RoCyberCon

- prima conferinta online din Romania a ITistilor -

“XSS este mai mult decat o simpla amenintare”

http://rocybercon.worldit.info:9090

[19:06] <@Andrei> .mode +m
[19:06] == mode/#rocybercon [+m] by Guardian
[19:06] == kNigHt [webchat@WIT-31658D9A.cust.vpntunnel.org] has joined #rocybercon
[19:06] <@Andrei> asa :)
[19:07] <@Andrei> Buna seara tuturor si bine ati venit la o noua conferinta, momentan am blocat discutiile ca sa va linistiti :D
[19:07] <@Andrei> pentru cei care ati intrat dupa 7, va recomand sa accesati de pe clientul nostru web
[19:08] <@Andrei> pentru ca prezentarea va fi sustinuta si cu ajutorul unor slide-uri prin slideshare
[19:08] <@Andrei> cei care nu vor avea bunul simt sa taca
[19:08] <@Andrei> vor fi banati (adica redusi la tacere), dar vor putea sa continue sa priveasca
[19:09] <@Andrei> .mode -m
[19:09] == mode/#rocybercon [-m] by Guardian
[19:09] == cossin [webchat@CBB01EE.D1E07B76.6856A64.IP] has joined #rocybercon
[19:09] <Ne0h> am inteles men :D
[19:09] <Ne0h> deci cand incepe treaba?
[19:09] <kNigHt> salut :D
[19:09] <bogdannbv> desigur :)
[19:09] <@Andrei>
[19:09] <denjacker> Liniste in sala.. urmariti SlideShow-ul si fiti atenti la Andrei
[19:09] <@Andrei> Dupa cum spune si titlul, XSS este o vulnerabilitate extrem de populara peste tot :)
[19:10] <Ne0h> da mai greu de exploatat
[19:10] <Alex_Baies> Andrei, trebuie sa intervin :D Daca nu le merge la toti ca mie datat trecuta ? :D
[19:10] <@Andrei> Doar ca toata lumea, sau aproape toata lumea prefera sa o considere una inutila
[19:10] <@Andrei> Daca nu a aparut acum o prezentare de pe slideshare reincercati cu un alt browser
[19:10] == Alex_Baies [webchat@34C2FB45.51F9B98F.1DE3F0FD.IP] has quit [Quit: Page closed]
[19:10] <Ne0h> pe firefox merge
[19:10] <@Andrei> eu o data la cateva minute voi reactualiza sincronizarea :)
[19:10] <@Andrei> continuand
[19:11] <Snoopy> pe internet explorer merge :)
[19:11] <@Andrei> $slideshare_page_2
[19:11] <lighto> nu merge pe Namoroka
[19:11] <TinKode> si pe chrome
[19:11] <TinKode> merge f bn
[19:11] <Ne0h> men da da mai departe
[19:11] <@Andrei> o mica istorie a acestei vulnerabilitati e dificil de amintit, ea exista de foarte multa vreme, practic o data cu aparitia acestor limbaje client side
[19:11] <Ne0h> ca m-am plictisit sa citesc introducerea
[19:11] <@Andrei> $slideshare_page_2
[19:11] <@Andrei> $slideshare_page_3
[19:11] <Ne0h> asa
[19:11] == cossin_ [webchat@CBB01EE.D1E07B76.6856A64.IP] has joined #rocybercon
[19:11] == lighto_ [webchat@AF887A70.4675B5D.3CEC8F46.IP] has joined #rocybercon
[19:12] == Alex_Baies [webchat@34C2FB45.51F9B98F.1DE3F0FD.IP] has joined #rocybercon
[19:12] <kNigHt> $slideshare_page_1
[19:12] <@Andrei> XSS este o vulnerabilitate, dupa cum spuneam ce afecteaza clientul
[19:12] == r00t [webchat@53C70069.2B7D1C5F.80CA61CB.IP] has joined #rocybercon
[19:12] <@Andrei> dar poate fi dusa la cealalta extrema si prin diverse situatii "bune" ajungem sa exploatam si partea server side
[19:12] <@Andrei> de cele mai multe ori ne bazam pe injectiile javascript

[19:12] <@Andrei> dar nu e ceva general valabil
[19:13] == Catalin [webchat@D06E285.CA4D55FD.2906B74E.IP] has joined #rocybercon
[19:13] <@Andrei> cum spuneam - foarte raspandita - locul 2 in clasamentele Infosesc si OWASP
[19:13] == Crisalixx [webchat@64204DB8.5D3A6CC4.A1DF996A.IP] has quit [Quit: Page closed]
[19:13] <@Andrei> iar ca resurse avem numeroase
[19:13] <bcman> care e pe locul 1 in clasamente?
[19:13] <TinKode> HrN e pe acii?
[19:13] <lighto> This document has either been rmeoved or made private by its owner
[19:13] <@Andrei>
[19:13] == cossin [webchat@CBB01EE.D1E07B76.6856A64.IP] has quit [Ping timeout]
[19:13] <@Andrei> $slideshare_page_4
[19:14] == Mihai [webchat@D38FE02B.65A441C3.96EEA9AC.IP] has joined #rocybercon
[19:14] <@Andrei> exista cateva tipuri de atacuri care claseaza atacurile XSS :)
[19:14] <lighto_> done, works on chromium
[19:14] <@Andrei> cele nepersistente, sau reflected
[19:14] <@Andrei> cele mai populare dintre cele 3 categorii
[19:14] == Mihai [webchat@D38FE02B.65A441C3.96EEA9AC.IP] has quit [Quit: Page closed]
[19:14] == Ne0h [webchat@1713ECA9.191B2C30.6071C639.IP] has quit [Quit: Page closed]
[19:14] == tw8 [webchat@D38FE02B.65A441C3.96EEA9AC.IP] has joined #rocybercon
[19:14] <@Andrei>
[19:15] <@Andrei> au nevoie de cele mai multe ori de o interpretare din partea serverului pentru a putea fi executate, o interpretare proasta
[19:15] == Eduard [webchat@F868B15E.FDAFBB27.CD727EDC.IP] has quit [Quit: Page closed]
[19:15] == Petrila [webchat@E81C4B7.C7F3E82F.161E8394.IP] has joined #rocybercon
[19:15] <@Andrei> apoi, cele persistente, la fel, interpretare venita din partea serverului, sunt extrem de periculoase pentru ca oricine acceseaza o pagina cu un xss injectat risca sa aiba probleme
[19:16] <@Andrei> si cea de-a treia categorie - dom-based
[19:16] == r00t [webchat@53C70069.2B7D1C5F.80CA61CB.IP] has quit [Quit: Page closed]
[19:16] == cro-mag [webchat@5C78D768.CC48E247.161E8394.IP] has quit [Quit: Page closed]
[19:16] == Catalin [webchat@D06E285.CA4D55FD.2906B74E.IP] has quit [Quit: Page closed]
[19:16] == test [webchat@53C70069.2B7D1C5F.80CA61CB.IP] has joined #rocybercon
[19:16] == cossin_ [webchat@CBB01EE.D1E07B76.6856A64.IP] has quit [Ping timeout]
[19:16] <@Andrei> ele au aparut acum cu noul val de abuz al tehnologiei pe partea de client side
[19:16] == lighto [webchat@AF887A70.4675B5D.3CEC8F46.IP] has quit [Ping timeout]
[19:17] <@Andrei> nu e necesara interpretarea directa de catre server si astfel poti vedea si ce filtre foloseste site-ul
[19:17] <@Andrei> sunt extrem de populare in retelele sociale, asa ca aveti grija ce faceti
[19:17] <@Andrei> exemple?
[19:17] == cosmin77 [webchat@92.86.56.119] has joined #rocybercon
[19:17] <@Andrei> o multime
[19:17] <@Andrei>
[19:17] <@Andrei> $slideshare_page_5
[19:17] <Petrila> le injectam cu xss ;))
[19:17] <@Andrei> amazon
[19:17] <@Andrei> $slideshare_page_6
[19:18] == LegendKiller [webchat@469D36D3.59F8F5B7.F9A7F15E.IP] has joined #rocybercon
[19:18] <@Andrei> chiar facebook
[19:18] <@Andrei> $slideshare_page_7
[19:18] <@Andrei> google? Nici ei nu au scapat

[19:18] <@Andrei> $slideshare_page_8
[19:18] <johane> Andrei, la faceshit ma astept la orice
[19:18] <@Andrei> ebay
[19:18] == Petrila [webchat@E81C4B7.C7F3E82F.161E8394.IP] has quit [Quit: Page closed]
[19:18] <@Andrei> alt site urias :)
[19:18] <@Andrei> johane, toate sunt predispuse :)
[19:18] <@Andrei> $slideshare_page_9
[19:18] <@Andrei> si muuuulte altele
[19:18] <bcman> chiar si wit
[19:18] <@Andrei> chiar si worldit a avut vulnerabilitati prin diverse extensii prost create de catre dezvoltatorii lor :)
[19:19] <@Andrei> nimeni nu scapa
[19:19] <ZeroCold> si triburile.ro este vulerabil :)))
[19:19] <bcman> de la google ma asteptam la o securitate mai buna
[19:19] <@Andrei> nu as vrea sa amintesc de yahoo, poate cel mai testat site ca sa spun asa
[19:19] == test [webchat@53C70069.2B7D1C5F.80CA61CB.IP] has quit [Ping timeout]
[19:19] == LegendKiller [webchat@469D36D3.59F8F5B7.F9A7F15E.IP] has quit [Quit: Page closed]
[19:19] <bogdannbv> si oradea.net :))
[19:19] <@Andrei> bcman e discutabil si stii bine ca problemele apar
[19:19] <@Andrei> $slideshare_page_10
[19:19] <kNigHt> cand ai milioane de linii de cod nu ai cum sa faci totu perfect
[19:20] <@Andrei> exact
[19:20] <kNigHt> si nu ai cum sa filtrezi totul printr-ul filtru xss
[19:20] <kNigHt> sunt unele imputuri care ar trebui sa aiba content foarte asemanator
[19:20] <@Andrei> corect
[19:20] <@Andrei> problemele apar sub diverse forme
[19:20] <bcman> poti folosi scanere de vulnerabilitati
[19:20] <@Andrei> care de care mai complexe si mai interesante pentru persoanele ce studiaza asta
[19:20] <kNigHt> nici alea nu au rata de 100%
[19:20] == eXcEsuHk [webchat@B36998FA.7C3494A1.1DE3F0FD.IP] has quit [Quit: Page closed]
[19:20] == cosmin77 [webchat@CBB01EE.D1E07B76.6856A64.IP] has quit [Ping timeout]
[19:20] == bexa [webchat@3992622E.65ED80B3.B7B9B306.IP] has joined #rocybercon
[19:20] <kNigHt> de detectie
[19:21] <@Andrei> bcman, un scanner e invatat sa scaneze ceea ce stie, noi discutam de cele mai multe ori de proiecte cu abordari originale si probleme originale
[19:21] <@Andrei> de aceea cand cineva spune ca trebuie sa stim programare ca sa stim securitate trebuie sa fie ascultat
[19:21] <@Andrei> revenind
[19:21] <TinKode> un msn cookie grabber are careva?
[19:21] <@Andrei> unde gasim vulnerabilitati?
[19:21] <@Andrei> $slideshare_page_12
[19:21] <@Andrei> $slideshare_page_11
[19:21] <@Andrei> hmm, le putem gasi peste tot
[19:21] == sorinax [webchat@49C7451D.873CFFFA.9513385E.IP] has joined #rocybercon
[19:21] <kNigHt> tinkode da-mi xss si iti fac grabber intr-o ora
[19:21] <kNigHt> :))
[19:22] <@Andrei> exista o regula clara pentru noi - tot ce vine din partea utilizatorilor nu e de incredere
[19:22] <TinKode> pe ala live?

[19:22] <TinKode> msn
[19:22] <@Andrei> .ban tinkode
[19:22] == mode/#rocybercon [+b *!*?b?h?t@*.*6EEA9A?.I?] by Guardian
[19:22] <@Andrei> vulnerabilitatile le gasim de obicei in variabilele globale (in cazul PHP - Get, post, cookie samd
[19:23] == gimii [webchat@37514D6F.C0F13D23.EF37DABA.IP] has joined #rocybercon
[19:23] <@Andrei> sfatul este sa fiti ingeniosi si sa priviti cat mai suspect orice informatie care o tratati si provine de la client
[19:23] <@Andrei> :)
[19:23] <@Andrei> $slideshare_page_12
[19:23] <kNigHt> uitati o clasa de validare pe care o folosesc eu, poate va ajuta: http://pastebin.com/sSnYbRBQ
[19:23] <Cyborg> Title: PHP | (at pastebin.com)
[19:23] <gimii> :))
[19:23] <@Andrei> cateva exemple simple de vectori cu care puteti descoperi vulnerabilitati
[19:24] == gimii [webchat@37514D6F.C0F13D23.EF37DABA.IP] has quit [Quit: Page closed]
[19:24] <@Andrei> primul exemplu e cel mai simplu din toate
[19:24] <@Andrei> .unban tinkode
[19:24] == mode/#rocybercon [-b *!*?b?h?t@*.*6EEA9A?.I?] by Guardian
[19:24] <@Andrei> afecteaza in mod evident javascript
[19:24] <@Andrei> al doilea incearca sa inchida un tag html si apoi sa mearga pe aceeasi idee ca primul
[19:25] <@Andrei> al treilea si al 4lea pot fi folosite ca bypass in diverse situatii
[19:25] <@Andrei> spre exemplu al 4lea poate fi folosit atunci cand avem filtrate < >
[19:25] <@Andrei> si totusi primim input intr-un tag
[19:25] <@Andrei> <input value="mesajul care il putem modifica">
[19:25] <@Andrei> e cel mai simplu exemplu
[19:25] == cristian77 [webchat@49C7451D.873CFFFA.9513385E.IP] has joined #rocybercon
[19:25] <@Andrei>
[19:25] <kNigHt> la 3 si 4 nu ar trebui sa fie si un <script> ca sa mearga alertul?
[19:25] <@Andrei> nu
[19:26] <@Andrei> html-ul are diverse evenimente care vor executa cod javascript
[19:26] <kNigHt> da, scuze, nu ma uitasem atent
[19:26] <@Andrei> onerror, onclick samd sunt cateva exemple :D
[19:26] == sorinax [webchat@49C7451D.873CFFFA.9513385E.IP] has quit [Ping timeout]
[19:26] <@Andrei> urmeaza apoi alte doua exemple prin care putem executa cod javascript fara a avea nevoie de ghilimele :)
[19:26] == Danut [webchat@FBAD82F0.CD5D1B7E.3CEC8F46.IP] has joined #rocybercon
[19:27] == bexa [webchat@3992622E.65ED80B3.B7B9B306.IP] has quit [Quit: Page closed]
[19:27] == bexa [webchat@3992622E.65ED80B3.B7B9B306.IP] has joined #rocybercon
[19:27] <@Andrei> din pacate unele browsere/configurari proaste ale headerelor pot permite executarea unor injectii folosind encodarea mesajului
[19:27] <@Andrei>
[19:27] == ghitzZza [webchat@2F081D0E.D82CCA6.2766FEC8.IP] has joined #rocybercon
[19:27] == Stoian [webchat@A9C19469.4FD5F760.CB27CEAF.IP] has joined #rocybercon
[19:27] <@Andrei> de asemenea putem injecta xss-uri prin meta-uri, style samd
[19:27] <@Andrei>
[19:27] <@Andrei> $slideshare_page_13
[19:28] <@Andrei> mai departe, cativa vectori mai dificili, spun eu

[19:28] <kNigHt> prima nu merge in ie
[19:28] <@Andrei> primul abordeaza un tip extrem de util in diverse cazuri atat la injectii client side, dar si la cele server side
[19:28] == Stoian [webchat@A9C19469.4FD5F760.CB27CEAF.IP] has quit [Quit: Page closed]
[19:28] == cristian77 [webchat@49C7451D.873CFFFA.9513385E.IP] has quit [Ping timeout]
[19:29] <@Andrei> knight nu te astepta sa mearga toate, unele sunt mai vechi, altele sunt extrem de noi si merg cu variantele actuale ale browserelor
[19:29] <@Andrei> ideea e sa ne facem o idee cum putem gasi noi urmatorii vectori in acest sens
[19:29] <TinKode> prin headere
[19:29] <@Andrei> urmeaza apoi un exemplu prin style obvustucat
[19:29] <@Andrei> de asemenea si xml nu scapa
[19:29] == ghitzZza [webchat@2F081D0E.D82CCA6.2766FEC8.IP] has left #rocybercon []
[19:29] == Bubu [webchat@2E9D0402.9E5F7A21.673BE40F.IP] has quit [Quit: Page closed]
[19:30] <@Andrei> anti-penultimul vector este unul foarte foarte interesant din cateva perspective
[19:30] <@Andrei> apoi avem un exemplu de unicode injection abuzand de niste chestii care sunt considerate deprecated de ceva vreme
[19:30] == ghitzZza [webchat@2F081D0E.D82CCA6.2766FEC8.IP] has joined #rocybercon
[19:30] <@Andrei> :)
[19:30] == kty [webchat@154F35BC.52C2E5B8.3CEC8F46.IP] has quit [Quit: Page closed]
[19:30] <Xenon> pardon*
[19:31] == ghitzZza [webchat@2F081D0E.D82CCA6.2766FEC8.IP] has quit [Quit: Page closed]
[19:31] <@Andrei> desigur, daca aveti si voi exemple mai smechere nu ezitati sa le sharuiti :)
[19:31] <@Andrei> $slideshare_page_14
[19:31] <@Andrei> mai nou, avem html 5
[19:31] <Synthesis> Am dat si eu aici http://www.worldit.info/articole/despre-cross-site-scripting-xss/ cateva exemple
[19:31] == Snoopy [webchat@8D9AEE84.A819D838.79CBE436.IP] has quit [Quit: Page closed]
[19:31] <Cyborg> Title: Despre Cross Site Scripting (XSS) | WorldIT (at www.worldit.info)
[19:31] <@Andrei> tehnologie noua, vulnerabilitati noi :)
[19:31] == ghitzZza [webchat@B8B8D9B.398F9D3.2C14242A.IP] has joined #rocybercon
[19:32] <@Andrei> avem noi taguri, noi evenimente, noi structuri de date
[19:32] <@Andrei> cum e al patrulea exemplu :)
[19:32] == fly [webchat@8FA5A40.70F805E2.70D253C3.IP] has joined #rocybercon
[19:32] <@Andrei> autofocus este iar o chestie smechera din html 5 de care se poate abuza pentru a genera injectii dragute
[19:32] <@Andrei>
[19:33] <TinKode> ohh yeah, like youtube xss
[19:33] <@Andrei> urmeaza un abuz al local storage-ului :)
[19:33] <@Andrei> ultimul exemplu este unul extrem de interesant
[19:33] <@Andrei> a aparut o functie in history-ul nou
[19:33] == Xenon [webchat@BF07C3FF.F6B031F4.304B3D6E.IP] has quit [Ping timeout]
[19:33] <@Andrei> ce ne permite sa modificam pagina curenta (cea din link) cu ce vrem noi, pastrand domeniu
[19:33] <kNigHt> adica dau back la pagina si dau de scam?
[19:33] == qbert [webchat@3A7A0A3B.8B18C574.3CEC8F46.IP] has joined #rocybercon
[19:34] <@Andrei> asta inseamna ca un payload prin get va putea fi sters si linkul va parea normal
[19:34] == soso [webchat@WIT-A4B02663.ghst.net] has joined #rocybercon
[19:34] <@Andrei> un exemplu live in acest sens
[19:34] <@Andrei> este http://bit.ly/pushStateXSS

[19:34] <Cyborg> Title: How to Conceal XSS Injection in HTML5 - demo.hakoniemi.net (at bit.ly)
[19:34] <Synthesis> asta poate fi folosit si pentru XSHM
[19:34] <@Andrei> daca veti observa parametrul (inainte de redirectare) veti observa o injectie mascata impecabil
[19:35] <@Andrei> da, se poate folosi chiar foarte bine
[19:36] <@Andrei> daca aveti intrebari pana acum, sper ca nu v-am speriat prea tare :))
[19:36] == Laz [webchat@59B55C36.1D487C48.4C97F1AF.IP] has quit [Ping timeout]
[19:36] <@Andrei> ascult
[19:36] <bcman> as avea ceva de zis
[19:36] <bcman> dar nu intrebare
[19:36] <@Andrei> sigur :D
[19:36] <bcman> microsoft are un filtru in ie
[19:36] <bcman> smart screen filter
[19:36] <@Andrei> ajungem imediat si la el :D, pe scurt e doar o tentativa esuata de a face ceva
[19:37] <bcman> imediat dupa lansare, au fost descoperite numeroare bug-uri
[19:37] <@Andrei> e un plus, dar nu cel mai bun :)
[19:37] <@Andrei> la fel ca si restul noscript si trupa
[19:37] <bcman> facea ca site-urile sa fie vulnerabile
[19:37] <bcman> chiar daca nu erau
[19:37] <bcman> la xss
[19:37] <bcman> microsoft a primit premiul Most Epci Fail la blackhat 2010
[19:38] <bcman> epic*
[19:38] <johane> :))
[19:38] <@Andrei> mmm, da, imi amintesc de problema aia, din pacate mi-a scapat sa o amintesc. Bcman are dreptate, era o problema in sistemul de protectie de la IE care genera erori fara ca acestea sa existe daca nu ma insel
[19:38] <bcman> exact
[19:38] <kNigHt> pe ce versiuni mai merge? :))
[19:39] <@Andrei> observ ca sunteti timizi asa ca mergem putin mai departe, la bypass-ing :)
[19:39] <@Andrei> $slideshare_page_15
[19:39] <bcman> @knight nu cred ca mai merge deloc
[19:39] <@Andrei> fiecare sistem de protectie nou aduce cu el diverse abordari pentru a solutiona sau a preveni atacurile (cel putin pe cele mai simple dintre ele)
[19:39] <@Andrei> majoritatea functioneaza pe expresii regulate
[19:39] <@Andrei> sau creaza niste ponderi ale mesajului
[19:40] == lighto_ [webchat@AF887A70.4675B5D.3CEC8F46.IP] has quit [Quit: Page closed]
[19:40] <@Andrei> daca ponderea depaseste un prag, mesajul respectiv este procesat si se incearca eliminarea contentului respectiv
[19:40] == Alex_Baies [webchat@34C2FB45.51F9B98F.1DE3F0FD.IP] has quit [Quit: Page closed]
[19:40] <@Andrei> aici am o lista cu o serie de vectori ce incearca sa treaca de filtre de la IE, NoScript si compania
[19:40] == Maverick [webchat@1A267546.A014A42E.798C5272.IP] has joined #rocybercon
[19:40] <@Andrei> majoritatea acum nu mai trec
[19:41] <@Andrei> dar asta nu inseamna ca nu-i poate face utili atunci cand ne confruntam cu sisteme interne care fac lucruri similare
[19:41] <@Andrei> spre exemplu primul ne demonstreaza cum putem injecta ceva fara spatii
[19:41] <@Andrei>
[19:41] <@Andrei> apoi o alternativa la src, un tag care probabil multi dintre noi nici nu il stiu
[19:42] == soso [webchat@WIT-A4B02663.ghst.net] has quit [Ping timeout]

[19:42] <@Andrei> urmeaza un bypass pentru generarea erorilor care l-am abordat si eu de cateva ori
[19:42] == qbert [webchat@3A7A0A3B.8B18C574.3CEC8F46.IP] has quit [Ping timeout]
[19:42] == nobody [webchat@30A6AFC4.19D040A0.C6239117.IP] has quit [Quit: Page closed]
[19:42] <@Andrei> se foloseste de faptul ca noi putem accesa prin evenimente diverse variabile ale tag-ului
[19:42] <@Andrei> tag.*
[19:42] <@Andrei> scuze, this.*
[19:42] <@Andrei> in cazul respectiv : this.src si this.alt
[19:43] <@Andrei> apoi o alta abordare pentru a compromite verificarile ce au loc
[19:43] <@Andrei> payload-ul se incarca, (pare unuil valid pentru filtre), dar realitatea e ca el incarca adevaratul exploit ce se afla dupa #
[19:43] <@Andrei> trei alternative pentru a abuza de cookie-uri :)
[19:44] <@Andrei> unele picau la anumite filtre
[19:44] <@Andrei> si chiar mai pica si acum
[19:44] <@Andrei> putem executa functii si fara () sau =
[19:44] <@Andrei> si din nou, HTML 5
[19:44] <@Andrei> :D
[19:44] <@Andrei> acum putem folosi evenimente la tagurile ce le inchidem, pare ciudat, nu am inteles avantajul
[19:44] <@Andrei> dar distruge unele sisteme de protectie
[19:45] <@Andrei> acum putem face injectii prin xss-uri direct din style fara pic de javascript (aparent)
[19:45] <@Andrei> putem abuza (ma repet) de faptul ca unele filtre detecteaza javascript sau alte limbaje, dar nu stiu sa se asigure ca nu primest informatiile spre exemplu in base64 (penultimul exemplu)
[19:46] <@Andrei> ultimul e un atac de tipul HPP - Http parameter pollution :)
[19:46] <@Andrei> se foloseste des in SQLi si poate reprezenta o alternativa extrem de utila in anumite cazuri :)
[19:47] == dorinbz [webchat@CBB01EE.D1E07B76.6856A64.IP] has joined #rocybercon
[19:47] <@Andrei>
[19:47] <@Andrei> intrebari pana aici? sau completari? sau nelamuriri? :)
[19:47] <kNigHt> da
[19:47] <kNigHt> la style background url
[19:47] <kNigHt> la cel doar din css
[19:48] <kNigHt> ce putem injecta?
[19:48] <@Andrei> exista undeva acolo unde scrie attacker?log[]=
[19:48] <@Andrei> nu seamana cu un stealler? :)
[19:49] <kNigHt> aaa
[19:49] <kNigHt> chiar
[19:49] <@Andrei> il fortezi sa execute imaginea (care e defapt un fisier php, eventual cu extensie de imagine) care logheaza tot:D
[19:49] <kNigHt> deci retine input value intr-o variabila
[19:49] <@Andrei> ;)
[19:49] == __ [webchat@C309A7C7.F59A8808.96EEA9AC.IP] has joined #rocybercon
[19:50] <Maverick> dar in loc sa le retina intr-o variabila nu le poate trimite direct undeva?
[19:50] <denjacker> o retine ptr eventuale prelucrari..
[19:51] <@Andrei> defapt //atacker?log[]=a e ca si cum ai inlocui cu http://atacator.com?grab=cookie-uri :D
[19:51] == GrigoritaIulianCristian [webchat@16C0926F.A7BCA0AE.2906B74E.IP] has quit [Quit:

Page closed]
[19:51] <Maverick> log[] e un array?
[19:51] <@Andrei> da
[19:52] <@Andrei> tot asa pot aparea vulnerabilitatile FPD, dar intram in offtopic :))
[19:52] <Maverick> :)
[19:52] <kNigHt> FPD = ?
[19:52] <ZeroCold> FPD?
[19:52] <@Andrei> full path disclosure
[19:52] <@Andrei> nu are legatura cu vulnerabilitile XSS
[19:53] <kNigHt> fiindca variabila e array in loc de string?
[19:53] <@Andrei> exact :)
[19:53] <BuBu_> ce mai e pe aici ?
[19:53] == bcman [webchat@CF171E56.EC5945EF.96EEA9AC.IP] has quit [Quit: Page closed]
[19:53] <@Andrei> continuand, mergem la ceea ce va fi probabil cel mai interesant
[19:53] <@Andrei> si anume ce putem face cu aceste probleme de securitate?
[19:53] <@Andrei> $slideshare_page_16
[19:54] <@Andrei> raspunsul e "MUULTE" :)
[19:54] <@Andrei> $slideshare_page_17
[19:54] <Maverick> $slideshare_page_17
[19:54] <@Andrei> putem redirecta utilizatorul pe paginile in care avem un trojan, putem sa facem trafic artificial
[19:54] <@Andrei> daca avem norocul sa dam peste un xss permanent
[19:55] <@Andrei> este o vulnerabilitate extrem de populara si care o poate "implementa" cam toata lumea
[19:55] <@Andrei> clickjacking este foarte folosit in phishing
[19:55] <@Andrei> !google clickjacking
[19:55] <Cyborg> Andrei: Clickjacking - Wikipedia, the free encyclopedia: <http://en.wikipedia.org/wiki/Clickjacking>; Clickjacking - OWASP: <http://www.owasp.org/index.php/Clickjacking>; FAQ: Clickjacking -- should you be worried? - Computerworld: <http://www.computerworld.com/s/article/9115818/FAQ_Clickjacking_should_you_be_worried_>; Clickjacking: Researchers raise alert for scary new cross-browser ...: (2 more messages)
[19:56] <@Andrei> credibilitatea unei pagini creste extrem de mult intr-o astfel de situatie
[19:56] == __ [webchat@C309A7C7.F59A8808.96EEA9AC.IP] has quit [Ping timeout]
[19:56] <@Andrei> cred ca e cea mai abuzata metoda prin randul celor care stiu sa exploateze un xss si doresc sa-l foloseasca la phishing :)
[19:56] <@Andrei> $slideshare_page_18
[19:56] <@Andrei> url spoofing :)
[19:57] <@Andrei> la fel, phishing-ul e domeniul care e atras de ea
[19:57] <@Andrei> cream impresia unui url user friendly, dar continutul paginii este modificat si datele sunt trimise unde dorim noi sa fie
[19:58] == Catalin [webchat@FD64A32F.AE2DD352.EDCFCEAE.IP] has joined #rocybercon
[19:58] <@Andrei> ca sa puteti intelege - imaginati-va ca intrati pe pagina de logare de la google si totul arata in regula dar T. a abuzat de un xss direct in acea pagina si a modificat tot ca sa trimita datele de autentificare la el
[19:58] <@Andrei> in combinatie cu history.pushState din html 5 poti face minuni chiar daca e un xss temporar
[19:58] <@Andrei> :D
[19:59] <@Andrei> $slideshare_page_19

[19:59] == IonutC [webchat@2EB5166B.F46D5BD3.CB27CEAF.IP] has joined #rocybercon
[19:59] <@Andrei> session hijacking, probabil prietenul celor care au auzit de XSS-uri
[19:59] <@Andrei>
[19:59] <@Andrei> de cele mai multe ori abuzeaza de cookie-uri :)
[20:00] <@Andrei> dar nu e neaparat, o sesiune poate fi transmisa prin multe alte metode - get/post samd
[20:00] == tjmobile [webchat@5F9E5143.235C2994.258CCCEA.IP] has joined #rocybercon
[20:00] <@Andrei> la noi cele mai cautate sunt vulnerabilitatile in *.yahoo.com pentru ca toti vrem sa avem oportunitatea de a abuza de "amicul" nostru :)
[20:01] == Catalin [webchat@FD64A32F.AE2DD352.EDCFCEAE.IP] has quit [Ping timeout]
[20:01] <@Andrei> aceste "exploituri" folosesc un asa zis cookie grabber sau session stealler ce trimite sesiunea unui utilizator la o pagina a hackerului
[20:01] <@Andrei> si aceasta poate sa le foloseasca in scopurile sale - autentificandu-se cu ele
[20:02] <@Andrei> $slideshare_page_20
[20:02] == anonv [webchat@DF349B82.23891AF7.36076090.IP] has joined #rocybercon
[20:02] <@Andrei> cookie stuffing
[20:02] <BuBu_> :))
[20:02] <@Andrei> foarte folosite in black hat market, cine stie cunoaste cum se spune :)
[20:02] == Birkoff [webchat@188.25.35.119] has joined #rocybercon
[20:02] <@Andrei> presupune modificarea unor cookie-uri ale site-ului in cauza
[20:02] <@Andrei>
[20:02] <@Andrei> si targetarea lor catre ale tale
[20:03] == zYztem [zyztem@aes.overta.ru] has joined #rocybercon
[20:03] == eu [webchat@5462F282.FD67D153.2906B74E.IP] has joined #rocybercon
[20:03] <@Andrei> asta inseamna ca toti userii ce si-au schimbat handlerul, atunci cand vor cumpara ceva de pe un afiliat vor trimite comisioniul hackerului
[20:03] <@Andrei> se poate gasi sub numeroase forme - de la pop-upuri pana la flash :)
[20:03] <@Andrei> toate prind
[20:03] == tjmobile [webchat@5F9E5143.235C2994.258CCCEA.IP] has quit [Ping timeout]
[20:03] <@Andrei>
[20:04] <@Andrei> $slideshare_page_21
[20:04] <@Andrei> ad hijacking, nu stiu daca exista aceasta denumire pe internet dar mi-am permis sa o introduc
[20:04] == r00t [webchat@53C70069.2B7D1C5F.80CA61CB.IP] has joined #rocybercon
[20:04] <@Andrei> la fel, se poate folosi in black market in special atunci cand avem xss-uri permanente
[20:04] == bang [webchat@596BFA43.6DD1DFB4.EDCFCEAE.IP] has joined #rocybercon
[20:04] <@Andrei> putem modifica toate bannerele de pe un site cu ad-urile noastre (de la google spre exemplu)
[20:04] <@Andrei> ghiciti cine va primi banii :)
[20:04] <@Andrei>
[20:05] <@Andrei> $slideshare_page_21
[20:05] <@Andrei> $slideshare_page_22
[20:05] == IonutC [webchat@2EB5166B.F46D5BD3.CB27CEAF.IP] has quit [Quit: Page closed]
[20:05] <@Andrei> atacurile csrf (sau xsrf)
[20:05] <@Andrei> le folosim de cele mai multe ori atunci cand serverul are incredere in cineva si are acces mai mare asupra unor functii
[20:06] <@Andrei> spre exemplu daca un utilizator va intra pe pagina http://hacker.com/administrator/?page=addAdministrator&name=Andrei

[20:06] <@Andrei> nu se va intampla nimic
[20:06] <ZeroCold> dar daca intra un administrator...
[20:06] <@Andrei> dar daca va intra administratorul, serverul il va considera o persoana de incredere
[20:06] <@Andrei> si ma va adauga pe mine ca administrator
[20:06] <@Andrei> csrf abuzeaza de astfel de probleme
[20:07] <@Andrei> si injecteaza imagini, false cu link-ul respectiv de exemplu
[20:07] <@Andrei> si cand administratorul va accesa pagina cu xss-ul (temporar sau permanent) ma va face admin
[20:07] <@Andrei> nu trebuie sa ne limitam la parametri prin GET, POST e la fel de predispus la astfel de vulnerabilitati :)
[20:08] <@Andrei> $slideshare_page_23
[20:08] <@Andrei> history stealling
[20:08] <@Andrei> am amintit si mai devreme de asta intr-o alta forma - aceea de a ne masca prezenta
[20:09] <@Andrei> in anumite situatii dorim sa stim ce site-uri mai acceseaza "victima" noastra
[20:09] <@Andrei> putem abuza de faptul ca javascript & css merg mana in mana
[20:09] <@Andrei> css poate fi setat ca un link sa aiba o anumita culoare daca e vizitat
[20:09] <@Andrei> iar prin js putem crea asta dinamic
[20:10] <@Andrei> atat generarea unei liste cu linkuri care ne intereseaza(vrem sa facem spreading, stealling samd)
[20:10] <@Andrei> cat si verificarea :)
[20:10] <@Andrei> nu e folosita la puterea maxima, zic eu, dar ar putea fi :)
[20:10] <@Andrei> $slideshare_page_24
[20:10] <@Andrei> poate o chestie lame pentru unii, dar care poate face pagube unei corporatii multi-nationala
[20:11] <@Andrei> deface-ul nu trebuie sa fie pe partea de server ca acesta sa existe, o pagina poate fi alterata prin javascript si da impresia unui real deface
[20:11] <@Andrei> oricum ar fi acesta (temporar sau permanent) poate strica imaginea
[20:11] <@Andrei> sau poate starni confuzie:)
[20:12] == tsuby [webchat@7732DCBD.D175D565.673BE40F.IP] has joined #rocybercon
[20:12] <@Andrei>
[20:12] <@Andrei> $slideshare_page_25
[20:12] <Danut> Face deface-ul pe serverul site-ului atacat sau pe alt server?
[20:12] <@Andrei> evident ca pe ala care il vizezi :)
[20:12] == bang [webchat@596BFA43.6DD1DFB4.EDCFCEAE.IP] has quit [Quit: Page closed]
[20:12] <@Andrei> putem inregistra si ce tasteaza userul
[20:12] <@Andrei> sau cum isi misca mouse-ul
[20:12] <Danut> Nu asta vroiam sa zic, iti baga o pagina in fata. Aia unde e hostata?
[20:13] <@Andrei> aa, poti sa pui o imagine hostata la tine acasa sau poti sa modifici pur si simplu contentul html :)
[20:13] <Maverick> Danut modifici direct pagina sau poti adauga tu sa apara ceva peste pagina respectiva
[20:13] <Birkoff> m-ar interesa pe langa descrierea acestor tipuri de atacuri si solutii de prevenire, cred ca toti ar trebui sa avem idee atat despre atac cat si depsre cum se poate preveni
[20:13] <@Andrei> desi realitatea e ca el e acelasi (fizic) adevarul e ca dinamic nu e :)
[20:13] == kty [webchat@154F35BC.52C2E5B8.3CEC8F46.IP] has joined #rocybercon
[20:14] <@Andrei> Birkoff, finalul are si o prevenire a lor care clarifica situatia - sa rezolvi toate trebuie sa ajungem la inceput - XSS-uri :)
[20:14] == tsuby [webchat@7732DCBD.D175D565.673BE40F.IP] has quit [Quit: Page closed]
[20:14] <Birkoff> k, ms

[20:14] <@Andrei> ;)
[20:14] <@Andrei> revenind
[20:14] <@Andrei> putem inregistra ce tasteaza o victima
[20:15] <@Andrei> din pacate acest lucru nu se poate face permanent, ca sa avem o sansa trebuie sa cream o sesiune la victima respectiva si practic sa-i controlam tab-ul deschis
[20:15] <@Andrei> imediat dupa ce acesta va fi inchisa, prea putine sanse mai sunt sa mai inregistrezi ceva
[20:15] <@Andrei> astfel de functionalitati le au XSS shell-urile :)
[20:15] == m0loka [webchat@DA2CED29.DA1BA286.1DE3B360.IP] has joined #rocybercon
[20:16] <@Andrei> (crearea unei sesiune si astfel posibilitatea de a avea o a doua sansa de abuzare a victimei)
[20:16] <@Andrei>
[20:16] == eu [webchat@5462F282.FD67D153.2906B74E.IP] has quit [Quit: Page closed]
[20:16] <@Andrei> $slideshare_page_26
[20:16] <@Andrei> ati obosit? :D
[20:16] <denjacker> nuuuu :D
[20:16] <m0loka> nu'
[20:16] <ZeroCold> neaaa
[20:16] <m0loka> avandei
[20:16] <@Andrei> daca da, pacat, abia de acum vin cele mai grave probleme :)
[20:16] <ZeroCold> mai vrem...:D
[20:16] <r00t> deja am idei...
[20:16] <@Andrei> $slideshare_page_27
[20:17] <@Andrei> atunci trecem la partea a doua a posibilelor probleme
[20:17] == kty [webchat@154F35BC.52C2E5B8.3CEC8F46.IP] has quit [Quit: Page closed]
[20:17] <@Andrei> $slideshare_page_28
[20:17] <@Andrei> si incepem cu browser hijacking, de care aminteam in urma cu cateva clipe :D
[20:17] == Romeo [webchat@EF110349.E5708F15.3CEC8F46.IP] has joined #rocybercon
[20:18] <@Andrei> cunoscut si ca tab hijacking ne permite sa ne facem o sesiune permanenta (totusi temporar, dar de durata mai lunga)
[20:18] <@Andrei> de obicei creezi un iframe ce il controlezi si in care tot continutul userului curge lin
[20:18] <m0loka> tehnicile prezentate se pot folosi cu xss simplu sau permanent
[20:18] <@Andrei> el nu observa ca tot continutul paginilor intra in iframe
[20:18] <@Andrei> toate pot fi folosite si cu unul simplu si cu unul permanent
[20:19] <@Andrei> in combinatiile potrivite
[20:19] <Danut> Cele permanente presupun ca au avantaje in anumite situatii:D
[20:19] <@Andrei> da, distribuirea mai rapida prin randul nostru :)
[20:19] <@Andrei> si link-uri mai putin suspecte
[20:20] <@Andrei> revenind, singurul dezavantaj in cazul tab hijacking il reprezinta adress bar-ul
[20:20] * Romeo slaps Romeo around a bit with a large fishbot
[20:20] <@Andrei> acesta nu va fi schimbat pentru ca tot continutul userului ruleaza in iframe
[20:21] <@Andrei> cum spuneam si mai devreme, puteti implementa chiar voi o astfel de prelungire a duratei de viata
[20:21] <@Andrei> sau puteti sa folositi un shell
[20:21] <@Andrei> $slideshare_page_29
[20:21] <Romeo> Salut Andrei cum merge?
[20:22] <@Andrei> distributed port scanning
[20:22] <@Andrei> pare un domeniu sf, cel putin pana acum :)
[20:22] <@Andrei> posibilitatea de a face request-uri asincrone pe site-uri remote ne permit sa abuzam

de aceasta functionalitate :)
[20:22] <@Andrei> browserele moderne au inceput sa suporte websockets
[20:22] == pax [webchat@BD0D090E.60C58624.55DDAF6B.IP] has joined #rocybercon
[20:23] <pax> oops
[20:23] <@Andrei> chrome, firefox 4, safari si sa speram ca si IE se vor bucura de asta :)
[20:23] <pax> am intarziat
[20:23] <m0loka> :))
[20:23] <@Andrei>
[20:23] <pax> AM INTARZIAT
[20:23] <pax> !
[20:23] <pax> :))
[20:23] <@Andrei> .ban pax
[20:23] == mode/#rocybercon [+b *!*??c?a*@*?5?*D*??B.IP] by Guardian
[20:23] <m0loka> esti scutit pax
[20:23] <Maverick> ce pacat :)
[20:23] <@Andrei> .unban pax
[20:23] == mode/#rocybercon [-b *!*??c?a*@*?5?*D*??B.IP] by Guardian
[20:23] == m0loka [webchat@DA2CED29.DA1BA286.1DE3B360.IP] has quit [Quit: Page closed]
[20:23] <pax> yay
[20:23] <@Andrei> testele arata ca putem scana cu un singur calculator un port in 100ms
[20:23] <ZeroCold> bai, liniste, lasati-l pe Andrei sa vorbeasca
[20:24] <Maverick> Andrei cu ce ne ajuta daca scanam niste porturi?
[20:24] == UnuTreiTreiSapteRST [webchat@DA2CED29.DA1BA286.1DE3B360.IP] has joined #rocybercon
[20:24] <@Andrei> maverick, la multe
[20:24] <Maverick> cum ar fi?
[20:24] <pax> @ andrei : 100ms ? cu nmap acoperi 1k in 3 secunde
[20:24] <@Andrei> de la un fingerprinting pana la aflarea unor noi portite prin care putem testa
[20:24] == ovidiu [webchat@1F028B0.2320BB60.331745B6.IP] has joined #rocybercon
[20:24] <Birkoff> poti intra in calculatorul victimei prin anumite porturi si sa injectezi shelluri...
[20:25] <Maverick> ok am inteles :)
[20:25] <@Andrei> pax e adevarat, dar gandeste-te ce faci cand chrome raporteaza o crestere de 40% a vitezei doar la un shift de versiune
[20:25] <@Andrei> :)
[20:25] <pax> s-a jucat cineva cu db_autopwn pana acum ?
[20:25] <@Andrei> ce se intampla la alte cateva
[20:25] == adry [webchat@D83E48E5.4E6DA01C.4A5FD458.IP] has joined #rocybercon
[20:25] <UnuTreiTreiSapteRST> Andrei, imi poti da exemplu de XSS Shell, ce poti face cu acesta?
[20:25] <@Andrei> sigur, dar cand va fi momentul :D
[20:25] == Romeo [webchat@EF110349.E5708F15.3CEC8F46.IP] has quit [Ping timeout]
[20:25] <@Andrei>
[20:25] <@Andrei> cand puneti intrebarile, formulati-le atunci cand discutam de problema sau cand e momentul intrebarilor :D
[20:26] <@Andrei> revenind, scanarea unor porturi pot dezvalui informatii cu privire la ce folosesc oamenii
[20:26] <UnuTreiTreiSapteRST> Ok, scuze
[20:26] == DeeL [webchat@D04BD1B8.64B59A79.1B258699.IP] has joined #rocybercon
[20:26] <@Andrei> sau putem descoperi pe o clasa de ip-uri daca avem port-ul Y deschis
[20:26] <@Andrei> port Y la care noi stim o vulnerabilitate 0-day spre exemplu

[20:26] <pax> 1337 : cum adica sa dea exemplu de xss shell ? gandeste-te ca e un fel de tunneling intre browseru clientului si atacator
[20:26] <@Andrei> pax calm :D
[20:27] <@Andrei> pentru cei care nu rezista
[20:27] <@Andrei> !google xss shell
[20:27] <Cyborg> Andrei: SecuriTeam - XSS Shell: <http://www.securiteam.com/tools/6X00120HFO.html>; YouTube - Hacking websites with XSS Shell (tutorial by Killer-TR): <http://www.youtube.com/watch?v=vgrxDZVApdI>; XSS Shell v0.3.9 - Cross Site Scripting Backdoor Tool | Darknet ...: <http://www.darknet.org.uk/2006/12/xss-shell-v039-cross-site-scripting-backdoor-tool/>; Portcullis - Free Tools: <http://www.portcullis- (2 more messages)
[20:27] <@Andrei> continuand
[20:27] <@Andrei> $slideshare_page_30
[20:27] <pax> cu ce ? ca n-am prins ce se dezbate
[20:27] == adry [webchat@D83E48E5.4E6DA01C.4A5FD458.IP] has quit [Quit: Page closed]
[20:27] <@Andrei> de la port scanning la ddos e doar un pas, evident :)
[20:27] <pax> ah, slide-ul
[20:28] == tw8 [webchat@D38FE02B.65A441C3.96EEA9AC.IP] has quit [Quit: Page closed]
[20:28] <@Andrei> acum atacurile pe stratul 7 al unei conexiuni poate lasa urme mult mai usor decat s-a putut pana acum :)
[20:28] <@Andrei> trist e ca procesarea COR are loc chiar si atunci cand nu existenta aceasta permisiune :)
[20:29] <denjacker> poti sa dezvolti putin chestia cu stratul 7 si urmele?
[20:29] <@Andrei> asta inseamna ca serverul este atins chiar si atunci deci apare o mica incarcare
[20:29] == Romeo [webchat@EF110349.E5708F15.3CEC8F46.IP] has joined #rocybercon
[20:29] <@Andrei> sigur
[20:29] <@Andrei> cele mai concrete exemple sunt cele doua care bantuie acum internetul
[20:29] <pax> <iframe sandbox="value">
[20:29] <@Andrei> GET si POST :)
[20:29] <pax> allow-same-origin = Allow the content to be treated as being from the same server instead of another domain/server
[20:30] <@Andrei> exista un atac prin POST care permite sa abuzezi de o conexiune stabila pe o durata mare de timp
[20:30] <@Andrei> mai exact
[20:30] <@Andrei> daca noi specificam ca avem de trimis 100000 bytes la server
[20:30] <@Andrei> si ii trimitem cate 1 pe secunda
[20:30] <@Andrei> putem suprasolicita serverul, ocupandu-i toate conexiunile available
[20:31] <@Andrei> restul userilor asteptand, si asteptand
[20:31] <pax> @andrei : depinde cum e configurat serverul web
[20:31] <@Andrei> corect, depinde, majoritatea pica
[20:31] <@Andrei> mai ales apache
[20:31] <pax> badea a picat
[20:31] <UnuTreiTreiSapteRST> mana lui nemesis
[20:32] <pax> zic ca am testat smecheria cu post si get
[20:32] <pax> si am dat pe badea
[20:32] <pax> si a picat
[20:32] <@Andrei> testele arata ca putem genera un ddos foarte lejer cu 600 de persoane "compromise"
[20:32] == lighto [webchat@AF887A70.4675B5D.3CEC8F46.IP] has joined #rocybercon
[20:32] <@Andrei>

[20:32] <UnuTreiTreiSapteRST> pax
[20:32] <ZeroCold> depide de viteza pe care o are atacatorul?
[20:32] <@Andrei> dezavantajul in cazul acestor atacuri ddos e ca nu le poti mentine permanent
[20:32] <pax> zerocold : nu
[20:32] <@Andrei> adica ar trebui sa fie un val masiv de infectii
[20:32] <ZeroCold> mersi
[20:32] <@Andrei> in 5 minute sa spunem
[20:33] == lighto [webchat@AF887A70.4675B5D.3CEC8F46.IP] has quit [Quit: Page closed]
[20:33] <@Andrei> care sa-si mentina tab-ul deschis (hijacking tab) suficient cat sa creezi acel ddos :)
[20:33] <@Andrei> $slideshare_page_31
[20:33] <pax> a aparut paper si pe exploitdb cu tab hijacking
[20:33] <@Andrei> da
[20:34] <pax> palaria jos pentru baieti
[20:34] <@Andrei> xss tunnelling-ul
[20:34] <pax> simplu si original
[20:34] <@Andrei> am putea spune ca e un protocol de comunicare intre victima temporara si client
[20:35] <UnuTreiTreiSapteRST> Eu pot naviga cu ipul siteului pe care am bagat shell
[20:35] <@Andrei> in zilele noastre ajax e folosit intens (victima trimite permanent request-uri) doar ca acum putem folosi si comet push
[20:35] <@Andrei> comunicare asincrona
[20:35] <@Andrei> acum putem abuza de cross site requests
[20:35] <@Andrei> prin tunnelling putem sa ne facem proxy temporar chiar
[20:35] <@Andrei> asta inseamna ca tot traficul sa mearga prin victima (atata timp cat se poate evident)
[20:35] <@Andrei> si abia apoi noi sa-l primim
[20:36] <@Andrei> interesant ar fi de dezvoltat un canal de tipul ssh (comunicare securizata intr-un loc public)
[20:36] <tdxev> cum se trece peste .same origin??
[20:36] <@Andrei> tu trimiti requesturile la victime criptat, ei decripteaza, executa cererile, returneaza criptat la tine, si tu decriptezi
[20:36] <@Andrei> :)
[20:37] <@Andrei> comet push & browserele moderne
[20:37] <pax> cu un xss shell n-ai treaba cu serverul, doar cu clientii pe care se incarca jsul
[20:37] <@Andrei> browserel moderne suporta cross origin
[20:37] <@Andrei> browserele *
[20:37] <tdxev> k
[20:37] <pax> tdxev : ne-am chinuit zilele trecute sa facem cumva cross domain dar n-am reusit. am luat legatura cu niste baieti mari de prin securitate si nici ei n-au idee
[20:38] <pax> andrei : Allow the content to be treated as being from the same server instead of another domain/server
[20:38] <pax> andrei : http://www.w3schools.com/html5/att_iframe_sandbox.asp
[20:38] <Cyborg> Title: HTML5 iframe sandbox Attribute (at www.w3schools.com)
[20:38] <@Andrei> da :)
[20:39] == Tudy [webchat@8786EE6B.E0E6FDB5.CD727EDC.IP] has quit [Ping timeout]
[20:39] <pax> hmm, ar merge ce vorbeam zilele trecute ? cu iframe-ul si innerhtmlu ?
[20:39] <@Andrei> discutam alta data despre aia
[20:39] <@Andrei> $slideshare_page_31
[20:39] == bogdannbv [webchat@F40744D1.C9A35F5A.673BE40F.IP] has quit [Quit: Page closed]
[20:39] <@Andrei> $slideshare_page_32

[20:39] == ovidiu [webchat@1F028B0.2320BB60.331745B6.IP] has quit [Quit: Page closed]
[20:39] <@Andrei> ajungem la spargerea parolelor in mod asincron si distribuit :)
[20:40] == Johane_ [webchat@95C37CE6.B9DBE3C4.CB27CEAF.IP] has quit [Quit: Page closed]
[20:40] <@Andrei> acum putem 100k hash-uri pe secunda cu o singura masina
[20:40] == Johane_ [webchat@95C37CE6.B9DBE3C4.CB27CEAF.IP] has joined #rocybercon
[20:40] <@Andrei> 100 de masini pot echivala puterea unui computer modern iar tot ce este peste 100 devine deja un plus
[20:40] <UnuTreiTreiSapteRST> Adica ~ cat un procesor sa zicem i7
[20:40] <@Andrei> asta acum, si testele nu iau in calcul chrome 10
[20:40] == Bianca [webchat@5F7D186F.FF984D6.8A354A5B.IP] has quit [Ping timeout]
[20:40] <@Andrei> calculator normal :)
[20:41] <UnuTreiTreiSapteRST> vorbesc de cracking fara java
[20:41] <Maverick> daca putem face 100k pe secunda cu o singura masina de ce ne-ar trebui mai multe?
[20:41] <pax> crackingu se face cu gpu nu cpu
[20:41] <@Andrei> pai la un brute mai rapid inseamna un cracking mai rapid
[20:41] <@Andrei> asta inseamna ca ajungem mai repede la complexitati mai mari ale parolelor
[20:41] <UnuTreiTreiSapteRST> de obicei programele folosesc sincron si gpu si cpu
[20:41] <@Andrei> si cele de 6 caractere devin slabe
[20:41] <@Andrei> cele de 10 devin slabute
[20:42] <@Andrei> si trebuie sa te gandesti la parola de 10-20 caractere ca sa fie mai dificil de spart
[20:42] <Birkoff> deja compui poeme ca sa ai o parola buna :D
[20:42] <@Andrei> Ravan e o aplicatie sincronizata bazata pe javascript care suporta sha & md5, ar trebui sa aruncati o privire peste ea
[20:43] <@Andrei> :))))
[20:43] <pax> nytro sta cam 25 secunde sa-si scrie parola
[20:43] <pax> si era si beat
[20:43] <pax> si n-a gresit
[20:43] <tdxev> :))
[20:43] <@Andrei> o abordare buna :)
[20:43] <tdxev> scrie luceafarul :))
[20:43] <@Andrei> mergem mai departe
[20:43] <Birkoff> da :P inveti si poezii cu ocazia asta :P
[20:43] <@Andrei> $slideshare_page_33
[20:43] == ZeroCold [webchat@494AB790.9F5A7B22.5D663353.IP] has quit [Ping timeout]
[20:44] <@Andrei> spreading, un domeniu care observ ca a prins in romania in ultima perioada
[20:44] <@Andrei> in aceste situatii e preferabil un xss permanent pentru daune mari
[20:44] == creactivity [webchat@WIT-CE40D132.skynet-telecom.ro] has joined #rocybercon
[20:44] <UnuTreiTreiSapteRST> a prins de toti copii
[20:44] <@Andrei>
[20:44] <@Andrei> din pacate
[20:44] == Andrei__ [webchat@DD91964B.13F0EEF3.6856A64.IP] has joined #rocybercon
[20:44] <pax> andrei, la noi e doar spreading manual. ala adevarat e ce face sality
[20:44] <@Andrei> exista mai multe tipuri de worm care au avut ceva de spus
[20:45] <@Andrei> warhol ar fi un vierme la putere absoluta - ar infecta internetul in 15 minute
[20:45] == Xenon [webchat@BF07C3FF.F6B031F4.304B3D6E.IP] has joined #rocybercon
[20:45] <@Andrei> acest lucru este intradevar imposibil din diverse motive evidente
[20:45] <@Andrei> urmeaza apoi viermii liniari
[20:46] <@Andrei> acestia exploateaza o singura tinta - spre exemplu google

[20:46] <@Andrei> si incearca sa se raspandeasca doar prin acest mediu
[20:46] == Johane_ [webchat@95C37CE6.B9DBE3C4.CB27CEAF.IP] has quit [Ping timeout]
[20:46] <@Andrei> viermii hydra abuzeaza si de alte site-uri : au infectat un cont de google, dar hai sa incercam si ceva la yahoo :D
[20:47] <@Andrei> nu prea au mai fost inregistrati viermi devastatori ca putere de raspandire de ceva vreme, myspace a cam fost ultima
[20:47] <@Andrei> dar asta nu inseamna ca nu au mai fost
[20:47] <@Andrei> twitter si facebook zilnic au probleme cu aplicatii de acest gen
[20:47] <@Andrei> daca nu zilnic, foarte des :)
[20:48] <UnuTreiTreiSapteRST> Andrei, sa nu uitam ca Twitterul a avut XSS recent
[20:48] <@Andrei> la ce se poate ajunge? la atasarea unui malware, la fel cu o problema 0-day ce va executa automat :)
[20:48] <@Andrei> Exact :)
[20:48] <@Andrei> chiar zilele astea aparuse ceva in care vorbeau despre xss-urile din twitter :)
[20:49] <@Andrei> $slideshare_page_34
[20:49] == ZeroCold [webchat@83AA49FA.CC3053BC.5D663353.IP] has joined #rocybercon
[20:49] <@Andrei> aici intram intr-o chestie care am subliniat-o la inceputul conferintei - xss e o problema pe partea de client dar poate ajunge usor una pe partea de server
[20:49] <pax> arbitrary file exec a mers si cu http header injection acu ceva timp
[20:49] <@Andrei> in 2008 nici nu trebuia sa ne complicam prea tare
[20:49] <pax> si tot ie
[20:50] <@Andrei> acum e mai usor sa facem un privilege escalation si sa ajungem la acces complet
[20:50] == Andrei__ [webchat@DD91964B.13F0EEF3.6856A64.IP] has quit [Ping timeout]
[20:50] <creactivity> eu nu inteleg de ce microsoft la cati bani are/face nu rezolva odata pt totdeauna bug-urile si exploiturile din ie
[20:50] <@Andrei> un tip a demonstrat cum, o vulnerabilitate xss in wordpress, ne poate permite sa modificam fisiere (abuzand de csrf) php din plugin-urile wordpress
[20:50] <@Andrei> :)
[20:51] <@Andrei> creactivity nu-i vorba numai de bani
[20:51] == s1gma [webchat@797E4BE6.23E22AD0.F9A7F15E.IP] has joined #rocybercon
[20:51] <UnuTreiTreiSapteRST> asta ducand la shell
[20:51] <@Andrei> exact
[20:51] <Maverick> si daca utilizatoru wordpress are pluginuri gen wordpress firewall?
[20:51] <Maverick> nu ajuta la nimic?
[20:51] <UnuTreiTreiSapteRST> nu cred
[20:51] == Xenon [webchat@BF07C3FF.F6B031F4.304B3D6E.IP] has quit [Ping timeout]
[20:51] <@Andrei> depinde ce face acel firewall
[20:51] <Maverick> filtreaza unele taguri
[20:51] <Maverick> folosite in requesturi
[20:52] <Maverick> gen group_concat
[20:52] == Synthesis [webchat@E54AA167.417BC0DA.673BE40F.IP] has quit [Quit: Page closed]
[20:52] <@Andrei> corect, si ajungem la discutia de la inceput - bypass-ing :)
[20:52] <pax> eram entuziasmat zilele trecute ca am gasit xss in wordpress la commenturi; ceea ce nu stiam era ca adminul poate posta html :))
[20:52] == mariandev [webchat@DE35E364.6D0FF774.B0CF34D6.IP] has joined #rocybercon
[20:52] <@Andrei>
[20:52] <@Andrei> $slideshare_page_34
[20:52] <pax> STIU CUM A LUAT NEME ACCES LA BLOGURI
[20:52] <pax> AHAHAHAHAH

[20:52] <UnuTreiTreiSapteRST> CUM>
[20:52] <creactivity> pai le filtreaza...dar daca sunt puse ca si de admin... cred ca nu le mai filtreaza
[20:52] <Maverick> pax stii cine sunt?
[20:52] <pax> nu ma intereseaza cine esti
[20:53] <Maverick> perfect atunci iti urez un gg fiindca stii :P
[20:53] <tdxev> luke :))
[20:53] <kNigHt> back, ce-am ratat?
[20:53] <UnuTreiTreiSapteRST> estineme
[20:53] <Maverick> cum a spart nemesis blogurile
[20:53] <@Andrei> sa nu intram baieti in offtopic :D
[20:53] <pax> destul de usor
[20:53] <@Andrei> conteaza ce scrie, nu cine este :)
[20:53] <pax> si nu m-am gandit pana acum
[20:53] <pax> @ andrei : tine de pluginuri ;)
[20:53] <@Andrei> revenind, problema aceasta este una grava, iar in combinatie cu un csrf ajungem exact aici :)
[20:54] == s1gma [webchat@797E4BE6.23E22AD0.F9A7F15E.IP] has quit [Quit: Page closed]
[20:54] <pax> poti sa aplici csrf daca stii structura panoului
[20:54] <@Andrei> si asta e un aspect bine subliniat
[20:54] <Romeo> numai oamenii stiu sa scrie!!
[20:54] <UnuTreiTreiSapteRST> daca vorbim de wordpress cred ca majoritatea stiu
[20:54] <@Andrei> .ban Romeo
[20:54] == mode/#rocybercon [+b *!*webch?t@*.*???4?.*?] by Guardian
[20:55] <@Andrei> .unban Romeo
[20:55] == mode/#rocybercon [-b *!*webch?t@*.*???4?.*?] by Guardian
[20:55] <@Andrei> alte intrebari, completari aici? :)
[20:55] <kNigHt> la ce pagina eram
[20:55] <kNigHt> ?
[20:55] <Birkoff> 34
[20:55] <@Andrei>
[20:55] <@Andrei> $slideshare_page_34
[20:55] <@Andrei> daca nu, continuam :)
[20:55] <@Andrei> $slideshare_page_35
[20:56] <@Andrei> intranet hacking
[20:56] <@Andrei> suna putin mai bizar decat ce ne spun cunostintele despre xss-uri
[20:56] <@Andrei> intranet & internet sunt doua concepte diferite
[20:56] <@Andrei> dar daca ajungem la controlul browserului de ce nu putem merge mai departe?
[20:56] == Jesan [webchat@95C37CE6.B9DBE3C4.CB27CEAF.IP] has joined #rocybercon
[20:56] <pax> rsnake a vorbit despre intranet haxing, destul de devreme
[20:57] <@Andrei> un link daca ai e foarte util :D
[20:57] <@Andrei> practic noi putem fi protejati de un firewall
[20:58] <@Andrei> dar el nu ne asigura protectia si la portul prin care comunicam pe internet, sau nu ofera suficient
[20:58] <@Andrei> asta inseamna ca dupa un xss
[20:58] <@Andrei> putin control al paginii (tab hijacking)
[20:58] <@Andrei> putem sa incepem analiza interna a victimei
[20:58] <kNigHt> asta cu intranetu e aproape imposibila daca nu stii cum e conceputa reteaua respectiva si unde sa tintesti.. gresesc?
[20:58] <@Andrei> $slideshare_page_36

[20:58] <@Andrei> knight pentru asta e fingerprinting :)
[20:58] <@Andrei> care e procedura pentru a ajunge la intranet hacking?
[20:58] <kNigHt> nu cunosc...
[20:59] <@Andrei> cam aceeasi pentru orice injectie permanenta
[20:59] <denjacker> iti dai seama ca pentru un astfel de atac sofisticat ai nevoie de niste stiudiu de caz preventiv
[20:59] <@Andrei> corect, dar nu am spus nimic ca discutam de cazuri simple - astea au fost primele :D
[20:59] <creactivity> http://ha.ckers.org/blog/20090122/more-intranet-cookie-xss-fun/
[20:59] <@Andrei> ne putem pregati foarte bine in acest sens
[21:00] <Cyborg> Title: More Intranet Cookie XSS Fun ha.ckers.org web application security lab (at ha.ckers.org)
[21:00] <@Andrei> $slideshare_page_36
[21:00] <@Andrei> $slideshare_page_37
[21:00] <@Andrei> ce putem afla?
[21:00] <@Andrei> putem afla printr-un applet java "our NAT'ed IP" cum se spune :)
[21:00] <@Andrei> putem face port scanning local
[21:00] <@Andrei> putem incerca un blind fingerprinting al unui server
[21:01] <@Andrei> putem incerca vulnerabilitati locale pe porturile descoperite
[21:01] == Jesan [webchat@95C37CE6.B9DBE3C4.CB27CEAF.IP] has quit [Ping timeout]
[21:01] <@Andrei> va aduceti aminte de interfata de la DSL? de multe ori parolele sunt lasate default :)
[21:01] == mariandev [webchat@DE35E364.6D0FF774.B0CF34D6.IP] has quit [Quit: Page closed]
[21:01] <@Andrei> desi nu am testat, o posibilitate foarte buna e accesarea locala a fisierelor (e o idee netestata!!!)
[21:02] <creactivity> :) pai testeaza andrei
[21:02] <@Andrei> ne putem folosi de unelte ce automatizeaza acest proces
[21:02] <creactivity> :))
[21:02] <@Andrei> da :D
[21:02] <pax> oricum nu face public, stai linistit
[21:02] <@Andrei> din ce stiam se pot afla si adresele mac
[21:02] <Maverick> lasal sa viseze :)
[21:03] <@Andrei> :)))
[21:03] <r00t> alternativa pentru server cu multe fisiere puse pe net, realizate in reteaua intranet a serverului ------ fingerprinting cu FOCA
[21:03] <Maverick> foca fiind fabricat original cu aluminiu sa inteleg?
[21:03] <pax> copii, gasiti xss in wordpress, pluginuri, orice, si luam shelluri pe banda, sal
[21:03] <creactivity> foca - fabricat original cu aluminiu?
[21:03] <Maverick> explica si tu ce e aia FOCA
[21:03] <creactivity> :))
[21:04] <creactivity> deocamdata doi care urmarim robotzi
[21:04] <Birkoff> FOCA -> Fabricat Original Cu Aluminiu? :))
[21:04] <@Andrei> toti stim :)
[21:04] <denjacker> Ce faci FOCA? .. Bine MO.. uite stric conferinta :-|
[21:04] <UnuTreiTreiSapteRST> vroiam sa zic
[21:04] <@Andrei> .mode +m
[21:04] <creactivity> 3
[21:04] <creactivity> 4
[21:04] == mode/#rocybercon [+m] by Guardian

[21:04] <@Andrei> shht :)
[21:04] <@Andrei> .mode -m
[21:04] == mode/#rocybercon [-m] by Guardian
[21:04] <@Andrei> offtopic-ul la sfarsit :D
[21:04] <r00t> ok
[21:04] <creactivity> ok. scuze
[21:05] <@Andrei> ideea e ca trebuie sa fim inventivi si la acest capitol, orice putem face din browser trebuie sa incercam sa facem si unuia remote
[21:05] <@Andrei> :)
[21:05] <kNigHt> totusi ce e FOCA? :))
[21:05] <Birkoff> youtube foca ...
[21:05] <Maverick> knight poti itnreba si la sfarsit
[21:05] * denjacker slaps kNigHt around a bit with a large fishbot
[21:05] <Birkoff> sau robotzi
[21:05] <@Andrei> $slideshare_page_37
[21:05] <@Andrei> $slideshare_page_38
[21:05] <Birkoff> yeee
[21:06] <Birkoff> ajungem si la prevenire :D
[21:06] <UnuTreiTreiSapteRST> Andrei, si totusi o intrebare care nu este legata de XSS sper sa nu o consideri offtopic, daca am un fisier PHP cu care pot descarca ce fisier doresc de pe server cum pot urca shell prin acel script
[21:06] <ZeroCold> :))
[21:06] <kNigHt> gasind un script care face chiar treaba inversa (upload) si sa incerci sa pui shell prin null char :P
[21:07] <@Andrei> sau poti afla datele de comunicare/autentifacare/baza de date samd
[21:07] <@Andrei> anyway
[21:07] <creactivity> FOCA: Fingerprinting and Organisation with Collected Archives
[21:07] <@Andrei> revenind
[21:07] == BuBu_ [webchat@2DF69316.FBD9425B.673BE40F.IP] has quit [Quit: Page closed]
[21:07] <@Andrei> ajungem la partea dorita de Birkoff si anume prevenirea
[21:07] <@Andrei> evident ca nu ne putem proteja de toate aceste probleme decat prin taierea problemei de la radacini
[21:07] <@Andrei> filtrarea e una din metode atunci cand suntem siguri ca nu avem nevoie de tag-uri
[21:08] <Birkoff> adica scrieti nene cod bun :D
[21:08] <creactivity> si cum gasesti TOATE radacinile?
[21:08] <@Andrei> filtrarea permisiva deja risca
[21:08] <@Andrei> radacinile nu le poate gasi decat cel care scrie codul sau care ii face un audit
[21:08] <creactivity> mai ales cand ai cod scris de 2-3 progs diferiti
[21:08] <@Andrei> ideea este sa urmaresti cam cum opereaza aceaste vulnerabilitati
[21:08] <@Andrei> sa le vezi similaritatile
[21:09] <Birkoff> in primul rand nu cred ca ai nevoie de anumite cheie in get si cookie si filtrezi pentru acele cuvinte cheie (http, ../ etc)
[21:09] <@Andrei> pentru ca toate pana la urma se rezuma la abuzul de incontrol al datelor
[21:09] <Birkoff> cuvinte cheie*
[21:09] <@Andrei> depinde si acele cuvinte cheie cum le validezi
[21:09] <Birkoff> exact
[21:09] <@Andrei> spre exemplu pot aparea situatii cand tu dai replace la xss cu "" //null
[21:09] <@Andrei> daca vei urma acel procedeu vei ajunge nicaieri
[21:10] <@Andrei> xxssss

[21:10] <Birkoff> da
[21:10] <@Andrei> exemplu asta va trece lejer :)
[21:10] <@Andrei> ideea este ca trebuie sa incercam sa ne controlam tot ce poate ajunge la client si ce poate veni de la client, dificil de explicat asta si mai dificil de pus in practica
[21:11] <Birkoff> trim scoate astfel de caractere...
[21:11] <creactivity> da...tre sa ai doishpe kile de creier sa faci de unu singur asta
[21:11] <@Andrei> cateva idei simple sunt filtrarea, asa cum am zis, encoding-ul datelor si incercarea de oprire a caracterelor cheie
[21:11] <@Andrei> nu
[21:11] <kNigHt> htmlspecialchars din php e eficient dupa parerea ta? in cazul in care nu-ti trebe html in input...
[21:11] <@Andrei> depinde de la caz la caz
[21:11] <@Andrei> spre exemplu
[21:11] <@Andrei> daca eu fac ceva de genu
[21:11] <creactivity> sau o echipa de progz, pe care sa ii imbuibi cu cafea, redbull si gogosi
[21:12] <@Andrei> $x = "var x = '".$_GET['xss']."'";
[21:12] <Maverick> creativity nu ne prea intereseaza detaliile de genu fii ontopic
[21:12] <@Andrei> si sa spunem ca aplicam entities
[21:12] <@Andrei> nu vom rezolva cu nimic
[21:12] <@Andrei> pentru ca un mesaj de genul var x = ''; alert(1); va trece
[21:12] <Birkoff> o buna solutie cred eu ca ar fi ceva de genul htmlspecialchars(trim(strip_tags($_GET['ceva'])), ENT_QUOTES, UTF-8)
[21:13] <@Andrei> da, de la caz la caz e buna, insa trebuie urmati acele proceduri simple
[21:13] <@Andrei> nu tu variabile fara ghilimele, nu tu permiterea unei variabile fara encodarea ei
[21:13] <@Andrei> dar ajungem si la situatii in care suntem nevoiti sa folosim bbcode (implementan de noi) sau tag-uri mai simple
[21:14] == fly [webchat@8FA5A40.70F805E2.70D253C3.IP] has quit [Quit: Page closed]
[21:14] <@Andrei> gen doar
[21:14] <Birkoff> da, exact, cum am spus prima oara, sa se scrie cod bun (adica cu verificari la fiecare pas)
[21:14] <kNigHt> unde merge, puteti face filtrul dupa caracterele admise, in loc sa faceti lista de caractere invalide
[21:14] == Radu [webchat@17AF3AEA.E9957030.8ADF52B3.IP] has joined #rocybercon
[21:14] <Radu> hey
[21:14] <@Andrei> knight caracterele invalide se fac in functie de situatie :)
[21:14] <Radu> am pierdut ceva?:)
[21:14] <@Andrei> cam tot :D
[21:14] <@Andrei> :))
[21:14] <Maverick> radu ai pierdut cam tot
[21:14] <Birkoff> exact :)
[21:14] <Birkoff> macar acum aflii cum te protejezi
[21:14] <@Andrei> oricum log-ul apare azi/maine pe blog :)
[21:15] <Radu> i use condoms 4 protection
[21:15] <Radu> :)
[21:15] <Radu> bine
[21:15] <Radu> o sa ma uit cu interes
[21:15] <@Andrei> revenind, o alta politica, bunicica sunt expresiile regulate
[21:15] == tjmobile [webchat@A98C5F20.8618FA70.258CCCEA.IP] has joined #rocybercon
[21:15] <@Andrei>

[21:15] <@Andrei> dar aici trebuie avuta mare grija ce valideaza acestea
[21:16] <Birkoff> o alta filtrare buna e ca daca stii ca trebuie sa primesti un numar, il convertesti automat in numar cu intval($_GET['ceva'])
[21:16] <@Andrei> da
[21:16] <pax> ah, un lucru important pe care l-am descoperit, trebuie sa definiti charsetul in meta
[21:16] <pax> utf-8
[21:16] <@Andrei> astept doar litere, cifre si _ de ce sa accepti si altceva?
[21:16] <@Andrei> foarte important pax e acest lucru :)
[21:16] <@Andrei> multe xss-uri prind pentru ca dupa il definesti tu
[21:16] <@Andrei> cum vrei (tu = hackerul)
[21:17] <@Andrei> apoi vin numeroasele alternative de pe internet (pentru protectia proprie)
[21:17] <@Andrei> noscript e o solutie buna
[21:17] <pax> pentru chrome a aparut ceva anti js ?
[21:17] <UnuTreiTreiSapteRST> e ceva
[21:17] <UnuTreiTreiSapteRST> cu block
[21:18] <Radu> pt chrome mai bine apare o versiune de flash stabila:D
[21:18] <@Andrei> apoi pe langa asta putem folosi un private session atunci cand nu stim ce face un link :)
[21:18] <pax> eu am block pentru flash, cookie si ads
[21:18] <@Andrei> eventual o masina virtuala
[21:18] <@Andrei> eu folosesc des chrome si cand am link-uri ce nu le cunosc fug repede pe firefox & noscript cu private session
[21:18] <@Andrei> pentru ca firefox nu-l folosesc la nimic altceva decat asta
[21:18] <Radu> nu va inteleg cu masinile virtuale...
[21:19] <Birkoff> sandbox daca nu iti plac masinile virtuale :D
[21:19] <UnuTreiTreiSapteRST> stii si alte sandboxuri inafara de sandboxie
[21:19] <johane> Birkoff, stiu eu
[21:19] <johane> Jail
[21:19] <Radu> acum sincer.. voi stiti ce inseamna sa implementezi un sandbox intr-un mediu de productie corporativ?
[21:19] <johane> Jails
[21:20] <Birkoff> prin masina virtuala ma refer la virtualpc, vmware, virtualbox etc
[21:20] <@Andrei> Radu e discutabila treaba, depinde de politica fiecarei corporatii
[21:20] <kNigHt> @Radu intr-un mediu de productie corporativ cred c-ar fi indicat un deepfreeze pe partitia cu os-ul
[21:21] <Radu> nu este o solutie viabila:)
[21:21] <ghostwhite855> si eu merg pe deepfreeze
[21:21] <Radu> sa zicem ca ai 8-900 de calculatoare
[21:21] <TinKode> daca ati stii cate se pot face cu un sandboxie:))
[21:21] <TinKode> si nu ma ref la ce testati cu el
[21:21] <TinKode> :))
[21:21] <kNigHt> whut?
[21:21] <UnuTreiTreiSapteRST> TinKode exemple?
[21:21] <@Andrei> Tinkode asta e offtopic, stim noi ce stii :)
[21:21] <ZeroCold> exemplu?
[21:21] <TinKode> ci la ce face defapt
[21:21] <TinKode> in leg cu IP-urile
[21:21] <TinKode> :)
[21:22] <kNigHt> te face socks? :))

[21:22] <TinKode> nup
[21:22] <TinKode> :)
[21:22] <UnuTreiTreiSapteRST> ne-ai facut curiosi
[21:22] <TinKode> trebuie sa vad daca pot face ceva cu unu de pe elhackers :)
[21:22] <TinKode> daca merge
[21:22] <TinKode> uhuu
[21:22] <pax> socks6, try em out
[21:23] <@Andrei> Radu cred ca cea mai simpla politica abordabila e cea de care am amintit Noscript + firefox in private session ca alternativa de browser, nu cel default :)
[21:23] <@Andrei> .ban tinkode
[21:23] == mode/#rocybercon [+b *!*web*hat@*.9?EE?9AC.??] by Guardian
[21:23] <Radu> brb.. smoke si o sa ma intorc sa va dau niste argumente:)
[21:23] <pax> care e treaba cu zombie cookies ? nu inteleg cum manipuleaza cookie-urile astea browseru ca sa nu poata fii sterse
[21:25] <UnuTreiTreiSapteRST> pax ce sa caut pe google la ddos'u ala
[21:25] <Birkoff> daca informatia e stocata intr-o sesiune pe un server si tu stergi cookie dar ai sesiunea inca deschisa... logic ca acel cookie se creaza automat din nou
[21:25] <pax> gata, am gasit
[21:25] <pax> cauta r-u-dead-yet.py
[21:25] <UnuTreiTreiSapteRST> thx
[21:26] <pax> si totusi, nu ai sesiunea deschisa
[21:26] <pax> tot nu poti sa stergi
[21:26] == tjmobile [webchat@A98C5F20.8618FA70.258CCCEA.IP] has quit [Ping timeout]
[21:26] <@Andrei> .unban Tinkode
[21:26] == mode/#rocybercon [-b *!*web*hat@*.9?EE?9AC.??] by Guardian
[21:26] <@Andrei> avand in vedere ca subiectul a fost aproape complet, ramane intrebarea :
[21:27] <@Andrei> $slideshare_page_39
[21:27] <Birkoff> nop :D
[21:27] <Danut> A fost vreodata?
[21:27] <@Andrei> in conceptia unora da :)
[21:27] <UnuTreiTreiSapteRST> nu
[21:27] <Maverick> :) se pot face mult mai multe lucruri fata de cate stiam
[21:27] <ZeroCold> nu.
[21:27] <Birkoff> e cea mai comuna metoda de a ataca un site
[21:27] <TinKode> app
[21:27] <@Andrei> daca nu eu va multumesc pentru atentie
[21:27] <UnuTreiTreiSapteRST> pax au sters tot de pe google source nu il mai gasesc
[21:27] <@Andrei> $slideshare_page_40
[21:28] <@Andrei> sesiune libera de acum pentru comunicare
[21:28] <Birkoff> andrei pot da un link cu tutoriale pentru cine e interesat sa studieze mai multe?