

Contents

1. Editorial
2. Neuerungen der scip AG
3. Neue Sicherheitslücken
4. Hintergrundbericht
5. Linktipps
6. Softwaretipps
7. Kreuzworträtsel
8. Literaturverzeichnis
9. Impressum

1. Editorial

Haushalt der Zukunft?

IT-Sicherheit ist kein neues Thema. Seit geraumer Zeit befassen sich spezialisierte Firmen oder Teams innerhalb von Grossfirmen ausschliesslich mit den mannigfaltigen Aspekten und Details dieses Themengebietes. Dennoch oder gerade aus diesem Grund ist einer der ursprünglichen Wünsche dieser Security Spezialisten, die direkt integrierte Applikationssicherheit, bis zum heutigen Tag nicht im Massenmarkt umgesetzt. Um dieses Manko auszubügeln, gibt es eine unzählige Anzahl von Produkten. Diese wiederum basieren auf einer relativ geringen Anzahl von Grundtechnologien zur Etablierung der gewünschten IT-Sicherheit. Daran hat auch das Jahr 2003 nichts geändert.

Einer der Indikatoren zur Einstufung der Sicherheit einer Software sind dessen spezifischen Verletzbarkeiten. Diese werden in den unterschiedlichsten Datenbanken



gespeichert und dem Endanwender (juristische und nicht juristische Personen) gegen Endgeld oder unentgeltlich zur Verfügung gestellt. Betrachten wir uns diese Statistiken der vergangenen Jahren, so sehen wir, dass populäre Anwendungen in jedem Jahr ein mehr an gefundenen und rapportierten Fehlern aufweisen. Dies mag damit zusammenhängen, dass es immer mehr Spezialisten gibt, welche sich damit beschäftigen, der schierem Grösse des Quellcodes, der Vielzahl an Features oder des immer komplexer werdenden Zusammenspiels der eingesetzten Komponenten. Sicher ist, jede durch Menschenhand erstellte Software wird ihre Fehler haben. Doch dazu später.

Wechseln wir den Blick von der Vergangenheit in Richtung Zukunft. Einer der grössten Änderungen, im IT-Bereich, gegenüber heute wird wohl die Zunahme der Vernetzung in den Privathaushalten sein [scip AG 2003a]. Um einen Grossteil der Bevölkerung damit einzudecken, ist es unumgänglich, dass nebst Spielkonsole, Telefon, Mobiltelefon und Computer auch die alltäglichen Gebrauchsgegenstände darin eingebunden werden. So verwundert es nicht,

dass es heute bereits Kühlschränke, Mikrowellen, Lichtschalter und Lampen mit IP-Stack, also aus dem Netzwerk ansprechbar sind, gibt. Nebst diesen einzelnen Utensilien ist auch die grundlegende elektrische Infrastruktur zu nennen. Bei Firmen sind bereits seit mehreren Jahren grosse Lichtinstallationen über einen Bus verbunden und werden zentral oder dezentral per

Computer, von Hand oder automatisiert, gesteuert. Diese Entwicklung wird in naher Zukunft wohl unsere heimischen Wohnungen revolutionieren.

So sehr ich diese Entwicklung begrüsse, mich darauf freue und als positiv erachte, umso mehr muss ich auf die Risiken hinweisen, welche wir damit möglicherweise eingehen. Mal abgesehen

von elektronischen Schwankungen welche ein Chaos in heimischen Gefilden verursachen könnten, sehe ich vorallem die Möglichkeit der ungewollten externen Interaktion. Durch eine solche externe Interaktion ist das wichtigste unseres Lebensraums, die Privatsphäre in Gefahr. Zum Beispiel können über vernetzte Kühlschränke oder Apothekerkästchen sehr intime Details einer Person in Erfahrung gebracht werden. Es sind auch handfeste Streiche durch Jugendliche denkbar. Lassen wir doch mal schnell den Tiefkühler des Nachbarn auftauen oder der „bösen“ Lehrerin einen gehörigen Schrecken einjagen, indem wir den Mikrowellenherd periodisch ein- und wieder ausschalten.

Der Fortschritt ist nicht aufzuhalten, das sind wir uns heute bewusst. Stellen wir uns deshalb lieber die Fragen wie wir die neue Technik nutzen und diese potentiellen externen Eingriffe vereiteln können. Eine mögliche Antwort lautet: Einsatz sicherer Technik und die Sensibilisierung der Anwender.

Interessieren sich Privatpersonen heute um IT-Sicherheit? Genehmigen wir uns einen Blick in das beliebteste Medium, das Fernsehen. Das Thema IT-Sicherheit wird in der Öffentlichkeit und den darauf aufbauenden Medien (Einschaltquoten) sehr zaghaft behandelt. Die einzigen Meldungen bezüglich IT-Sicherheit resultieren aus Vorfällen im Zusammenhang mit Viren und Konsorten [scip AG 2003b], zumindest bis eine Woche nach Ausbruch.

Kehren wir zurück zu unserem Haushalt der Zukunft und die möglicherweise eingesetzte Technik. Die in den kommenden, vernetzbaren Haushaltsgeräten integrierten Softwares werden wohl von den derzeit populären Herstellern sein. Diese haben die finanziellen Mittel, das bekannte Touch and Feel und einen Namen bei der Bevölkerung. Hier schliesst sich der Kreis. Wie sieht es schon wieder mit den Verletzbarkeiten dieser Softwares aus? Können diese als in sich sichere Techniken betrachtet werden? Firmen stellen eigene IT-Security Budgetposten zusammen. Doch ich als Privatperson bin dazu nicht in der Lage. Ich bin davon abhängig welchen Sicherheitsstandard die bei mir im Einsatz stehenden Haushaltsgeräte bieten.

Zusammenfassend gesehen sieht es nicht gerade positiv aus. Beide Gegenmassnahmen sind mit einem: nicht umgesetzt zu beantworten. Weder bauen Hersteller Software mit dem Fokus der Sicherheit noch sind die Privatpersonen genügend sensibilisiert um ausreichend Druck gegen unsichere Software aufzubauen und die

Hersteller somit zur Erarbeitung von sicherer Software zu zwingen.

Dennoch werden die ersten Geräte einen grossen Markt finden. Updates sind ja schnell draufgespielt [scip AG 2003c].

Simon Zumstein <sizu@scip.ch>
Geschäftsleiter
Zürich, 16. Januar 2004

2. Neuerungen der scip AG

2.1 Workshops

Januar 2004	
26.01.2004	Log-Management [LMFT]
Februar 2004	
04.02.2004	Profiling [PRPT]
18.02.2004	Firewallpolicy [FWFT]
20.02.2004	scip Quality Circle [QCFO]

Das scip AG Workshop-Portfolio finden Sie auf der Firmenwebseite <http://www.scip.ch>.

3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter <http://www.scip.ch/cgi-bin/smss/showadvf.pl> einsehbar.

Die Dienstleistungspakete [\)scip\(pallas](#) liefern Ihnen jene Informationen, die genau für Ihre Systeme relevant sind.

Contents:

3.1 Microsoft Internet Explorer 5.01 bis 6.0
showHelp() Dateien ausführen

3.1 Microsoft Internet Explorer 5.01 bis
6.0 showHelp() Dateien ausführen

Einstufung: **sehr kritisch**

Remote: Ja

Datum: 30.12.2003

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=462>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Arman Nayyeri weist in seinem Posting auf der bekannten Sicherheits-Mailingliste Bugtraq darauf hin, dass durch die Funktion showHelp() beliebige Dateien geöffnet und Programme ausgeführt werden können. Problematisch ist das ganze vor allem, weil durch die Zeichenkette "..\" eine klassische Directory Traversal ermöglicht wird. Ein Angreifer kann diesen Umstand nutzen, um zum Beispiel Hintertüren, Viren oder Dialer zu installieren. Zusammen mit dem Advisory wurde auch ein Exploit bzw. ein Link zu einem proof-of-concept Exploit publiziert. Berichten zur Folge wird die jüngste Technik schon von diversen Dialer-Anbietern genutzt, um ihre zwielichtige Software zu installieren. Einschränkung dieses Angriffs ist, dass nur auf Dateien der Partition zugegriffen werden kann, auf der Windows installiert wurde. Microsoft wurde über das Problem informiert und wird voraussichtlich in den kommenden Wochen mit einem Patch reagieren [<http://www.heise.de/security/news/meldung/43474>]. Als Workaround wird empfohlen Active Scripting zu deaktivieren.

Expertenmeinung:

Dieser Angriff ist sehr kritisch, da er zusammen mit anderen Schwachstellen zur kompletten Komprimierung des Systems führen kann, ohne dass der Benutzer überhaupt etwas davon mitbekommen könnte. Es ist daher umso wichtiger, schnellstmöglich Gegenmassnahmen

zu ergreifen und beim Erscheinen eines Patches diesen unverzüglich auf den betroffenen Systemen einzuspielen.

4. Hintergrundbericht

Dieser dreiteilige Hintergrundbericht zum Mythos „Virus“ ist als fundierte Aufarbeitung eines alltäglichen und breitgefächerten IT-Security Themas gedacht.

Nach Mythos und Geschichte [scip2003d], lesen Sie, im folgenden zweiten Teil über den klassischen Aufbau von Viren und deren Funktionsweisen zur Infizierung des Wirt-Programms.

In den kommenden zwei Teilen geht der Autor, Marc Ruef, dedizierter auf den Aufbau, die Funktionsweisen, die bestehenden Gefahren und die Einfallsmechanismen ein.

4.1 Der Mythos „Virus“

Klassischer Aufbau und Funktionsweise eines Computervirus

Jeder Virus besteht aus drei, meist vier Programmteilen: Beim ersten Teil handelt es sich um eine Art Kennung, das Hex-Pattern, durch das der Virus sich selbst erkennen kann. Mit seiner Hilfe kann ein Virus jederzeit überprüfen, ob eine Datei bereits infiziert ist. Dieses Vorgehen soll eine doppelte Infektion verhindern, die Einbussen in der Performance bzw. Effizienz und zur schnelleren Entdeckung führen würden.

Der zweite Teil enthält die eigentliche Infektionsroutine. Hierbei handelt es sich zuerst um eine Routine, die nach einer nicht infizierten, ausführbaren Datei sucht. Ist eine solche Datei gefunden, kopiert der Virus seinen Programmcode in die Datei. Ausserdem befindet sich in diesem Teil auch der Programmcode, der bei Bedarf die Datei so umbaut, dass der Virus beim Aufruf des Programms sofort aktiv werden kann. Auch die Routine für einen eventuellen Tarnmechanismus befindet sich in diesem Teil des Programms.

Der dritte Teil entscheidet darüber, ob es sich um einen harmlosen Virus handelt, der nur einen kleinen Scherz macht, oder um einen destruktiven Typ, der eine mittlere oder grössere Katastrophe auslöst. Im harmlosen Fall steht hier die Anweisung, dass der Virus am Tag X ein Bild auf den Monitor zeichnet oder einen bestimmten Text ausgeben soll. Hier kann sich aber auch der Befehl befinden: "Formatiere nach dem x-ten Neustart die Festplatte."

Mit dem vierten Teil schliesst sich der Kreis. Hier befindet sich der Befehl mit dem das Programm

nach Ausführung des Virencodes wieder zu der Stelle zurückkehrt, an der der Virus den Programmablauf unterbrochen hat.

Wie wird das Wirt-Programm infiziert

Die grössten Unterschiede bei der Infektion von Dateien liegen in der Art wie ein Virus sich in einem Programm festsetzt. Viele Viren hängen ihren eigenen Programmcode an das Ende einer ausführbaren Datei und setzen am Anfang einen Zeiger auf diesen Code. Wird das Programm gestartet, springt es vor der Ausführung seiner eigentlichen Aufgaben zuerst auf das Virusprogramm. Ist dieses ausgeführt, springt es wieder an die Stelle zurück, an der der Ablauf ursprünglich unterbrochen wurde. Der Benutzer bemerkt allenfalls eine minimale Veränderung an der Aufrufgeschwindigkeit. Jedesmal, wenn das Programm jetzt aufgerufen wird, startet zuerst der Virus. Er sucht von diesem Moment an nach nicht infizierten, ausführbaren Dateien, um sich auch an diese heranzumachen. Die Infektion durch dieses Anhängen, des Virencodes richtet keinen bleibenden Schaden, an der befallenen Datei an. Diese Viren lassen sich wieder entfernen.

Manche Viren gehen allerdings viel radikaler vor und überschreiben einfach so viel von der Datei, wie sie für ihren Programmcode benötigen. Ist das Wirtsprogramm genauso groß oder größer als der Virus, geschieht das relativ unauffällig. Ist der Virus größer als sein Wirt, überschreibt er die Datei komplett und verlängert sie um den Platz, den er darüber hinaus benötigt.

Eine Sorte von Viren verschiebt den Original-Bootsektor, schreibt das eigene Ladeprogramm in den Bootstrap (eine Routine, die das BIOS auffordert, das Betriebssystem zu laden) und versteckt sich dann selbst irgendwo auf dem Datenträger. Wird beim Rechnerstart auf den Bootsektor zugegriffen, startet der Virus-Lader zuerst den Virus und leitet den Zugriff danach auf den verpflanzten Original-Bootstrap um. Dadurch kann sich ein Virus auch auf Disketten verbreiten, die nur Dateien und keine Programme enthalten, da auch nicht-bootfähige Disketten einen minimalen Bootsektor haben. Wird bei einem Bootversuch kein Betriebssystem gefunden, gibt das Ladeprogramm lediglich die Meldung am Bildschirm aus: "keine Systemdiskette..." Eine solche Diskette kann einen Virus dann als Krücke zum Starten verwenden.

Andere Viren überschreiben die in der FAT enthaltenen Informationen über ein Verzeichnis und geben bei jedem Programm als Adresse die des Virusprogrammes an. Die Original-Adressen

legt der Virus selbst in einer geordneten Liste ab. Wird nun ein Programm aufgerufen, startet es zuerst den Virus. Dieser leitet den Zugriff dann an die richtige Adresse weiter. Von jedem dieser Infektionswege gibt es einige Varianten. Auch Kombinationen aus mehreren Methoden kommen häufig vor. Deswegen lassen sich Viren auch zunehmend schwerer klassifizieren.

5. Linktipps

5.1 NEC Research Institute CiteSeer - Eine geniale Bibliothek

<http://citeseer.nj.nec.com/cs>

Thema: Informatik, Computer,
Netzwerke, Sicherheit
Kategorie: Nachschlagewerk,
Suchmaschine

Aufmachung	Gut
Umfang	Sehr gut
Suchfunktion	Sehr gut
Ergonomie	Sehr gut
Gesamtbewertung	Sehr gut

Der österreichische Journalist und Publizist Dr. Georg Wailand schrieb einmal, dass wer im Internet surft, das Gefühl hat, über den Ärgernissen des Alltags zu schweben. Statt aber im Himmel zu landen, findet man sich alsbald im Fegefeuer des Informations-Überangebotes wieder. Wer sich für Computer und deren Sicherheit interessiert kennt dieses Problem nur allzu gut. Früher war man um jede Information froh, die man zu diesem Thema bekam. Heute wäre man froh, wenn mal ein Tag verstreichen würde, an dem sich nicht durch einen Haufen neuer und trotzdem aufregender Publikationen wühlen müsste.

Dem Problem Herr zu werden ist lediglich mit einem gut sortierten und dokumentierten Archiv möglich. Genau hier versucht das NEC Research Institute CiteSeer den Kreis zu schliessen.

Die kleine Suchmaschine der Informatik

Beim Projekt handelt es sich in erster Linie um ein Archiv von Texten zum Thema Informatik. Dokumente werden wie in einer Index-Suchmaschine aufgenommen und archiviert, so dass man mittels Suchfunktion diese nach bestimmten Text-Stellen durchsuchen kann.

Dies ist eigentlich soweit nichts neues und unterscheidet sich eigentlich auch kaum von der

Funktionalität, die uns moderne Index-Suchmaschinen wie Google bieten. Vorteil ist lediglich, dass wirklich nur Publikationen ihren Eingang finden, wenn sich diese auch wirklich mit dem Thema beschäftigen auf einem annehmbaren Level beschäftigen. So findet man vorwiegend wissenschaftliche und wissenschaftlich anerkannte Dokumente. Ein Garant dafür, nicht in der Informationsflut von Halbwissen unter zu gehen.

Das Verzeichnis

Als das Internet Mitte der 90er Jahre seinen grossen Boom erlebte, herrschte noch eine strenge Unterteilung zwischen automatisierten Index-Suchmaschinen und betreuten Webverzeichnissen. Auf der einen Seite stand AltaVista mit einer Vielzahl an indizierten Webseiten - Auf der anderen Seite hielt Yahoo mit der kleinen aber feinen Auswahl die Stellung. Im Jahr 2004 gehen diese Dinge jedoch Hand in Hand. Google, das als Nachfolger von AltaVista galt, ist lange nicht mehr nur eine reine Suchmaschine. Längst wurde ein betreutes Webverzeichnis auf die Beine gestellt. Ebenso ist deshalb auch die CiteSeer-Webseite mit einem Verzeichnis ausgestattet. In diesem werden die Dokumente zusätzlich in verschiedene Kategorien, die hierarchisch aufgebaut sind, geordnet.

Ideal für Literaturverzeichnisse

Die grösste und interessanteste Innovation des Projekts ist jedoch Funktionalität der Referenzierung. So werden die Dokumente auf ihre Referenzierung in anderen Publikationen überprüft. So entsteht ein Netzwerk von Dokumenten, die sich gegenseitig ergänzen und anfechten. Wer eine wissenschaftliche Arbeit zu einem Thema schreiben möchte, ist noch so froh um die Möglichkeit solcher Querverweise. Verhältnismässig schnell kann man so seine Referenzen auf den neuesten Stand bringen und erweitern.

Fazit

Dieses Archiv und die dazugehörige Suchmaschine sind eine Bereicherung für jeden, der sich intensiv mit der Informatik beschäftigt. Vor allem Leute, die selber Publikationen dazu verfassen - Studenten, Schriftsteller und Autoren - werden das Projekt als enorme Bereicherung empfinden. Jede solide Publikation glänzt durch ein hochwertiges Literaturverzeichnis.

6. Softwaretipps

6.1 RegExp Tools

<http://www.regexlib.com>

Thema: Reguläre Ausdrücke,
Programmieren
Kategorie: Utility, Entwicklung
Plattform: Microsoft Windows
Lizenztyp: Freeware

Funktionalität	Sehr gut
Technik	Sehr gut
Ergonomie	Gut
Gesamtbewertung	Sehr gut

Was sind reguläre Ausdrücke?

Reguläre Ausdrücke (Abk. RegExp, engl. regular expression) bilden eine Familie von kompakten, leistungsfähigen formalen Sprachen, mit denen sich (Unter-)Mengen von Zeichenketten beschreiben lassen. Diese Sprachen werden von vielen Texteditoren und Hilfsprogrammen (hauptsächlich unter Unix) verwendet, um bestimmte Muster zu suchen und dann durch etwas anderes zu ersetzen oder eine Aktion auszuführen.

Programme, die reguläre Ausdrücke benutzen sind z.B. egrep, sed und awk, aber auch in Programmiersprachen wie Perl und Tcl, oder Texteditoren wie Emacs und vi lassen sich reguläre Ausdrücke verwenden.

Sinn und Zweck regulärer Ausdrücke

Reguläre Ausdrücke stellen ein powervolles Tool dar, um nach etwas, das einem vordefinierten Modell entspricht, Ausschau zu halten. Suchen und Ersetzen spielt dabei eine wichtige Rolle, wobei hingegen die Eingabeüberprüfung am hilfreichsten ist. Das Schreiben von CGI-Skripten, die von tausenden von Benutzern genutzt werden sollen, ist nicht gerade eine angenehme Aufgabe. Die Aufgabe des Programmierers besteht darin herauszufinden, welche Eingaben die Benutzer tätigen könnten und daraufhin diese Daten so umzuformen, damit die Software auch damit zurecht kommt.

Das grundlegende Problem

Reguläre Ausdrücke sind sehr flexibel, was leider ein hohes Mass an Komplexität mit sich bringt.

Der Ausdruck `^[a-zA-Z]\w{3,14}$` prüft eine Eingabe auf die folgenden Bedingungen:

Das erste Zeichen muss ein Buchstabe sein

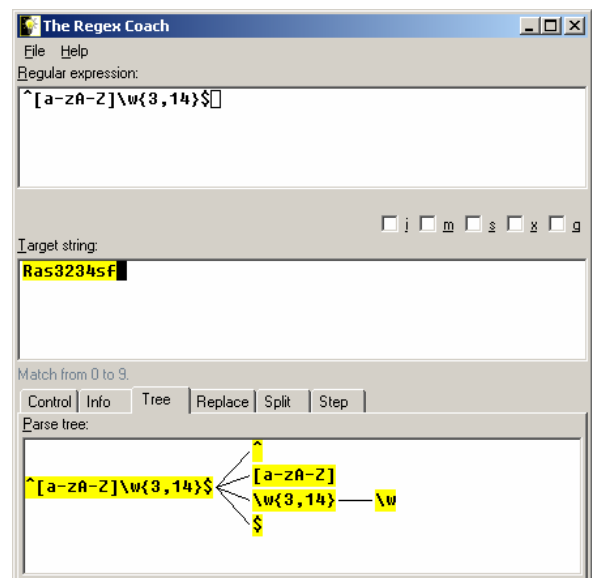
Es müssen mindestens 4 und höchstens 15 Zeichen enthalten sein
Lediglich Buchstaben, Ziffern und das Underscore-Zeichen sind enthalten

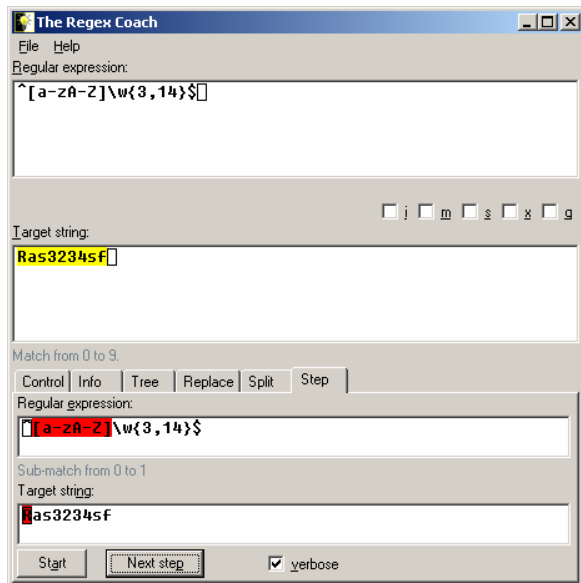
Verzichten Sie jedoch auf das an anführende `^`, werden sonderbare Dinge passieren.

Als Hilfe für die defensive Entwicklung (definiert als "machen, was wir denken, sollte gemacht werden") eignen sich die folgenden Tools: [The Regex Coach](#), [RegexDesigner.NET](#), [Regular Expression Designer](#).

Der Regex-Coach

Der Regex Coach ist eine Applikation für Windows und Linux mit grafischer Oberfläche. Sie kann genutzt werden, um mit Perl-kompatiblen regulären Ausdrücken zu experimentieren.



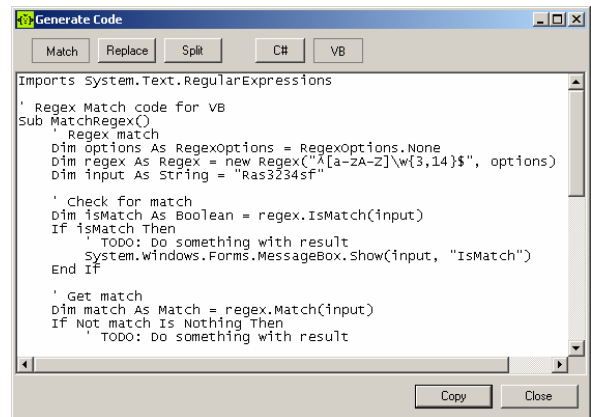
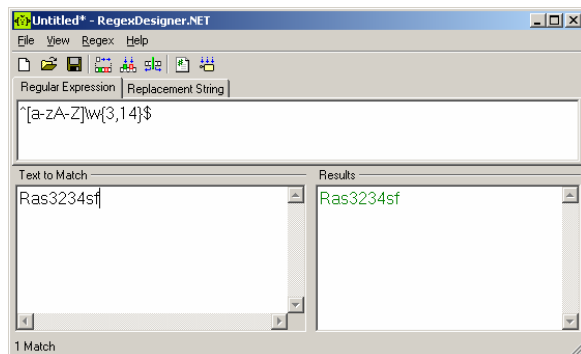


Ein grosses Plus der Software ist die Baumdarstellung der Ausdrücke, Step-by-Step Ausführung zum Debugging und die Echtzeit-Analyse.

Als Negativpunkte sind die Unhandlichkeit und Instabilität bei langen Ausdrücken anzusehen.

RegexDesigner .NET

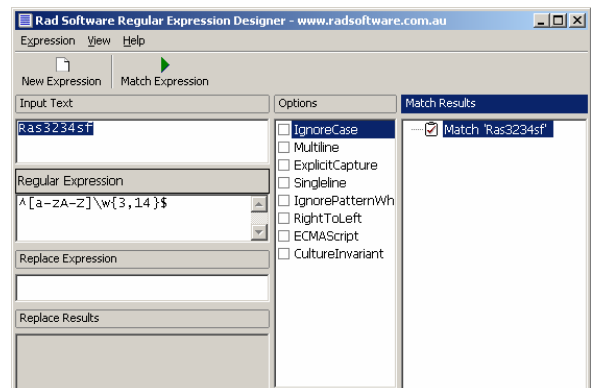
Der RegexDesigner.NET ist ein umfangreiches Tools zur Entwicklung und Überprüfung regulärer Ausdrücke für .NET auf Windows. Sehr einfach lassen sich so Ausdrücke für entsprechende .NET-Anwendungen, wie C# und VB.NET, ausarbeiten.



Falls Sie reguläre Ausdrücke in Microsoft-Programmen umsetzen wollen, ist dies die geeignete Anwendung dafür. Sie können einfach überprüft werden und der Code lässt sich einfach für C#, VB.NET oder kompilierte DLLs ausgeben.

Rad Software Regular Expression Designer

Rad Software Regular Expression Designer ist ein freies Tool, das einem Programmierer dabei hilft zu lernen, wie reguläre Ausdrücke entwickelt und getestet werden können. Die Windows-Applikation ist sehr einfach handzuhaben.



Die Software erlaubt eine sehr detaillierte Analyse der Eingabe. Falls Sie sich mit der Darstellung der Microsoft Registry angefreundet haben, werden Sie sich auch sehr schnell mit diesem Tool zurecht finden.

Weitere Informationen zu regulären Ausdrücken finden sich in der RegExLib Library unter <http://www.regexlib.com>.

7. Kreuzworträtsel

Programmierschnittstelle für Windows	Unix Erzeugen eines Verzeichnisses	Spielkonsole von Microsoft	Buch-Verlag mit Tieren auf den Covers	Konkurrenz-Produkt zu Netstumbler	Gedruckte Schaltung	Gleitkomma-Prozessor	Internet Protocol
Bedienoberfläche für OS/2		Vorname des verstorbenen Hackers Tron	2		Zentraleinheit eines Computers		Webadresse
			Taste für Sonderfunktionen bzw. Steuerzeichen		Symbol für Firewalling		5
CGI-Scanner für Linux	Daten bleiben unverändert	Security Consulting Information Process	Eine unteilbare Sicherheitsanforderung	Hersteller von Antiviren-Lösungen	Top-Level-Domain von Schweden	Lautes Lachen	
Webserver von Microsoft		Datendefinitionssprache (in SQL)	6			Vertikales Transportprotokoll	
Vorgänger von Windows 2000			DOS: Löscht den Bildschirm		Deutscher Hacker-Club		Klassischer UNIX-Texteditor
	Les- und Schreibbarer Speicher			Klassisches Intrusion Detection-System	4	Linux Kopiert Dateien	Unix Löschen einer Datei
Vorgänger der VGA-Auflösung			Hersteller von Solaris		Datenaustausch (Mail) zwischen UNIX-klassischen	Cross Site Scripting	
		Kleiner Bruder von HTML	UDP-Portscanner unter Windows	Common Vulnerabilities and Exposures	Nachfolger der PS2-Stecker		
Künstliche Intelligenz			Programmierbare Schildkröte		Grosses Auktionshaus		
	automat. Buchstabenerkennung				ICMP-Typ für Test der Erreichbarkeit	3	
Digital-Analog-Wandler				Wo befinden sich die Konfigurationsdateien unter UNIX			
	1	Verschlüsselungs-Software			"alte Suchmaschine"		
			An ETH Zürich entwickeltes Betriebssystem	0			
Bezeichnung für einen Computer-Freak							

Wettbewerb

Gewinnen Sie einen Monat unserer Dienstleistung **ipallas**, im Wert von bis zu **285CHF** (197EUR). Die **drei** ersten Einsendungen des richtigen Lösungswortes gewinnen. Mailen Sie das erarbeitete Schlüsselwort an die Adresse <mailto:info@scip.ch>. Einsendeschluss ist der **15.02.2004**. Die GewinnerInnen werden nur auf ihren ausdrücklichen Wunsch publiziert. Dieser Wettbewerbsgewinn (Packetgrösse EXA und Wertauszahlung ausgeschlossen) kann auf einem bestehenden Abonnement oder einer Neuanschaffung verbucht werden.

Die Auflösung der Security-Kreuzworträtsel finden Sie jeweils online auf <http://www.scip.ch> unter Publikationen > scip monthly Security Summary und dann bei Errata.

8. Literaturverzeichnis

scip AG, 2003a, scip monthly Security Summary, Ausgabe 19. September 2003 – Buchtipps: Die Neuromancer Trilogie, <http://www.scip.ch>

scip AG, 2003b, scip monthly Security Summary, Ausgabe 19. August 2003 - Editorial, <http://www.scip.ch>

scip AG, 2003c, scip monthly Security Summary, Ausgabe 19. April 2003 - Editorial, <http://www.scip.ch>

scip AG, 2003d, scip monthly Security Summary, Ausgabe 19. Dezember 2003 – Hintergrundbericht: Der Mythos Virus, <http://www.scip.ch>

9. Impressum

Herausgeber:

scip AG

Technoparkstrasse 1

CH-8005 Zürich

T +41 1 445 1818

<mailto:info@scip.ch>

<http://www.scip.ch>

Zuständige Person:

Marc Ruef

Security Consultant

T +41 1 445 1812

<mailto:maru@scip.ch>

PGP:

http://www.scip.ch/firma/facts/maru_scip_ch.asc

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserung möglich. Senden Sie Ihr Schreiben an smss-feedback@scip.ch. Anfragen bezüglich der Erstellung eines **Erfahrungsaustausch Artikels**, senden Sie bitte an die E-Mail <mailto:sizu@scip.ch>.

Die ausgewiesenen IT-Security Spezialisten der scip AG verfügen, in diesem sehr komplexen sowie breitgefächerten Spezialgebiet, über jahrelang erarbeitetes und angewandtes Wissen. Wir sind der **effiziente** und **persönliche** Partner im Sektor: IT-Sicherheit. Bei Fragen, Schulungen, Assessments und Projekten im Bezug zur IT-Security finden Sie eine kompetente Anlaufstelle in uns.

Nutzen Sie unsere Dienstleistungen!

Das Errata (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summary's finden Sie online unter <http://www.scip.ch/publikationen/smss/>.

Der Bezug des scip monthly Security Summary ist **kostenlos**. Sie können sich mit einer Email an die Adresse smss-subscribe@scip.ch eintragen. Um sich auszutragen, senden Sie Ihr Email an die Adresse smss-unsubscribe@scip.ch