

Spis treści

WSTĘP	15
Podziękowania	17
I	
BEZPIECZEŃSTWO W ŚWIECIE APLIKACJI WWW	19
Podstawy bezpieczeństwa informacji	19
Flirtowanie z rozwiązaniami formalnymi	20
Zarządzanie ryzykiem	22
Oświecenie przez taksonomię	24
Rozwiązania praktyczne	26
Krótką historią sieci WWW	27
Opowieści z epoki kamienia: 1945 do 1994	27
Pierwsze wojny przeglądarek: 1995 do 1999	30
Okres nudy: 2000 do 2003	31
Web 2.0 i drugie wojny przeglądarek: 2004 i później	32
Ewolucja zagrożeń	34
Użytkownik jako problem bezpieczeństwa	34
Chmura, czyli radość życia w społeczności	35
Rozbieżność wizji	36
Interakcje między przeglądarkami: wspólna porażka	37
Rozpad podziału na klienta i serwer	38
CZĘŚĆ I: ANATOMIA SIECI WWW	41
2	
WSZYSTKO ZACZYNA SIĘ OD ADRESU	43
Struktura adresu URL	44
Nazwa schematu	44
Jak rozpoznać hierarchiczny adres URL?	45
Dane uwierzytelniające dostęp do zasobu	46
Adres serwera	47
Port serwera	48
Hierarchiczna ścieżka do pliku	48

Tekst zapytania	48
Identyfikator fragmentu	49
A teraz wszystko razem	50
Znaki zarezerwowane i kodowanie ze znakiem procenta	52
Obsługa znaków spoza podstawowego zestawu ASCII	54
Typowe schematy adresów URL i ich funkcje	58
Obsługiwane przez przeglądarkę protokoły pobierania dokumentów	59
Protokoły obsługiwane przez aplikacje i wtyczki firm trzecich	59
Pseudoprotokoły niehermetyzujące	60
Pseudoprotokoły hermetyzujące	60
Ostatnia uwaga na temat wykrywania schematów	61
Rozwiązywanie względnych adresów URL	61
Ściąga	64
11.1. Podczas tworzenia nowych adresów URL	
na podstawie danych otrzymanych od użytkownika	64
Podczas projektowania filtrów adresów URL	64
Podczas dekodowania parametrów otrzymanych w adresach URL	64
3	
PROTOKÓŁ HTTP	65
Podstawowa składnia ruchu sieciowego HTTP	66
Konsekwencje utrzymywania obsługi standardu HTTP/0.9	68
Dziwna obsługa znaków nowego wiersza	69
Żądania proxy	70
Obsługa konfliktujących lub podwójnych nagłówków	72
Wartości nagłówków rozdzielane średnikami	73
Zestaw znaków nagłówka i schematy kodowania	74
Zachowanie nagłówka Referer	76
Typy żądań HTTP	77
GET	77
POST	78
HEAD	78
OPTIONS	78
PUT	79
DELETE	79
TRACE	79
CONNECT	79
Inne metody HTTP	79
Kody odpowiedzi serwera	80
200 – 299: Sukces	80
300 – 399: Przekierowanie i inne komunikaty o stanie	80
400 – 499: Błędy po stronie klienta	81
500 – 599: Błędy po stronie serwera	82
Spójność sygnałów wynikających z kodów HTTP	82
Sesje podtrzymywane	82
Przesyłanie danych w częściach	84

Pamięć podręczna	85
Semantyka ciasteczek HTTP	87
Uwierzytelnianie HTTP	90
Szyfrowanie na poziomie protokołu i certyfikaty klientów	91
Certyfikaty rozszerzonej kontroli poprawności	93
Reguły obsługi błędów	93
Ściąga	95
Przy obsłudze nazw plików podanych przez użytkownika oraz nagłówków Content-Disposition	95
Przy umieszczaniu danych użytkownika w ciasteczkach HTTP	95
Przy wysyłaniu kontrolowanych przez użytkownika nagłówków Location	95
Przy wysyłaniu kontrolowanych przez użytkownika nagłówków Redirect	95
Przy konstruowaniu innych rodzajów żądań i odpowiedzi kontrolowanych przez użytkownika	96
4	
JĘZYK HTML	97
Podstawowe pojęcia używane w dokumentach HTML	98
Tryby parsowania dokumentu	99
Walka o semantykę	101
Poznać zachowanie parsera HTML	102
Interakcje pomiędzy wieloma znacznikami	103
Jawne i niejawne instrukcje warunkowe	104
Przydatne wskazówki do parsowania kodu HTML	105
Kodowanie encji	105
Semantyka integracji HTTP/HTML	107
Hiperłącza i dołączanie treści	108
Proste łącza	109
Formularze i uruchamiane przez nie żądania	109
Ramki	112
Dołączanie treści określonego typu	112
Uwaga dotycząca ataków międzydomenowego fałszowania żądań	114
Ściąga	116
Zasady higieny we wszystkich dokumentach HTML	116
Podczas generowania dokumentów HTML z elementami kontrolowanymi przez atakującego	116
Podczas przekształcania dokumentu HTML w zwykły tekst	117
Podczas pisania filtra znaczników dla treści tworzonych przez użytkownika	117
5	
KASKADOWE ARKUSZE STYLÓW	119
Podstawy składni CSS	120
Definicje właściwości	121
Dyrektywy @ i wiązania XBL	122
Interakcje z językiem HTML	122

Ryzyko ponownej synchronizacji parsera	123
Kodowanie znaków	124
Ściąga	126
Podczas ładowania zdalnych arkuszy stylów	126
Gdy wstawiasz do kodu CSS wartości podane przez atakującego	126
Podczas filtrowania stylów CSS podanych przez użytkownika	126
Gdy umieszczasz w znacznikach HTML wartości klas podane przez użytkownika	127

6

SKRYPTY DZIAŁAJĄCE W PRZEGLĄDARCE 129

Podstawowe cechy języka JavaScript	130
Model przetwarzania skryptów	131
Zarządzanie wykonaniem kodu	135
Możliwości badania kodu i obiektów	136
Modyfikowanie środowiska uruchomieniowego	137
JSON i inne metody serializacji danych	139
E4X i inne rozszerzenia składni języka	142
Standardowa hierarchia obiektów	143
Model DOM	145
Dostęp do innych dokumentów	148
Kodowanie znaków w skryptach	149
Tryby dołączania kodu i ryzyko zagnieżdżenia	150
Żywy trup: Visual Basic	152
Ściąga	153
Podczas ładowania zdalnego skryptu	153
Podczas parsowania danych JSON otrzymanych od serwera	153
Gdy umieszczasz dane przesłane przez użytkownika w blokach JavaScriptu	153
Podczas interakcji z obiektami przeglądarki po stronie klienta	154
Jeżeli chcesz pozwolić na działanie skryptów użytkownika na swojej stronie	154

7

DOKUMENTY INNE NIŻ HTML 155

Pliki tekstowe	155
Obrazy bitmapowe	156
Audio i wideo	157
Dokumenty związane z formatem XML	158
Ogólny widok XML	159
Format SVG	160
MathML	161
XUL	161
WML	162
Kanały RSS i Atom	163
Uwaga na temat nierysowanych typów plików	163
Ściąga	165
Udostępniając dokumenty w formacie wywiedzionym z XML	165
W przypadku wszystkich typów dokumentów nie-HTML	165

RYSOWANIE TREŚCI ZA POMOCĄ WTYCZEK PRZEGLĄDARKI	167
Wywoływanie wtyczki	168
Zagrożenia w obsłudze wartości nagłówka Content-Type we wtyczkach	169
Funkcje wspomagające rysowanie dokumentu	171
Platformy aplikacji wykorzystujące wtyczki	172
Adobe Flash	172
Microsoft Silverlight	175
Sun Java	176
XBAP	177
Kontrolki ActiveX	178
Inne wtyczki	179
Ściąga	181
Gdy udostępniasz pliki obsługiwane za pomocą wtyczek	181
Gdy osadzysz w stronach pliki obsługiwane przez wtyczki	181
Jeżeli chcesz napisać nową wtyczkę dla przeglądarek albo kontrolkę ActiveX	182

CZĘŚĆ II: FUNKCJE BEZPIECZEŃSTWA PRZEGLĄDAREK **183**

LOGIKA IZOLACJI TREŚCI	185
Reguła tego samego pochodzenia w modelu DOM	186
document.domain	187
postMessage(...)	188
Interakcje z danymi uwierzytelniającymi	190
Reguła tego samego pochodzenia i API XMLHttpRequest	191
Reguła tego samego pochodzenia w technologii Web Storage	193
Reguły bezpieczeństwa dla ciasteczek	194
Wpływ ciasteczek na regułę tego samego pochodzenia	196
Problemy z ograniczeniami domen	197
Nietypowe zagrożenie wynikające z nazwy „localhost”	198
Ciasteczka i „legalna” kradzież domen	199
Reguły bezpieczeństwa wtyczek	200
Adobe Flash	201
Microsoft Silverlight	204
Java	205
Obsługa dwuznacznego lub nieoczekiwanego pochodzenia	206
Adresy IP	206
Nazwy hostów z dodatkowymi kropkami	207
Nie w pełni kwalifikowane nazwy hostów	207
Pliki lokalne	208
Pseudoadresy URL	209
Rozszerzenia przeglądarek i interfejsu użytkownika	209
Inne zastosowania koncepcji pochodzenia	210

Ściąga	211
Prawidłowa higiena reguł bezpieczeństwa dla wszystkich witryn	211
Gdy używasz ciasteczek HTTP w procesie uwierzytelniania	211
Podczas międzydomenowej komunikacji w skryptach JavaScript	211
Podczas wstawiania na stronę pochodzących z zewnętrznych źródeł aktywnych treści obsługiwanych przez wtyczki	211
Gdy udostępniasz własne treści obsługiwane przez wtyczki	212
Gdy tworzysz własne rozszerzenia dla przeglądarek	212

10

DZIEDZICZENIE POCHODZENIA

213

Dziedziczenie pochodzenia dla stron about:blank	214
Dziedziczenie pochodzenia dla adresów data:	216
Dziedziczenie w przypadku adresów javascript: i vbscript:	218
Uwagi na temat ograniczonych pseudoadresów URL	219
Ściąga	221

11

ŻYCIE OBOK REGUŁY TEGO SAMEGO POCHODZENIA

223

Interakcje z oknami i ramkami	224
Zmiana lokalizacji istniejących dokumentów	224
Mimowolne umieszczanie w ramkach	228
Międzydomenowe wstawianie treści	232
Uwaga do międzydomenowych podzasobów	235
Kanały poboczne wpływające na prywatność	236
Inne luki w regule SOP i sposoby ich wykorzystania	238
Ściąga	239
Prawidłowa higiena bezpieczeństwa dla wszystkich witryn	239
Gdy włączasz na stronę zasoby z innych domen	239
Gdy tworzysz międzydomenową komunikację w skryptach JavaScript	239

12

INNE FUNKCJE BEZPIECZEŃSTWA

241

Nawigowanie do wrażliwych schematów	242
Dostęp do sieci wewnętrznych	243
Porty zakazane	245
Ograniczenia nakładane na ciasteczka stron trzecich	247
Ściąga	250
Podczas tworzenia aplikacji WWW w sieciach wewnętrznych	250
Podczas uruchamiania usług nie-HTTP, w szczególności działających na niestandardowych portach	250
Gdy używasz ciasteczka stron trzecich w różnych gadżetach lub treściach umieszczanych w piaskownicy	250

13		
MECHANIZMY ROZPOZNAWANIA TREŚCI		251
Logika wykrywania rodzaju dokumentu		252
Nieprawidłowe typy MIME		253
Wartości dla specjalnych rodzajów treści		254
Nierozpoznane rodzaje treści		256
Ochronne zastosowanie nagłówka Content-Disposition		258
Dyrektywy Content dotyczące podzasobów		259
Pobrane pliki i inne treści nie-HTTP		260
Obsługa zestawów znaków		262
Znacznik kolejności bajtów		264
Dziedziczenie i pokrywanie zestawu znaków		265
Zestaw znaków przypisany znacznikiem do zasobu		266
Wykrywanie zestawu znaków w plikach przesłanych protokołem innym niż HTTP		267
Ściąga		269
Prawidłowe praktyki bezpieczeństwa dla witryn		269
Gdy generujesz dokumenty zawierające treści kontrolowane przez atakującego		269
Gdy przechowujesz pliki wygenerowane przez użytkownika		269
14		
WALKA ZE ZŁOŚLIWYMI SKRYPTAMI		271
Ataki odmowy świadczenia usługi (DoS)		272
Ograniczenia czasu wykonania i wykorzystania pamięci		273
Ograniczenie liczby połączeń		274
Filtrowanie wyskakujących okienek		275
Ograniczenia użycia okien dialogowych		277
Problemy z wyglądem i pozycją okien		278
Ataki czasowe na interfejs użytkownika		282
Ściąga		285
Gdy umożliwisz umieszczanie na swojej stronie gadżetów użytkownika zamkniętych w ramkach <iframe>		285
Gdy tworzysz bezpieczne interfejsy użytkownika		285
15		
UPRAWNIENIA WITRYN		287
Uprawnienia witryn definiowane w przeglądarkach i wtyczkach		288
Z góry zdefiniowane domeny		289
Menedżery haseł		289
Model stref Internet Explorera		291
Mechanizmy mark of the web i Zone.Identifier		294
Ściąga		296
Gdy żądasz podniesienia uprawnień dla aplikacji WWW		296
Gdy tworzysz wtyczki lub rozszerzenia korzystające z uprzywilejowanego pochodzenia		296

16		
PLANOWANE NOWE FUNKCJE BEZPIECZEŃSTWA		299
Metody rozbudowy modelu bezpieczeństwa		300
Żądania międzydomenowe		300
XDomainRequest		304
Inne zastosowania nagłówka Origin		305
Schematy ograniczeń modelu bezpieczeństwa		306
Reguła bezpieczeństwa treści		307
Ramki w piaskownicy		312
Strict Transport Security		314
Tryby przeglądania prywatnego		316
Pozostałe projekty		316
Porządkowanie kodu HTML w przeglądarce		317
Filtrowanie XSS		318
Ściąga		320
17		
INNE MECHANIZMY PRZEGLĄDAREK		321
Propozycje zmian w adresach URL i protokołach		322
Funkcje na poziomie treści		324
Interfejsy wejścia-wyjścia		326
18		
TYPOWE PODATNOŚCI SIECI WWW		329
Podatności aplikacji WWW		330
Problemy, o których trzeba pamiętać podczas projektowania aplikacji WWW		332
Typowe problemy związane z kodem działającym po stronie serwera		334
EPILOG		337
UWAGI		339
SKOROWIDZ		353