Backup File Disclosure:

این کلمه منسوخ شده و به جای آن Predictable File Location وجود دارد.

Basic Authentication:

یک شکل ساده از Authentication طرف کاربر که در HTTP پشتیبانی می شود. کاربر HTTP یک header درخواست که شامل رمز شده نام کاربری و پسورد با الگوریتم Base64 است به طرف سرور می فرستد. اگر نام کاربری و پسورد معتبر باشد، سرویس دهنده وب اجازه دسترسی به منابع درخواست شده را به کاربر می دهد.

Brute Force:

یک فرایند خودکار است که از روش آزمایش و خطا برای حدس زدن رشته سری که از یک سیستم محافظت می کند، استفاده می کند. مثال های از این رشته محرمانه می تواند نام های کاربری، رمزهای عبور یا کلیدهای مخفی باشد.

Buffer Overflow:

یک تکنیک سو استفاده است که جریان یک برنامه کاربردی را با بازنویسی قسمتی از حافظه به نفع خود تغییر می دهد. Buffer Overflow ها نتیجه معمول عملکرد بد نرم افزارهاست. اگر داده ای که در بافر نوشته می شود از حد خود عبور کند، حافظه مجاور آن خراب می شود و به صورت معمول ایجاد خطا می کند. مهاجم ممکن است بتواند از وضعیت سرریز بافر برای تغییر فرایند اجرای برنامه بهره برداری کند. سرریز کردن بافر و نوشتن مجدد اشاره گر پشته (memory-stack) ممکن است منجر به اجرای دستورات دلخواه سیستم عامل شود.

CGI Scanner:

یک برنامه امنیتی خودکار که به دنبال آسیب پذیری های شناخته شده سرویس دهنده های وب و برنامه های تحت وب پرکاربرد و رایج می گردد. اغلب CGI Scannerها در بررسی های خود خیلی دقیق نیستند و فقط یک سری از درخواست های HTTP را در مقابل رشته های CGI شناخته شده بررسی می کنند.

CGI Security:

این اصطلاح منسوخ شده. به جای آن از Web Application Security استفاده می کنند.

Client-Side Scripting:

یک خصیصه مرورگر وب است که کارایی و پویایی صفحات HTML را افزایش می دهد. مثال هایی از زبان های Client-Side Scripting (در طرف کاربر) عبارتند از JavaScript، JScript و VBScript.

Common Gateway Interface:

به صورت مخفف CGI. یک استاندارد برنامه سازی برای نرم افزار ها جهت وصل شدن به برنامه های کاربردی مقیم در سرویس دهنده های وب و اجرای آنها می باشد.

Configuration File Disclosure:

این اصطلاح منسوخ شده. Predictable File Location را ببینید.

Content Spoofing:

تکنیک حمله ای است که در آن یک کاربر فریب یک سایت تقلبی را می خورد و فکر می کند که سایت تقلبی همان سایت اصلی با اطلاعات درست است.

Cookie:

داده های کوچکی که به وسیله یک سرویس دهنده به سمت کاربر وب ارسال می شوند، که می توانند ذخیره شوند و بعدا بازیابی گردند.

Cookie Manipulation:

تغییر دادن و دستکاری مقادیر کوکی ها، روی مرورگر وب کاربر، برای به کارگیری یک ضعف امنیتی آشکار شده روی برنامه کاربردی تحت وب را Cookie Manipulation گویند. مهاجمان معمولا مقادیر کوکی های خود را برای به دست آوردن هویت جعلی در یک وب سایت دستکاری می کنند. این حالت یک مثال از مشکل اعتماد کردن به کاربر است که فرض شود همیشه ورودی های معقول می فرستد.

Cookie Poisoning:

این اصطلاح منسوخ شده است. اصطلاح Cookie Manipulation را ببینید.

Cross-Site Scripting:

به طور خلاصه XSS نامیده می شود. یک تکنیک حمله است که یک وب سایت را مجبور می کند تا داده های تهیه شده توسط کاربر را انعکاس دهد تا در مرورگر یک کاربر دیگر اجرا شود. وقتی یک کاربر مورد حمله XSS واقع می شود، مهاجم به تمام محتویات مرور گر وب وی (نظیر کوکی ها، تاریخچه، نسخه برنامه های کاربردی و مانند آن) دسترسی دارد.

Debug Commands:

ویژگی های اشکال زدایی برنامه های کاربردی یا فرمان هایی که کمک به شناسایی خطاهای برنامه نویسی در حین فرایند توسعه نرم افزار می کنند.

Denial of Service:

به طور خلاصه DoS. تکنیک حمله ایست که تمامی منابع موجود وب سایت را به قصد متوقف کردن دسترسی های مجاز مصرف می کند. این منابع شامل زمان CPU، به کارگیری حافظه، پهنای باند، فضای دیسک و مانند آن می باشند. وقتی یکی از این منابع به ظرفیت نهایی خود برسد، دسترسی معمولی کاربر به سیستم قطع خواهد شد.

Directory Browsing:

این اصطلاح منسوخ شده. Directory Indexing را ببینید.

Directory Enumeration:

این اصطلاح منسوخ شده. Predictable File Location را ببینید.

Directory Indexing:

خصیصه عادی یک سرویس دهنده وب معمول است که باعث نمایش محتویات یک پوشه وقتی هیچ فایل اصلی ای موجود نباشد می شود.

Directory Traversal:

تکنیکی برای سو استفاده از وب سایت است که از طریق دسترسی به فایل ها و فرامین فراتر از پوشه اصلی اسناد حاصل می شود. بسیاری از وب سایت ها دسترسی کاربران را به یک قسمت مشخص از فایل های سیستم که به طور نمونه پوشه اصلی اسناد یا پوشه اصلی CGI نامیده می شود، محدود می کنند. این پوشه ها شامل فایل ها و اجرا شدنی هایی برای استفاده عموم هستند. در بیشتر حالات، یک کاربر نباید به فایل هایی فراتر (بیرونتر) از این نقطه دسترسی پیدا کند.

DOM Based Cross Site Scrpiting:

DOM Based Cross-Site Scripting یا DOM Based XSS یک حمله Cross-Site Scripting است که از یک برنامه نویسی Javascript نا امن (یا به صورت کلی طرف کاربر) استفاده می کند که در صفحات پاسخ، شرایط یک XSS اتفاق می افتد. در این تکنیک، مهاجم اجرای Javascript را در صفحه ای که به صورت غیر امن از داده های URL یا Referer (صفحه ای که از آن آمده) استفاده می کند، تغییر می دهد. این script ممکن است تابع eval() را برای اجرای کدهای مغرضانه و یا جاسازی کردن آن در DOM (که بنابراین مرورگر آن را به عنوان یک Javascript می انگارد و آن را اجرا می کند) به کار برد. این تکنیک با یک XSS استاندارد که در آن داده های مغرضانه از طرف سرور در یک صفحه جا سازی می شوند، متفاوت است. در برخی حالات، Dom Based XSS می تواند طوری هدایت شود که کدهای مخرب حتی به سرویس دهنده وب نیز نرسند که در این حالت وقوع حمله از دید سرویس دهنده مخفی می ماند.

Encoding Attacks:

یک تکنیک سو استفاده است که به وسیله تغییر شکل داده های کاربر و گذر از فیلترهای بررسی کننده، به وقوع حمله کمک می کند.

Extension Manipulation:

این اصطلاح منسوخ شده است. عبارت Filename Manipulation را ببینید.

File Enumeration:

این اصطلاح منسوخ شده است. عبارت Predictable File Location را ببینید.

Filename Manipulation:

یک تکنیک حمله برای سو استفاده از وب سایت است که با دستکاری نام فایلها در URL باعث رخ دادن خطا در برنامه، کشف محتویات پنهان یا نمایش کدهای منبع یک برنامه می شود.

Filter-Bypass Manipulation:

Encoding Attacks را ببینید.

Forced Browsing:

Predictable File Location را ببینید.

Form Field Manipulation:

تغییر یا دستکاری مقادیر ورودی فرم های HTML یا داده های پست شده HTML به منظور سو استفاده از ضعف های امنیتی به وجود آمده در برنامه می باشد.

Format String Attack:

یک تکنیک سو استفاده است که جریان برنامه را با استفاده از ویژگیهای کتابخانه فرمت رشته ها، برای دسترسی به دیگر فضاهای حافظه تغییر می دهد.

Frame Spoofing:

این اصطلاح منسوخ شده است. Content Spoofing را ببینید.

HyperText Transfer Protocol:

مخفف آن HTTP است. یک پروتکل است که در World Wide Web مورد استفاده قرار می گیرد. HTTP راه فرستادن درخواست ها از کاربر به سرویس دهنده و همچنین چگونگی پاسخ سرویس دهنده به درخواست ها را مشخص می کند.

HTTP Request Smuggling:

HTTP Request Smuggling از اختلاف های تجزیه ای (parsing) وقتی یک یا چند دیوایس (مثل cache server، proxy server، web application firewall و مانند آن) در مسیر جریان داده بین کاربر و سرویس دهنده وب وجود دارند، بهره می گیرد. این کار در حالی که حمله های مختلفی را مانند Web Cache Poisoning، Session Hijacking، Cross-Site Scripting رقم می زند، توانایی عبور از دیوار آتش حفاظتی برنامه کاربردی تحت وب را دارد. مهاجم بسته های فریب دهنده مخصوصی به صورت درخواست

های HTTP می فرستد که باعث می شود دو دیوایس مورد حمله (مثلا پروکسی و سرویس دهنده وب یا دیوار آتش و سرویس دهنده وب) دو درخواست متفاوت از هم را ببینند که به نفوذگر اجازه می دهد تا درخواست خود را به صورت مخفیانه به یک دیوایس برساند بدون آنکه دیوایس دیگر متوجه آن شود.

HTTP Response Smuggling:

این تکنیک قدرت یافته تکنیک HTTP Response Splitting می باشد که می تواند پیشگیری های ضد HTTP Response Splitting را دور بزند. این تکنیک از حالت مشابه HTTP Request Smuggling استفاده می کند و از اختلافات بین آنچه ضد HTTP Response Splitting به عنوان HTTP response stream می شناسد و response streamای که به وسیله یک سرویس دهنده پروکسی (یا یک مرورگر) تجزیه شده است بهره می برد. بنابراین در حالیکه مکانیسم ضد HTTP Response Splitting ممکن است یک response stream را بی ضرر در نظر بگیرد (single HTTP response)، یک پروکسی یا مرورگر می تواند هنوز آن را به عنوان دو HTTP response تجزیه کند و بنابراین در معرض خطر تمامی نتیجه های تکنیک اصلی HTTP Response Splitting قرار بگیرد. برای مثال برخی از مکانیسم های ضد HTTP Response Splitting که در بعضی موتورهای برنامه کاربردی استفاده می شوند، برنامه را از ورود یک header شامل CR+LF برای پاسخ ممنوع می کنند. با این حال مهاجم هنوز می تواند برنامه را مجبور به ورود یک header شامل CRها کند، پس مکانیسم دفاع را دور می زند. بعضی از سرویس دهنده های پروکسی ممکن است هنوز CR را فقط به عنوان یک جداکننده header (و پاسخ) در نظر بگیرند، و در چنین شرایطی ترکیب سرویس دهنده وب و سرویس دهنده پروکسی هنوز در مقابل حمله ای که ممکن است cache پروکسی را آلوده کند آسیب پذیر است.

HTTP Response Splitting:

این حمله باعث می شود تا سرویس دهنده وب دو پاسخ HTTP بفرستد، که در حالت معمول باید تنها یک پاسخ HTTP می فرستاد (به همین دلیل Response Splitting نامگذاری شده). این حمله ممکن است به

صورت تزریق پاسخ HTTP (HTTP response injection) توصیف شود، و معمولا به وسیله تزریق داده های مخرب به یک header پاسخ HTTP هدایت می شود و از کاراکترهای CR+LF برای شکل دهی و اتمام پاسخ اول استفاده می کند و سپس پاسخ اضافی را شکل داده و آن را کنترل می کند. وجود قسمت دوم، پاسخ غیر مترقبه به مهاجم کمک می کند تا کاربری را که این پاسخ اضافی را دریافت کرده بفریبد و او را مجبور کند تا ابتدا درخواست دوم را بفرستد. سپس این کاربر پاسخ دوم (کنترل شده توسط مهاجم) را با قسمت دوم درخواست (کنترل شده توسط مهاجم) مطابقت می دهد. نتیجه نهایی آنکه (با توجه به جفت دوم درخواست-پاسخ کاربر) کاربر مجبور می شود تا درخواست دلخواه مهاجم را به طرف سرور نفوذپذیر بفرستد و در پاسخ، کاربر جواب فریبنده دلخواه مهاجم را دریافت می کند.

Information Leakage:

وقتی است که یک وب سایت داده های حساس نظیر توضیحات برنامه نویس یا پیغام های خطا را آشکار می کند که نفوذگر را در سو استفاده از سیستم کمک می کند.

Insufficient Authentication:

زمانیست که وب سایت به مهاجم اجازه می دهد تا به اطلاعات حساس یا توابع سیستم بدون بررسی هویت، دسترسی پیدا کند.

Insufficient Authorization:

زمانیست که وب سایت به مهاجم اجازه می دهد تا به اطلاعات حساس یا توابع سیستم که نیازمند افزایش سطح دسترسی محدود هستند، دسترسی پیدا کند.

Insufficient Session Expiration:

زمانیست که وب سایت به مهاجم اجازه می دهد تا از Session Credential های قدیمی یا Session ID ها برای اهراز هویت، مجددا استفاده کند.

Insufficient Process Validation:

زمانیست که یک وب سایت به مهاجم اجازه می دهد تا جریان بررسی برنامه کاربردی را دور بزند یا فریب دهد.

Java:

یک زبان برنامه نویسی معمول که توسط Sun Microsystems(tm) توسعه یافته است.

Java Applets:

یک applet برنامه ایست که با زبان Java نوشته می شود و می تواند در یک صفحه وب به کار رود. وقتی که یک مرورگر با توانایی دیدن Java، یک صفحه شامل applet را مرور کند، کد ها توسط Java Virtual Machine(JVM) اجرا می شوند.

JavaScript:

یک زبان معمول اسکریپت نویسی طرف کابر که برای ایجاد محتویات صفحه وب پویا استفاده می شود.

Known CGI file:

Predictable File Location را ببینید.

Known Directory:

Predictable File Location را ببینید.

LDAP Injection:

یک تکنیک برای سو استفاده از وب سایت به وسیله تغییر عبارات LDAP انتهایی از طریق دستکاری ورودی برنامه می باشد. شبیه متدولوژی SQL Injection می باشد.

Meta-Character Injection:

یک تکنیک حمله است که با فرستادن کاراکترهای مخصوص به عنوان داده ورودی که هرکدام معانی خاصی برای برنامه کاربردی تحت وب دارند، از وب سایت سو استفاده می کند. Meta-Characterها کاراکترهایی با معانی خاص برای زبان های برنامه نویسی، فرمان های سیستم های عامل، فرایندهای خاص برنامه، درخواست های پایگاه داده و مانند آن هستند. این کاراکترهای خاص می توانند رفتار یک برنامه کاربردی تحت وب را کاملا تغییر دهند.

Null Injection:

یک تکنیک سو استفاده است که برای گذر از فیلترهای بررسی صحت داده با استفاده از اضافه کردن کاراکترهای null-byte رمز شده در URL، به عنوان داده ورودی کاربر، انجام می شود. وقتی توسعه دهندگان برنامه های کاربردی تحت وب را با زبان های گوناگون می سازند، این برنامه های کاربردی معمولا داده ها را برای پردازش بیشتر و کارایی بالاتر به توابع C سطح پایین تر می فرستند. حال اگر رشته فرستاده شده توسط کاربر شامل

کاراکتر null (\0) باشد، برنامه کاربردی تحت وب ممکن است پردازش رشته را در نقطه null متوقف کند. Null Injection یک شکل حمله Meta-Character است.

OS Command Injection:

OS Commanding را ببینید.

OS Commanding:

یک تکنیک حمله است که از وب سایت، به وسیله اجرای فرمان های سیستم عامل از طریق دستکاری ورودی برنامه کاربردی، سو استفاده می کند.

Page Sequencing:

Insufficient Process Validation را ببینید.

Parameter Tampering:

تغییر یا دستکاری نام پارامترها و ارزش آنها را در یک URL گویند. همچنین به عنوان URL Manipulation شناخته می شود.

Password Recovery System:

یک فرایند خودکار که به کاربر اجازه می دهد تا در صورت فراموش کردن یا گم کردن رمز عبور خود، آن را بازیابی یا ریست کند.

Predictable File Location:

تکنیکی برای دسترسی به محتویات یا توابع پنهان یک سایت است که به وسیله حدس زدن های هوشمندانه به صورت دستی یا خودکار روی نام و مکان فایل ها انجام می شود. مکان های قابل پیشبینی می تواند شامل دایرکتوری ها، CGIها، فایل های تنظیمات، فایل های پشتیبان، فایل های موقت و مانند آن باشد.

Secure Sockets Layer:

به صورت مخفف SSL. یک پروتکل کلید عمومی استاندارد صنعتی که برای ساختن تونل های امن بین دو دیوایس مرتبط در شبکه به کار می رود. برای ارتباطات وب HTTP به HTTPS تبدیل می شود.

Session Credential:

رشته ای از داده است که توسط سرویس دهنده وب درست می شود و معمولا در یک کوکی یا URL ذخیره می شود.

Session Fixation:

یک تکنیک حمله است و کاری میکند تا Session Credential یا Session ID کاربر یک مقدار ثابت معلوم را اختیار کند.

Session Forging:

Session Prediction را ببینید.

Session Hi-Jacking:

نتیجه فاش شدن session کاربر توسط مهاجم است. مهاجم می تواند از این session دزدیده شده استفاده کند و خودش را به جای کاربر اصلی جا بزند.

Session ID:

یک رشته داده است که توسط سرویس دهنده ساخته می شود و معمولا در یک کوکی یا یک URL ذخیره می شود. یک Session ID نشست کاربر را دنبال می کند و یا شاید فقط پیمودن یک سایت توسط وی را پیگیری کند.

Session Manipulation:

یک تکنیک حمله برای دزدیدن نشست کاربر دیگر به وسیله تغییر مقدار Session ID یا Session Credential است.

Session Prediction:

یک تکنیک حمله برای ساختن Session Credential های تقلبی یا حدس زدن Session ID فعلی کاربر است و اگر موفق باشد، مهاجم می تواند با استفاده از نشست دزدیده شده خودش را به جای یک کاربر دیگر جا بزند.

Session Replay:

وقتی است که یک وب سایت به مهاجم اجازه می دهد تا دوباره از یک Session Credential قدیمی یا Session ID قدیمی برای Authorization استفاده کند.

Session Tampering:

Session Manipulation را ببینید.

SQL Injection:

یک تکنیک حمله برای سو استفاده از یک وب سایت به وسیله تغییر عبارات SQL نهایی از طریق دستکاری ورودی های برنامه کاربردی می باشد.

SSI Injection:

یک تکنیک حمله طرف سرور است که به مهاجم اجازه می دهد تا کدهای خود را داخل برنامه کاربردی بفرستد که به وسیله سرویس دهنده وب اجرا خواهد شد.

Transport Layer Security:

به صورت مخفف TLS. یک جانشین امن تر به جای SSL. پروتکل TLS پوشیدگی ارتباطات در اینترنت را تامین می کند. این پروتکل به برنامه های کاربردی (client/server) اجازه می دهد تا ارتباطات خود را به گونه ای برقرار کنند تا از استراق سمع کردن، تغییر های نادرست یا پیام های جعلی در امان بمانند. TLS بر پایه پروتکل SSL بنا شده اما این دو سیستم قابل کارکردن به طور همزمان نیستند (باهم سازگار نیستند).

Universal Resource Locator:

به صورت مخفف URL. یک راه استاندارد برای تشخیص مکان یک شی، معمولا یک صفحه وب، روی اینترنت می باشد.

Unvalidated Input:

وقتی است که یک برنامه کاربردی تحت وب، صحت داده های فرستاده شده توسط کاربر را به درستی بررسی نمی کند.

URL Manipulation:

تغییر یا دستکاری نام و مقادیر پارامترهای یک برنامه کاربردی تحت وب را URL Manipulation گویند.

User-Agent Manipulation:

تکنیکی برای گذر از محدودیت نوع مرورگر توسط یک وب سایت است که به وسیله تغییر مقدار فرستاده شده در header تحت عنوان HTTP User-Agent انجام می شود.

Verbose Messages:

قسمت های اطلاعات جزئی که توسط یک وب سایت آشکار می شوند که می توانند مهاجم را در سو استفاده از سیستم یاری دهند.

Visual Verification:

شیو های تصویرگرای ضد سیستم های خودکار هستند و برای توقف برنامه های خودکار که از کارایی یک وب سایت استفاده می کنند، به این صورت که وجود یک هوشیاری را می سنجند، به کار می روند.

Weak Password Recovery Validation:

زمانیست که وب سایت اجازه می دهد تا مهاجم به طور غیر قانونی رمز عبور کاربر دیگر را به دست آورد، تغییر دهد یا بازیابی کند.

Web Application:

یک نرم افزار کاربردی که به وسیله سرویس دهنده وب (که به درخواست های صفحات وب پویا پاسخ می دهد) اجرا می شود.

Web Application Scanner:

Web Application Vulnerability Scanner را ببینید.

Web Application Security:

علم امنیت اطلاعات در رابطه با World Wide Web، HTTP و نرم افزار های کاربردی تحت وب را Web Application Security گویند.

Web Application Firewall:

یک دیوایس واسط که بین کاربر وب و سرویس دهنده وب قرار می گیرد و پیغام های OSI Layer-7 را برای تشخیص تخطی از سیاست امنیتی برنامه ریزی شده، بررسی می کند. دیوار آتش برنامه کاربردی تحت وب به عنوان یک دیوایس حفاظت کننده سرویس دهنده وب از حملات استفاده می شود.

Web Application Vulnerability Scanner:

یک برنامه خودکار امنیتی است که به دنبال آسیب پذیری های امنیتی نرم افزارها روی برنامه های کاربردی تحت وب می گردد.

Web Browser:

برنامه ای برای نمایش صفحات وب HyperText Markup Language (HTML) فرستاده شده توسط یک سرویس دهنده است.

Web (or browser) Cache Poisoning:

عمل اضافه کردن یا بازنویسی cache وارده (caching یک سرویس دهنده پروکسی یا یک مرورگر) با داده های مخرب یا فریب دهنده را Cache Poisoning گویند. در حالت قوی این عمل، یک مهاجم می تواند ورودی های دلخواه (نظیر URL انتخابی، یا یک صفحه با محتویات دلخواه) را وارد cache کند. در HTTP Response Splitting (توضیح داده شده) مهاجم می تواند مسیر URL و پرس و جو (host، port و scheme باید پذیرنده آسیب پذیری باشند) و کل محتویات صفحه را به دلخواه انتخاب کند. در HTTP Request Smuggling مهاجم می تواند مانند HTTP Response Splitting، URL را انتخاب کند اما محتویات صفحه را باید از یک URL روی همان سایت انتخاب کند. در هر صورت Cache Poisoning می تواند به عنوان یک شکل از تغییر ظاهر (defacement) در نظر گرفته شود که وسعت آن به وسیله منطقه زیر پوشش cache (مثل broswer برای 1 کاربر، forward proxy برای 1 سازمان یا ISP، reverse proxy

برای همه کاربران) و توانایی حمله (دسترسی به تمامی صفحه روی /index.html و یا دسترسی به بخشی از آن) تعیین می شود.

Web Security:

Web Application Security را ببینید.

Web Security Assessment:

فرایند اجرای وارسی امنیتی یک برنامه کاربردی تحت وب به وسیله جستجوی عیوب طراحی، آسیب پذیری ها و ضعف های ذاتی آن است.

Web Security Scanner:

Web Application Vulnerability Scanner را ببینید.

Web Server:

یک نرم افزار همه منظوره است که با در خواست های HTTP سر و کار دارد و به آنها پاسخ می دهد. یک سرویس دهنده وب ممکن است از یک برنامه کاربردی تحت وب برای محتویات صفحات وب پویا استفاده کند.

Web Service:

یک نرم افزار کاربردی است که از پیام ها با قالب Extensible Markup Language(XML) برای ارتباط روی HTTP استفاده می کند. عمدتا نرم افزارهای کاربردی ترجیحا با سرویس های وبی (web services) بیشتر از کاربران معمولی فعل و انفعال دارند.