



ISACA Finland 24.1.2008

Timo Meriläinen
Antti Laulajainen

OWASP

24.1.2008

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org>

Agenda 24.1.2008 14:00 -

- Esittelyt
- Johdanto
- Mikä on OWASP
- OWASP projektien esittelyä
- OWASP Finland
- Muita tarkastajan kannalta mielenkiintoisia Open Source tietoturvaprojekteja
- Kysymyksiä & Keskustelua

Esittelyt

■ Timo Meriläinen, CISA, CISSP

- ▶ 1985 – 2001 Erilaisia ATK-tehtäviä
- ▶ 2001 – 2007 Tietojärjestelmätarkastus ja tietoturvallisuuden asiantuntijatehtävät
- ▶ 2007- Tietoturva-arkkitehti

■ Antti Laulajainen, CISSP

- ▶ 1999-2003 Infrastruktuuriasiantuntija, käyttöjärjestelmän tietoturva
- ▶ 2004-2007 Järjestelmäarkkitehti, Tietoturva konsultoinnit ja suunnitelutehtävät käyttöjärjestelmille
- ▶ 2007- Tietoturvakonsultti, Sovellustietoturva ja kehitystehtävät

Johdanto

- Muutama sana www-sovelluksista
- Tarkastajan näkökulma www-sovellukseen

Muutama sana www-sovelluksista 1

- Perusmallina asiakas/palvelin-malli, jossa
 - ▶ asiakkaana yleensä käyttäjän www-selain
 - ▶ palvelimena www-palvelin ja sen takana olevat sovellus- ja tietokantapalvelimet ja integraatiokerrokset
- Samaa tekniikkaa voidaan käyttää myös sovellusten välillä (webservices)

ISACA kotisivu - esimerkki

The screenshot shows a Mozilla Firefox browser window displaying the ISACA Finland website. The browser's address bar shows the URL <http://www.isaca.fi/>. The website has a header with navigation links: [lähetä artikkeli](#), [laajennettu etsintä](#), [sivuston tilastot](#), and [My Downloads](#). The main content area features the ISACA logo and a banner that reads "Tervetuloa yhdistyksemme sivuille". Below the banner, there is a sidebar with the text "Liity Jäseneksi!" and a main content area with the text "Liity joukkoomme! Katso lisätietoja toiminnastamme. Jäseneksi voit liittyä ottamalla yhteyttä yhdistyksen toimistoon. Näille sivuille rekisteröitymisen voit aloittaa tästä."

Overlaid on the bottom right of the browser window is a Wireshark packet capture window. The filter is set to "ip". The packet list shows a series of TCP and HTTP packets. The packet details pane shows the structure of a packet, including Ethernet II, Internet Protocol, User Datagram Protocol, and NetBIOS Datagram Service. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Done

Muutama sana www-sovelluksista 2

- “On vain kahdenlaisia www-sivuja”
 - ▶ Niitä, jotka ovat olemassa (staattiset sivut)
 - ▶ Ja niitä, jotka jokin ohjelma tekee lennossa (dynaamiset sivut)
- www-sivujen dynaamiset osat voidaan toteuttaa
 - ▶ Palvelimella
 - ▶ Selaimessa
- Selain tulkitsee palvelimen lähettämän HTML-koodin laajennuksineen (CSS-tyylitiedot, Javascript) käyttäjälle näytettäväksi käyttöliittymäksi

Muutama sana www-sovelluksista 3

- Palvelimilla lukuisia eri tapoja ja kieliä käytettävissä
 - ▶ cgi-bin
 - ▶ Microsoft ASP.Net
 - ▶ Java J2EE JSP, servletit
 - ▶ PHP, Ruby, etc.
- Selaimessa toiminnallisuuksiin voidaan käyttää
 - ▶ Selaimen tukemia scriptikieliä (Javascript, VBScript)
 - ▶ Active-X komponentteja (IE-selaimet)
 - ▶ Java appletteja (selaimessa Java Runtime tuki)
 - ▶ AJAX (JavaScript + XML) -tekniikka

Muutama sana www-sovelluksista 4

- Selaimen (tai muun asiakasohjelma) ja palvelimen välisessä tietoliikenteessä protokollona yleensä
 - ▶ http – tiedot siirretään selväkielisenä
 - ▶ https – tiedot suojataan salauksella
- http(s) on tilaton protokolla, joten käyttäjän istuntotietoa on välitettävä jollain tavalla selaimen ja palvelimen välillä. Tapoina esim.
 - ▶ Evästeessä (Cookie) oleva istuntotunnus
 - ▶ Istuntotunnus osa selaimen lähettämää URL-osoitetta
 - ▶ Muu, sovellustasolla toteutettu tapa

Cookie esimerkki

WebScarab - conversation 18

Previous Next 18 - GET http://www.isaca.org:80/Graphics/ACF9E46.gif 200 OK

Parsed Raw

Method URL Version

GET http://www.isaca.org:80/HierMenu/HM_ScriptDOM.js HTTP/1.1

Header	Value
Host	www.isaca.org
User-Agent	Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.11) Gecko/20071204 Ubuntu/7.10 (gutsy) Firefox/2.0.0.11
Accept	*/*
Accept-Language	en-us,en;q=0.5
Accept-Encoding	gzip,deflate
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive	300
Proxy-Connection	keep-alive
Referer	http://www.isaca.org/
Cookie	CFID=14467769; CFTOKEN=17b0327%2D74f2655e%2D94bc%2D4d93%2D8b12%2D76b64fcc2ec8; HASCOOKIES=true

Hex

Position 0 1 2 3 4 5 6 7 8 9 A B C D E F String

Parsed Raw

Version Status Message

HTTP/1.1 200 OK

Header	Value
Content-length	45576
Content-Type	application/x-javascript
Last-Modified	Wed, 07 May 2003 19:07:06 GMT
Accept-Ranges	bytes
ETag	"0e9b5d9cb14c312cf"
Server	Microsoft-IIS/6.0

Text Hex



Tarkastajan näkökulma 1

- **www-sovelluksessa useita eri kerroksia**
 - ▶ www-käyttöliittymä
 - ▶ sovelluspalvelin- ja tietokantataso
 - ▶ integraatio taustajärjestelmiin
- **Näiden lisäksi myös**
 - ▶ Palvelinten perusturvallisuus (kovennot)
 - ▶ Tietoliikenne
 - ▶ Seuranta ja valvonta, varmistukset
 - ▶ Sekä ympäristön hallinnollinen tietoturva
 - Muutoshallinta
 - Käyttövaltuuksien hallinta
 - Haavoittuvuuksien hallinta (päivitykset)

Tarkastajan näkökulma 2

- Haavoittuvuuksia ja konfigurointivirheitä voi olla
 - ▶ Sovellusta suojaavissa verkkokomponenteissa (palomuurit, kuormantasaajat, reitittimet ja kytkimet)
 - ▶ Sovelluksen palvelinalustassa (www-palvelin, proxyt)
 - ▶ Itse sovelluksessa
- Haavoittuvuuksien vakavuus
 - ▶ WWW-käyttöliittymässä olevat haavoittuvuudet ovat kaikkien palveluun pääsevien ulottuvilla
 - ▶ Muiden tasojen haavoittuvuuksien hyväksikäyttö edellyttää yleensä pääsyä tuotantoympäristön sisään

Tarkastajan näkökulma 3

■ “Hyökkääjä hallitsee selainta”

- ▶ Internet sovelluksissa oletuksena on se, että käyttäjä hallitsee täysin oman työasemaympäristön ja selaimen
- ▶ Erilaisilla työkaluilla voidaan simuloida selainta testaus- ja murtotarkoituksissa
- ▶ Selaimeen ladattavat scriptit, appletit ja komponentit voidaan analysoida ja näitä voidaan muuttaa
- ▶ Sisäverkossa työaseman selainta voidaan yrittää kontrolloida tiukemmin, mutta tällöin keskeistä yleensä ympäristön muiden kontrollien toimivuus

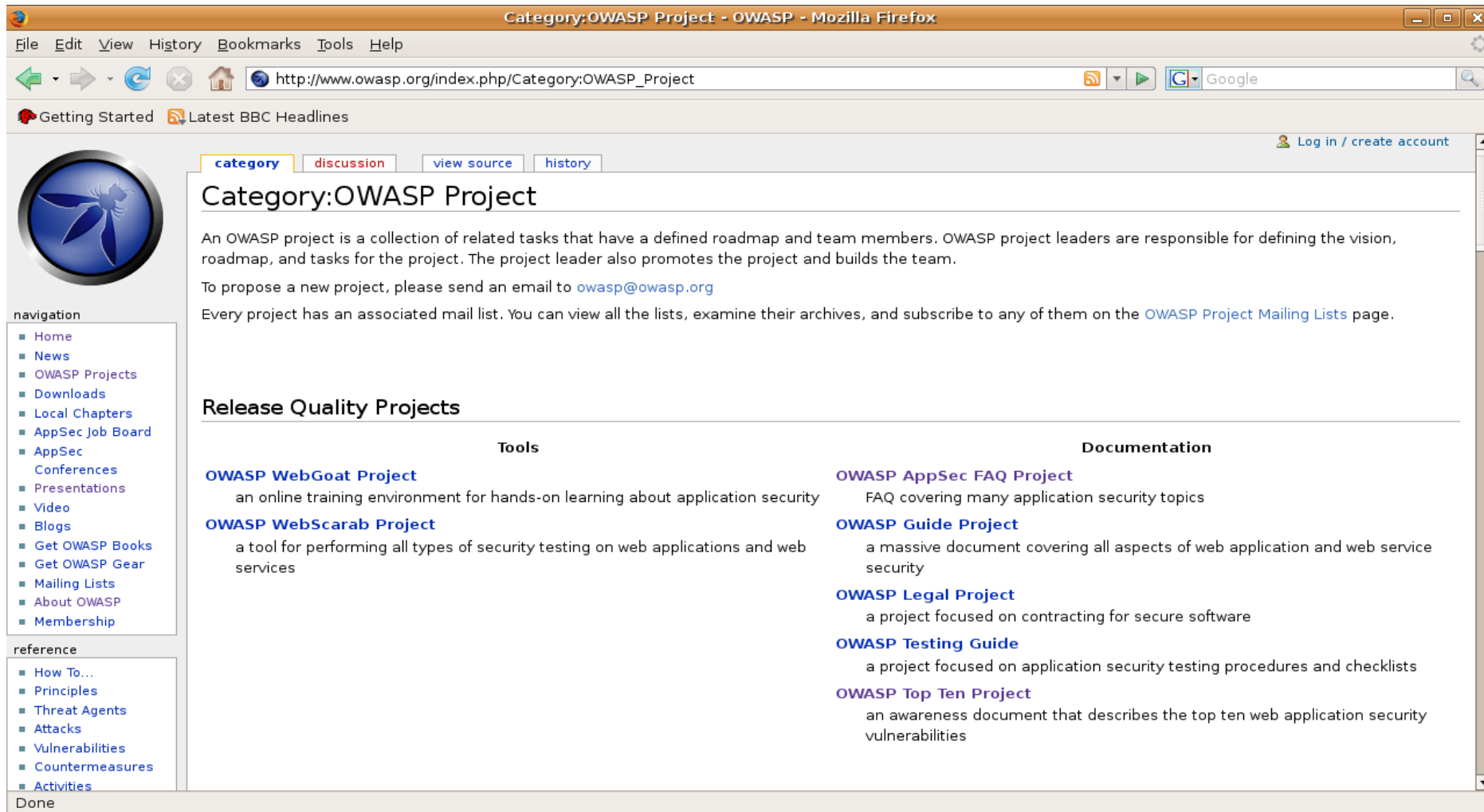
Mikä on OWASP

- OWASP taustaa
- Joitain OWASP-projekteja ja dokumentteja
- OWASP Helsinki Chapter

OWASP taustaa

- WWW-sovellusten tietoturvallisuuden keskittyvä OpenSource -yhteisö
- Perustettu maailmalla 2000-luvun alkupuoliskolla
- Toiminta
 - ▶ erilaisissa projekteissa
 - ▶ paikallisissa yhteisöissä (Chapter)
- Paikallista toimintaa eri puolilla maailmaa, myös Suomessa

OWASP Projektien kotisivu



The screenshot shows a Mozilla Firefox browser window with the title "Category:OWASP Project - OWASP - Mozilla Firefox". The address bar displays the URL "http://www.owasp.org/index.php/Category:OWASP_Project". The browser's menu bar includes "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help". The toolbar contains navigation buttons (back, forward, home, search) and a search bar with the text "Google". Below the toolbar, there are links for "Getting Started" and "Latest BBC Headlines". The main content area is titled "Category:OWASP Project" and includes a description of OWASP projects, a link to propose a new project, and a link to view all project mail lists. The left sidebar contains a "navigation" section with links to Home, News, OWASP Projects, Downloads, Local Chapters, AppSec Job Board, AppSec Conferences, Presentations, Video, Blogs, Get OWASP Books, Get OWASP Gear, Mailing Lists, About OWASP, and Membership. Below this is a "reference" section with links to How To..., Principles, Threat Agents, Attacks, Vulnerabilities, Countermeasures, and Activities. The main content area also features a "Release Quality Projects" section with two columns: "Tools" and "Documentation". The "Tools" column lists "OWASP WebGoat Project" and "OWASP WebScarab Project". The "Documentation" column lists "OWASP AppSec FAQ Project", "OWASP Guide Project", "OWASP Legal Project", "OWASP Testing Guide", and "OWASP Top Ten Project".

Category:OWASP Project

An OWASP project is a collection of related tasks that have a defined roadmap and team members. OWASP project leaders are responsible for defining the vision, roadmap, and tasks for the project. The project leader also promotes the project and builds the team.

To propose a new project, please send an email to owasp@owasp.org

Every project has an associated mail list. You can view all the lists, examine their archives, and subscribe to any of them on the [OWASP Project Mailing Lists](#) page.

Release Quality Projects

Tools	Documentation
OWASP WebGoat Project an online training environment for hands-on learning about application security	OWASP AppSec FAQ Project FAQ covering many application security topics
OWASP WebScarab Project a tool for performing all types of security testing on web applications and web services	OWASP Guide Project a massive document covering all aspects of web application and web service security
	OWASP Legal Project a project focused on contracting for secure software
	OWASP Testing Guide a project focused on application security testing procedures and checklists
	OWASP Top Ten Project an awareness document that describes the top ten web application security vulnerabilities

OWASP Projekteja

■ Dokumentit ja oppaat

- ▶ OWASP Top Ten Project
- ▶ OWASP AppSec FAQ Project
- ▶ OWASP Guide Project
- ▶ OWASP Testing Guide
- ▶ OWASP CLASP

■ Työkalut

- ▶ OWASP WebScarab Project
- ▶ OWASP WebGoat Project

■ Näiden lisäksi myös muita projekteja

OWASP TOP TEN (2007)

Top 10 2007 - OWASP - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.owasp.org/index.php/Top_10_2007#Summary

Getting Started Latest BBC Headlines

- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link

Summary

A1 - Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.
A2 - Injection Flaws	Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
A3 - Malicious File Execution	Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.
A4 - Insecure Direct Object Reference	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
A5 - Cross Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.
A6 - Information Leakage and Improper Error Handling	Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.
A7 - Broken Authentication and Session Management	Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.
A8 - Insecure Cryptographic Storage	Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
A9 - Insecure Communications	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
A10 - Failure to Restrict URL Access	Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

Table 1: Top 10 Web application vulnerabilities for 2007

Done



OWASP Application Security FAQ

OWASP Application Security FAQ - OWASP - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.owasp.org/index.php/OWASP_AppSec_FAQ

Getting Started Latest BBC Headlines

Log in / create account

article discussion view source history

OWASP Application Security FAQ

(Redirected from [OWASP AppSec FAQ](#))

Contents [\[hide\]](#)

- 1 Login Issues
 - 1.1 What are the best practices I should remember while designing the login pages?
 - 1.2 Is it really required to redirect the user to a new page after login?
 - 1.3 How does the salted MD5 technique work?
 - 1.4 How can my "Forgot Password" feature be exploited?
 - 1.5 In "Forgot Password", is it safe to display the old password?
 - 1.6 Is there any risk in emailing the new password to the user's authorized mail id?
 - 1.7 What is the most secure way to design the Forgot Password feature?
 - 1.8 How do I protect against automated password guessing attacks?
 - 1.9 How can I protect against keystroke loggers on the client machine?
 - 1.10 My site will be used from publicly shared computers. What precautions must I take?
- 2 SQL Injection
 - 2.1 What is SQL Injection?
 - 2.2 Is it just ASP and SQL Server or are all platforms vulnerable?
 - 2.3 Apart from username and password which variables are candidates for SQL Injection?
 - 2.4 How do we prevent SQL Injection in our applications?
 - 2.5 I'm using stored procedures for authentication, am I vulnerable?
 - 2.6 I'm using client side JavaScript code for checking user input. Isn't that enough?
 - 2.7 Are java servlets vulnerable to SQL injection?
 - 2.8 Can an automated scanner discover SQL Injection?
- 3 Variable Manipulation
 - 3.1 Why can't I trust the information coming from the browser?
 - 3.2 What information can be manipulated by the attacker?
 - 3.3 How do attackers manipulate the information? What tools do they use?
 - 3.4 I'm using SSL. Can attackers still modify information?

navigation

- Home
- News
- OWASP Projects
- Downloads
- Local Chapters
- AppSec Job Board
- AppSec
 - Conferences
- Presentations
- Video
- Blogs
- Get OWASP Books
- Get OWASP Gear
- Mailing Lists
- About OWASP
- Membership

reference

- How To...
- Principles
- Threat Agents
- Attacks
- Vulnerabilities
- Countermeasures
- Activities

Done



OWASP Guide ja Testing guide

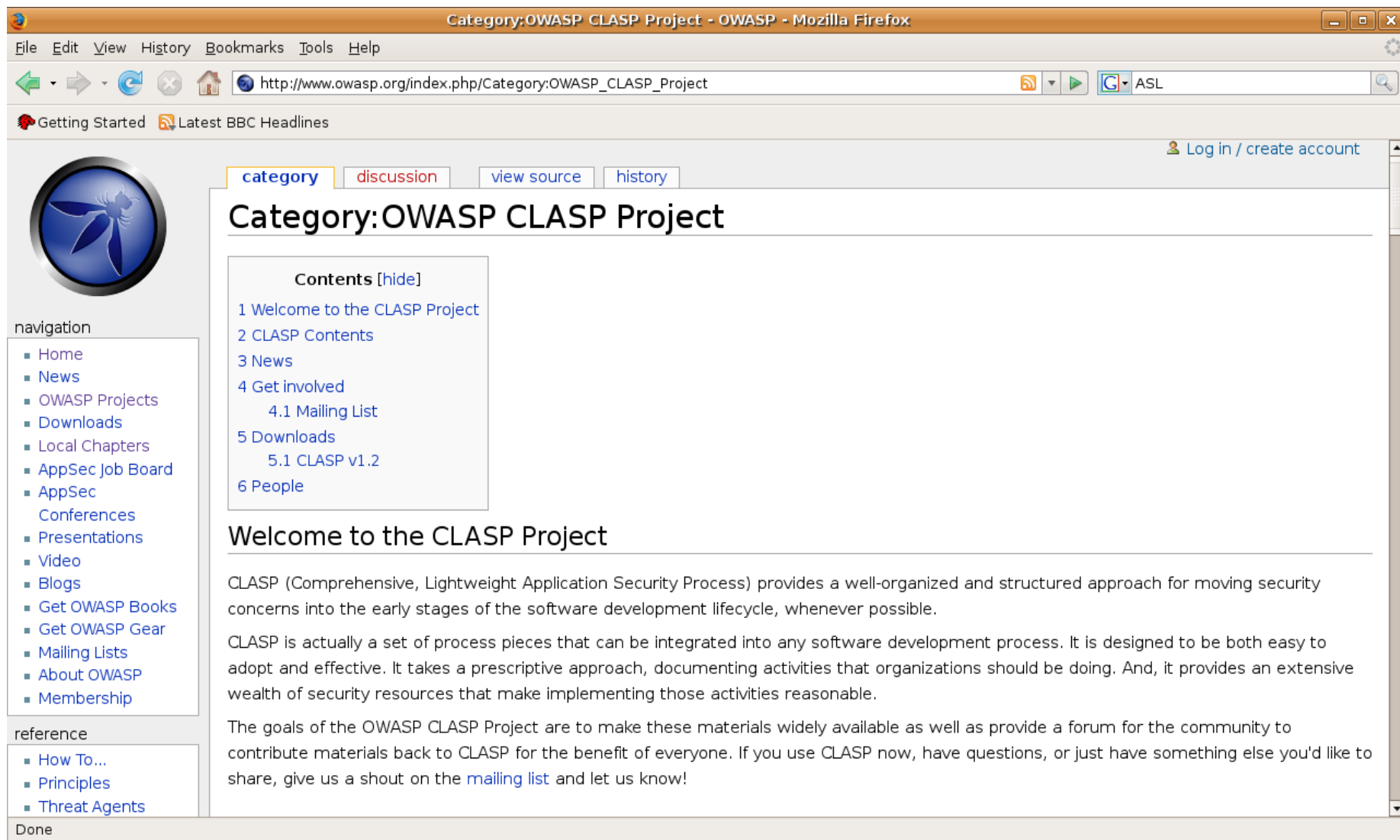
■ Guide

- ▶ sovelluskehittäjille ja arkkitehteille tarkoitettu opas
- ▶ PDF-versio ladattavissa OWASP:in sivuilta
- ▶ Saatavana myös kirjana

■ Testing guide

- ▶ www-sovellusten tietoturvallisuuden testaajille tarkoitettu tekninen opas
- ▶ PDF-versio ladattavissa OWASP:in sivuilta
- ▶ Saatavana myös kirjana

OWASP CLASP



The screenshot shows a Mozilla Firefox browser window with the title "Category:OWASP CLASP Project - OWASP - Mozilla Firefox". The address bar shows the URL "http://www.owasp.org/index.php/Category:OWASP_CLASP_Project". The page content includes a navigation menu on the left, a main content area with tabs for "category", "discussion", "view source", and "history", and a "Contents" section with a list of links. The main content area also features a "Welcome to the CLASP Project" section with a paragraph of text and a "reference" section with a list of links.

Category:OWASP CLASP Project - OWASP - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.owasp.org/index.php/Category:OWASP_CLASP_Project

Getting Started Latest BBC Headlines

Log in / create account

category discussion view source history

Category:OWASP CLASP Project

Contents [hide]

- 1 Welcome to the CLASP Project
- 2 CLASP Contents
- 3 News
- 4 Get involved
 - 4.1 Mailing List
- 5 Downloads
 - 5.1 CLASP v1.2
- 6 People

Welcome to the CLASP Project

CLASP (Comprehensive, Lightweight Application Security Process) provides a well-organized and structured approach for moving security concerns into the early stages of the software development lifecycle, whenever possible.

CLASP is actually a set of process pieces that can be integrated into any software development process. It is designed to be both easy to adopt and effective. It takes a prescriptive approach, documenting activities that organizations should be doing. And, it provides an extensive wealth of security resources that make implementing those activities reasonable.

The goals of the OWASP CLASP Project are to make these materials widely available as well as provide a forum for the community to contribute materials back to CLASP for the benefit of everyone. If you use CLASP now, have questions, or just have something else you'd like to share, give us a shout on the [mailing list](#) and let us know!

reference

- How To...
- Principles
- Threat Agents

Done



OWASP WebScarab

- Käyttäjän työasemassa käytettävä välityspalvelinohjelmisto (Proxy)
- Web-testaajan “McGywer veitsi”
- Mahdollistaa mm.
 - ▶ Selaimen ja www-palvelimen välisen tietoliikenteen analysoinnin ja muokkaamisen
 - ▶ Cookie-tietojen analysointi ja muokkaus
 - ▶ www-palvelimen hakemistorakenteen analysoinnin
 - ▶ www-sivuilla olevien scriptien ja kommenttien analysoinnin

WebScarab – esimerkki 1

WebScarab

File View Tools Help

Summary Messages Proxy Manual Request WebServices Spider Extensions XSS/CRLF SessionID Analysis Scripted Fragments Fuzzer Compare Search

☐ Tree Selection filters conversation list

Url	Methods	Status	Possible In...	Injection	Set-Cookie	Comments	Scripts
http://www.googleadservices.com:80/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
http://www.isaca.fi:80/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
http://www.isaca.org:80/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
https://ssl.google-analytics.com:443/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
https://statse.webtrendslive.com:443/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
https://www.googleadservices.com:443/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
https://www.isaca.org:443/			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ID	Date	Method	Host	Path	Parameters	Status	Origin	Possible Injection	XSS
28	2008/01/...	GET	http://www.isaca.org:80	/Graphics/governance_on.gif		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
27	2008/01/...	GET	http://www.isaca.org:80	/Graphics/security_on.gif		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
26	2008/01/...	GET	http://www.isaca.org:80	/Graphics/Assurance_on.gif		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
25	2008/01/...	GET	http://www.isaca.org:80	/Graphics/TraditionalChinese_on.gif		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
24	2008/01/...	GET	http://www.isaca.org:80	/Graphics/Spanish_on.gif		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
23	2008/01/...	GET	http://www.isaca.org:80	/Graphics/SimplifiedChinese_on.gif		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
22	2008/01/...	GET	http://www.isaca.org:80	/Graphics/Korean_on.gif		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
21	2008/01/...	GET	http://www.isaca.org:80	/Graphics/Japanese_on.gif		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
20	2008/01/...	GET	http://www.isaca.org:80	/Graphics/Italian_on.gif		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
19	2008/01/...	GET	http://www.isaca.org:80	/HierMenu/HM_ScriptDOM.js		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
18	2008/01/...	GET	http://www.isaca.org:80	/Graphics/ACF9E46.gif		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
17	2008/01/...	GET	http://www.isaca.org:80	/Graphics/Hebrew_on.gif		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
16	2008/01/...	GET	http://www.isaca.org:80	/Graphics/Dutch_on.gif		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
15	2008/01/...	GET	http://www.isaca.org:80	/Graphics/German_on.gif		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
14	2008/01/...	GET	http://www.isaca.org:80	/Styles/Styles.css		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
13	2008/01/...	GET	http://www.isaca.org:80	/favicon.ico		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
12	2008/01/...	GET	http://www.isaca.org:80	/		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
11	2008/01/...	GET	http://www.isaca.fi:80	/layout/isaca/images/img_contentbottomgfx...		304 Not ...	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
10	2008/01/...	GET	http://www.isaca.fi:80	/layout/isaca/images/img_footer_bg.jpg		304 Not ...	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
9	2008/01/...	GET	http://www.isaca.fi:80	/layout/isaca/images/img_block_title_bg.gif		304 Not ...	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
8	2008/01/...	GET	http://www.isaca.fi:80	/layout/isaca/images/img_navigation_li_bg.gif		304 Not ...	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
7	2008/01/...	GET	http://www.isaca.fi:80	/layout/isaca/images/img_content_bg.jpg		304 Not ...	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
6	2008/01/...	GET	http://www.isaca.fi:80	/layout/isaca/images/img_txt_kirjautuminen...		304 Not ...	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
5	2008/01/...	GET	http://www.isaca.fi:80	/layout/isaca/images/img_contentshadowto...		304 Not ...	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
4	2008/01/...	GET	http://www.isaca.fi:80	/layout/isaca/images/print.png		304 Not ...	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
3	2008/01/...	GET	http://www.isaca.fi:80	/layout/isaca/images/img_isaca_fi_logo.jpg		304 Not ...	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
2	2008/01/...	GET	http://www.isaca.fi:80	/layout/isaca/css/global.css		304 Not ...	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
1	2008/01/...	GET	http://www.isaca.fi:80	/		200 OK	Proxy	<input type="checkbox"/>	<input type="checkbox"/>

Used 16.73 of 487.31MB



OWASP WebGoat

- Itseopiskeluun ja koulutuskäyttöön tarkoitettu www-sovellus, johon on tarkoituksella tehty haavoittuvuuksia
- 12 erillistä aihetta, joita voi käydä läpi omaan tahtiinsa
- WebScarab oiva apuväline opiskelussa

WebGoat -esimerkki 1

How to Exploit Hidden Fields - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.0.20:8080/WebGoat/attack?Screen=3&menu=110

Getting Started Latest BBC Headlines

Logout ?

How to Exploit Hidden Fields

OWASP WebGoat V5

Admin Functions
General
Code Quality
Unvalidated
Parameters

Restart this Lesson

Try to purchase the HDTV for less than the purchase price, if you have not done so already.

Shopping Cart

Shopping Cart Items -- To Buy Now	Price:	Quantity:	Total
56 inch HDTV (model KTV-551)	2999.99	1	\$2999.99

The total charged to your credit card: \$2999.99

[Update Cart](#) [Purchase](#)

ASPECT SECURITY
Application Security Specialists

OWASP Foundation | Project WebGoat

Broken Access Control
Broken Authentication and Session Management
Cross-Site Scripting (XSS)
Buffer Overflows
Injection Flaws
Improper Error Handling
Insecure Storage
Denial of Service
Insecure Configuration Management



WebGoat -esimerkki 2

Edit Request

Intercept requests : ☒ Intercept responses : ☐

Parsed **Raw**

Method **URL** **Version**

POST http://192.168.0.20:8080/WebGoat/attack?menu=110 HTTP/1.1

Header	Value
Host	192.168.0.20:8080

URLEncoded **Text** **Hex**

Variable	Value
QTY	1
SUBMIT	Purchase
Price	2999.99

Parsed **Raw**

Version **Status** **Message**

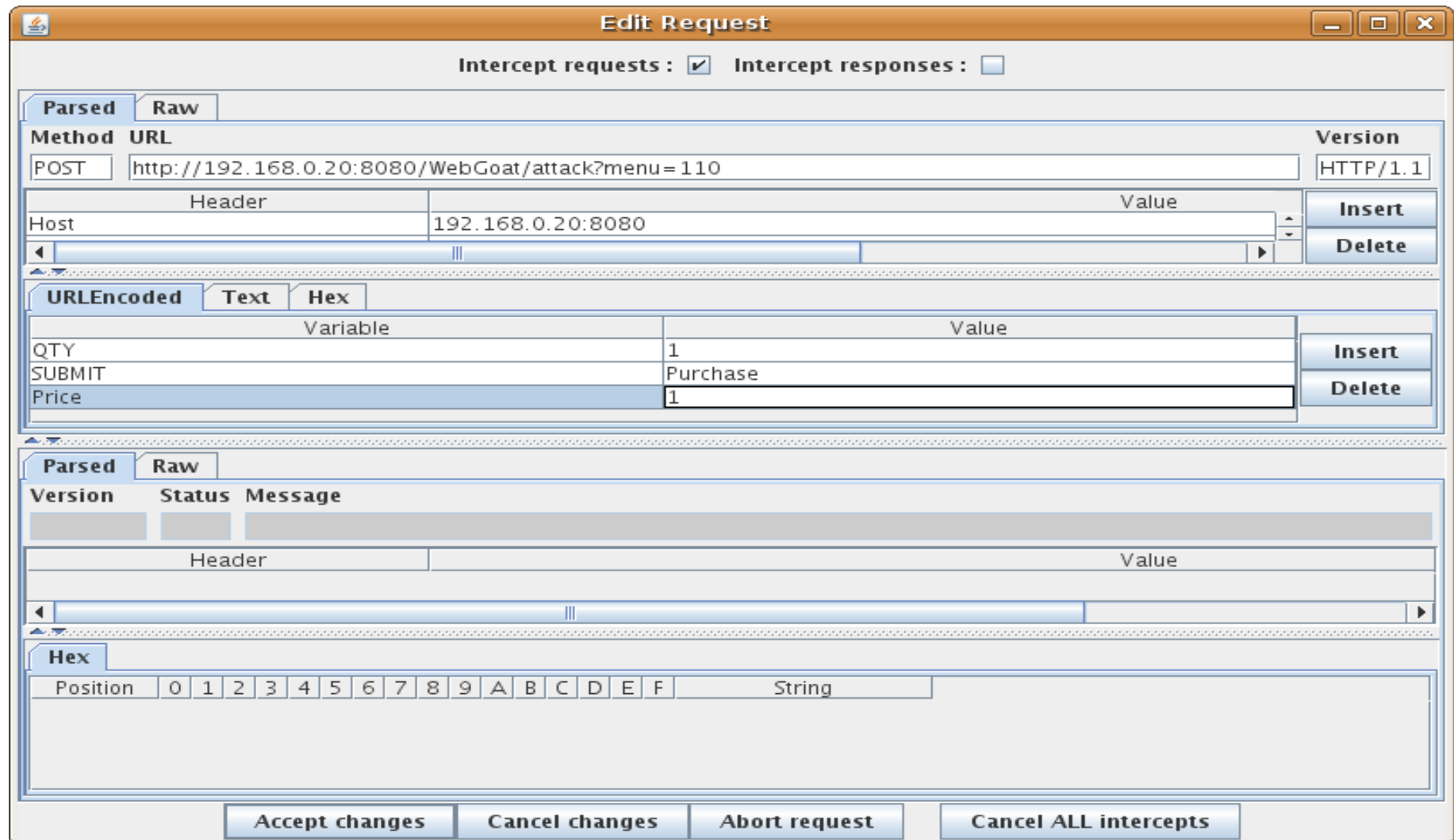
Header	Value
--------	-------

Hex

Position	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	String
----------	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	--------

Accept changes **Cancel changes** **Abort request** **Cancel ALL intercepts**

WebGoat -esimerkki 3



The image shows the 'Edit Request' dialog box in Burp Suite. It is divided into two main sections: 'Request' and 'Response'. The 'Request' section is currently active and shows a POST request to 'http://192.168.0.20:8080/WebGoat/attack?menu=110'. The 'Response' section is empty. The 'Request' section has tabs for 'Parsed' and 'Raw', and 'Intercept requests' is checked. The 'Response' section has tabs for 'Parsed' and 'Raw', and 'Intercept responses' is unchecked. The 'Request' section has a table for 'Headers' and a table for 'Parameters'. The 'Parameters' table has columns for 'Variable' and 'Value'. The 'Response' section has a table for 'Headers' and a 'Hex' section for raw data.

Edit Request

Intercept requests : ☒ Intercept responses : ☐

Parsed **Raw**

Method **URL** **Version**

POST http://192.168.0.20:8080/WebGoat/attack?menu=110 HTTP/1.1

Header	Value
Host	192.168.0.20:8080

URLEncoded **Text** **Hex**

Variable	Value
QTY	1
SUBMIT	Purchase
Price	1

Parsed **Raw**

Version **Status** **Message**




Header	Value
--------	-------

Hex

Position	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	String
----------	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	--------




Accept changes Cancel changes Abort request Cancel ALL intercepts

WebGoat -esimerkki 4

Applications Places System  Tmo  Tue Jan 22, 9:47 PM 

How to Exploit Hidden Fields - Mozilla Firefox

File Edit View History Bookmarks Tools Help

 <http://192.168.0.20:8080/WebGoat/attack?menu=110>  ASL 

Getting Started Latest BBC Headlines

Logout ?

How to Exploit Hidden Fields

OWASP WebGoat V5

Hints Show Params Show Cookies Show Java Lesson Plans

Admin Functions
General
Code Quality
Unvalidated
Parameters

Restart this Lesson

Try to purchase the HDTV for less than the purchase price, if you have not done so already.

*** Congratulations. You have successfully completed this lesson.**

Your total price is: **\$1.0**

This amount will be charged to your credit card immediately.

ASPECT SECURITY
Application Security Specialists

OWASP Foundation | Project WebGoat

Broken Access
Control
Broken Authentication
and Session
Management
Cross-Site Scripting
(XSS)
Buffer Overflows
Injection Flaws
Improper Error
Handling
Insecure Storage
Denial of Service
Insecure
Configuration

Waiting for 192.168.0.20...

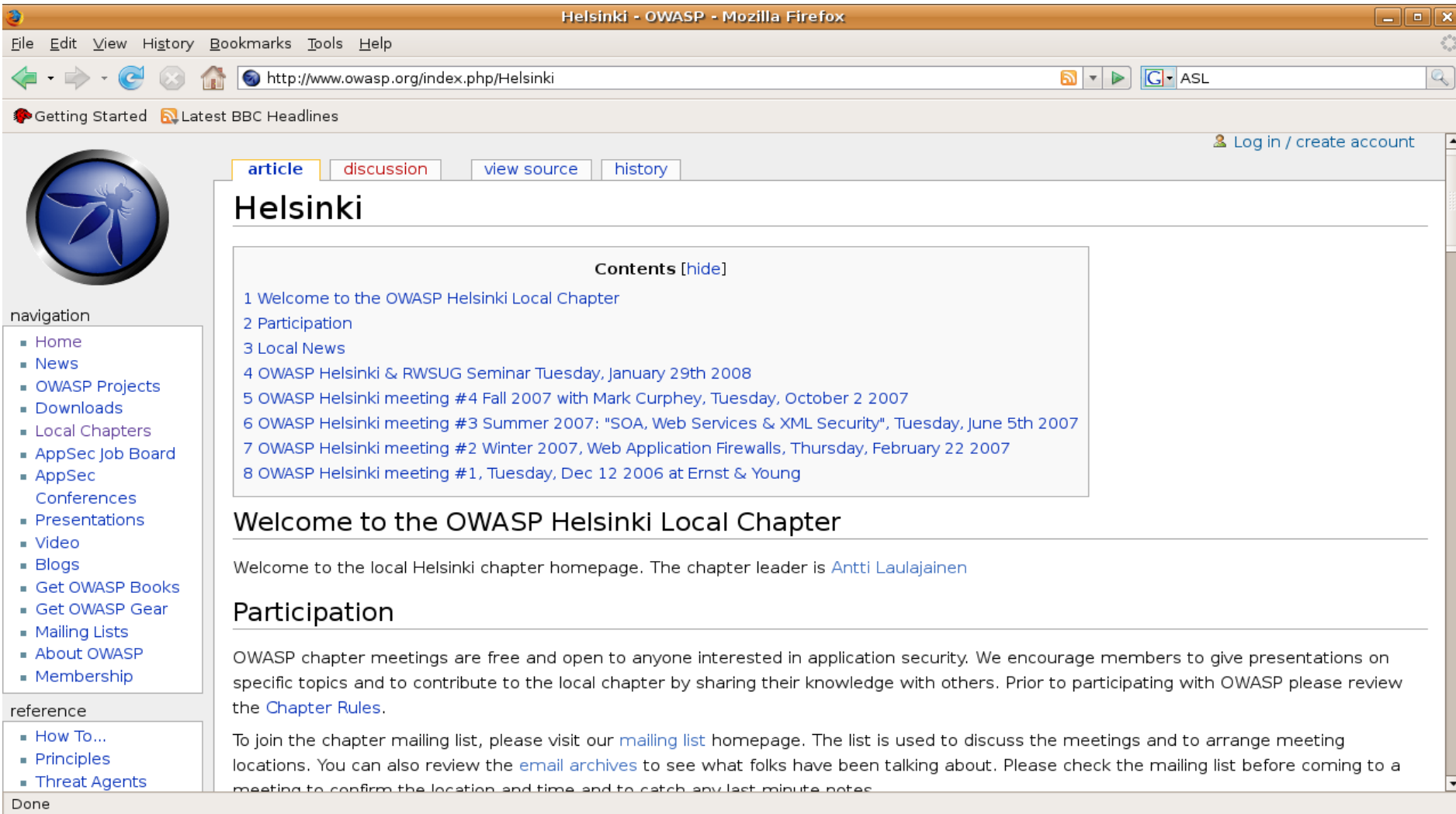
How to Exploit Hidde...



OWASP Helsinki Chapter

- “Perustettu” Suomessa 2006 (Mikko Saario)
 - ▶ ISACA / TiVaKo 2002-kurssilla tietty vaikutus asiaan
- Vapaamuotoinen verkosto, jossa mukana tietoturva-ammattilaisia ja sovelluskehittäjiä
 - ▶ Jäsenkokouksia ajankohtaisista, yleensä teknisistä aiheista
 - ▶ Postituslista
- Jatkossa tarkoituksena tavoittaa tietoturva-ammattilaisten lisäksi
 - ▶ IT-arkkitehdit, määrittelijät
 - ▶ Suunnittelijat ja sovelluskehittäjät
 - ▶ Testaajat ja tarkastajat

OWASP Helsinki chapter



The screenshot shows a Mozilla Firefox browser window with the title "Helsinki - OWASP - Mozilla Firefox". The address bar displays "http://www.owasp.org/index.php/Helsinki". The page features a navigation menu on the left with links like Home, News, OWASP Projects, Downloads, Local Chapters, AppSec Job Board, AppSec Conferences, Presentations, Video, Blogs, Get OWASP Books, Get OWASP Gear, Mailing Lists, About OWASP, and Membership. The main content area has tabs for "article", "discussion", "view source", and "history". The "article" tab is selected, showing the "Helsinki" page. The page content includes a "Contents [hide]" section with a list of 8 items, a "Welcome to the OWASP Helsinki Local Chapter" section, and a "Participation" section. The "Participation" section explains that OWASP chapter meetings are free and open to anyone interested in application security, and provides information on how to join the mailing list and review the email archives.

Helsinki - OWASP - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.owasp.org/index.php/Helsinki

Getting Started Latest BBC Headlines

Log in / create account

article discussion view source history

Helsinki

Contents [hide]

- 1 Welcome to the OWASP Helsinki Local Chapter
- 2 Participation
- 3 Local News
- 4 OWASP Helsinki & RWSUG Seminar Tuesday, January 29th 2008
- 5 OWASP Helsinki meeting #4 Fall 2007 with Mark Curphey, Tuesday, October 2 2007
- 6 OWASP Helsinki meeting #3 Summer 2007: "SOA, Web Services & XML Security", Tuesday, June 5th 2007
- 7 OWASP Helsinki meeting #2 Winter 2007, Web Application Firewalls, Thursday, February 22 2007
- 8 OWASP Helsinki meeting #1, Tuesday, Dec 12 2006 at Ernst & Young

Welcome to the OWASP Helsinki Local Chapter

Welcome to the local Helsinki chapter homepage. The chapter leader is [Antti Laulajainen](#)

Participation

OWASP chapter meetings are free and open to anyone interested in application security. We encourage members to give presentations on specific topics and to contribute to the local chapter by sharing their knowledge with others. Prior to participating with OWASP please review the [Chapter Rules](#).

To join the chapter mailing list, please visit our [mailing list](#) homepage. The list is used to discuss the meetings and to arrange meeting locations. You can also review the [email archives](#) to see what folks have been talking about. Please check the mailing list before coming to a meeting to confirm the location and time and to catch any last minute notes.

Done

Muita OpenSource projekteja

- OSSTMM - Open Source Security Testing Methodology Manual
- Erilaisiin työkaluihin liittyvät projektit
 - ▶ Wireshark -tietoliikenteen analysointiohjelmisto
 - ▶ Nessus -haavoittuvuusskanneri
- Tietoliikenteen ja palvelinalustojen turvallisuuteen liittyvät projektit
 - ▶ Snort IDS-järjestelmä
 - ▶ OSSEC Open Source Host-based intrusion detection system

Kysymyksiä & Keskustelua