Link: https://www.tecchannel.de/a/millionen-dsl-router-hochgradig-gefaehrdet,1993878

15 Jahre TecChannel - der beliebteste Artikel im Jahr 2009

Millionen DSL-Router hochgradig gefährdet

Datum: 08.04.2009
Autor(en): ALBERT LAUCHNER

Cross Site Request Forgery als Angriffsvektor wurde lange unterschätzt. Doch jetzt ist es TecChannel gelungen, über einfache CSRF-Attacken DSL-Router von A wie AVM Fritz!Box bis Z wie ZyXEL über das Internet von außen anzugreifen. Surft man mit dem PC auf eine manipulierte Website, kann die komplette Konfiguration der DSL-Router unbemerkt modifiziert werden.

Bislang gelten Cross Site Scripting und Injection-Angriffe als Haupteinfallsvektor für erfolgreiche Attacken auf Web-Server. Doch in der aktuellen Liste der gefährlichsten Fehler, die regelmäßig von der OWASP (Open Web Application Security Project) herausgegeben wird, hat sich Cross Site Request Forgery (CSRF) inzwischen auf Platz fünf hochgearbeitet.

Wie gefährlich dieser bislang unterschätzte Angriffsweg tatsächlich ist, zeigen aktuelle Sicherheitstests von TecChannel. Im Folgenden erläutern wir zunächst die gar nicht so schwierige Theorie hinter CSRF. Anschließend demonstrieren wir zwei Angriffe auf unserer eigene Site TecChannel.de, die einige harmlose CSRF-Schwachstellen enthält. Aber dann geht es ans Eingemachte:

Über CSRF-Attacken ist es uns gelungen, die Konfiguration der **AVM Fritz!Box**[1], des **Cisco/Linksys WAG 160 N**[2] und eines **ZyXEL P-660HW**[3] beliebig zu modifizieren. Aber auch die meisten anderen DSL-Router dürften gefährdet sein. Für den Angriff genügt es, dass der Anwender eine präparierte Website besucht. Diese kann dann Konfigurationsarameter, die über die Web-Oberfläche des DSL-Routers zu erreichen sind, beliebig ändern. Ein Besuch einer manipulierten Seite, und alle Telefonate laufen bei einem Router mit Telefoniefunktion über eine teure 0900er-Vorwahl.

Der Passwortschutz der Router erwies sich dabei als nicht ausreichend. Welches Gefahrenpotenzial sonst noch in dem CSRF-Angriff steckt und was man gegen die Attacken auf die DSL-Router unternehmen kann, lesen Sie am Ende dieses Beitrags.

Weitere Beiträge zur AVM Fritz!Box

Teil 1: Tuning und Hacks für die Fritz!Box[13]

Teil 2: Fritz!Box-Hack: Computer über das Internet starten und fernsteuern[14]

Teil 3: Die Fritz!Box als Least Cost Router[15]

Teil 4: VPN-Direktkopplung mit der Fritz!Box[16]

Teil 5: Rettung für die defekte Fritz!Box[17]

Teil 6: Eigene Firmware mit Freetz erstellen[18]

[Hinweis auf Bildergalerie: **15 Jahre TecChannel Jubiläumspaket -**] [gal1]

1. Angriffsvektor CSRF (XSRF oder Session Riding)

Die Non-Profit-Organisation **OWASP**[4] veröffentlicht alle zwei Jahre eine Liste der gängigen Angriffe auf Web-Anwendungen. Ziel ist es, Web-Entwickler, Web-Designer und Firmen mit Web-Anwendungen für die aktuellen Gefahren zu sensibilisieren. Seit Jahren belegen die inzwischen hinlänglich bekannten Cross Site Scriptings und Injections die vorderen Plätze. Bei diesen Attacken schreibt der Angreifer ausführbaren Code in Eingabefelder von Web-Anwendungen. Wird die Eingabe nicht sauber gefiltert und umcodiert, führt beim Cross Site Scripting der Browser bösartigen Code aus. Bei Injections hingegen gelangt der Code bis zu den Servern. Bei SQL-Injections etwa schleust man so SQL-Anweisungen zur Datenbank durch und kann dann Daten entwenden oder zerstören. In der Regel ist der Angreifer beim Cross Site Scripting oder bei Injections selbst aktiv und gibt den kritischen Code über seinen Browser ein.

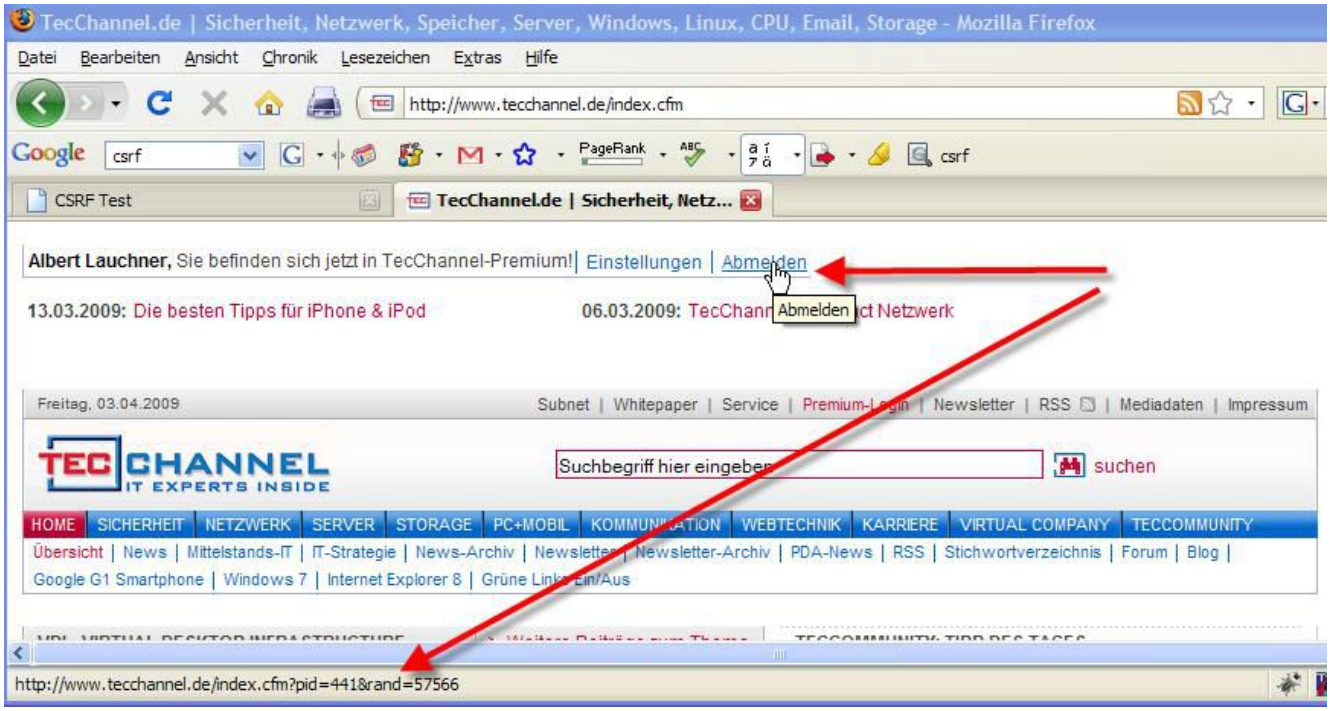
Cross Site Request Forgery wählt einen ganz anderen Weg. Hierbei wird ein nichtsahnender Surfer als Mittelsmann für den Angriff missbraucht. Eine bösartige Website nutzt die Vertrauensstellung des PCs oder Browsers des Mittelsmanns gegenüber einer anderen Seite aus.

Ein ganz einfacher Fall ist ein in das Intranet einer Firma eingeloggter Anwender. Surft dieser in einem zweiten Browserfenster eine präparierte Seite irgendwo im Netz an, so kann ein darin enthaltener Schadcode mit den legitimen Rechten des Anwenders auf das Intranet zugreifen. Ist der Login auf das Intranet gar über ein Cookie automatisiert, muss der Anwender nicht einmal aktiv eingeloggt sein, um über diesen Weg einen Angriff zu starten.

2. CSRF-Logout-Button-Attacke

Zum besseren Verständnis dazu gleich ein einfaches Praxisbeispiel, das aber nur Abonnenten von **TecChannel-Premium**[5] selbst live testen können: Geschütze Bereiche, die nur nach einem Login erreichbar sind, findet man überall im Web. Ob ein Forum, ein Intranet oder eine Web-Anwendung, stets ist ein Login nötig. Und wo ein Login ist, da sollte es auch einen Logout geben.

Oftmals ist dieser Logout nur ein einfacher Link, der sich hinter einem Text oder einem Icon verbirgt. Wird dieser Link, wie auch im Premium-Bereich von TecChannel umgesetzt, aufgerufen, beendet der Web-Server die Session und loggt den User aus.



Logout-Link: Der Logout aus TecChannel-Premium erfolgt durch den Aufruf einer speziellen Seite.

Im Fall von TecChannel Premium genügt ein Aufruf der URL **http://www.tecchannel.de/index.cfm?pid=441&rand=57566**[6] für die Abmeldung. Meldet man sich öfter an und ab, erkannt man, dass sich der hintere Parameter „&rand=xxxx“ zwar stets ändert. Gibt man die URL zum Test manuell ein und lässt den hinteren Parameter ganz weg oder benutzt einen bereits benutzen Wert, so wird man aber dennoch ausgeloggt. Somit genügt ein stets gleicher Link für den Logout. Jetzt stellt sich die Frage, wie man dies für einen Angriff nutzen kann.

3. Angriff über das <img> Tag

Rein technisch gesehen gibt es so etwas wie den Aufruf eines Links für einen Web-Server gar nicht. Das Klicken mit der Maus auf einen Link behandelt ja der Browser. Der Browser erkennt, dass der User einen Link geklickt hat. Daraufhin fordert er vom Web-Server die Daten für die gewünschte URL an. Der Web-Server von TecChannel.de erhält also vom Browser bei einem Kick auf den Logout-Text einfach nur die Aufforderung, die Daten der Seite **http://www.tecchannel.de/index.cfm?pid=441&rand=57566**[7] an den Browser zu senden. Diese Seite gibt es aber gar nicht. Der Seitenaufruf wird lediglich als Kommunikationsmittel genutzt. Erhält der Web-Server eine Anfrage dieser Seite, interpretiert er dies als Wunsch zum Logout und schickt die normale TecChannel-Homepage an den Browser.

Nun gibt es aber weitere Möglichkeiten, Daten vom Web-Server anzufordern. Besonders einfach geht dies über das Image-Tag, mit dem normalerweise Bilder in Seiten eingebunden werden. Findet der Browser im Quelltext einer Seite ein Element wie

```
<img src=http://www.tecchannel.de/img/tecchannel_logo.gif>
```

, so fordert er diese Daten vom Server an. Technisch gesehen nutzt der Browser beim Anfordern sowohl einer HTML-Seite als auch eines Bildes das HTTP-Kommando GET mit der gewünschten Adresse als Parameter.

Für die harmlose XSRF-Attacke auf den Logout nutzt man jetzt aus, dass

- das Bild auch von einem anderen Server und einer anderen Domain kommen kann

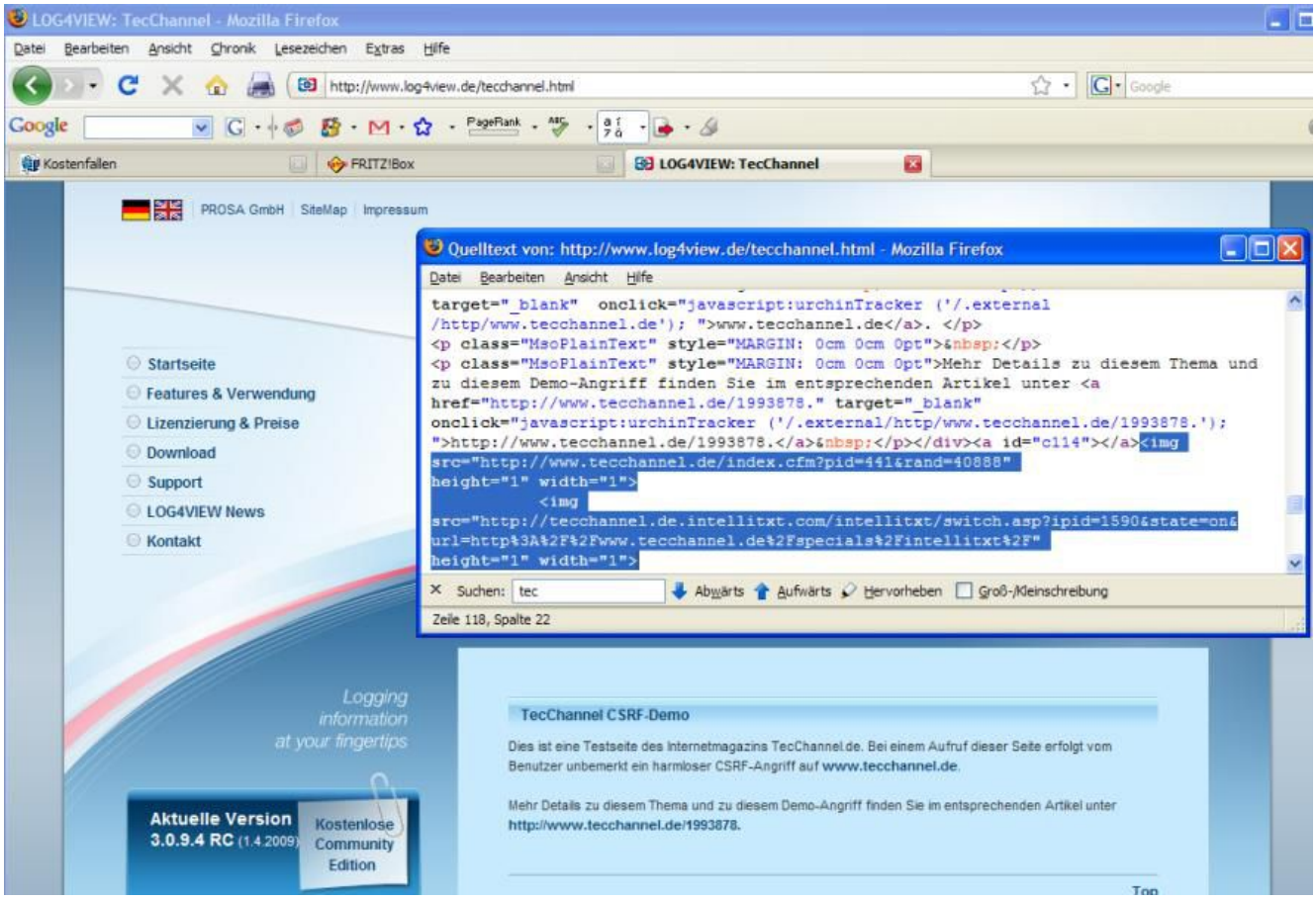
- das „Bild“ keine passende Dateiendung wie .gif , .png oder .jpg haben muss
- bei fehlerhaft zurückgelieferten Daten der Browser an der Stelle des Bilds nichts anzeigt.

4. Datenverkehr im Detail

Somit genügt es, auf einer beliebigen Website, die gar nichts mit TecChannel zu tun hat, das Element

```
<img src=http://www.tecchannel.de/index.cfm?pid=441&rand=57566>
```

einzufügen. Surft ein eingeloggter Premium-Anwender die so präparierte Seite an, fordert der Browser von TecChannel die vermeintlichen Bilddaten an und loggt den User dadurch aus.



Demo-Seite: Auf der harmlos aussehenden Seite, die mit der Domain TecChannel.de nichts zu tun hat, sind die beiden Angriffs-Images eingebettet.

Zum Test haben wir unter **www.log4view.de/tecchannel**[8] eine dementsprechend präparierte Seite eingerichtet, sodass Premium-User den Angriff live testen können. Beim Aufruf erfolgt dann auch gleich noch die nächste Stufe eines CSRF-Angriffs, die Manipulation von Cookies. Dies können alle Leser von TecChannel.de live ausprobieren.

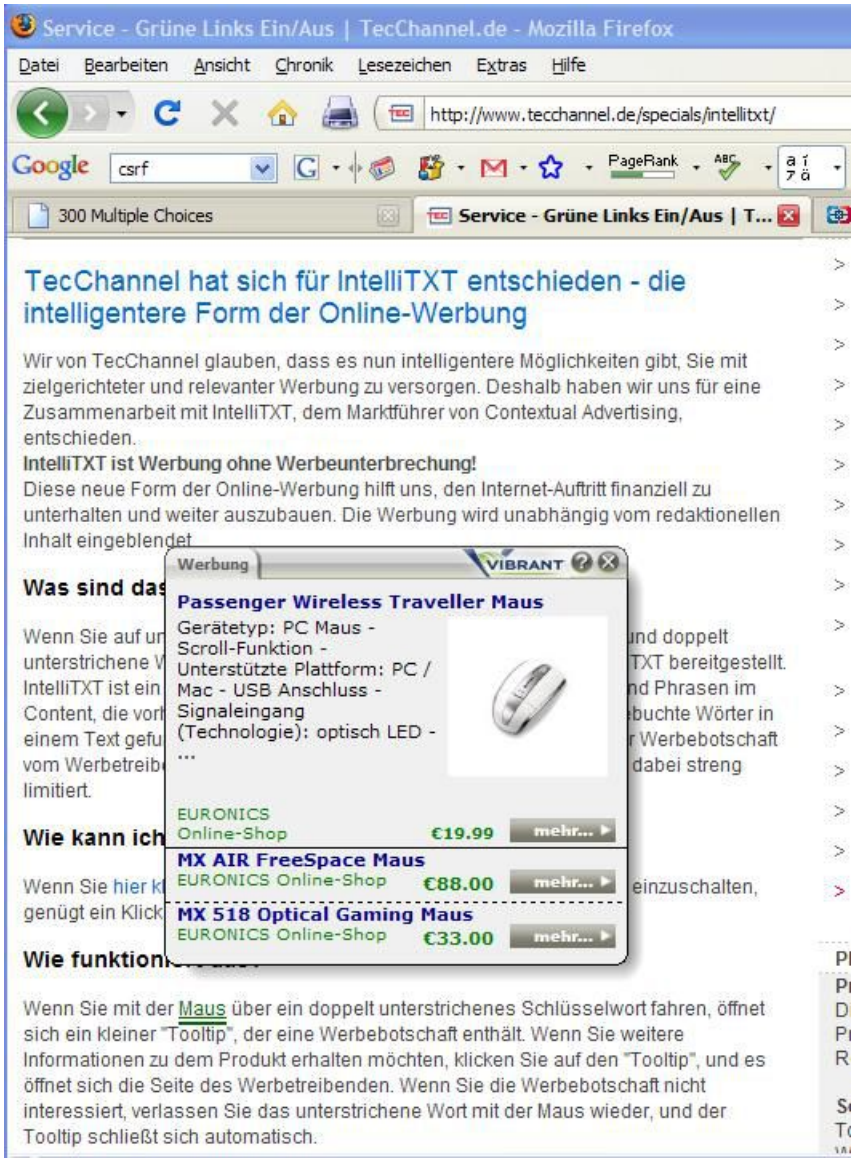
In der Bildergalerie haben wir den Datenverkehr mit einem sogenannten HTTP-Debugging Poxy mitgeschnitten. Dort werden die einzelnen Zusammenhänge nochmals erläutert.

[Hinweis auf Bildergalerie: **Bildergalerie: Der CSRF-Angriff auf den Premium-Logout im Detail.**] gal2

5. Cookie-Manipulation mit CSRF

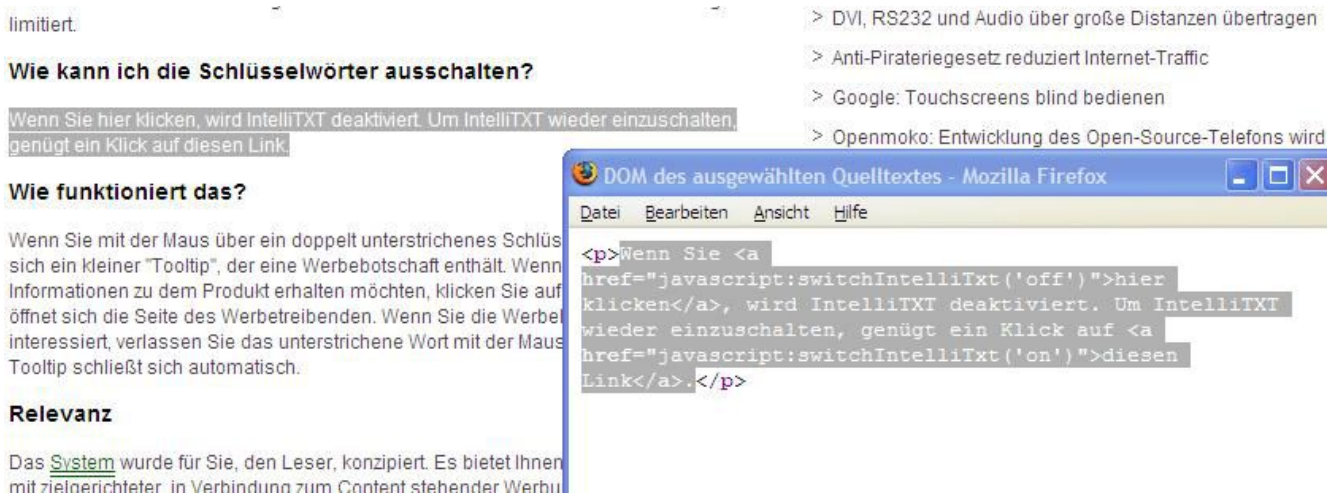
Das nächste Beispiel eines CSRF-Angriffs ist schon etwas hinterhältiger. Ist beim Logout-Angriff die Auswirkung sofort zu sehen, manipulieren wir nun ein Cookie. Damit wird eine Eigenschaft dauerhaft verändert, und die Auswirkung zeigt sich eventuell erst viel später.

Zunächst ein paar Worte zur „Versuchsumgebung“. Wie **hier auf TecChannel beschrieben**[9], nutzen wir als spezielle Werbeform IntelliTXT. Dabei werden bestimmte Schlüsselwörter mit grünen Werbe-Links hinterlegt.



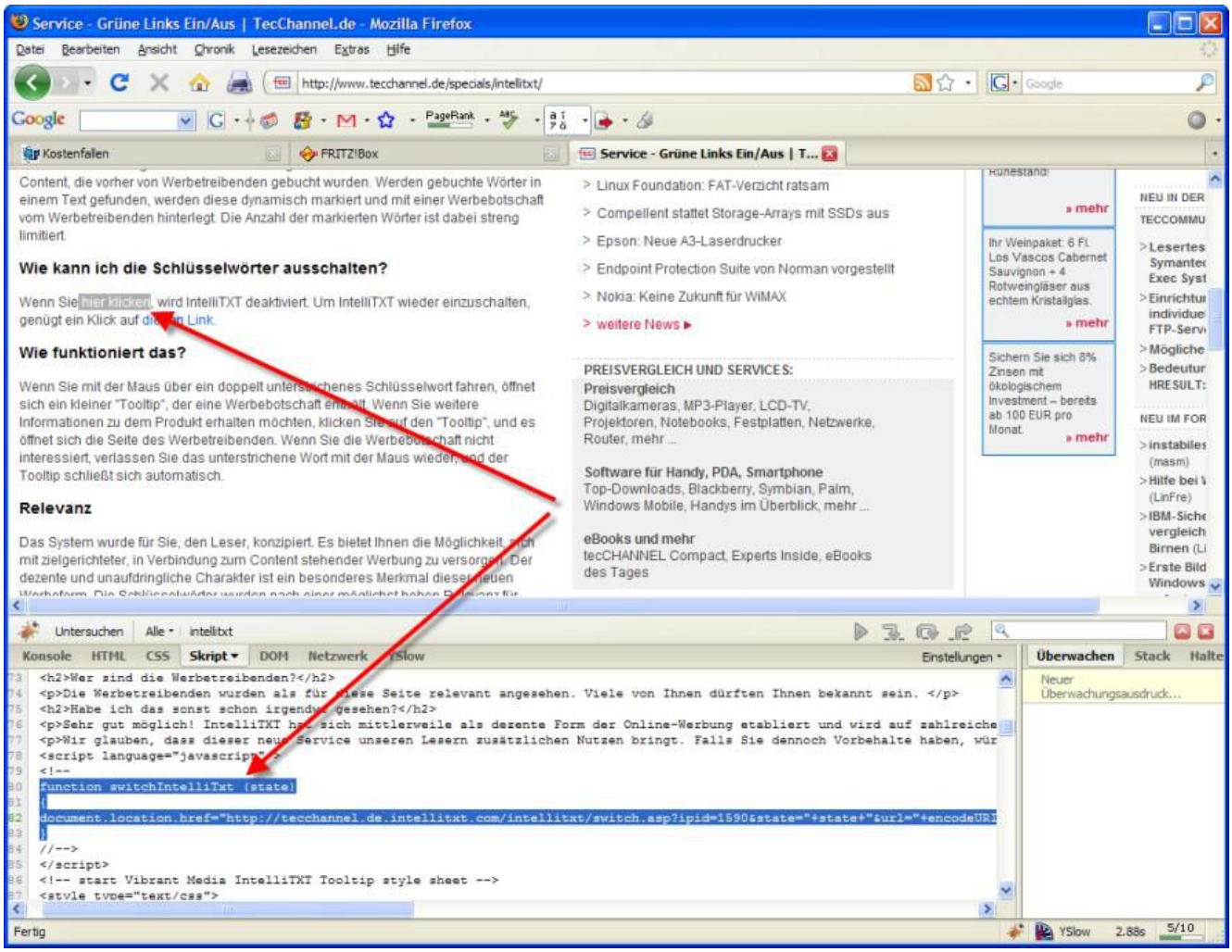
IntelliTXT: Der Anwender kann die IntelliTXT-Werbeform optional ein- und ausblenden.

Diese Werbeform kann vom Leser ein- und ausgeschaltet werden. Sieht man sich den Sourcecode der Seite an, erfolgt die Auswahl über einen Link, der ein Javascript aufruft. Um dies zu analysieren, ist aber ein wenig Aufwand nötig, da es nicht in den HTML-Code eingebettet ist, sondern nachgeladen wird.



Javascript: Die Auswahl erfolgt normalerweise über ein Javascript, das man erst noch in einer externen Library suchen muss.

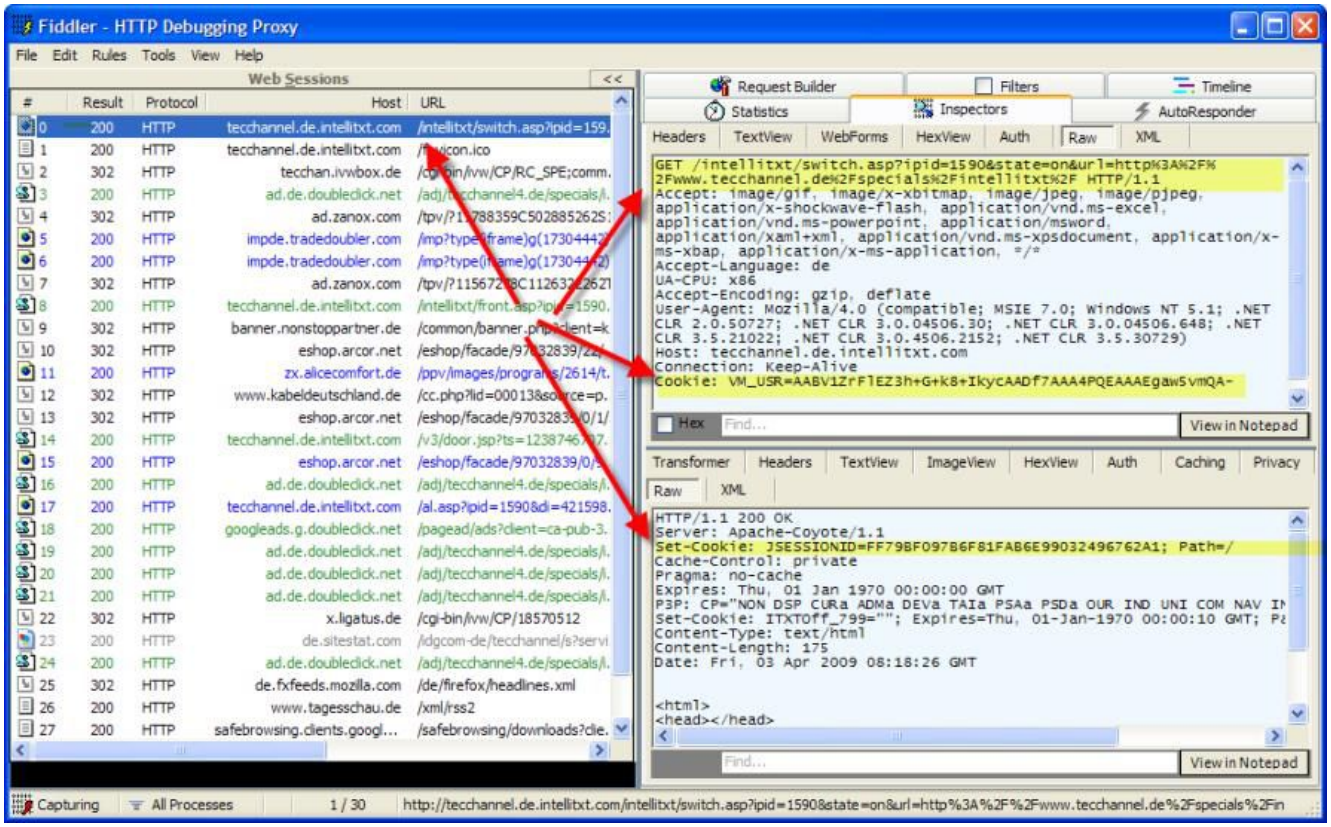
Die Analyse des Sourcecodes erleichtern zwar Debugging-Tools wie Firebug. Aber es geht auch viel einfacher.



Javascript: Mit der Firefox-Erweiterung „Firebug“ kann man das IntelliTXT-Script aufspüren.

6. Analyse mit dem Debugging Proxy

Zum Test der IntelliTXT-Funktionen klemmen wir uns zunächst in den Datenverkehr zwischen Browser und Server. Ideal für diesen Zweck ist die Freeware **Fiddler**[10], mit der man HTTP-Pakete mitschneiden, analysieren und sogar modifizieren kann. Klickt man auf TecChannel.de den Link zum Einschalten von IntelliTXT, so sieht man im oberen Bereich von Fiddler, dass im Prinzip nur wieder eine bestimmte URL auf intellitxt.com aufgerufen wird (GET). Wie im unteren Bereich des Screenshots zu sehen, liefert der Server von IntelliTXT daraufhin ein Cookie zurück, in dem der Browser die Erlaubnis zum Anzeigen der Werbung speichert.



Debugging Proxy: Fiddler zeigt das zum Aktivieren gesendete Paket und die Antwort des Servers darauf an.

Fügt man nun wieder den mit Fiddler gefundenen Link als Image mit

```
<img src= "http://tecchannel.de.intellitxt.com/intellitxt/switch.asp? ipid=1590&state=on&url=http%3A%2F%2Fwww.tecchannel.de%2F special s%2Fintellitxt%2F" height="1" width="1">
```

auf eine beliebige Website ein, wird bei deren Besuch IntelliTXT auf TecChannel.de aktiviert.

Das Frappierende daran ist das Management des Cookies, das wir wieder anhand unserer Demo-Seite aufzeigen:

- Das nichtsahnende Opfer greift auf die Seite **www.log4view.de/tecchannel**[11] zu.
- Diese Seite ruft nun über ein manipuliertes Image eine Adresse auf intellitxt.com auf. Wie die URL

  ```
  tecchannel.de.intellitxt.com
  ```

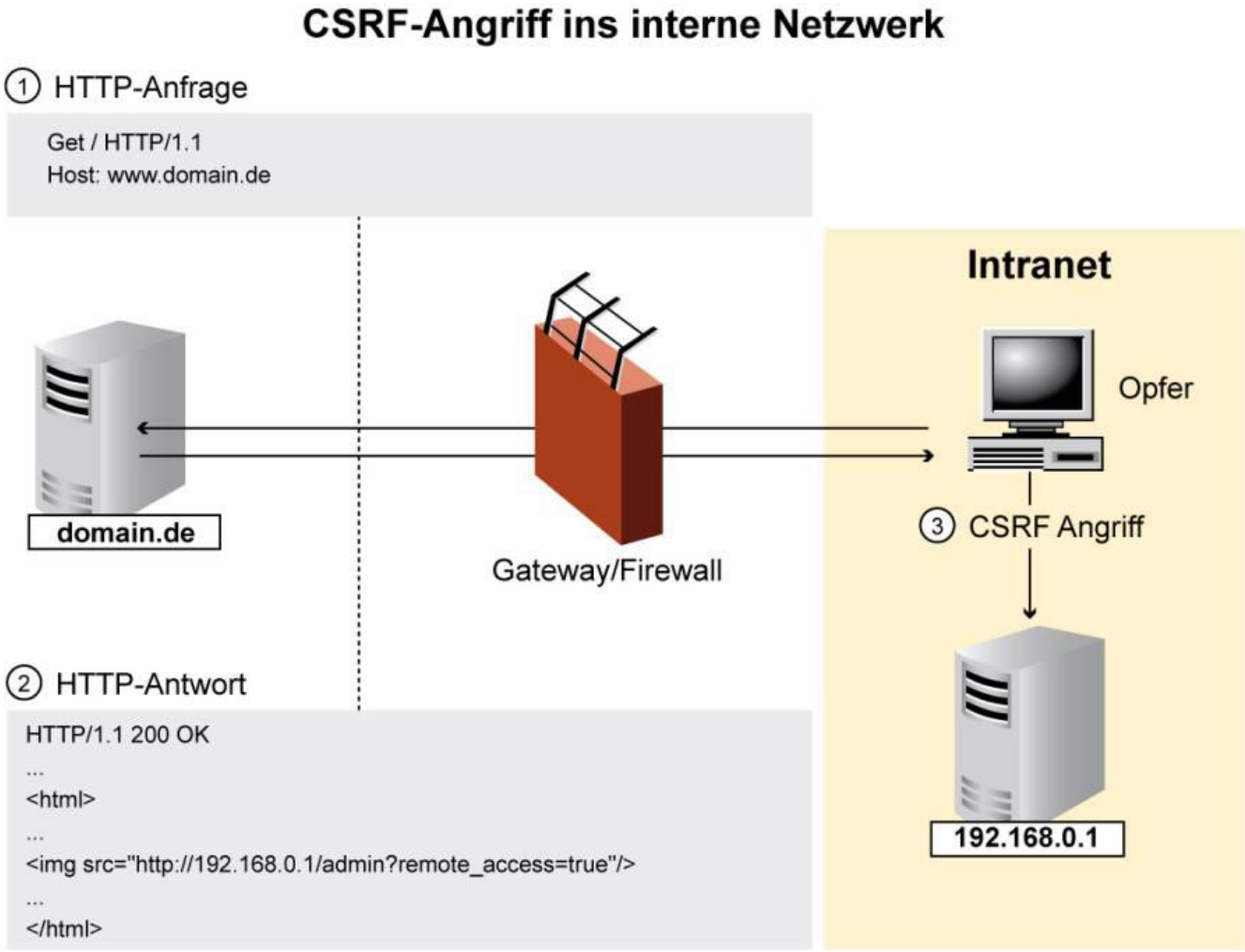
  vermuten lässt, ist im vorderen Teil kodiert, für welche Domain die Werbung bei IntelliTXT freigeschaltet werden soll.
- Der Server von IntelliTXT interpretiert den Seitenaufruf nun als einen Klick auf den Link zum Einschalten der Werbung auf TecChannel.
- Wie im unteren Teil des Fiddler-Screenshots zu sehen, sendet er nun ein Cookie zurück, in dem er sich diese Erlaubnis merkt.

Das Opfer war während der ganzen Zeit nicht auf TecChannel.de. Doch wenn er das nächste Mal TecChannel.de besucht, wird er die IntelliTXT-Werbung in den Artikeln sehen.

Noch ein Anmerkung zum Test: Diese Werbeform ist generell nur in Artikeln und nicht auf der Homepage oder den Übersichtsseiten aktiviert.

7. CSRF-Angriff auf das interne Netz

Die bislang demonstrierten Sicherheitslücken waren gegen Server gerichtet, die sich im frei zugänglichen Internet befinden. Das Hinterhältige an einem CSRF-Angriff ist jedoch, dass die Aktion immer vom Browser eines unwissenden Opfers ausgeht und somit dessen Rechte besitzt. Dadurch sind von außen gesteuert jederzeit Angriffe auf Rechner im Intranet möglich. Diese sind normalerweise weniger gut geschützt, da die Administratoren davon ausgehen, nur interne Mitarbeiter hätten darauf einen Zugriff und die normale Firewall würde externe Attacken abblocken.



Durch die Firewall: Da das Opfer hinter der Firewall sitzt, ist auch ein Angriff auf das interne Netz möglich.

Wie das Diagramm zeigt, ändert sich am prinzipiellen Vorgehen beim CSRF-Angriff auf das interne Netzwerk gar nichts. Der Firmenmitarbeiter an seinem Arbeitsplatz greift auf eine manipulierte externe Seite zu. Darin ist ein Image mit einer Adresse eines firmeninternen Servers eingebunden. Beim Laden des vermeintlichen Bildes löst der Browser dann Aktionen auf dem Server, der eigentlich durch die Firewall von außen gar nicht zugänglich ist.

Jetzt stellt sich natürlich die Frage, woher ein externer Angreifer Details wie lohnende Server, deren darauf laufende Web-Anwendung und zudem noch die IP-Adresse im internen Netz kennen sollte. Eine Möglichkeit ist die Rache eines entlassenen Mitarbeiters, der sein Insiderwissen preisgibt oder ausnutzt.

Ein weitaus einfacheres Ziel ist aber ein DSL-Router. Die Fritz!Box beispielsweise steht millionenfach in deutschen Haushalten und kleinen Büros, ist im internen Netz immer unter fritz.box erreichbar, und die darauf laufende Web-Anwendung ist für jeden einfach analysierbar. Im Folgenden dienen die AVM-Router lediglich als Beispiel, da diese in Deutschland weit verbreitet sind. Selbstverständlich sind auch alle anderen DSL-Router, die per Web-Interface konfiguriert werden, potenzielle Opfer – sofern die Hersteller keinen wirksamen Schutz implementiert haben. In unseren Tests konnten wir beispielsweise den Cisco/Linksys WAG 160 N und einen ZyXEL P-660HW über den gleichen Weg angreifen.

8. Sicherheitsrisiko DSL-Router

Die komplette Konfiguration der Fritz!Box erfolgt wie bei den meisten DSL-Routern über ein Web-Interface. Auf der Fritz!Box läuft ein einfacher Web-Server, der HTML-Seiten mit Formularfeldern ausliefert. Die im Bild dargestellte WLAN-Konfiguration ist ein HTML-Formular, das ein paar Checkboxen, ein paar Dropdown-Felder und einige Textfelder enthält.

Web-Formular: Im Prinzip besteht die Konfiguration nur aus einem einfachen Formular.

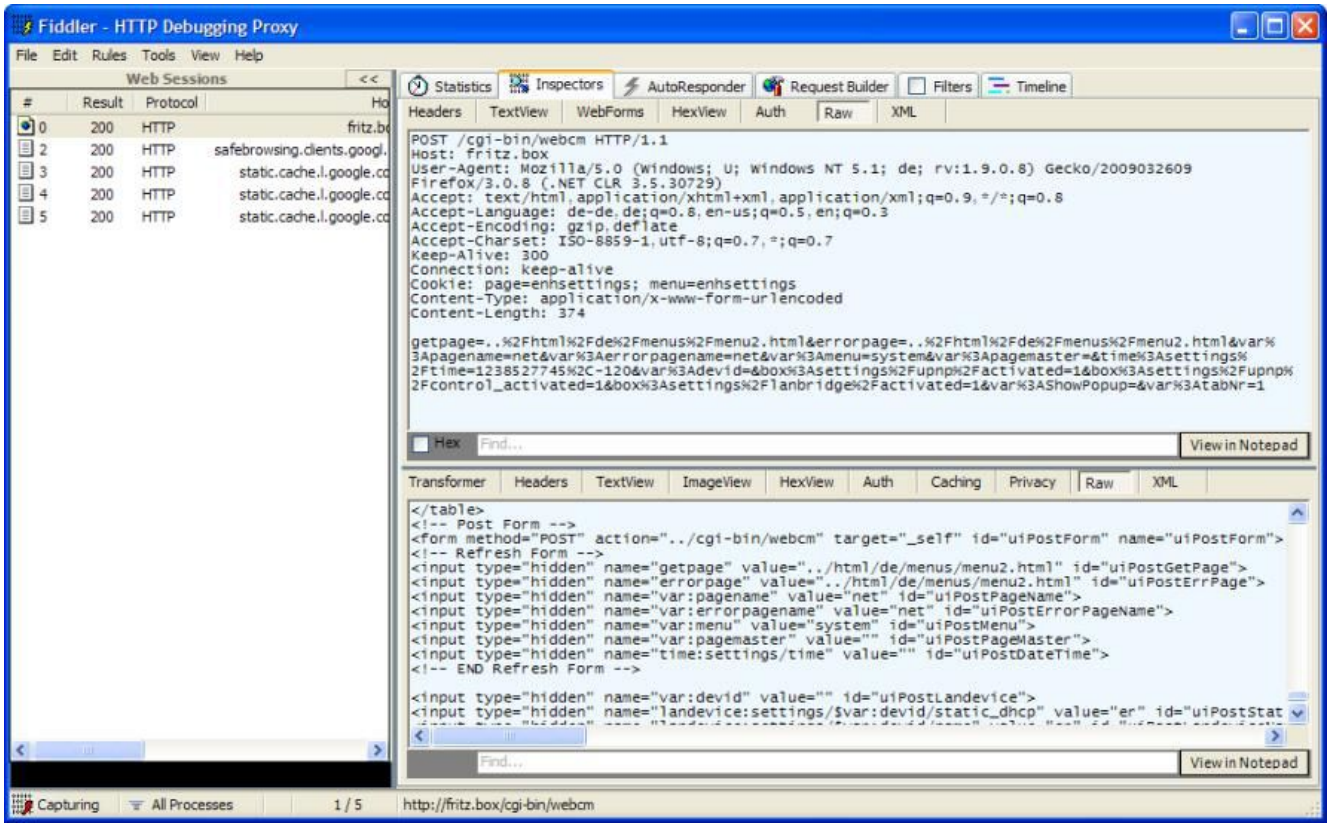
Der User kann in diesem Formular die Werte verändern. Klickt er auf „Übernehmen“, sendet der Browser die Daten zur Fritz!Box, die dann die Werte übernimmt. Dabei erfolgt keine weitere Sicherheitsabfrage. Gelingt es, über einen CSRF das Senden der Formulardaten zu simulieren, kann ein kleines Code-Fragment in einer externen Website die Fritz!Box beliebig umkonfigurieren.

In der Bildergalerie sieht man sehr schön, was der Browser per HTTP-Post an die Fritz!Box sendet. Neben den Rohdaten kann Fiddler sogar in der Ansicht „WebForms“ die einzelnen Formulardaten mit ihren Details darstellen.

[Hinweis auf Bildergalerie: **Bildergalerie: Analyse der Kommunikation mit dem Web-Interface verschiedener DSL-Router.**] gal3

9. AVM bestätigt Angriff

TecChannel ist der CSRF-Angriff auf die komplette Konfiguration der Fritz!Box relativ schnell gelungen. Da die Fritz!Box im deutschen Markt die größte Verbreitung hat, wurde AVM über das Sicherheitsrisiko sofort informiert und hat dieses inzwischen auch bestätigt. Um Missbrauch zu vermeiden, haben wir uns jedoch entschlossen, weder den genauen Angriffsweg noch den Code zu publizieren. Deshalb werden wir auch keine entsprechende Testsite live zur Verfügung stellen.



Kommunikation über POST: Ein simpler POST an den Web-Server der Fritz!Box genügt zum Verändern von Daten.

Aufmerksam wurde TecChannel auf diesen Angriffsvektor durch eine kleine Randbemerkung auf den TrendTagen der Sicherheitsexperten von **cirosec**[12]. Dieser IT-Dienstleister hat sich schon vor Jahren auf die Verwundbarkeitsanalyse und den Schutz von Web-Anwendungen spezialisiert. Mehrmals im Jahr hält cirosec kostenlose Veranstaltungen zu aktuellen Sicherheitsthemen ab.

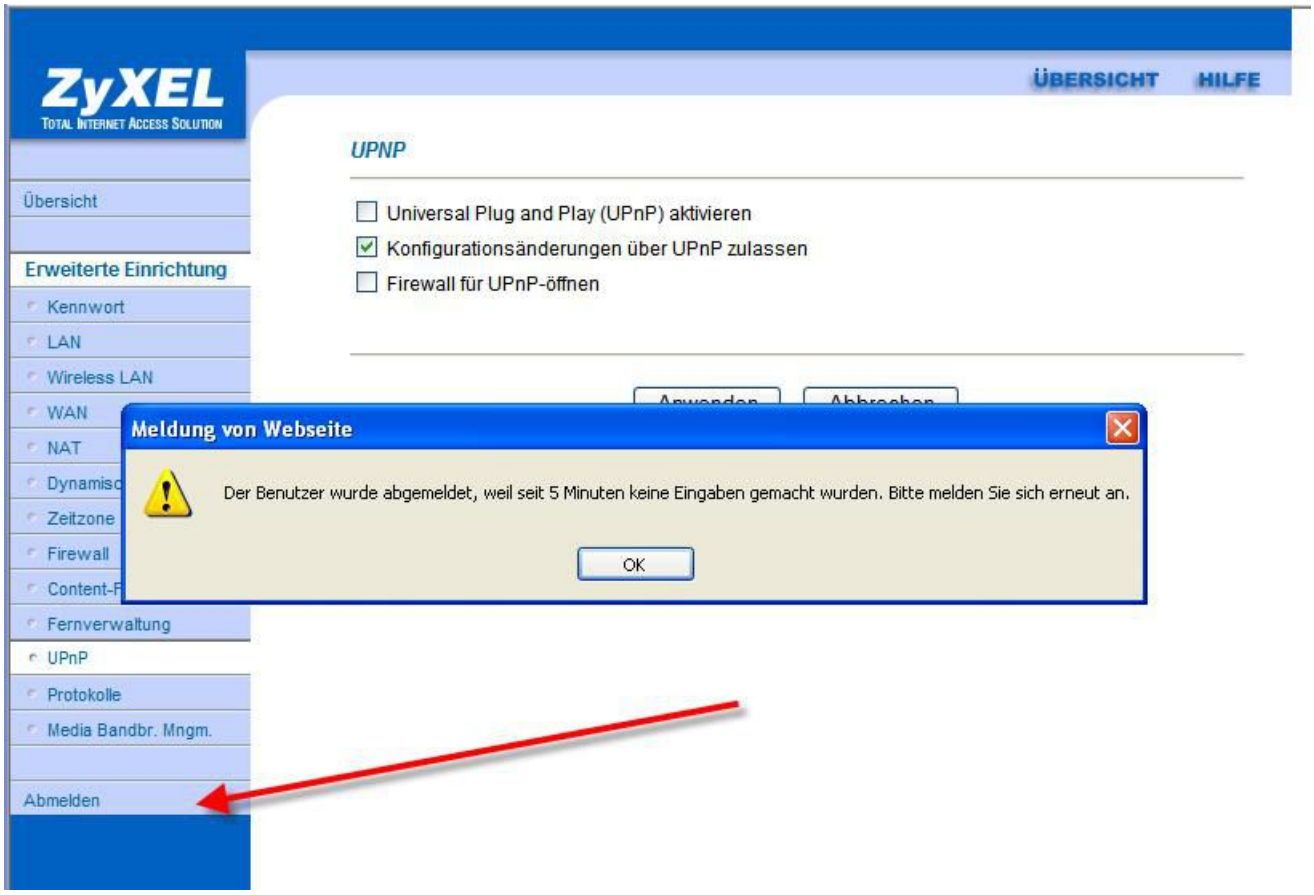
10. Das Passwort allein schützt nicht

Beim Angriff gibt es eine einzige Hürde: Das Web-Interface der DSL-Router ist meist über ein Passwort geschützt, an dem auch ein simulierter „POST“ nicht ohne Weiteres vorbeikommt. Da sich AVM des Sicherheitsrisikos seit geraumer Zeit bewusst ist, wird man bei der ersten Konfiguration der Fritz!Box über den Web-Browser seit einigen Firmware-Revisionen eindringlich zur Vergabe eines Passwortschutzes gedrängt. Bei einigen anderen Router-Herstellern ist der Passwortschutz sogar zwingend erforderlich und kann gar nicht deaktiviert werden. Aber um es gleich vorwegzunehmen: Der Schutz der Web-Oberfläche durch das Passwort ist mitunter wirkungslos und der CSRF-Angriff gelingt dennoch.

Außerdem zeigt die Erfahrung, dass viele Anwender immer noch auf ein Passwort verzichten oder die Werkseinstellungen nicht verändern. Aus dem internen Netz vermuten sie keine Angriffe, hinter der Firewall fühlen sie sich mit ihren privaten IP-Adressen sicher. Auch das Argument einer Gefährdung durch ein WLAN gilt seit der sicheren Verschlüsselung mit WPA nicht mehr, sodass man aus Bequemlichkeit den Kennwortschutz nicht nutzt.

Aber selbst wenn ein Kennwort gesetzt ist: Wer beim Browsen mehrere Fenster geöffnet hat und in einem davon auf dem DSL-Router eingeloggt ist, ist von allen anderen Fenstern aus komplett ungeschützt. Bei Zugriffen auf einen Server nutzt der Browser trotz mehrerer Tabs nämlich immer nur eine Session. Alle Zugriffe auf den DSL-Router erfolgen in diesem Fall mit den Rechten des legal eingeloggten Browser-Tabs. Dabei ist es auch kein Schutz, wenn Browser wie Chrome oder der IE8 für jedes Tab einen eigenen Prozess starten. Daher werden CSRF-Angriffe oft auch als Session Riding bezeichnet.

Aber es kommt noch schlimmer: Das Web-Interface der Fritz!Box beispielsweise kennt keinen Logout. Wie uns AVM auf Nachfrage bestätigt hat, hält die Fritz!Box nach einem Zugriff die Session noch fünf Minuten lang geöffnet. Auch Linksys und ZyXEL verwenden wie die meisten DSL-Router ein derartiges Zeitfenster. Erst wenn mehrere Minuten lang keine User-Aktion mehr stattfand, loggen die DSL-Router den Besucher automatisch aus.



Lobenswert: ZyXEL bietet neben dem automatischen Logout nach fünf Minuten auch einen Menüpunkt zum sofortigen Abmelden an.

Auch wenn man den Browser-Tab mit der Fritz!Box-Konfiguration also längst geschlossen hat, kann man innerhalb dieses Zeitfensters mit einem CSRF-Angriff ohne weitere Passwortabfrage die Konfiguration der Fritz!Box beliebig modifizieren. Schafft es ein Angreifer, den Schadcode in einem Fritz!Box-affinen Umfeld wie einem DSL-Forum oder einem Workshop zur Fritz!Box zu platzieren, hat er gute Chancen auf einen Erfolg.

11. Potenzielle und reale Gefahren für DSL-Router

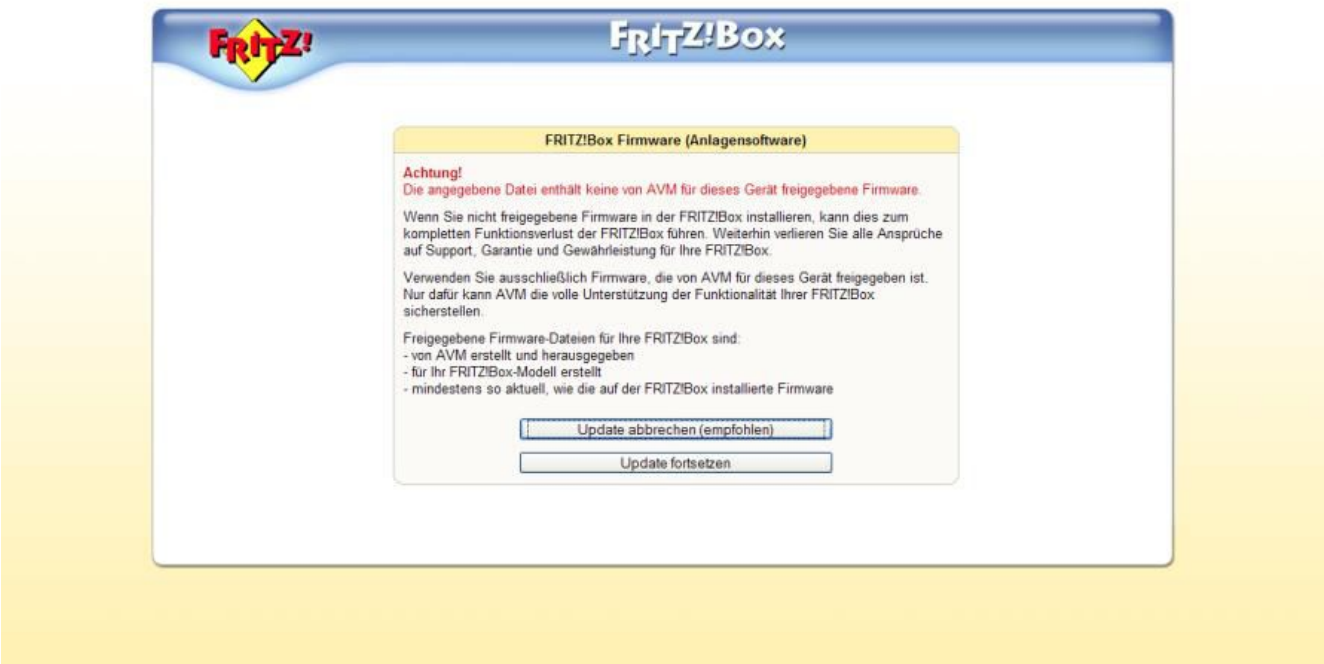
Was könnte ein Angreifer nun eigentlich machen, wenn er die Konfiguration eines DSL-Routers manipuliert? Eine Möglichkeit, die laut AVM bereits aktiv genutzt wurde, ist das Umändern der Wahlregeln. Damit leitet der Angreifer alle Anrufe über seine teure 0900er-Vorwahl um und bereichert sich so. Zumindest bei der Fritz!Box soll dieser Angriff laut AVM inzwischen nicht mehr möglich sein.

Durch das Freischalten von Ports kann der Angreifer auch Löcher durch die Firewall des DSL-Routers bohren und eine Weiterleitung auf bestimmte Rechner einrichten. So hat er dann Zugriff auf die PCs im Netzwerk und kann diese in einem zweiten Schritt attackieren.

Mit ein bisschen Aufwand kann man bei der Fritz!Box das Web-Interface zum Zugriff per https aus dem Internet freischalten. Dann reicht ein einmaliger einfacher Angriff zum Freischalten, den Rest erledigt man dann „ganz offiziell“ direkt über das Internet. Hierzu muss man jedoch neue Passwörter vergeben, sodass dies dem rechtmäßigen Anwender auffällt, wenn er wieder auf seine Fritz!Box zugreifen will.

Interessant ist auch das Umleiten des Traffics zur Analyse der Daten. Der Angreifer kann einen VPN-Tunnel von der Fritz!Box zu sich aufbauen. Dann routet er den ganzen Datenverkehr oder auch nur Anfragen auf bestimmte IP-Adressen zu sich und kann als Man-in-the-Middle alles manipulieren. Kreditkartenzahlungen sind hierdurch besonders gefährdet.

Fängt der Angreifer Zugriffe zum Router-Hersteller selbst ab, droht der Mega-GAU: Er kann ein neues Firmware-Update vortäuschen und dann dem Opfer eine modifizierte Software unterschieben. Dann könnte er aus den infizierten DSL-Routern ein gefährliches Bot-Netz aufbauen: rund um die Uhr online und keinerlei Virenscanner oder andere Sicherheits-Tools, die auf den Bots laufen. Zudem hat der Besitzer des DSL-Routers keine Chance zu erkennen, was er am Ausgang in das öffentliche Netz alles verschickt.



Digitale Signatur: Die Fritz!Box erkennt eine modifizierter Firmware.

AVM hat die Gefahr einer modifizierten Firmware aber nach eigenen Angaben schon seit Langem gebannt. Die Downloads besitzen eine digitale Signatur, sodass eine Fremd-Firmware bei der Installation auffällt. Allerdings haben nicht alle Router-Hersteller ein derartiges Sicherheits-Feature implementiert.

12. Schutzmaßnahmen

AVM ist sich der Gefahr durch CSRF-Angriffe seit Längerem bewusst. Doch bislang kann man keinen wirklich sicheren Schutz davor anbieten. Denn egal ob man beispielsweise Session-IDs oder Tokens in die Konfigurationsformulare mit einbettet: Nach Meinung von AVM könnte man diese Daten per Skript auswerten und passend wieder zurückschicken.

Die einzig sichere Lösung derzeit besteht daher aus drei Maßnahmen, die nur in ihrer Kombination helfen. TecChannel rät

- Ein Passwort für das Web-Interface der Fritz!Box vergeben
- Während des Zugriffs auf das Web-Interface der Fritz!Box keine weiteren Browser-Tabs geöffnet haben
- Nach dem Schließen des Web-Interfaces mindestens fünf Minuten lang keine andere Website besuchen und am besten den Browser beenden. Falls das Web-Interface des DSL-Routers einen manuellen Logout zulässt, sollte man diesen auch stets nutzen.

AVM will die Gefährdung jetzt mit hoher Priorität aus der Welt schaffen. Dabei will man sich nicht nur auf eine Risikominimierung etwa mittels eines Logout-Buttons beschränken. Im Extremfall könnte man beispielsweise den kompletten Internetverkehr eines PCs blockieren, wenn dieser auf den Konfigurationsseiten eingeloggt ist. Bis zur technischen Lösung setzt man auch auf die Abschreckung durch das Gesetz, da es eine strafbare Handlung sei, in fremde Computersysteme einzudringen, vor allem wenn es dazu einer gewissen kriminellen Energie bedarf.

Spezialisten für die Sicherheit von Web-Anwendungen wie Stefan Strobel von der cirosec GmbH sind der Meinung, dass es auch etablierte und einfach umzusetzende technische Möglichkeiten gibt, um das Problem zu lösen. Hier setzt man darauf, dass Anfragen, die beispielsweise die Konfiguration ändern, nicht statisch und somit nicht vorhersagbar sein dürfen. Zufällige Tokens würden diesen Zweck erfüllen, sofern die Anwendung nicht auch noch eine Cross-Site-Scripting-Schwachstelle hat.

13. Fazit

CSRF oder auch Session Riding steigt nicht ohne Grund in der Rangliste der Web-Gefährdungen immer weiter nach oben. Zahlreiche Web-Anwendungen sind dadurch angreifbar. Neuentwicklungen müssen unbedingt auf entsprechende Schwachstellen hin untersucht werden. Für bestehende Systeme in großen IT-Umgebungen bieten sich Web Application Firewalls (WAFs) an, um nachträglich einen Schutzschild zu installieren. Mehr dazu demnächst in einem Artikel zu diesem Thema.

Entwickler von einfachen Web-Interfaces zur Konfiguration von Peripheriegeräten stehen vor einem Problem und sollten ihre Software auf derartige Schwachstellen hin überprüfen.

Keinesfalls soll hier der Eindruck entstehen, das Problem existiere nur bei AVM, Cisco/Linksys und ZyXEL. Wer bei anderen Routern, Netzwerkdruckern und kleinen NAS-Systemen nach Schwachstellen im Web-Interface sucht, wird fündig. Allerdings ist bei AVM das Problem wegen der millionenfachen Verbreitung der Fritz!Box-DSL-Router besonders gravierend.

Dem Anwender kann man nur raten, Schutzmaßnahmen wie Passwörter überall zu nutzen. Das Arbeiten mit mehreren Tabs sollte man beim Zugriff auf geschützte Seiten vermeiden. Und wie die Falle mit dem offenen Zeitfenster zeigt, nutzt man, falls vorhanden, immer den Logout-Button, um eine Session zu beenden. Existiert kein geregelter Logout, wartet man nach dem Schließen der Web-Anwendung eine angemessene Zeit. Unkritisch ist es in diesem Fall, mit einem anderen Browser weiterzuarbeiten. Mit IE, Firefox, Chrome und Safari hat man ja inzwischen genügend Auswahl. (ala)

Weitere Beiträge zur AVM Fritz!Box

Teil 1: Tuning und Hacks für die Fritz!Box[19]

Teil 2: Fritz!Box-Hack: Computer über das Internet starten und fernsteuern[20]

Teil 3: Die Fritz!Box als Least Cost Router[21]

Teil 4: VPN-Direktkopplung mit der Fritz!Box[22]

Teil 5: Rettung für die defekte Fritz!Box[23]

Teil 6: Eigene Firmware mit Freetz erstellen[24]

Links im Artikel:

[1] **http://www.avm.de/**
[2] **http://www.linksysbycisco.com/**

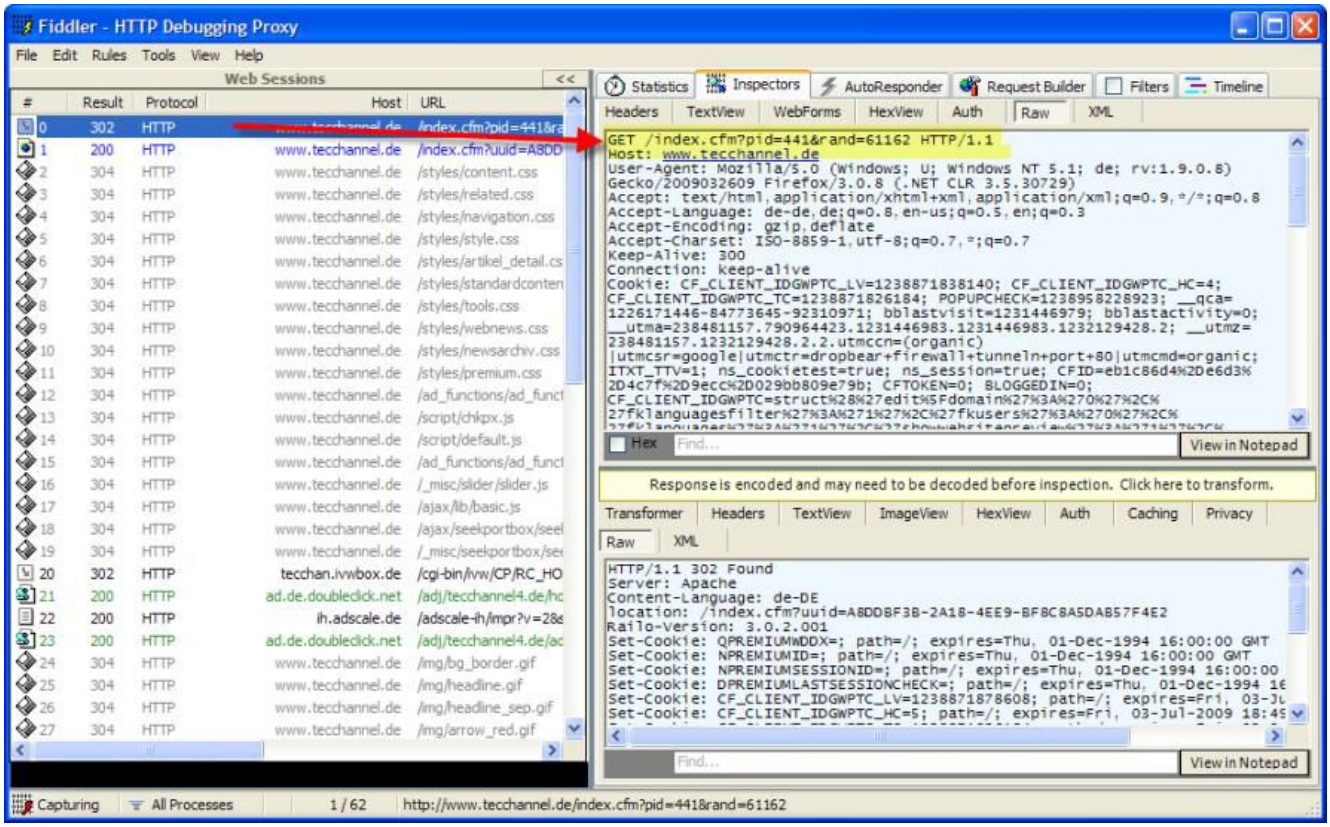
[3] **http://www.zyxel.de/**
[4] **http://www.owasp.org/index.php/Top_10_2007**
[5] **http://tecchannel.idgshop.de/websale7/?shopid=idg&act=category&cat_index=tecpremium**
[6] **https://www.tecchannel.de/index.cfm?pid=441&rand=57566**
[7] **https://www.tecchannel.de/index.cfm?pid=441&rand=57566**
[8] **http://www.log4view.de/tecchannel**
[9] **https://www.tecchannel.de/specials/intellitxt/**
[10] **http://www.fiddler2.com/fiddler2/**
[11] **http://www.log4view.de/tecchannel**
[12] **http://www.cirosec.de/**
[13] **https://www.tecchannel.de/link.cfm?pk=432803**
[14] **https://www.tecchannel.de/link.cfm?pk=432967**
[15] **https://www.tecchannel.de/link.cfm?pk=434025**
[16] **https://www.tecchannel.de/link.cfm?pk=435560**
[17] **https://www.tecchannel.de/link.cfm?pk=438995**
[18] **https://www.tecchannel.de/link.cfm?pk=1763341**
[19] **https://www.tecchannel.de/link.cfm?pk=432803**
[20] **https://www.tecchannel.de/link.cfm?pk=432967**
[21] **https://www.tecchannel.de/link.cfm?pk=434025**
[22] **https://www.tecchannel.de/link.cfm?pk=435560**
[23] **https://www.tecchannel.de/link.cfm?pk=438995**
[24] **https://www.tecchannel.de/link.cfm?pk=1763341**

Bildergalerien im Artikel:

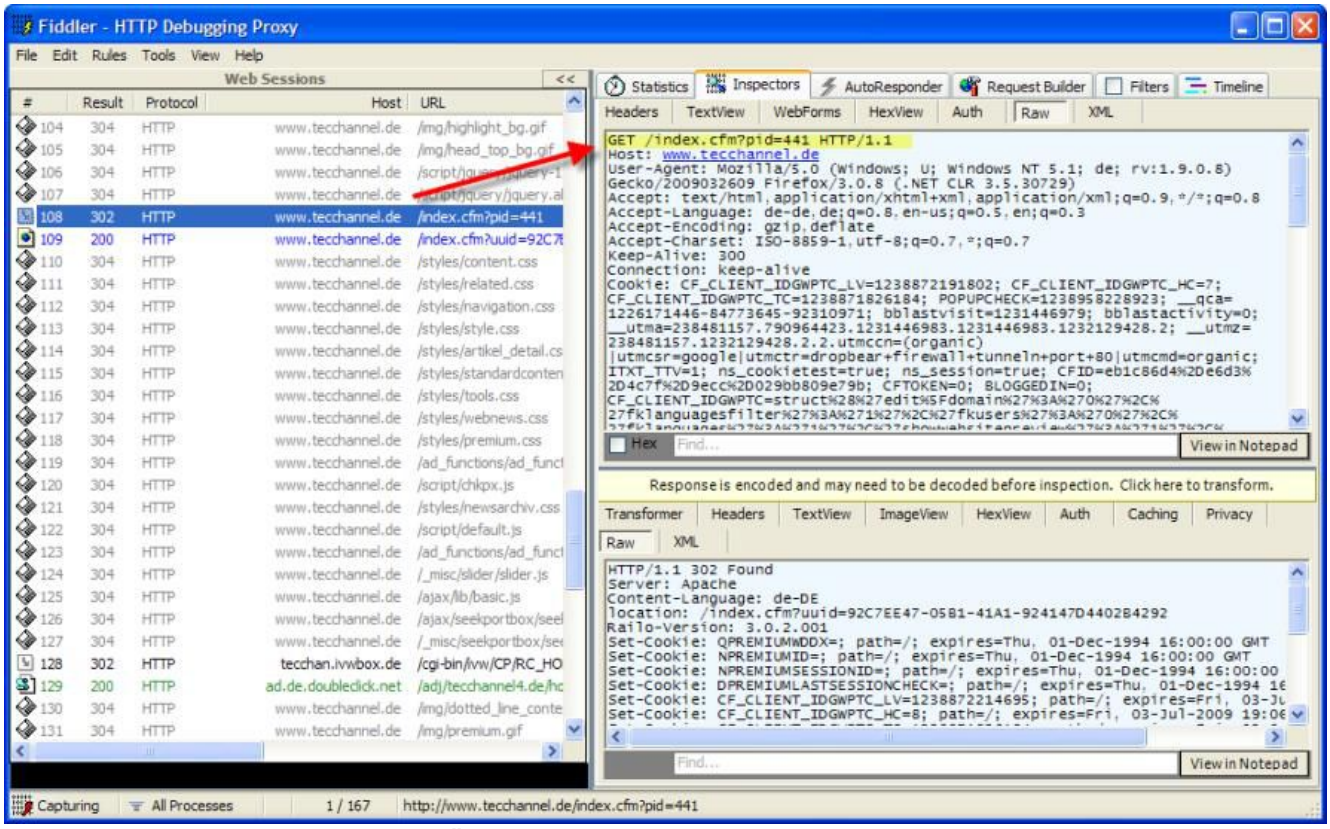
[gal1] **15 Jahre TecChannel Jubiläumspaket -**

Zum 15. Geburtstag hat das TecChannel-Team für Sie ein spezielles Jubiläumspaket geschnürt.

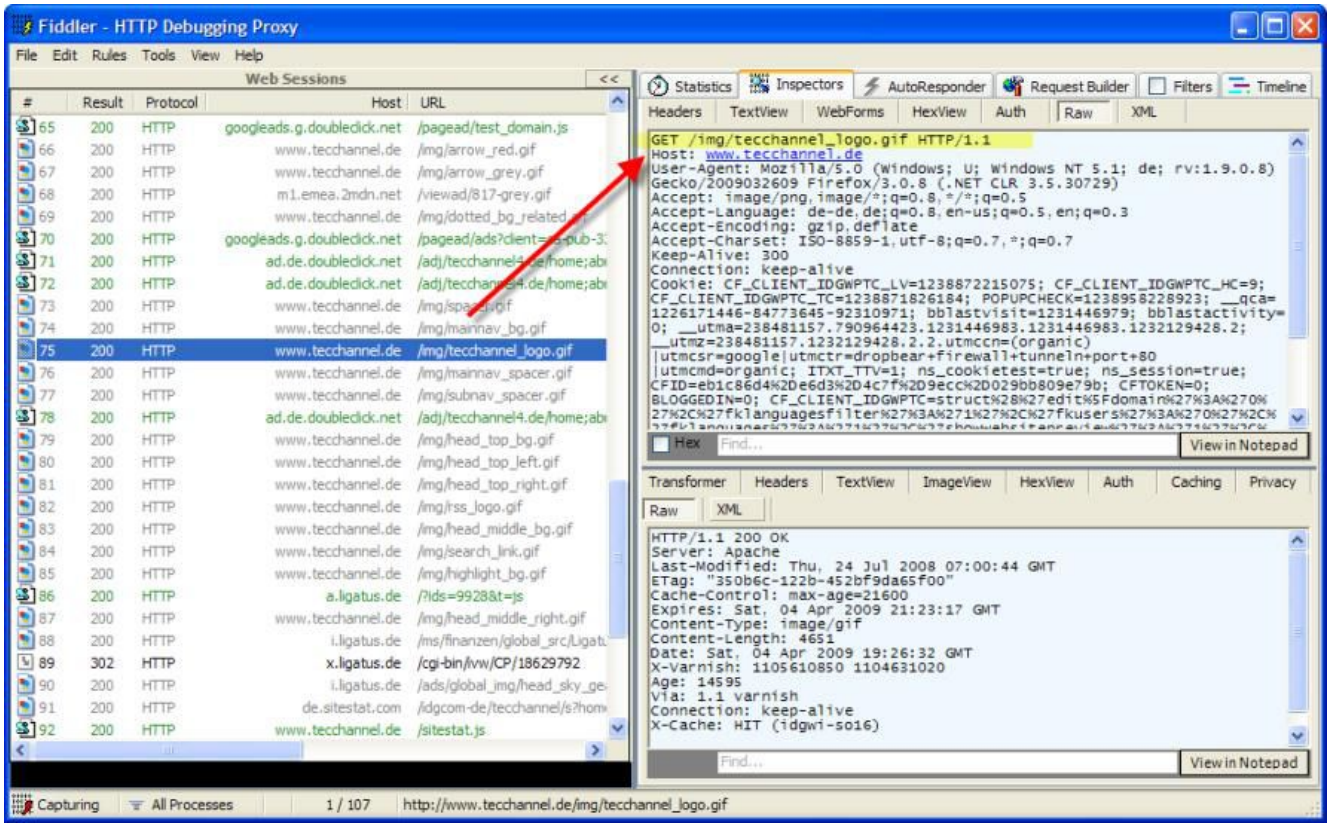
[gal2] **Bildergalerie: Der CSRF-Angriff auf den Premium-Logout im Detail.**



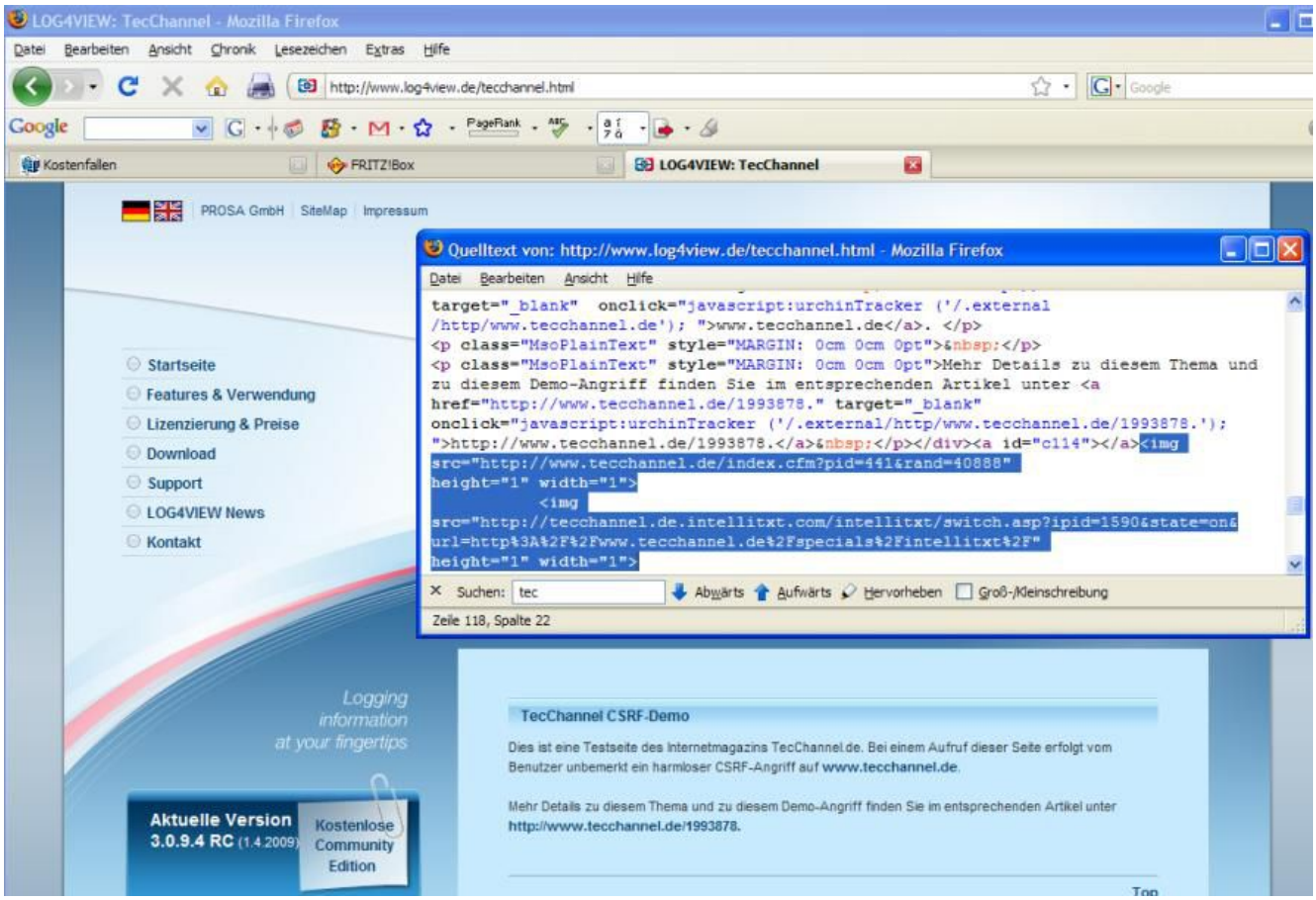
Ein manueller Klick löst ein HTTP-GET auf dem Server aus.



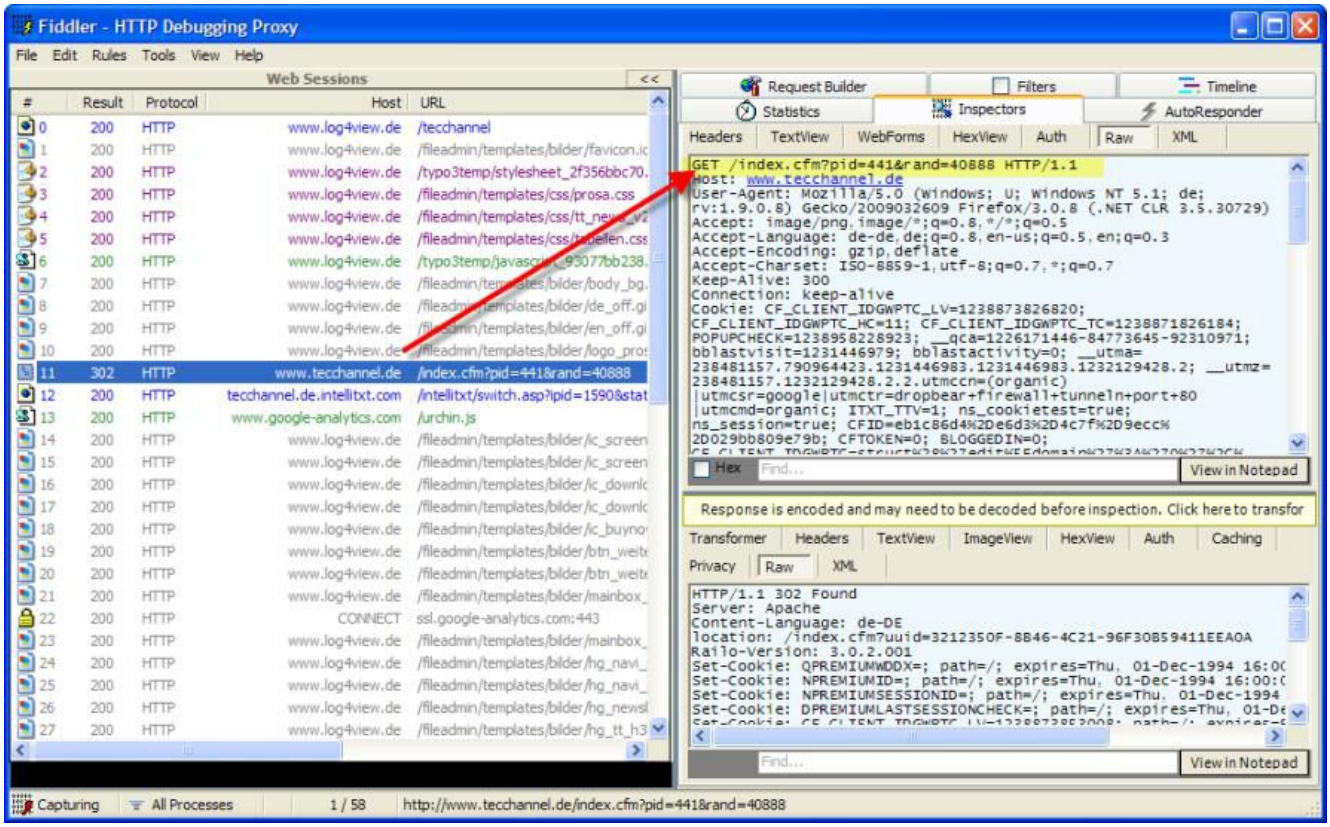
Auch ohne den sich stets verändernden rand-Parameter funktioniert der Logout.



Auch ein Bild wie hier das TecChannel-Logo erzeigt einen HTTP-GET auf dem Webserver.



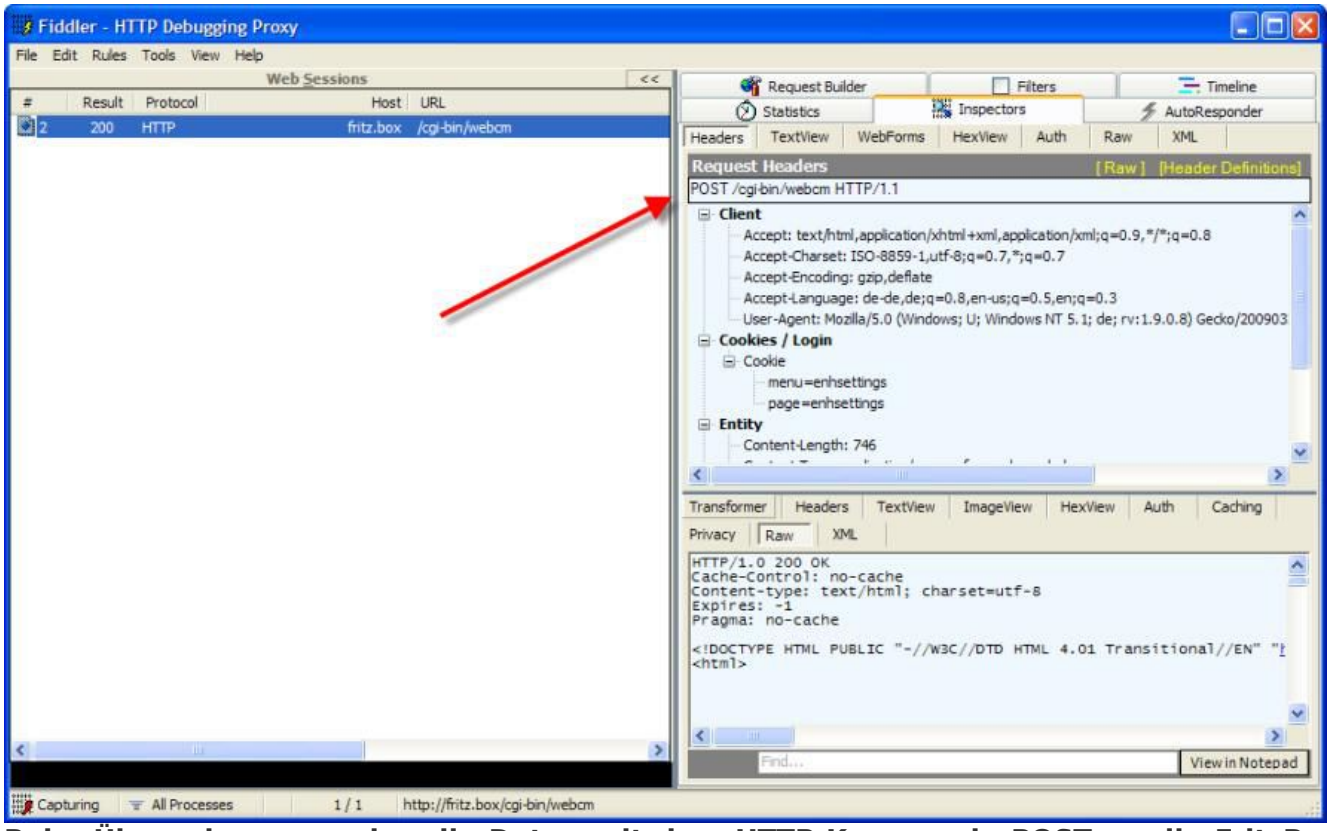
Auf einer Demoseite unter einer ganz anderen Domain ist der Logout-Link als falsches Image eingebettet.



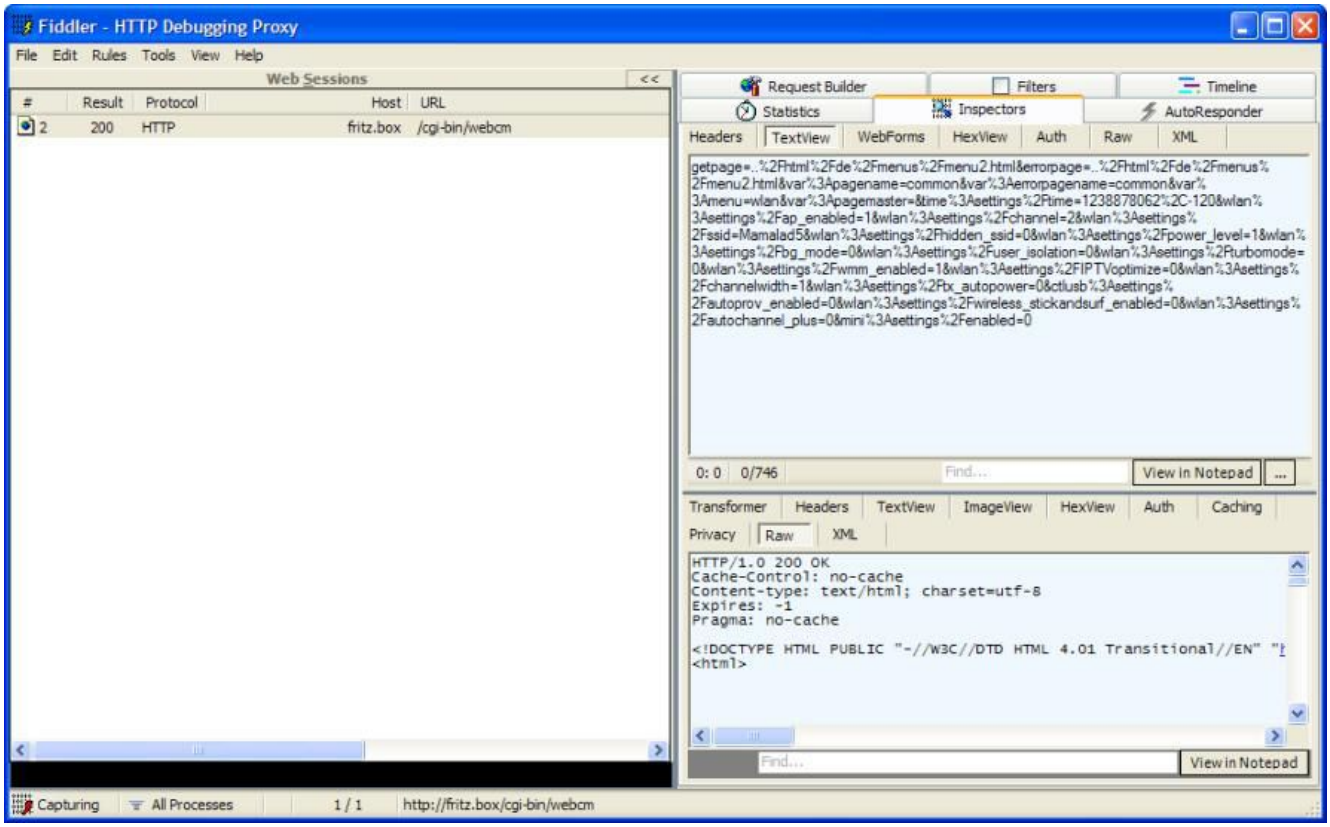
Der Server kann den Aufruf eines Bildes auf der Seite log4view.de nicht von einem Klick auf einen Link auf TecChannel.de unterscheiden.

gal3 **Bildergalerie: Analyse der Kommunikation mit dem Web-Interface verschiedener DSL-Router.**

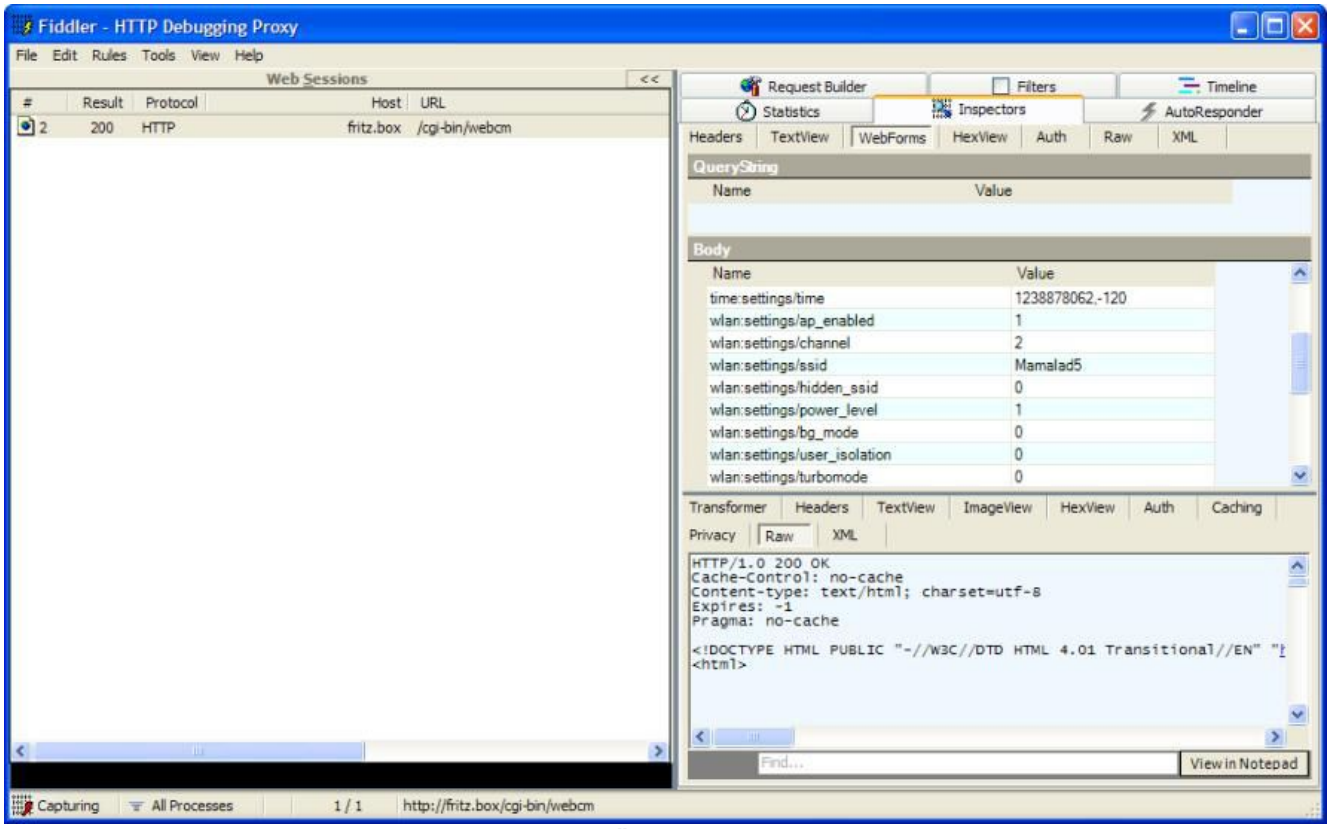
So sieht die WLAN-Konfigurationssseite der FritzBox im Browser aus.



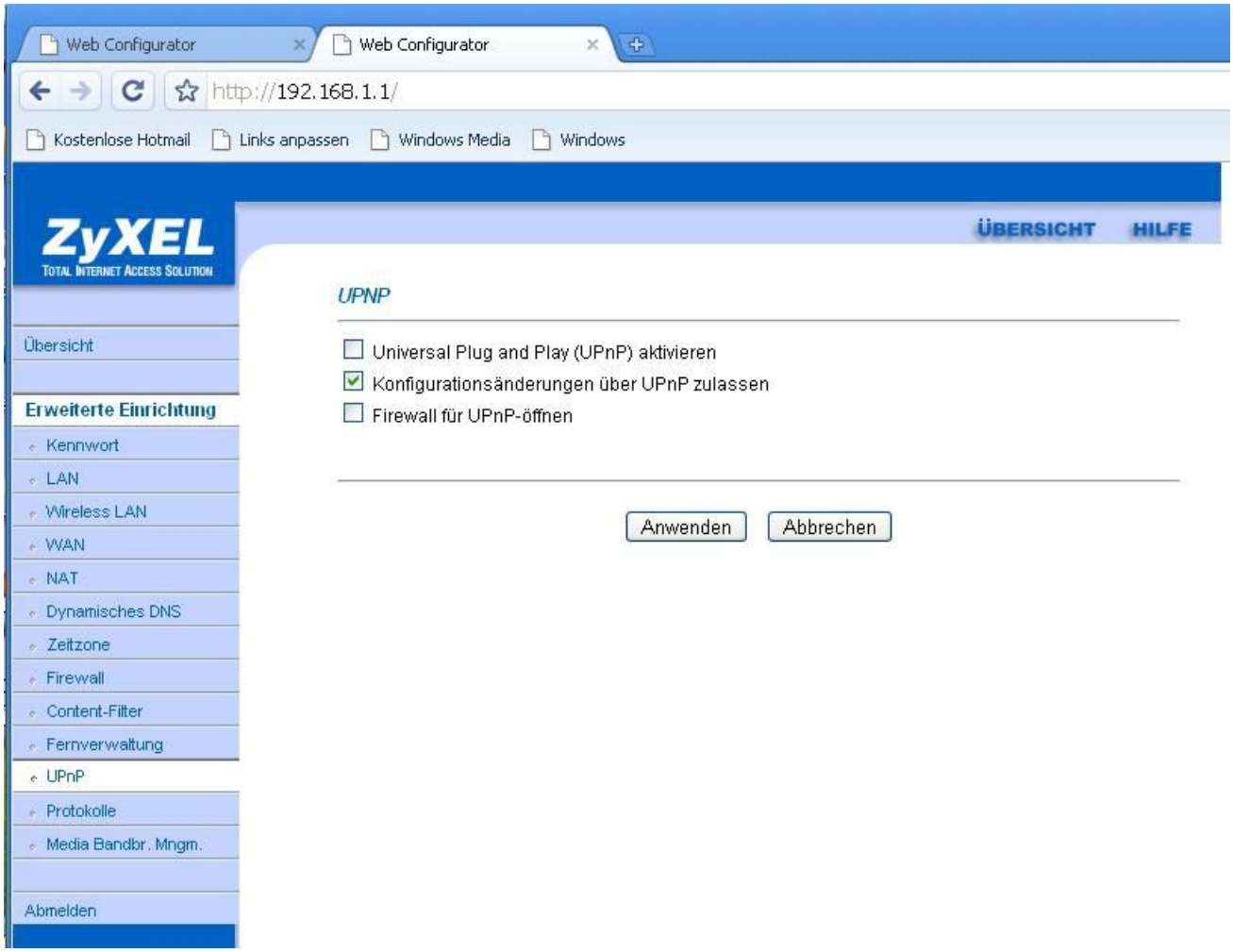
Beim Übernehmen werden die Daten mit dem HTTP-Kommando POST an die FritzBox gesendet



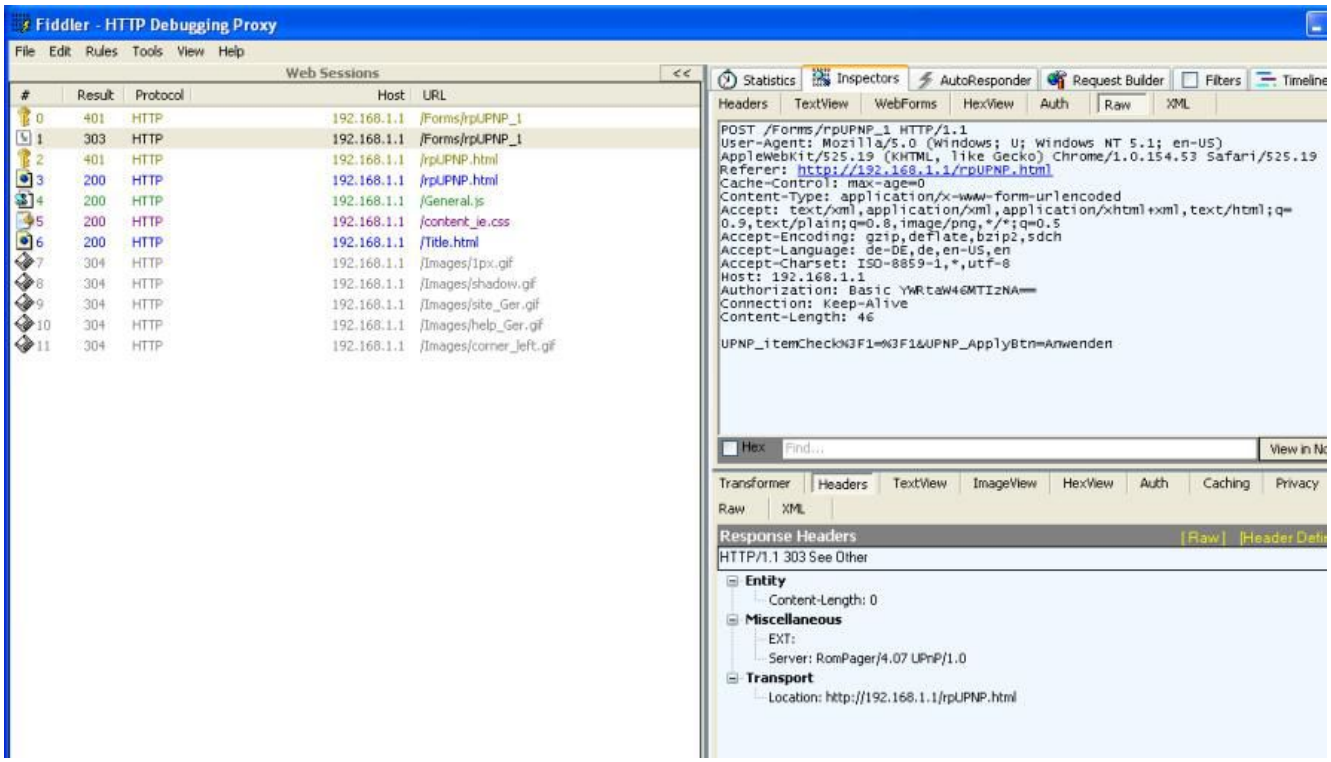
In der Textansicht zeigt Fiddler die Parameter, die über die Leitung gehen.



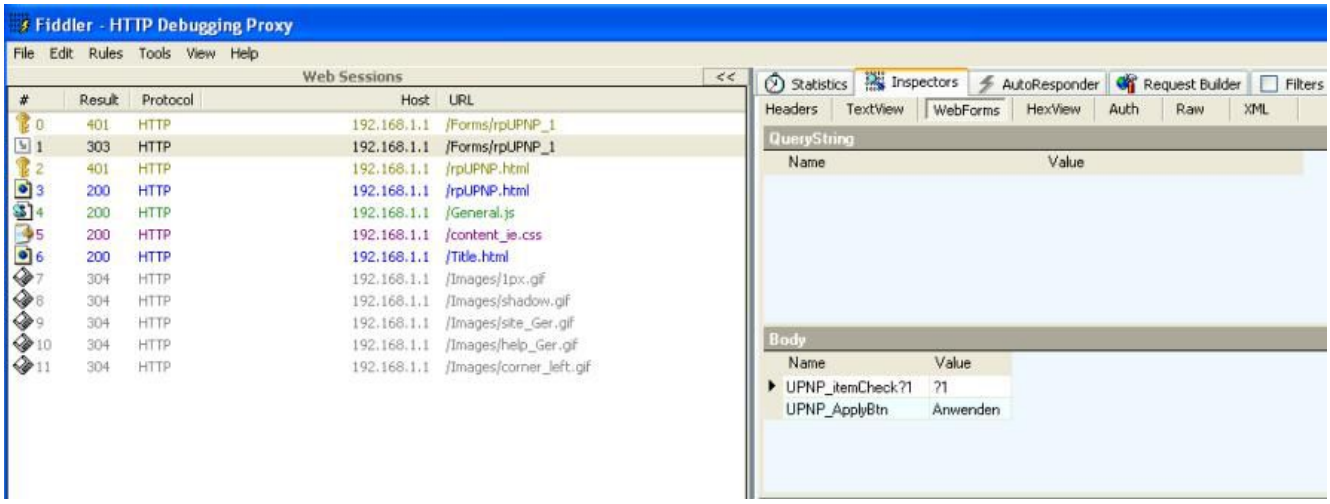
In der Ansicht WebForms sieht man schön die Formularfelder und ihre Daten.



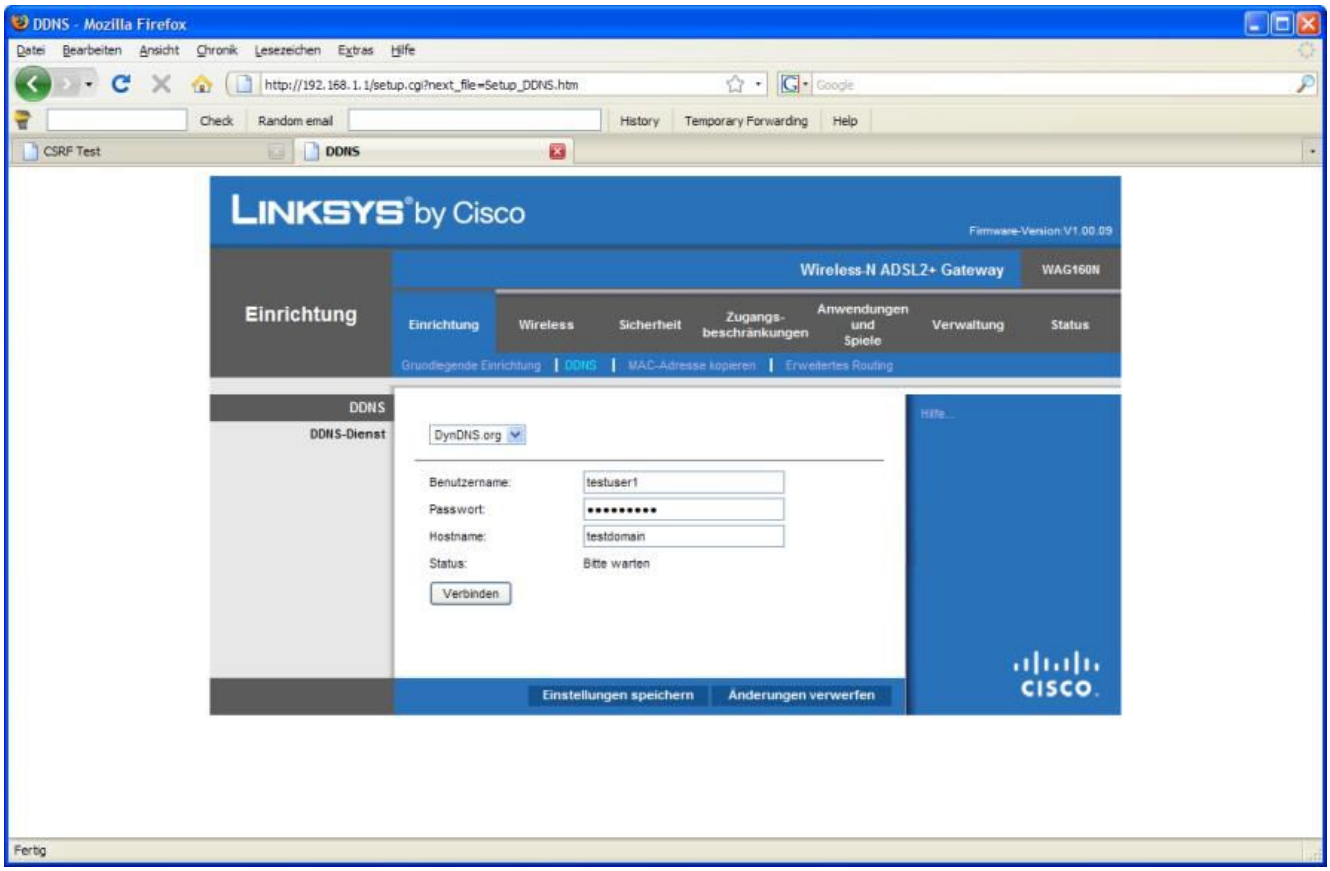
Bei ZyXEL sind die Formulare nicht nur auf den ersten Blick einfach.



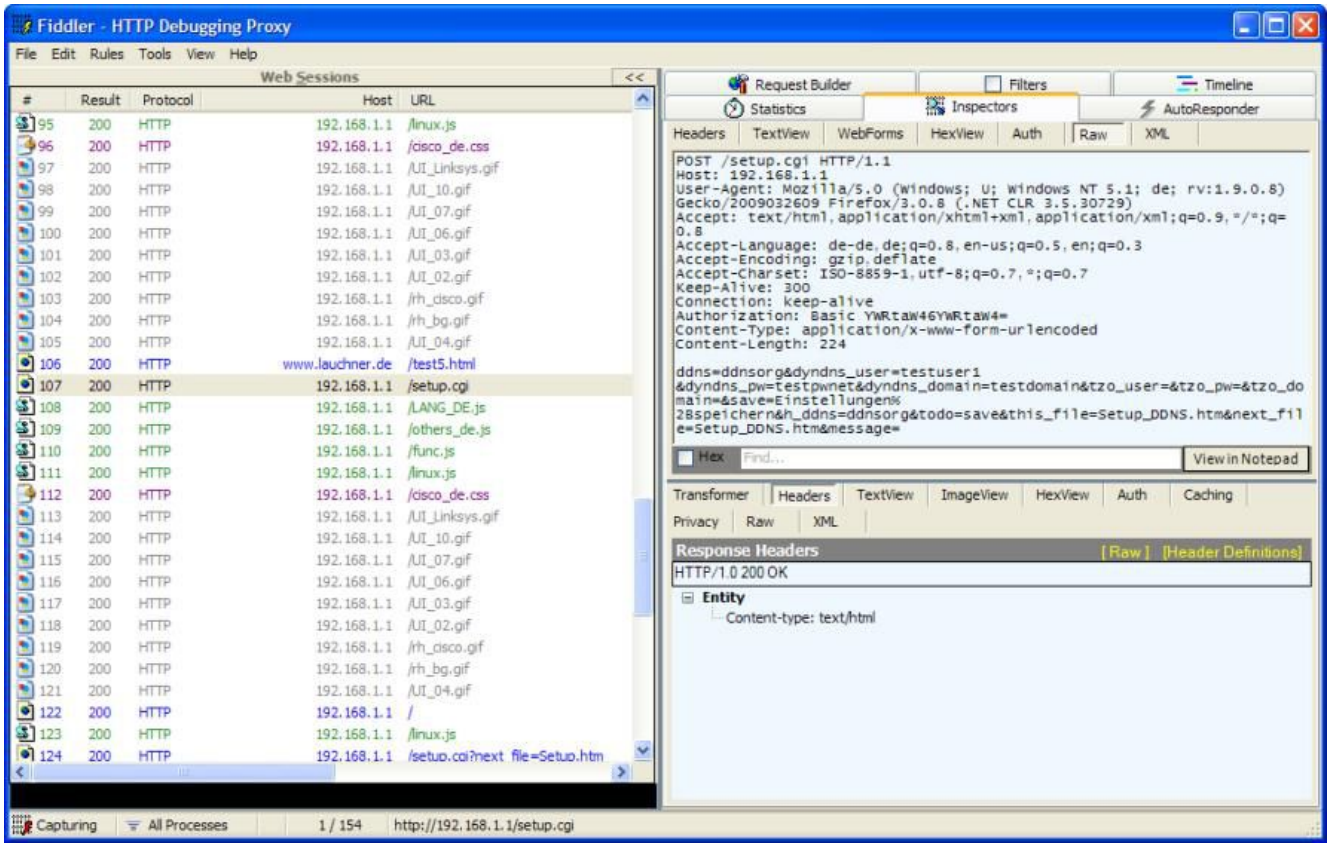
Fiddler zeigt, dass nur sehr wenige Daten bei ZyXEL übertragen werden und dass es keine versteckten Felder gibt.



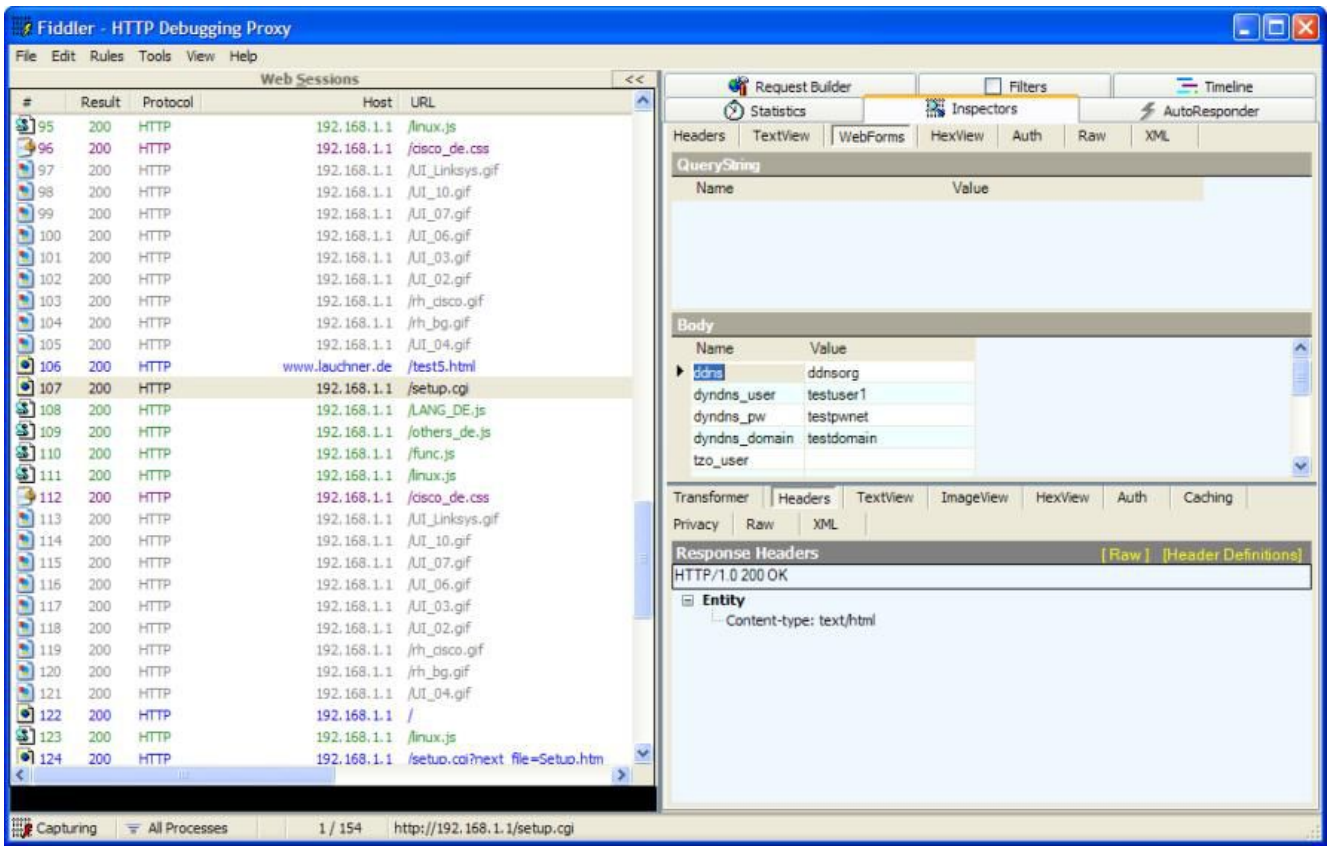
Ein Post der zwei im Body angezeigten Felder genügt zur Konfigurationsänderung.



Auch Linksys arbeitet mit HTML-Formularen.



Die Daten werden wie bei den meisten Routern per HTTP-POST eines Formulars gesendet.



In der WebForms-Ansicht werden die Formularfelder deutlich.

IDG Tech Media GmbH
Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH

keine Verantwortung.