

Abstrakt

Vor kurzem wurde eine neue Attacke auf Web-Anwendungen bekannt, die es einem Angreifer ermöglicht schützenswerte Cookies oder sogar Passwörter (bei BasicAuth) zu klauen. Die Attacke basiert auf einer Methode (Trace), welche von den meisten Web-Servern unterstützt wird. Dieser Artikel soll diesen Sachverhalt genauer erläutern und über Gegenmassnahmen unterrichten.

Session Identifikatoren

Einführung

Wenn man sich bei einer Web Anwendung, wie Online Shop oder e-Banking anmeldet, wird auf dem Server eine Session aufgebaut. Darin werden aktuelle Benutzerinformationen wie Inhalte eines Warenkorb oder der Fortschritt einer Zahlungserfassung abgespeichert. Der Server verknüpft diese Daten mit dem angemeldeten Benutzer. Damit dieser vom Server wieder erkannt wird ist ein Session Identifikator (SessionID) notwendig, welcher bei jeder Anfrage vom Client mitgeschickt wird. Dies wird über die folgenden Technologien bewerkstelligt:

- Cookies
- Hidden Form Fields
- URL Argumente
- SSL Session ID

Session Identifikatoren bilden ein attraktives Ziel für Hacker. Die SessionID ist dabei, während der Benutzung der Anwendung, die elektronische Identitätskarte des Benutzers. Ein Hacker könnte mit der SessionID die Identität des Benutzers annehmen.

Diebstahl der SessionID

Vier Attackenarten auf SessionIDs sind allgemein bekannt:

- Interception
Belauschen des Netzwerks oder mittels direkter Attacke z.B. via Cross Site Scripting
- Prediction
Erraten der SessionID
- Brute Force
Durchprobieren von Zeichenkombinationen
- Fixation
Vorgängiges Festlegen der SessionID

Session Management

Der allgemeingültige Ablauf beim Session Management von Web Anwendungen beginnt beim Aufruf der Startseite resp. beim Eingeben des Benutzerpasswortes. Der Server generiert zu diesem Zeitpunkt eine SessionID und sendet sie dem Benutzer. Dabei wird sichergestellt, dass die SessionID bei jeder nachfolgenden Anfrage vom Browser des Benutzers zum Server mitgesendet wird. Während ein Benutzer seine Einkäufe im Web Shop tätigt oder seine Zahlungen im e-Banking erfasst, wird nun immer die SessionID im Hintergrund mitgesendet, und so dem Server bei jedem Klick mitgeteilt wer sich auf der Benutzerseite befindet. Die Session endet mit dem Abmelden – der Server löscht die entsprechende Verknüpfung zwischen Benutzer und SessionID und löst somit die Session auf.

Cross-Site-Tracing (XST)

Trace Methode

Die Trace Methode ist zur einfacheren Fehlersuche in die Web-Server implementiert. Ein „Trace“ bewirkt, dass die gesamte Anfrage eines Webbrowsers vom Webserver zurückgeschickt wird (Echo).

```

Clients Request:
telnet www.csnc.ch 80
Trying 212.243.104.211...
Connected to www.csnc.ch.
Escape character is '^['.

TRACE / HTTP/1.1
Host: www.csnc.ch
X-TraceDemo: This text will be looped back!

Servers Response:
HTTP/1.1 200 OK
Server: Compass Security
Transfer-Encoding: chunked
Content-Type: message/http
TRACE / HTTP/1.1
Host: www.csnc.ch
X-TraceDemo: This text will be looped back!
    
```

Jeder Webserver welcher nach dem HTTP 1.1 Standard (RFC 2616, Kap. 9.8) implementiert ist, unterstützt die Trace Methode.

Ablauf der Attacke

Kombiniert nun ein Angreifer die Trace-Methode mit einer Cross-Site-Scripting Schwachstelle entsteht ein so genanntes Cross-Site-Tracing (XST). Auf diese Art können sämtliche Cookies geklaut werden.

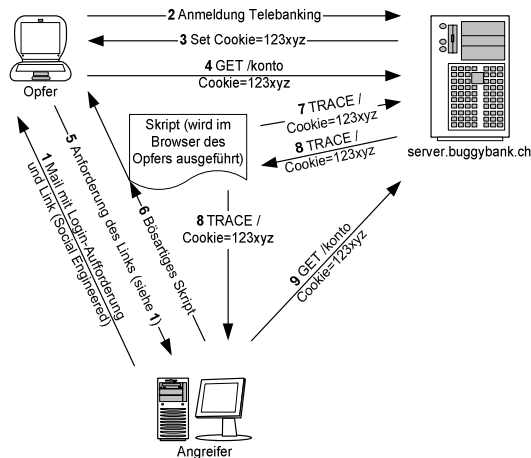
Beim folgenden Beispiel handelt es sich um eine e-Banking Anwendung. Ein Benutzer kann sich anmelden um online Zahlungen zu erfassen resp. seine Konten zu pflegen. Die SessionID wird, wie in den meisten E-Business Applikationen, mittels Cookie übertragen.

Der Angreifer versucht sein Opfer mittels Social Engineering¹ zu animieren in das Telebanking einzuloggen und danach auf einen Link zu klicken (1). Das ahnungslose Opfer meldet sich darauf beim Telebanking an (2) und erhält vom Server ein Cookie (3). Dieses Cookie wird nun zur Identifikation des angemeldeten Benutzers verwendet (4).

Nun klickt das Opfer auf den Link (5) im Mail und fordert ein Skript auf dem Webserver des Angreifers an (6). Dieses Skript wird danach im Browser des Opfers ausgeführt. Die Funktion des Skripts besteht darin ein Trace

auf den Telebanking Server abzusetzen (7) und die darauf folgende Serverantwort dem Angreifer zu senden (8).

Da der Browser automatisch das Cookie mitschickt, erscheint dieses auch wieder in der Antwort vom Server. Weil aber dieses Cookie mit einer aktiven Benutzer-Session verknüpft ist, kann der Angreifer nun in diese Session eintreten und das Telebanking im Namen des Opfers benutzen (9).



Cross-Site-Tracing Beispiel

httpOnly Flag

Mit dem Internet Explorer 6.0 SP1 hat Microsoft ein Sicherheitsfeature eingeführt, welches verhindern soll, dass JavaScripts mit der Methode document.cookie auf die Cookies zugreifen können (httpOnly).

Setzen von Cookies in JavaScript:

```

Ohne httpOnly Flag:
document.cookie = "TestCookie=foobar123";
    
```

```

Mit httpOnly Flag:
document.cookie = "TestCookie=foobar123;
httpOnly";
    
```

Dieses Flag erhöht die Sicherheit, nützt aber bei einer XST-Attacke nichts. Zudem wird diese Funktion von den anderen Browser wie Mozilla, Netscape oder Opera noch nicht unterstützt.

¹ Social Engineering ist eine Technik, mit welcher Personen beeinflusst werden etwas zu tun, was sie sonst nicht tun würden (z.B. Anklicken eines URL's oder Bekannt geben eines Passwortes).

Realität

Da jeder Webserver der nach HTTP 1.1 Standard implementiert ist, die Trace-Methode unterstützt sind viele Web Anwendungen von dieser Attackenart betroffen. Die goldene Regel der Sicherheit, dass alle unbenötigten Funktionen und Dienste abzustellen sind, belohnt einmal mehr die Minderheit welche sich diesen Grundsatz zu Herzen genommen hat. Anhand des Beispiels stellt man fest, dass dennoch einige Puzzleteile zusammen passen müssen, um eine erfolgreiche Attacke durchführen zu können.

- ❑ Ein Benutzer muss mittels Social Engineering dazu gebracht werden in die Web-Anwendung einzuloggen und danach auf einen Link zu klicken, um das böartige Skript zu anzufragen. Im schlechtesten Fall ist es dem Angreifer möglich dieses Skript automatisch ablaufen zu lassen. Dies könnte durch eine Schwachstelle im Telebanking-Server, einem schlecht programmierten Anwenderforum oder eingebettet in einem E-Mail zum Opfer gelangen.
- ❑ Ein Skript welches im Browser abläuft, darf theoretisch nur auf den Server zugreifen von welchem es auch herunter geladen wurde. Leider gibt es mehrere bekannte Schwachstellen in Browsern (Cross-Domain Vulnerabilities), um diese Sicherheitsmassnahme zu umgehen.

Gegenmassnahmen

Compass schätzt die Gefahr einer XST-Attacke als relativ hoch ein, da beinahe alle Web-Server die Trace-Methode unterstützen. Deshalb wird dringend empfohlen diese Methode bei Servern, auf welchen kritische Anwendungen laufen, abzuschalten. Achtung: Bei Reverse-Proxies muss sichergestellt werden, dass Trace-Requests nicht an dahinter liegende Systeme weitergeleitet werden. Ferner wird empfohlen die Browser auf dem aktuellen Patch-Level zu halten. Compass stellt einen Trace-Check zur

Verfügung um Web-Server zu testen (siehe Referenzen).

Apache

Bis beim Apache eine entsprechende Option in der Konfiguration verfügbar ist, muss die Trace-Methode mit dem mod_rewrite abgeschaltet resp. gefiltert werden. Folgende Zeilen im httpd.conf bewerkstelligen dies. Es ist zu beachten, dass die Rewrite-Rules im allgemeinen Teil der Konfiguration platziert sind.

```
LoadModule rewrite_module libexec/apache/mod_rewrite.so
AddModule mod_rewrite.c
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]
```

Siehe

http://httpd.apache.org/docs/mod/mod_rewrite.html

Internet Information Server

Einsatz des URLScan-Tools, ein ISAPI-Plug-in von Microsoft zum Filtern von Web-Server Requests, welches in der Standardeinstellung nur die GET-, HEAD- und POST-Methoden zulässt.

Siehe

<http://www.microsoft.com/technet/security/tools/urlscan.asp>

Netscape (iPlanet, Sun-one)

Das Hinzufügen der folgenden Zeilen in die obj.conf schaltet die Trace-Methode ab.

```
<Client method="TRACE">
  AuthTrans fn="set-variable"
  remove-headers="transfer-encoding"
  set-headers="content-length: -1"
  error="501"
</Client>
```

Siehe http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603&zone_32=category%3Asecurity



Cross-Site-Tracing Schwachstelle in Web Anwendungen

by Christoph Schnidrig
christoph.schnidrig@csnc.ch

Referenzen

- ❑ Paper von WhiteHat Security (Entdecker von XST)
http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
- ❑ Cert Meldung: Multiple vendors' web servers enable HTTP TRACE method by default
<http://www.kb.cert.org/vuls/id/867593>
- ❑ Trace-Test für Web-Server (HTTP)
<http://www.sicherheitstest.ch>
→ Browser→Test starten→Webserver Informationen→Trace Test
- ❑ RFC für HTTP 1.1
<http://www.ietf.org/rfc/rfc2616.txt>
- ❑ Cross Site Scripting & Session Fixation Schwachstelle
<http://www.csnc.ch/downloads/docs/techdocs/ocs/>
- ❑ Unpatched IE security holes
<http://www.pivx.com/larholm/unpatched/>

Über den Autor

Nach der Informatik TS arbeitete Christoph Schnidrig 3 Jahre als System Engineer bei Comline AG. Anfangs 2001 wechselte er zu Compass Security und nahm die Tätigkeit als Security Analyst auf. Ende 2001 schloss er ein Nachdiplomstudium in Wirtschaft ab.

Compass Security AG

Compass Security Network Computing AG konzentrierte sich seit der Gründung im Februar 1999 durch Walter Sprenger und Ivan Buetler auf Sicherheitsanalysen. Seit dem wurden viele Sicherheitsassessments in der Schweiz wie auch im Ausland durchgeführt.

Nach der Gründung konzentrierte man sich vor allem auf Standard Penetration Tests, welche über das Internet durchgeführt wurden. Dabei setzte man unter anderen automatisierende Tools (ISS, CyberCop, Satan, etc) ein. Währenddessen lernte man die Grenzen dieser Tools kennen. Vor allem bei komplexen Umgebungen konnte man sich nicht auf deren Aussage verlassen.

Darauf begann Compass mit Sicherheitsanalysen von e-Business Applikationen. Dabei wurden die meisten Test manuell durchgeführt. Es interessierten Fragen wie: Kann User A die Daten von User B sehen?

Compass versucht die eingesetzten Assessment Methoden ständig zu verbessern. Schwerpunkt wird auch auf die Schulung sicherheitsrelevanter Sachverhalte gelegt. Aus diesem Grund werden regelmässig Kurse angeboten. Neu wurde ein Application Security Kurs ins Portfolio aufgenommen, welcher unter anderem auf die in diesem Artikel behandelten Probleme eingeht.

Weiteres siehe: <http://www.csnc.ch>

02. April 2003 Version 1.1