Hier finden Sie einen Teil der Schwachstellen die wir identifizieren und wirkungsvoll ausschalten können. Bitte bedenken Sie, dass dies nicht alle für uns erkennbaren Web-Sicherheitslücken sind weil das Spektrum in diesem Bereich zu groß ist.

Banner Grabbing:

Banner Grabbing bezeichnet das Auslesen der vom Server gesendeten Versionsinformationen. Beispiele hierfür sind zB. wenn nach dem aufrufen einer nicht vorhandenen Datei folgendes erscheint:

Title > Not Found
The requested URL /datei.txt was not found on this server. Apache/2.2.3 (Debian) mod_python/3.3.1 Python/2.4.4 PHP/5.2.0-10+lenny1 mod_perl/2.0.2 Perl/v5.8.8 Server at localhost Port 80

Fehlermeldungen & Errors:

Fehlermeldungen gelten meistens als harmlos aber meistens beinhalten Sie einige Informationen, die für Angreifer sehr interessant erscheinen. Während sie für den normalen Anwender meist nur lästig sind können Fehlermeldungen für den Angreifer eine wertvolle Informationsquelle sein. Bei Webseiten können das z.B. SQL oder Server-Errors sein.

Information-Leaking:

Google als die vermutlich bekannteste Suchmaschine der Welt bietet Angreifern eine einfache Möglichkeit Informationen über ein konkretes Ziel zu sammeln, ohne direkten Kontakt aufnehmen zu müssen, oder auch wahllos, nach Systemen zu suchen die bestimmte Schwachstellen aufweisen. Ein klassisches Beispiel ist die Suchabfrage "inurl:passwort.txt" die alle Seiten ausgibt die passwort.txt in der URL enthalten (erstaunlicherweise klappt das bis heute;). Hier wird gleichzeitig deutlich was Information-Leaking ist.

Mail Order „Betrugs“:

Mail-Order Betrug ist eine Betrugsform, die man als spezifischen Wort einsetzt wenn jemand auf eine andere Identität z.B. in Versandhäusern oder Onlineshops bestellt. Darüber hinaus nutzt der Betrüger seine Kenntnisse im Bereich "Social-Engeneering" um in besitz der Ware zu kommen. Es heißt außerdem "Mail-Order" weil order für "Auftrag" steht und Mail für "Post". Das Wort Betrug wurde im deutschen angehangen um näher zu definieren wie im englischen das "fraud".

Password-Tests:

Sie haben schwache Passwörter in Web-Applikationen? Wir finden sie und weisen sie darauf hin!

SourceCode:

Im Quellcode der Seite können diverse Informationen vorhanden sein. Neben den Informationen zu den Namen von Formelementen oder clientseitig ausgeführtem Javascript Code usw. können auch durchaus sensiblere Daten im Quelltext stehen.

HTTP Header Manipulationen:

http-Header sind Anfragen die der Browser an den Webserver sendet diese können manipuliert werden um falsche Identitäten vorzutäuschen.

GET http://localhost:80/~cr/search.php?suchanfrage=test HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20070310 Iceweasel/2.0.0.3 (Debian-2.0.0.3-1)
Accept:text/xml,application/xml,application/xhtml+xml,text/html; q=0.9,text/plain; q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive Cookie: PHPSESSID=0198ad3203cd28c4e26df49ffdf9e2fa

HTTP Request Smuggling:

HTTP Request Smuggling ist eine Angriffsform die unterschiedliche Interpretationen von http Requests ausnutzt. Möglich ist dies wenn Proxy Server eingesetzt werden oder andere Dienste die HTTP Anfragen annehmen und auswerten. Ein Angreifer sendet dabei mehrere manipulierte HTTP Anfragen die von den beteiligten Systemen unterschiedlich interpretiert werden. Meistens brauchen alle Systeme den gleichen HTTP Standard. Der Apache Webserver und sogar der IIS verwerfen derartig manipulierte Pakete mittlerweile.

HTTP Response Splitting:

Beim HTTP Splitting wird die vom Server an den Client gesendete HTTP Antwort manipuliert indem eine URL mit manipuliertem Parameter an den Client gesendet wird und der Server diesen Parameter in seine Antwort ungefiltert übernimmt. Das ermöglicht verschiedene weitere Angriffsformen wie z.B. XSS, Web cache Poisoning oder auch Single/Cross User Defacement bei denen das Opfer eine falsche oder gehackte Seite sieht.

Cookie Manipulationen:

Cookie Manipulationen fassen die Angriffsarten zusammen bei denen der Angreifer versucht die Cookies seines Opfers zu manipulieren. Cookies sind hierbei kleine Textdateien die es der Webanwendung erlauben bestimmte Session Variablen, Logins oder ähnliches auf dem Clientrechner zu speichern.

Cross-Site-Scripting(XSS):

Cross Site Scripting zählt zu den am meisten verbreiteten Angriffsformen auf Webseiten. Dabei versucht der Angreifer Scriptcode so in die Webseiten einzubetten das dieser auf dem Rechner des Clients ausgeführt wird. Häufig wird als Scriptsprache dazu Javascript eingesetzt da diese in den meisten Browsern aktiviert ist. Denkbar wären jedoch auch andere Sprachen wie z.B. HTML, VBScript, ActiveX oder Flash. Für diese Art des Angriffes gibt es verschiedene Angriffsszenarien von denen die bekanntesten wohl das Cookie-Stealing oder das Session Hijacking sind. Cookie Stealing ist eine Technik die es dem Angreifer ermöglicht mit Hilfe eines eingebetteten Codes die Cookies fremder Nutzer auszulesen und deren Session zu übernehmen weshalb diese Technik auch Session Hijacking genannt wird.

Session-Fixation-Attack:

Session Fixation ist ein Angriff, bei dem der Angreifer sich selber eine gültige Session ID des anzugreifenden Systems generiert und diese dann diese dem Opfer zukommmen lässt. Wenn das Opfer sich beim nächsten mal in das System einloggt, nutzt es diese dem Angreifer bekannte Session ID, wodurch es dem Angreifer möglich ist die Session des Opfers zu übernehmen.

Verzeichnis Listing:

Mit Verzeichnis Listing ist das browsen der Dateistruktur gemeint. Wenn ein Webserver eine Anfrage an einen Pfad wie zB. www.example.com erhält sieht er im root Verzeichnis für die Domain nach einer index Datei. Häufige index Dateien sind index.htm index.html index.php. Wenn kein Index Dokument gefunden wird kommt entweder eine 403 Forbidden Fehlermeldung oder der Verzeichnisinhalt wird dargestellt. Ein Angreifer kann so eventuell Zugriff auf nicht öffentliche Dateien wie Logdateien oder andere sensible Daten erlangen.

Directory-Traversal:

Ein Directory-Traversal erlaubt Angreifern durch die Hierarchie von Verzeichnissen auf dem Webserver zu navigieren und beliebige Dateien einzusehen. Dies geschieht durch den ../ Befehl bzw. bei Windows Systemen mit Hilfe des Backslashes ..\, der in das nächst höhere Verzeichnis wechselt. Wenn diese Lücke auftritt haben externe Angreifer es sehr einfach und der Server gilt meistens schon als kompromittiert.

Remote File-Inclusion:
Eine File-Inclusion ist als eine der gefährlichsten Sicherheitsrisiken für Webseiten einzustufen, da sie dem Angreifer erlaubt eigenen Code auf dem System auszuführen. Ein Angreifer könnte den Code nicht nur ausnutzen um eigenen Code auszuführen sondern auch um z.B. eine Web-Shell einzuschleusen.

SQL-Injection:
SQL-Injektion bezeichnet das Ausnutzen einer Sicherheitslücke im Zusammenhang mit Datenbanken. Dabei sendet ein Angreifer SQL Steuerzeichen und eigene SQL Statements an die Datenbank um an sensible Informationen zu gelangen. Möglich wird dies wenn Eingabefelder für dynamische Datenbankabfragen nicht hinreichend gefiltert sind.

Remote Command Execution:
Command Execution bezeichnet das ausführen von Kommandos auf entfernten Systemen. Da so ein System vom Angreifer unter Kontrolle gebracht werden kann ist diese Art von Schwachstellen als sehr kritisch einzustufen.

Remote Buffer-Overflows:
Durch Fehler im Programmablauf und der Verarbeitung werden große Datenmengen „remote“ über Pakete in einen zu kleinen vorgesehenen Speicherbereich geschrieben. Dies hat dann zur Folge das Speicherbereich des Ziels alle darauf folgenden Speicherbereiche überschrieben werden.

Remote Format-Strings:
Bei einem Format-String Angriff versucht ein Angreifer Daten aus dem Stack auszugeben. Danach hat ein Angreifer die Möglichkeit mit an jede Stelle im Speicher zu schreiben. So kann der Angreifer, das Opfer-System übernehmen oder einfach zerstören und abschiessen.

Service Schwachstellen:
Diese Art von Schwachstellen umfassen keine über HTTP (Port 80) erreichbaren Services sondern zielen eher auf Services wie z.B. SSH, FTP, TELNET, IMAP, RPC & SMTP ab. Wir testen auf Versionsschwächen und andere Servicemängel in ihrer Infrastruktur.