Błędy w aplikacjach internetowych i rodzaje ataków na nie

dr inż. Maciej Miłostan

Przygotowano na podstawie materiałów :

Open Web Application Security Project

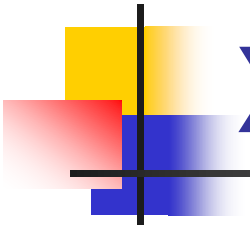
OWASP

- Open Web Application Security Project - Projekt Otwarty dedykowany Bezpieczeństwu Aplikacji Internetowych (Web-owych)
  http://www.owasp.org/index.php/Main_Page

- Projekty i materiały opracowane w ramach OWASP:
  - TOP 10
  - WebGoat
    WebScarab
  - CLASP (Comprehensive, Lightweight Application Security Process)
  - OWASP Legal
  - OWASP Testing Guide

OWASP TOP 10 – najczęstsze błędy i luki w aplikacjach internetowych

- A1 - Cross Site Scripting (XSS)
- A2 - Injection Flaws
- A3 - Malicious File Execution
- A4 - Insecure Direct Object Reference
- A5 - Cross Site Request Forgery (CSRF)
- A6 - Information Leakage and Improper Error Handling
- A7 - Broken Authentication and Session Management
- A8 - Insecure Cryptographic Storage
- A9 - Insecure Communications
- A10 - Failure to Restrict URL Access



XSS

- Cross site scripting (XSS) – jest de facto odmianą ataku typu „HTLM injection” (injekcji kodu HTML). XSS jest najbardziej rozpowrzechnionym i jednym z najgroźniejszych problemów bezpieczeństwa. Błędy XSS zawsze wtedy, gdy aplikacja pobiera dane od użytkownika i bezsprawdzania lub kodowania przesyła spowrotem do przeglądarki.
- Przykład: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4206

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Full-Screen View

CVE-ID

CVE-2006-4206
(under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Cross-site scripting (XSS) vulnerability in calendar.asp in ASPPlayground.NET Forum Advanced Edition 2.4.5 Unicode allows remote attackers to inject arbitrary web script or HTML via the calendarID parameter.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BUGTRAQ:20060811 Forum Software (c) ASPPlayground.NET Advanced Edition 2.4.5 Unicode Xss
- URL:http://www.securityfocus.com/archive/1/archive/1/443035/100/0/threaded
- BID:20335
- URL:http://www.securityfocus.com/bid/20335
- OSVDB:29232
- URL:http://www.osvdb.org/29232
- SREASON:1405
- URL:http://securityreason.com/securityalert/1405
- XF:aspplaygroundnet-calendar-xss(28352)
- URL:http://xforce.iss.net/xforce/xfdb/28352

Status

Candidate

This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.

Injection Flaws

- Błędy umożliwiające injekcję kodu(Injection flaws), np. SQL injection, często występują w aplikacjach Internetowych. Istnieje wiele rodzajów injekcji: SQL, LDAP, XPath, XSLT, HTML, XML, injekcja komend Systemu Operacyjnego i wiele, wiele więcej.
- Przykład kodu, który może być podatny w przypadku niewłaściwej walidacji:
  - *PHP:*
    $sql = "SELECT * FROM table WHERE id = '" . $_REQUEST['id'] . "'";
  - *Java:*
    String query = "SELECT user_id FROM user_data WHERE user_name = '" + req.getParameter("userID") + "' and user_password = '" + req.getParameter("pwd") +"'";
- Przykład: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5121

CVE-ID

CVE-2006-5121
(under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

SQL injection vulnerability in modules/Downloads/admin.php in the Admin section of PostNuke 0.762 allows remote attackers to execute arbitrary SQL commands via the hits parameter.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BUGTRAQ:20060929 Sql injection in PostNuke [Admin section]
- URL:http://www.securityfocus.com/archive/1/archive/1/447361/100/0/threaded
- CONFIRM:http://community.postnuke.com/index.php?name=News&file=article&sid=2783
- BID:20317
- URL:http://www.securityfocus.com/bid/20317
- FRSIRT:ADV-2006-3886
- URL:http://www.frsirt.com/english/advisories/2006/3886
- SECUNIA:22197
- URL:http://secunia.com/advisories/22197
- SREASON:1669
- URL:http://securityreason.com/securityalert/1669
- XF:postnuke-admin-sql-injection(29271)
- URL:http://xforce.iss.net/xforce/xfdb/29271

Status

Candidate

This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.

Phase

Assigned (20061002)

Malicious File Execution

- Błędy polegające na możliwości wykonania kodu ze „złośliwego” pliku (Malicious file execution) są błędami często znajdywanymi w wielu aplikacjach. Deweloperzy często używają potencjalnie nieprzyjazna zawartość, przekazywaną jako dane wejściowe, w funkcjach strumieniowych lub dołączają ją do plików, lub w sposób niewłaściwy ufają przekazywanym z zewnątrz plikom.
- Przykładowa, podatna, konstrukcja:
  - include $_REQUEST['filename’];
- Przykład błędu:
  - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0360

CVE-ID

CVE-2007-0360
(under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

PHP remote file inclusion vulnerability in lang/index.php in Oreon 1.2.3 RC4 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the file parameter.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BUGTRAQ:20070211 Oreon1.2.x Series Exploit Coded
- URL:http://www.securityfocus.com/archive/1/archive/1/459811/100/0/threaded
- MILW0RM:3150
- URL:http://milw0rm.com/exploits/3150
- BID:22107
- URL:http://www.securityfocus.com/bid/22107
- FRSIRT:ADV-2007-0229
- URL:http://www.frsirt.com/english/advisories/2007/0229
- XF:oreon-index-file-include(31568)
- URL:http://xforce.iss.net/xforce/xfdb/31568

Status

Candidate

This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.

Phase

Assigned (20070118)

Insecure Direct Object Reference

- Bezpośrednie odwołanie do obiektu – możliwe w przypadku, gdy deweloper umieścił w kodzie odwołanie do wewnetrznej implementacji aplikacji tj. odwołanie do pliku, katalogu, rekordu lub klucza w bazie danych w postaci URL-a lub parametru formy. Atakujący może modyfikować te parametry w celu uzyskania dostępu do innych obiektów bez autoryzacji, w przypadku gdy aplikacja nie sprawdza praw dostępu.
- Dla przykładu, w aplikacjach Bankowości Elektronicznej (Internetowej), powszechną praktyką jest używanie numerów kont bankowych jako kluczy głównych w relacjach bazy danych. W związku z tym bardzo kuszące jest użycie tych numerów wprost w interfejsie web-owym. Nawet jeśli programista użył sparametryzowanych zapytań SQL, żeby zapobiec „SQL injection", to i tak bez dodatkowego sprawdzania, że użytkownik jest faktycznie właścicielem konta i ma autoryzację do przeglądania konta, atakujący może poprzez modyfikację parametru przechowującego numer konta może przejrzeć lub zmodyfikować zawartość wszystkich kont.
- Ten typ ataku dotknął stronę *Australian Taxation Office's GST Start Up Assistance* w roku 2000, kiedy jeden z użytkowników poprzez modyfikację parametrów uzyskał dostęp do danych 17000 firm, poprzez modyfikację paremetru ABN (a company tax id) zawartego w URLu.
- Przykład:
  <select name="language"><option value="fr">Français</option></select>

  …

  require_once ($_REQUEST['language']."lang.php");

  Powyższy kod może zostać zaatakowany przy użyciu łańcuchów takich jak: "../../../../etc/passwd%00" używając techniki injekcji bajtu zerowego (znaku końca łańcucha) (null byte injection) (zobacz OWASP Guide w celu uzyskania większej liczby informacji) w celu uzyskania dostępu do jakiegokolwiek pliku w systemie plików serwera.

  Inny przykład:

  int cartID = Integer.parseInt(request.getParameter("cartID"));
  String query = "SELECT * FROM table WHERE cartID=" + cartID;
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0329

CVE-ID

CVE-2007-0329
(under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

download.php in Joonas Viljanen JV2 Folder Gallery allows remote attackers to read sensitive files via a relative pathname in the file parameter, as demonstrated by config/gallerysetup.php. NOTE: this issue might be resultant from a directory traversal vulnerability.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MILW0RM:3125
- URL:http://milw0rm.com/exploits/3125
- FRSIRT:ADV-2007-0180
- URL:http://www.frsirt.com/english/advisories/2007/0180
- SECUNIA:23724
- URL:http://secunia.com/advisories/23724

Status

Candidate

This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.

Phase

Assigned (20070117)

Votes

Cross Site Request Forgery (CSRF)

- Cross site request forgery – ten rodzaj ataku nie jest nowością, ale jest prosty i jednocześnie może być bardzo dotkliwy. Atak CSRF polega na zmuszeniu przeglądarki zalogowanego użytkownika, do wysłania żądania do podatnej aplikacji web, która dokonuje wybraną akcję z uprawnieniami ofiary ataku. Ten rodzaj błędów jest powszechnie rowpowszechniony, gdyż wiele aplikacji polegając na automatycznych mechanizmach logowania (sesje, funkcja zapamiętaj mnie, Kerberos token, przekazywanie loginu w żądaniach, źródłowy adres IP itp.) umożliwia przeprowadzenie operacji bez dodatkowej weryfikacji. Niestey obecnie większość aplikacji polega na tych mechanizmach. Rozwiązaniem jest: pozbycie się wszystkich błędów XSS, używanie metody POST zamiast GET i wprowadzenie losowych żetonów/tokenów do każdego URL-a i każdej formy. W przypadku krytycznych transakcji należy użyć re-autentykacji.
- Ten rodzaj ataku jest znany również pod nazwami: Session Riding, One-Click Attacks, Cross Site Reference Forgery, Hostile Linking, and Automation Attack. Akronim XSRF jest również często używany. Organizacje OWASP i MITRE ustandaryzowały nazewnictow na: Cross Site Request Forgery i CSRF.
- Przykład:
  Typowy atak CSRF przeciwko forum może przybrać postać skierowania użytkownika do wywołania pewnej funkcji np. takiej jak wylogowanie z aplikacji. Poniższy znacznik w stronie wyświetlanej przez przeglądarkę ofiary spowoduje wylogowanie go z systemu:
  <img src="http://www.example.com/logout.php">
- Jeżeli bank internetowy pozwala aplikacji przetwarzać żądania takie jak przelewy podobny atak może być możliwy:

  <img src="http://www.example.com/transfer.do?frmAcct=document.form.frmAcct&
  toAcct=4345754&toSWIFTid=434343&amt=3434.43">
- Przykład w CVE:
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0192

CVE-ID

CVE-2007-0192
(under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Cross-site request forgery (CSRF) vulnerability in the save_main operation in the ad_perms section in admin.php in MKPortal allows remote attackers to modify privilege settings, as demonstrated using a getURL of admin.php within a .swf file contained in an IFRAME element, aka the "All Guests are Admin" attack.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BUGTRAQ:20070104 MkPortal "All Guests are Admin" Exploit
- URL:http://www.securityfocus.com/archive/1/archive/1/455894/100/100/threaded
- SREASON:2137
- URL:http://securityreason.com/securityalert/2137

Status

Candidate

This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.

Phase

Assigned (20070110)

Votes

Comments

Candidate assigned on 20070110 and proposed on N/A

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.

FOR MORE INFORMATION: cve@mitre.org

Information Leakage and Improper Error Handling

- Aplikacje mogą, w wyniku problemów i błędów w funkcjonowaniu, w sposób niezamierzony udostępniać informacje o swojej konfiguracji, wewnętrznym sposobie działania, lub naruszać prywatność. Aplikacje mogą również udostępniać informacje o swoim stanie wewnętrznym poprzez różnice w czasie wykonywania niektórych operacji lub poprzez różne sposoby odpowiedzi na różne dane wejściowe np. poprzez wyświetlanie tych samych komunikatów, ale z różnymi numerami błędów. Aplikacje web-owe często prezentują informacje o swoim wewnętrznym stanie poprzez szczegółowe komunikaty o błędach lub informacje służące „debug-owaniu”. Często te informacje mogą posłużyć do przygotowania odpowiednio spreparowanego ataku, albo nawet zautomatyzować bardzo poważny, szeroko zakrojony atak.
- Przykład:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4899

CVE-ID

CVE-2006-4899
(under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The ePPIServlet script in Computer Associates (CA) eTrust Security Command Center 1.0 and r8 up to SP1 CR2, when running on Windows, allows remote attackers to obtain the web server path via a "'" (single quote) in the PIProfile function, which leaks the path in an error message.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

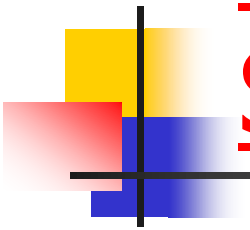
- BUGTRAQ:20060921 [CAID 34616, 34617, 34618]: CA eSCC and eTrust Audit vulnerabilities
- URL:http://www.securityfocus.com/archive/1/archive/1/446611/100/0/threaded
- BUGTRAQ:20060922 RE: Computer Associates eTrust Security Command Center Multiple Vulnerabilities
- URL:http://www.securityfocus.com/archive/1/archive/1/446716/100/0/threaded
- MISC:http://users.tpg.com.au/adsl2dvp/advisories/200608-computerassociates.txt
- CONFIRM:http://www3.ca.com/securityadvisor/blogs/posting.aspx?id=90744&pid=93243&date=2006/9
- CONFIRM:http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=34616
- BID:20139
- URL:http://www.securityfocus.com/bid/20139
- FRSIRT:ADV-2006-3738
- URL:http://www.frsirt.com/english/advisories/2006/3738
- OSVDB:29009
- URL:http://www.osvdb.org/29009
- SECTRACK:1016910
- URL:http://securitytracker.com/id?1016910
- SECUNIA:22023
- URL:http://secunia.com/advisories/22023
- XF:ca-etrust-eppiservlet-path-disclosure(29102)
- URL:http://xforce.iss.net/xforce/xfdb/29102

Status

Candidate

This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.

Broken Authentication and Session Management



- Właściwa uwierzytelnieni i zarządzanie sesją jest krytyczne w zapewnianiu bezpieczeństwa aplikacji internetowych. Błędy w tych obszarach bardzo często prowadzą do problemów z ochroną uprawnień (credentials) i identyfikatorów sesji, które powinny podlegać ścisłej ochronie w okresie całego cyklu ich użytkowania. Te błędy mogą prowadzić do przejęcia konta użytkownika bądź administratora, naruszenia mechanizmów autoryzacji i kontroli kont, oraz naruszenia polityk prywatności.
- Przykład: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6145

Insecure Cryptographic Storage

- Ochrona tzw. danych wrażliwych przy użyciu mechanizmów kryptograficznych stała się nieodzownym, wręcz kluczowym elementem większości aplikacji internetowych. Jednakże błędy polegające na nieszyfrowaniu tych danych są dość powszechne. Natomiast aplikacje, które szyfrują te dane często robią to w sposób niewłaściwy, tzn. wykorzystują słabe algorytmy kryptograficzne, niewłaściwe zaprojektowane algorytmy, lub w przypadku stosowania silnych algorytmów w niewłaściwy sposób się nimi posługują (np. w zły sposób generują klucze). Powyższe błędy mogą prowadzić do ujawniania poufnych danych i naruszenie zgodności z przyjętą polityką lub przepisami prawa.
- Przykład: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6145

CVE-ID

CVE-2006-6145
(under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

CRYPTOCard CRYPTO-Server before 6.4.56 stores LDAP credentials in plaintext in UninstallerData\installvariables.properties, which has insecure permissions and allows local users to obtain the credentials. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:21305
- URL:http://www.securityfocus.com/bid/21305
- FRSIRT:ADV-2006-4710
- URL:http://www.frsirt.com/english/advisories/2006/4710
- SECUNIA:22138
- URL:http://secunia.com/advisories/22138
- XF:crypto-ldap-information-disclosure(30557)
- URL:http://xforce.iss.net/xforce/xfdb/30557

Status

Candidate

This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.

Phase

Assigned (20061128)

Insecure Communications

- Aplikacje często nie szyfrują ruchu sieciowego zawierającego sensytywne dane. Szyfrowanie (ang. Encryption, zwykle SSL) musi być używane do wszystkich uwierzytelnionych połączeń, w szczególności w przypadku dostępu do stron dostępnych z Internetu, jak również w przypadku połączeń końcowcyh po stronie serwera. W przeciwnym razie aplikacja może ujawnić osobom postronnym (przechwytującym ruch) infromacje uwierzytelniając (hasla, nazwy uzytkownikow) lub identyfikatory i dane sesji. Dodatkowo, szyfroawnie powinno być używane w każdym przypadku przesyłania danych sensytywnych, takich jak numery kart kredytowych lub informacje zdrowotne. Aplikacje, które mogą być zmuszone do zaniechania szyfrowania mogą zostać naruszone przez atakującego.
- Standard PCI wymaga, by wszystkie dane zawierające informacje o karta kredytowych były szyfrowane na czas przesyłania przez sieć Internet.
- Przykłady:
  http://www.schneier.com/blog/archives/2005/10/scandinavian_at_1.html
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6430

CVE-ID

CVE-2006-6430
(under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Web services in Xerox WorkCentre and WorkCentre Pro before 12.060.17.000, 13.x before 13.060.17.000, and 14.x before 14.060.17.000 do not require HTTPS, which allows remote attackers to obtain sensitive information by sniffing the unencrypted HTTP traffic.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:http://www.xerox.com/downloads/usa/en/c/cert_XRX06_006_v1b.pdf
- BID:21365
- URL:http://www.securityfocus.com/bid/21365
- FRSIRT:ADV-2006-4791
- URL:http://www.frsirt.com/english/advisories/2006/4791
- SECUNIA:23265
- URL:http://secunia.com/advisories/23265
- XF:xerox-https-security-bypass(30679)
- URL:http://xforce.iss.net/xforce/xfdb/30679

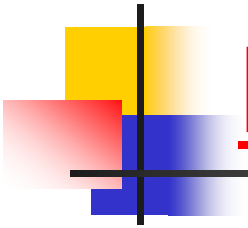
Status

Candidate

This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.

Phase

Assigned (20061209)



Failure to Restrict URL Access

- Częstokroć jedynym zabezpieczeniem dostępu do jakiejś strony jest nieudostępnianie linku (URL-a) do niej nieautoryzowanym użytkownikom. Tzn. do samej strony może dostać się każdy, kto zgadnie jej URL lub ustali go w bardziej wyrafinowany sposób. (Security by obscurity is not sufficient to protect sensitive functions and data in an application.) Kontrola dostępu powinna się odbywać zawsze przed przyznaniem dostępu do wrażliwych funkcji. Takowa kontrola powinna zapewniać, że użytkownik jest faktycznie uprawniony do wykonania tej funkcji.
- Przykład: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0147

CVE-ID

CVE-2007-0147
(under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Cuyahoga before 1.0.1 installs the FCKEditor component with an incorrect deny statement in a Web.config file, which allows remote attackers to upload files when these privileges were intended only for the Administrator and Editor roles.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:http://www.cuyahoga-project.org/10/section.aspx/61
- CONFIRM:http://cuyahoga.svn.sourceforge.net/viewvc/cuyahoga?view=rev&revision=551
- BID:21927
- URL:http://www.securityfocus.com/bid/21927
- SECUNIA:23662
- URL:http://secunia.com/advisories/23662

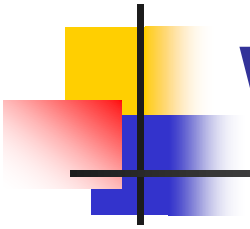
Status

Candidate

This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.

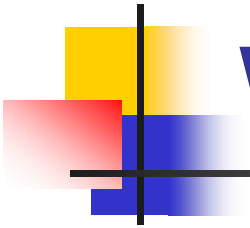
Phase

Assigned (20070109)



WebScarab

http://sourceforge.net/project/showfiles.php?group_id=64424&package_id=61823



WebGoat

http://code.google.com/p/webgoat/downloads/list

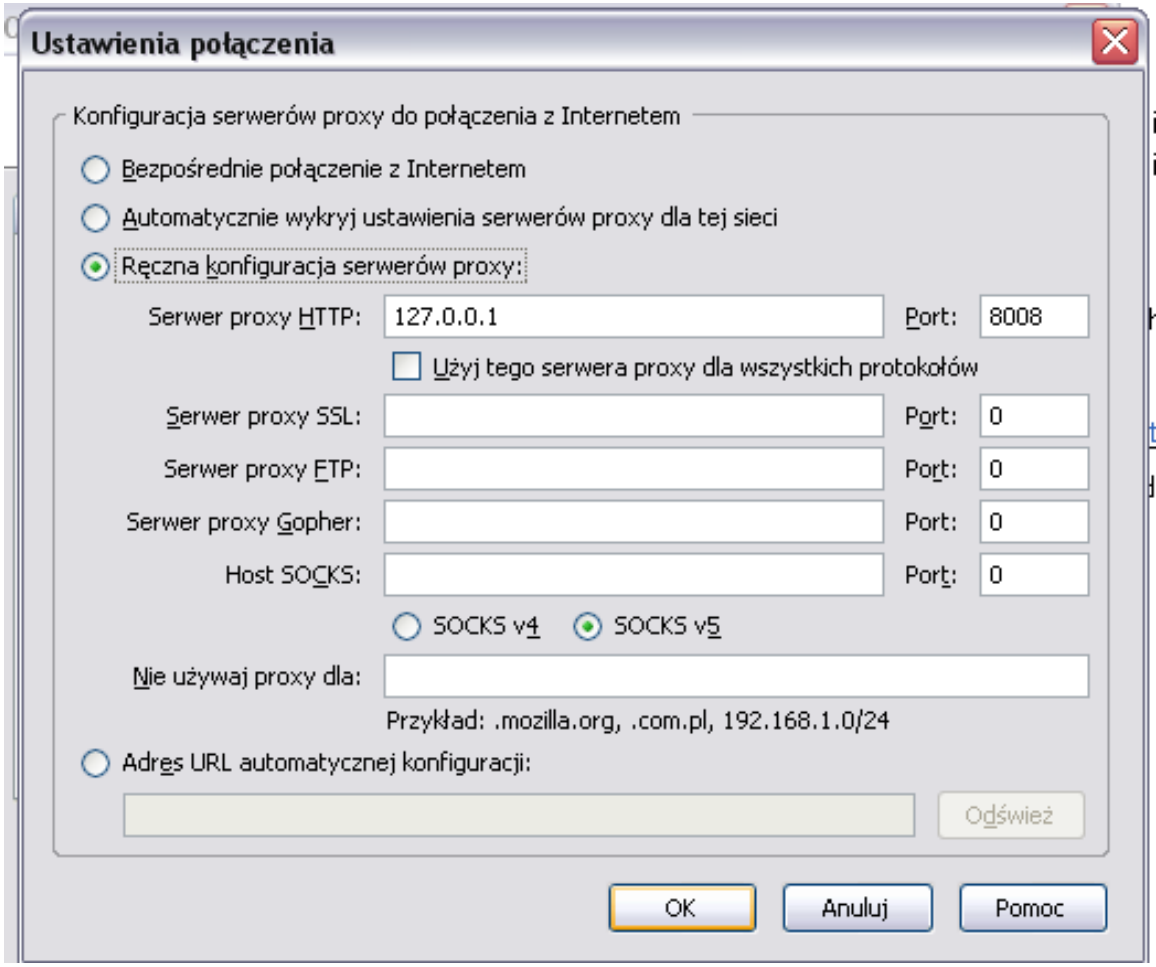
Ćwiczenia praktyczne

- Pobierz WebGoat-a
- Uruchom WebGoat
  - Rozpakuj pobrany plik zip
  - Przejdź do podkatalogu:
    - WebGoat-OWASP_Standard-5.1\WebGoat-5.1
  - Kliknij webgoat.bat
- Sprawdź, czy WebGoat działa:
  - http://localhost/WebGoat/attack

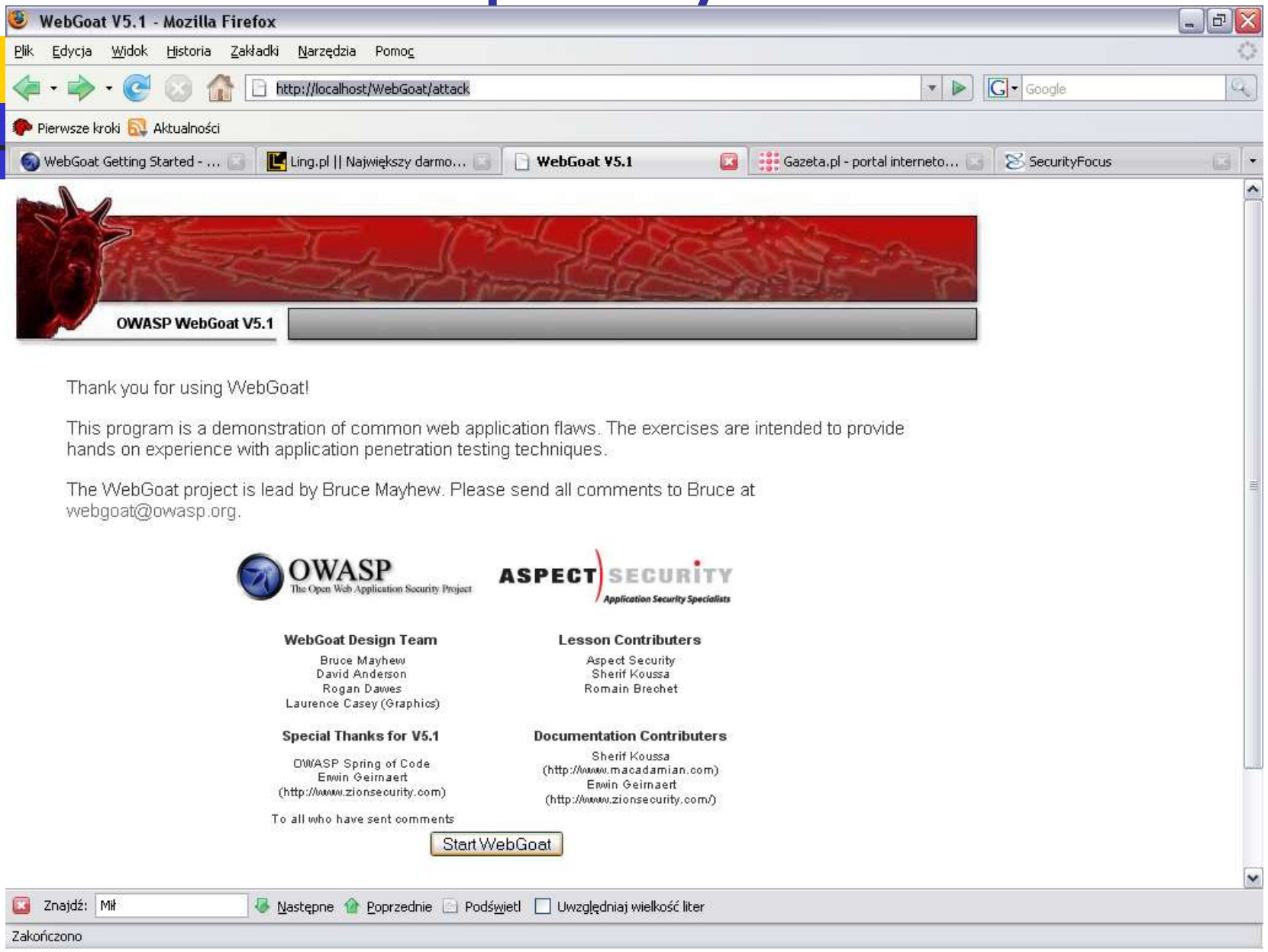
  Użytkownik:guest hasło:guest
- Pobierz WebScarab-a
- Uruchom WebScarab-a

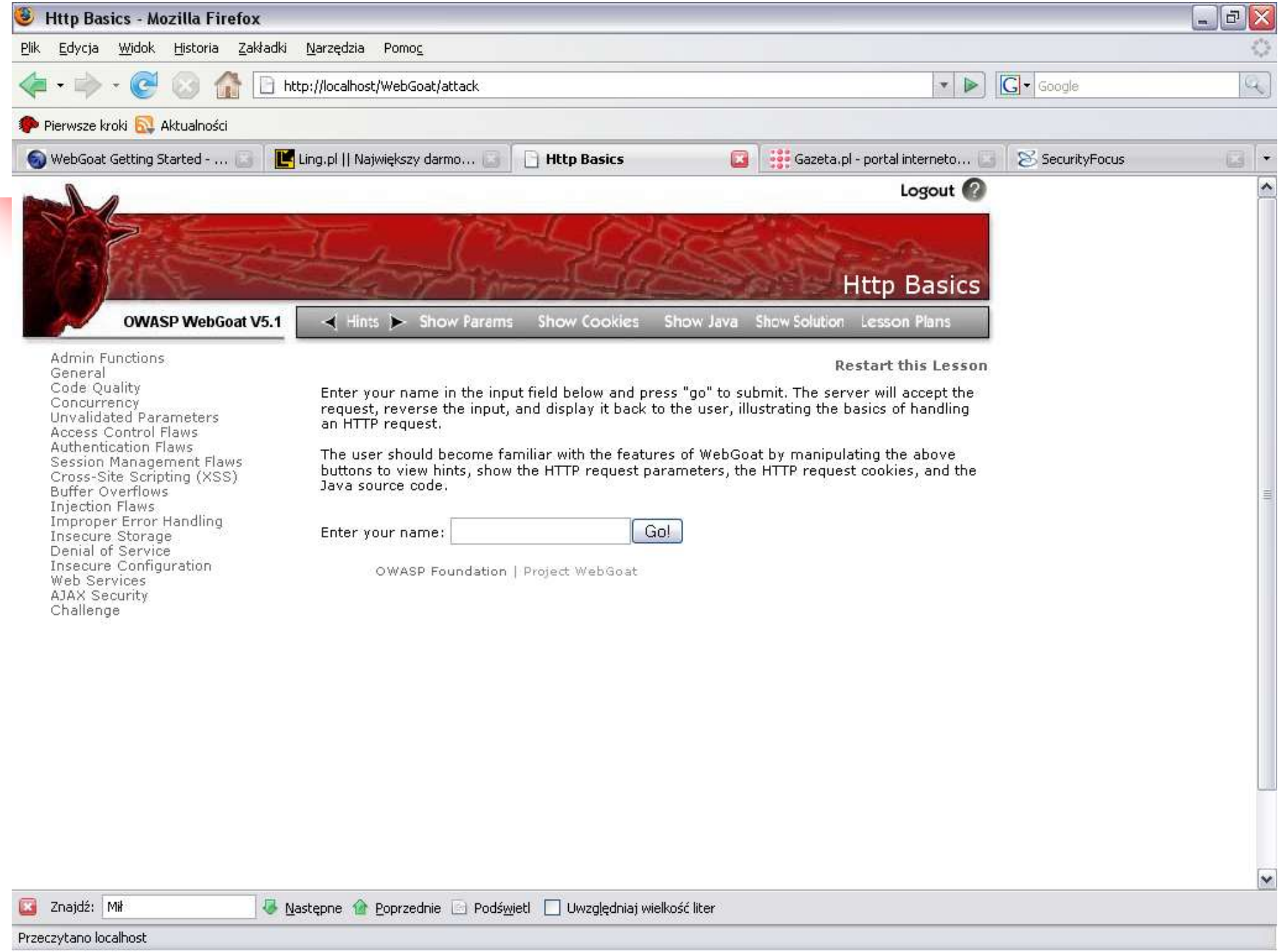
Ćwiczenia praktyczne

- Ustaw proxy w przeglądarce, by wszystkie żądania przechodziły przez WebScarab-a:
  - W Firefoxie:
    - Narzędzia-> Opcje-> Zaawansowane-> Sieć->Ustawienia



Ćwiczenia praktyczne




Http Basics - Mozilla Firefox
Plik Edycja Widok Historia Zakładki Narzędzia Pomoc
http://localhost/WebGoat/attack
Google
Pierwsze kroki Aktualności
WebGoat Getting Started - ...
Ling.pl || Największy darmo...
Http Basics
Gazeta.pl - portal interneto...
SecurityFocus
Logout
Http Basics
OWASP WebGoat V5.1
Hints Show Params Show Cookies Show Java Show Solution Lesson Plans
Admin Functions
General
Code Quality
Concurrency
Unvalidated Parameters
Access Control Flaws
Authentication Flaws
Session Management Flaws
Cross-Site Scripting (XSS)
Buffer Overflows
Injection Flaws
Improper Error Handling
Insecure Storage
Denial of Service
Insecure Configuration
Web Services
AJAX Security
Challenge
Restart this Lesson
Enter your name in the input field below and press "go" to submit. The server will accept the request, reverse the input, and display it back to the user, illustrating the basics of handling an HTTP request.
The user should become familiar with the features of WebGoat by manipulating the above buttons to view hints, show the HTTP request parameters, the HTTP request cookies, and the Java source code.
Enter your name:
Go!
OWASP Foundation | Project WebGoat
Znajdź: Mił
Następne Poprzednie Podświetl Uwzględniaj wielkość liter
Przeczytano localhost