Web Hacking & Defensing

February 19(Sun), 2017

Prof. Thomas Byeongnam YOON, PhD.
Content

1. Web Protocol
2. Web Log
3. Web Hacking Tool
4. Wrap Up
Learning Point: New Terminology Definition – Clear Concept

1. HTTP Protocol used for Webpages
   - Create Cyber Space by HTML Web Program Language
2. Paros Web Hacking Tool
   - Strong Tool for Web Vulnerability Measure, Java Open Source Based
3. Web Log Analysis
   - Fundamental Knowledge of Hacking Type Analysis
4. Web Defensing Know-How
   - Become a Cyber Soldier – Cyber Salvation Army
Internet Logical Architecture → Cyber Space L.A.
Intranet Logical Architecture
Web Server Platform – Web Programming Environment

Chronicle: HTML + [ASP Platform (MS) → JSP Platform (Sun) → HPH Platform (Open Source)]
Web Browser (UA Platform) – Cyber Space Shuttle (1993 Netscape Navigator)

Chronicle: **Netscape** (NCC) → **IE** (MS) → **Chrome** (Google: Open Source)

![Diagram of web browser and server interaction with user accessing webpage](image-url)
Cyber Space Protocol – HTTP (Hyper Text Transport Protocol)

1. Web Browser request Webpage
2. Server Process
3. Response Webpage
4. Execute HTML Engine & Java Script

- Show up Screen
- Translate HTML
- Connect, Session Start
- Request Webpage (URL/URI)
- Response (HTML File)
- Disconnect, Session End
- Process Web Program
- Response HTML Webpage
Cyber Space Protocol – HTTP (Hyper Text Transport Protocol)

Client
- Translate HTML
- Show up Screen

Server
- Process Web Program File

HTML File
- Connect (Session Start)
- Request Webpage (URL)
- Response (HTML File)
- Disconnect (Session End)

Image File
- Reuse Image File in Cash
- Otherwise Request

- Connect (Session Start)
- Request Image (URL/URI)
- Response (Image File)
- Disconnect (Session End)
Cyber Space Shuttle – Web Browser Doing:

→ Browser 3 Step Procedure

1. Session Start
2. Data Communication
3. Session End

Webpage Instances

→ HTML5, CSS, ...
→ Server-side Program: ASP, JSP, PHP, ...
→ SQL DBMS Language
→ Embedded Multi-Media Languages: Audio, Video, Image, Streaming Service
→ File Upload, Download
→ Send & Receive eMail
→ CSV, Excel file between DBMS, ... etc.
Cyber Space Protocol – HTTP: Step 1. Session Start Procedure

1. Request Connection (send SYN)
2. Accept Connection (Send SYN, ACK)
3. Confirm Connection (send ACK)
4. Session Start

Client
Server

Global Client-Server Communication Protocol
**Cyber Space Protocol – HTTP : Step 2. Data Communication Procedure**

1. Request Webpage *(HTTP method, Request document-PSH)*

2. Ready to service
   - TCP Checksum Routine *(Send ACK)*

3. Give Webpage *(document-PSH)*

4. Repeat until Completed

---

Global Client-Server Communication
Cyber Space Protocol – HTTP: Step 3. Session End Procedure

1. FIN-WAIT 1
   \textbf{(send FIN, ACK)}
   Request Disconnection

2. CLOSE-WAIT
   \textbf{(send ACK)}

3. FIN-WAIT 2

4. LAST ACK
   \textbf{(Send FIN, ACK)}

5. TIME WAIT
   \textbf{(send ACK)}

6. Session End

Global Client-Server Communication Protocol
# Cyber Space Protocol - TCP Date lossless Protocol Packet Format

## Transmission Control Protocol (TCP) Packet Header

<table>
<thead>
<tr>
<th>Bits</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Sequence Number</th>
<th>Acknowledgment Number</th>
<th>Data Offset</th>
<th>Reserved</th>
<th>Code</th>
<th>Window</th>
<th>Checksum</th>
<th>Urgent Pointer</th>
<th>Options</th>
<th>Padding</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Code - Flag Bits (Packet Control Code)

- **URG**: Urgent Packet
- **ACK**: Acknowledgement of Message Received Well
- **PSH**: Push Request Task
- **SYN**: Data Communication Session Creation
- **FIN**: Graceful Session End Request
- **RTS**: Emergent Session End Request
Cyber Space Protocol – HTTP Request & Response Message Format

HTTP Request Message

User (Browser) → Web Server

HTTP Response Message

Web Server → User (Browser)
Cyber Space Protocol – HTTP Request Message Format

**Header:**
- **HTTP Method + Host Domain + Client Platform Information**
  - GET /home/index.html HTTP/1.1
  - Host: www.evenstar.co.kr
  - Accept: text/html, text/plain
  - Accept-Encoding: gzip, compress
  - Accept-Language: ko
  - If-Modified-Since: Sat, 31 Jan 2004 12:00:00 GMT
  - User-Agent: Internet Explorer 6.0

**White Space One Line asSeparator**

**Body:**
- **Whole Parameters & Data**
  - 본문 (GET인 경우는 빈 공백임)
# Cyber Space Protocol – HTTP GET Method Request Message

- HTTP GET Method Format (Message Header Only)
- Message Size: Max 2K Byte Data Length?! (Not enough to BBS content, etc.)

<table>
<thead>
<tr>
<th>Method</th>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>GET [request-uri]?query_string HTTP/1.1 Host:[Hostname] or [IP]</td>
<td>GET Method request Webpage to Server with URI(URL) in its Message Header Part.</td>
</tr>
</tbody>
</table>

http://www.evenstar.co.kr/webpage/biglook.html : URL Window in Browser

URL/URI (Universal Resource Identification/Location)


URL/URI Query String
Cyber Space Protocol - HTTP GET Method Request Message

- **HTTP Method**: GET
- **Massage Header Part**:
  - `GET http://www.evenstar.co.kr/wizboard.php?BID=notice HTTP/1.0`
  - `Accept: */*
  - `Referer: http://www.evenstar.co.kr/webpage/top_menu.html`
  - `Accept-Language: ko`
  - `UA-CPU: x86`
  - `Proxy-Connection: Keep-Alive`
  - `User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; EmbeddedWB 14.52 from: http://www.bsalsa.com/EmbeddedWB 14.52; .NET CLR 1.1.4322; .NET CLR 2.0.50727); Paros/3.2.13`
  - `Host: www.evenstar.co.kr`
- **Massage Body Part is Empty**
Cyber Space Protocol – HTTP GET Method Request Message Scan

1. GET /index.html HTTP/1.1
   // Request Method, Webpage, HTTP Version

2. User-Agent: MSIE 6.0; Windows NT 5.0
   // User’s Web Browser; Platform Version

3. Accept: text/html; */*
   // Acceptable Data Type

4. Cookie: name = value
   // User Authenticate Information

5. Referer: http://www.bbb.com
   // Previous passage URL

6. Host: www.evenstar.co.kr
   // Request Domain
## Cyber Space Protocol – HTTP Post Method Request Method

- **HTTP Post Method Format (Header + Body)**
  - Message Size: **No limit**! (Enough to BBS content, etc.)

### Method | Format | Note
| --- | --- | --- |
| POST | POST [request-uri] HTTP/1.1  
Host:[Hostname] or [IP]  
Content-Length:[Bytes]  
Content-Type:[Content Type]  
One White Space Line  
[query-string] or [Data] | 1. Data Communication of Form Based Web Page with Various Data & Parameters.  
2. Browser can't show up it at URL Window! |
**Form based Webpage**

![Form based Webpage](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title of Paper</td>
<td>Experimental Validation of Multipoint Joint Processing of Range Measurement</td>
</tr>
<tr>
<td>Keyword</td>
<td>Analytical model, Distance measurement, Radar signal processing, Wireless Communication</td>
</tr>
<tr>
<td>Topics</td>
<td>Wireless Communication</td>
</tr>
<tr>
<td>Upload File</td>
<td>Choose File No file chosen PDF file only!</td>
</tr>
<tr>
<td>File Name</td>
<td>20170442 Paper.pdf</td>
</tr>
<tr>
<td>Confirmation</td>
<td>Please confirm your latest upload file</td>
</tr>
<tr>
<td>Do you want to upload your file?</td>
<td>Yes  No</td>
</tr>
<tr>
<td>Number of Pages</td>
<td>11</td>
</tr>
<tr>
<td>E-mail (One address only)</td>
<td><a href="mailto:grihafokin@gmail.com">grihafokin@gmail.com</a></td>
</tr>
</tbody>
</table>
Cyber Space Protocol – HTTP Post Method Request Message Scan

HTTP Method

POST http://www.evenstar.co.kr/wizboard/admin_log_check.php HTTP/1.0
Accept: */*

Header Part

Accept-Language: ko
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Proxy-Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; EmbeddedWB 14.52 from: http://www.bsalsa.com/EmbeddedWB 14.52; .NET CLR 1.1.4322; .NET CLR 2.0.50727) Paros/3.2.13

Body Part

BID=news&Mode=MemberLogin&category=&UID=&mode=login&nmode=write&CURRENT_PAGE=&MEMBERPASS=PASSWORD
Form based Webpage
HTTP Post Method
Request Message
Scan

POST http://icact.org/papersubmission/paper_update_proc.asp HTTP/1.1
Host: icact.org
Proxy-Connection: keep-alive
Content-Length: 16749
Cache-Control: max-age=0
Origin: http://icact.org
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2928.81 Safari/537.36
Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryRAAbnJ8TyEBu7i
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://icact.org/papersubmission/paper_update.asp
Accept-Language: ko-KR,ko;q=0.9,en-US,en;q=0.8
Cookie: ASPSESSIONID4OBBTQT=CCNNEPNACCCH0JDAKAP0D

-----WebKitFormBoundaryRAAbnJ8TyEBu7i
Content-Disposition: form-data; name="pno"
20170442

-----WebKitFormBoundaryRAAbnJ8TyEBu7i
Content-Disposition: form-data; name="ptitle"
Experimental Validation of Multipoint Joint Processing of Range Measurements via Software-Defined Radio Testbed

-----WebKitFormBoundaryRAAbnJ8TyEBu7i
Content-Disposition: form-data; name="keyword"
Analytical model, Distance measurement, Radar signal processing, Radio navigation, Software radio

-----WebKitFormBoundaryRAAbnJ8TyEBu7i
Content-Disposition: form-data; name="field"
Cyber Space Protocol – HTTP Response Message Format

1. HTTP/1.1  OK  200  // http version, Response Status Code
2. Server: NCSA/1.4.2  // Web Server version
3. Content-type: text/html  // MIME Type (Multipurpose Internet Message Extensions)

5. <html>
   <head></head>  // Requested HTML Webpage
   <Title>http protocol</Title>
   <body>
      The understanding of http protocol
   </body>
</html>
**Response Message:**

HTTP/1.1 200 OK

**Date:** Tue, 14 Feb 2017 08:28:32 GMT

**Server:** Microsoft-IIS/6.0

**X-Powered-By:** ASP.NET

**Content-Length:** 198081

**Content-Type:** text/html

**Cache-control:** private

---

**HTML Content:**

```html
<!DOCTYPE html>
<html>
<head>
	<title>www.icact.org</title>
</head>
<body>
<script type="text/javascript" language="javascript" src="/include/script.js"></script>
<script language="javascript" src="/include/common.js"></script>
</body>
</html>
```

---

**Additional Elements:**

- **Raw View**
- **Trap Request:** Not selected
- **Trap Response:** Selected
Form based Webpage

mission/paper_update.asp

- **Title of Paper**: Experimental Validation of Multipoint Joint Processing of Range Measurements
- **Keyword**: Analytical model, Distance measurement, Radar signal processing, Radio navigation
- **Topics**: Wireless Communication
- **Upload File**: Choose File, No file chosen. PDF file only!

20170442 Paper.pdf ←--- Please confirm your latest upload file here!

Do you want to upload your file?  Yes ☐  No ☐
- Abstract (1 page)
- Full Paper (Min. 3 pages)

- **Number of Pages**: 1
- **E-mail (One address only)**: grihafokin@gmail.com
Cyber Space Protocol – HTTP Response Status Code

- **Request(URL/URI)**
  - **200**: OK, Request Success
  - **201**: File Created in Server
  - **302**: Moved to Webpage (**Previous Webpage**)
  - **304**: Used Local Cache Info.
  - **401**: Fail Authenticate
  - **403**: Denied Access
  - **404**: Not Exist Webpage
  - **500**: Severe Error (**DB Access Error Injection**)
Cyber Space Web Programming Method – Stateless vs State Oriented

Cyber Space has Huge Users – Challenge & Chance
Pros & Cons : Web Server Cost Performance, but User Authentication needed

Client

Login = Thomas

Money Transfer = Who?

Confirm Balance = Who?

Log Out = Who?

Sever

Banking Service Work Flow
Stateless Web Programming Methods: Cookie

Client Keeps Cookie

Server User Authentication

Login = Thomas

Money Transfer = Thomas

Confirm Balance = Thomas

Log Out = Thomas
# Stateless Web Programming Methods: Cookie

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Persistence Cookie</th>
<th>Session Cookie</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>Disk File</td>
<td>Browser Memory</td>
</tr>
<tr>
<td>Life Time</td>
<td>Time-Out Value, Delete by User</td>
<td>Browser End</td>
</tr>
<tr>
<td>When Initial Website Connection</td>
<td>Send Cookie</td>
<td>No Send Cookie</td>
</tr>
<tr>
<td>Usage</td>
<td>Reconnect Website</td>
<td>Access Webpages</td>
</tr>
</tbody>
</table>
Stateless Web Programming Methods: Session Cookie Names

<table>
<thead>
<tr>
<th>Hidden Parameter</th>
<th>Cookie</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name, Password, Data</td>
<td>+UA</td>
<td>++Session ID</td>
</tr>
<tr>
<td>No Expire Time</td>
<td>Time-Out</td>
<td>Browser End</td>
</tr>
<tr>
<td>Very Simple</td>
<td>Secure</td>
<td>Very Secure</td>
</tr>
<tr>
<td>Store in Client</td>
<td>Store in Client</td>
<td>Critical Date in Server</td>
</tr>
</tbody>
</table>
Stateless Web Programming Methods: Cookie

1. Initial request Webpage
2. Create Cookie
3. Send Cookie
4. Store Cookie
5. Request Webpage + Cookie
6. User Authenticate

Client
- Show up Screen
- Translate HTML
- Connect, Session Start
- Request Webpage (URL/URI)
- Disconnect, Session End

Server
- Process Web Program
- Response HTML Webpage

Response (HTML File)
Cookie Programming Methods: Hidden Parameter from Server

```
<form name="frm" method="post">
  <input type="hidden" name="eMail" value="tomayoon@ieee.org" />
  <input type="hidden" name="pwd" value="1111" />
</form>

<script language="javascript">
    frm.action = "schedule.asp";
    frm.submit();
</script>

```

HTTP/1.1 200 OK
Date: Sun, 12 Feb 2017 06:03:15 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 532
Content-Type: text/html
Cache-control: private
Stateless Web Programming Methods: Cookie + Session ID
Cookie Programming Methods: User Authentication

icact.org says:
	tomayoon@ieee.org Authentication Successful! Go to the Annual Scheduler!
# Annual Schedule

<table>
<thead>
<tr>
<th>CK</th>
<th>ID_no (TCSnn, HOMnn, ORGnn, TPCnn, LOCnn)</th>
<th>D-day (MM-DD)</th>
<th>Task</th>
<th>InformTo</th>
<th>Owner (eMail)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HOM</td>
<td>01-</td>
<td>ICACT2017 Session Overview with Paper</td>
<td><a href="mailto:secretariat@icact.org">secretariat@icact.org</a></td>
<td><a href="mailto:tomayoon@ieee.org">tomayoon@ieee.org</a></td>
</tr>
<tr>
<td></td>
<td>HOM</td>
<td>02-</td>
<td>ICACT2017 Conference Proceedings</td>
<td><a href="mailto:secretariat@icact.org">secretariat@icact.org</a></td>
<td><a href="mailto:tomayoon@ieee.org">tomayoon@ieee.org</a></td>
</tr>
<tr>
<td></td>
<td>HOM</td>
<td>02-</td>
<td>ICACT2017 KwangWon Convention Bureau</td>
<td><a href="mailto:secretariat@icact.org">secretariat@icact.org</a></td>
<td><a href="mailto:tomayoon@ieee.org">tomayoon@ieee.org</a></td>
</tr>
<tr>
<td></td>
<td>LOC</td>
<td>02-</td>
<td>Invite Session Chair</td>
<td><a href="mailto:secretariat@icact.org">secretariat@icact.org</a></td>
<td><a href="mailto:tomayoon@ieee.org">tomayoon@ieee.org</a></td>
</tr>
<tr>
<td></td>
<td>VIP0</td>
<td>02-</td>
<td>ICACT2017 VIP Invite Confirmation</td>
<td><a href="mailto:secretariat@icact.org">secretariat@icact.org</a></td>
<td><a href="mailto:tomayoon@ieee.org">tomayoon@ieee.org</a></td>
</tr>
<tr>
<td></td>
<td>TCSI</td>
<td>05-</td>
<td>Confirm Committee Member</td>
<td><a href="mailto:secretariat@icact.org">secretariat@icact.org</a></td>
<td><a href="mailto:tomayoon@ieee.org">tomayoon@ieee.org</a></td>
</tr>
<tr>
<td></td>
<td>TCSI</td>
<td>05-</td>
<td>Invite General Chair</td>
<td><a href="mailto:secretariat@icact.org">secretariat@icact.org</a></td>
<td><a href="mailto:tomayoon@ieee.org">tomayoon@ieee.org</a></td>
</tr>
<tr>
<td></td>
<td>TCSI</td>
<td>05-</td>
<td>ICACT2017 CFP PDF</td>
<td><a href="mailto:secretariat@icact.org">secretariat@icact.org</a></td>
<td><a href="mailto:tomayoon@ieee.org">tomayoon@ieee.org</a></td>
</tr>
</tbody>
</table>
Cyber Space Protocol – HTTP Response Status Code

- **200**: OK, Request Success
- **201**: File Created in Server
- **302**: Moved to Webpage (Previous Webpage)
- **304**: Used Local Cache Info.
- **401**: Fail Authenticate
- **403**: Denied Access
- **404**: Not Exist Webpage
- **500**: Severe Error (DB Access Error Injection)
<table>
<thead>
<tr>
<th>Method</th>
<th>URL</th>
<th>Status Code</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td><a href="http://icact.org/index.asp">http://icact.org/index.asp</a></td>
<td>200 OK</td>
<td>628ms</td>
</tr>
<tr>
<td>GET</td>
<td><a href="http://icact.org/manage/index.asp">http://icact.org/manage/index.asp</a></td>
<td>302 Object moved</td>
<td>635ms</td>
</tr>
<tr>
<td>GET</td>
<td><a href="http://icact.org/manage/review/paper_list.asp">http://icact.org/manage/review/paper_list.asp</a></td>
<td>404 Not Found</td>
<td>10ms</td>
</tr>
<tr>
<td>GET</td>
<td><a href="http://icact.org/manage/review/paper_list.asp">http://icact.org/manage/review/paper_list.asp</a></td>
<td>404 Not Found</td>
<td>14ms</td>
</tr>
<tr>
<td>GET</td>
<td><a href="http://icact.org/program/papers.asp">http://icact.org/program/papers.asp</a></td>
<td>200 OK</td>
<td>2832ms</td>
</tr>
<tr>
<td>GET</td>
<td><a href="http://icact.org/upload/2016/0004/20160004_bioography.pdf">http://icact.org/upload/2016/0004/20160004_bioography.pdf</a></td>
<td>200 OK</td>
<td>125ms</td>
</tr>
<tr>
<td>GET</td>
<td><a href="http://icact.org/asp/schedule_login.asp">http://icact.org/asp/schedule_login.asp</a></td>
<td>200 OK</td>
<td>361ms</td>
</tr>
<tr>
<td>POST</td>
<td><a href="http://icact.org/asp/schedule_login_proc.asp">http://icact.org/asp/schedule_login_proc.asp</a></td>
<td>200 OK</td>
<td>14ms</td>
</tr>
<tr>
<td>POST</td>
<td><a href="http://icact.org/asp/schedule.asp">http://icact.org/asp/schedule.asp</a></td>
<td>200 OK</td>
<td>23ms</td>
</tr>
<tr>
<td>POST</td>
<td><a href="http://icact.org/asp/Schedule_proc.asp">http://icact.org/asp/Schedule_proc.asp</a></td>
<td>500 Internal Server...</td>
<td>18ms</td>
</tr>
<tr>
<td>GET</td>
<td><a href="http://icact.org/index.asp">http://icact.org/index.asp</a></td>
<td>200 OK</td>
<td>607ms</td>
</tr>
<tr>
<td>GET</td>
<td><a href="http://icact.org/manage/index.asp">http://icact.org/manage/index.asp</a></td>
<td>302 Object moved</td>
<td>540ms</td>
</tr>
<tr>
<td>GET</td>
<td><a href="http://icact.org/manage/review/paper_list.asp">http://icact.org/manage/review/paper_list.asp</a></td>
<td>404 Not Found</td>
<td>9ms</td>
</tr>
</tbody>
</table>
Hacking Concept - HTTP Intercept

1. Request

2. Modified Request

3. Response

4. Modified Response

User (Browser) → Hacking Tool → Web Server

Normal Access → Request → Response

21
Where are Hacking Points?!
Paros – Open Source HTTP Intercept Tool!!
HTTP Intercept Tool - **Paros!!**

**Paros Client Proxy Capability**

- **HTTP Analysis Capability**
- **Web Server Hacking**
- **Vulnerable Point Analysis**
HTTP Intercept Tool – Paros Installation !!

Paros download | SourceForge.net
https://sourceforge.net/projects/paros/
Rating: 2.7 - 5 votes
Aug 14, 2013 - Download paros-3.2.13-win.exe. A Java based HTTP/HTTPS proxy for application vulnerability. Other features include spiders, client certificate, proxy-cha scanning for XSS and SQL injections etc.

Paros - Browse /Paros/Version 3.2.13 at SourceForge.net
https://sourceforge.net/projects/paros/files/Paros/Version%203.2.13/
A Java based HTTP/HTTPS proxy for assessing web application vulnerability. It supports paros-3.2.13-win.exe (1.7 MB). Home / Paros / Version ...
HTTP Intercept Tool – **Paros Installation !!**

A Java based HTTP/HTTPS proxy for assessing web application vulnerability. It supports editing/viewing HTTP messages on-the-fly. Other features include spiders, client certificate, proxy-chaining, intelligent scanning for XSS and SQL injections etc.

**Description**

**Categories**

- Security
- License
  - Artistic License
HTTP Intercept Tool – **Paros Installation!!**
HTTP Intercept Tool – Paros Installation !!

Completing the Paros 3.2.13 Setup Wizard

Setup has finished installing Paros 3.2.13 on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.
Paros Developed for x86 environment only
Paros Execution
Paros is Java Application

Short Cut to Javaw.exe

Problem with Shortcut

The item 'javaw.exe' that this shortcut refers to has been changed or moved, so this shortcut will no longer work properly.

Nearest match based on size, date, and type:
C:\ProgramData\Adobe\CS5\re\bin\javaw.exe

Do you want to fix this shortcut to point to this target or do you just want to delete it?
Paros needs JDK
JDK Installation !!
JDK Installation !!

Java SE - Downloads | Oracle Technology Network | Oracle
www.oracle.com/technetwork/java/.../downloads/index-jsp-138363.html
Java SE downloads including: Java Development Kit (JDK), Server Java Runtime Environment (Server JRE), and Java Runtime Environment (JRE).

Java SE Development Kit 8
Java SE Development Kit 8
Downloads. Thank you for ...

Java SE Downloads
NetBeans - Java FX - Java - Java EE - ...

More results from oracle.com »

Java SE Runtime Environment
Java SE Runtime Environment 8
Downloads. Do you want to run ...

Server JRE (Java SE Runtime)
Server JRE (Java SE Runtime ... The
Server JRE is a runtime ...
## JDK Installation – x86

### Java SE Development Kit 8u121

You must accept the Oracle Binary Code License Agreement for Java SE to download this software.

<table>
<thead>
<tr>
<th>Product / File Description</th>
<th>File Size</th>
<th>Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux ARM 32 Hard Float ABI</td>
<td>77.86 MB</td>
<td>jdk-8u121-linux-arm32-vfp-hft.tar.gz</td>
</tr>
<tr>
<td>Linux ARM 64 Hard Float ABI</td>
<td>74.83 MB</td>
<td>jdk-8u121-linux-arm64-vfp-hft.tar.gz</td>
</tr>
<tr>
<td>Linux x86</td>
<td>162.41 MB</td>
<td>jdk-8u121-linux-i586.rpm</td>
</tr>
<tr>
<td>Linux x86</td>
<td>177.13 MB</td>
<td>jdk-8u121-linux-i586.tar.gz</td>
</tr>
<tr>
<td>Linux x64</td>
<td>159.96 MB</td>
<td>jdk-8u121-linux-x64.rpm</td>
</tr>
<tr>
<td>Linux x64</td>
<td>174.76 MB</td>
<td>jdk-8u121-linux-x64.tar.gz</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>223.21 MB</td>
<td>jdk-8u121-macosx-x64.dmg</td>
</tr>
<tr>
<td>Solaris SPARC 64-bit</td>
<td>139.64 MB</td>
<td>jdk-8u121-solaris-sparcv9.tar.Z</td>
</tr>
<tr>
<td>Solaris SPARC 64-bit</td>
<td>99.07 MB</td>
<td>jdk-8u121-solaris-sparcv9.tar.gz</td>
</tr>
<tr>
<td>Solaris x64</td>
<td>140.42 MB</td>
<td>jdk-8u121-solaris-x64.tar.Z</td>
</tr>
<tr>
<td>Solaris x64</td>
<td>96.9 MB</td>
<td>jdk-8u121-solaris-x64.tar.gz</td>
</tr>
<tr>
<td><strong>Windows x86</strong></td>
<td><strong>189.36 MB</strong></td>
<td><strong>jdk-8u121-windows-i586.exe</strong></td>
</tr>
<tr>
<td>Windows x64</td>
<td>195.51 MB</td>
<td>jdk-8u121-windows-x64.exe</td>
</tr>
</tbody>
</table>

### Java SE Development Kit 8u121 Demos and Samples Downloads

You must accept the Oracle Binary Code License Agreement to download this software.
JDK Installation !!

Welcome to the Installation Wizard for Java SE Development Kit 8 Update 121

This wizard will guide you through the installation process for the Java SE Development Kit 8 Update 121.

The Java Mission Control profiling and diagnostics tools suite is now available as part of the JDK.
JDK Installation Completed!!

Java SE Development Kit 8 Update 121 - Complete

Java SE Development Kit 8 Update 121 Successfully Installed

Click Next Steps to access tutorials, API documentation, developer guides, release notes and more to help you get started with the JDK.

Next Steps

Close
JDK Installation x86 - Confirm !!
JDK Installation - Confirm !!

```
C:\Users\Thomas>java -version
java version "1.8.0_121"
Java(TM) SE Runtime Environment (build 1.8.0_121-b13)
Java HotSpot(TM) 64-Bit Server VM (build 25.121-b13, mixed mode)
C:\Users\Thomas>
```
Paros License Agreement - the Clarified Artistic License.

For the other libraries included in Paros, please refer to respective licenses of the libraries enclosed with this package.

Gianluca Della Vedova

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:
PAROS Execution

Disclaimer: You should only use this software to test the security of your own web application or those you are authorized to do so. parosproxy.org takes no responsibility for any problems in relation to running Paros against any applications or machines.

This program is free software; you can redistribute it and/or modify it under the terms of the Clarified Artistic License as published in the Free Software Foundation. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the Clarified Artistic License for more details.

For queries please send to contact@parosproxy.org

This product includes softwares developed by the Apache Software Foundation http://www.apache.org licensed under Apache License 2.0. HSOLDB is licensed under BSD license. JDIC is licensed by Sun Microsystems, Inc under the LGPL license. The Copyrights of these softwares belong to their respective owners.
HTTP Intercept – PAROS Ready to Use!

User (Browser) → User Proxy → PAROS → Web Server

1. Request → 2. Modified Request
Cyber Space Hacking Tool – Paros

- Paros Main Functional Modules

1. **Crawl** : Collect URL Structure, Webpage Information
2. **Scan** : Find Vulnerable Pattern by Collected Information
4. **Proxy** : Provide HTTP Proxy Platform
Proxy Server Setting
IE Browser

Internet Options

To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.
- Never dial a connection
- Dial whenever a network connection is not present
- Always dial my default connection
  Current : None
  Set default

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.
Proxy Server Setting
IE Browser

Internet Options

Local Area Network (LAN) Settings

Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

- Automatically detect settings
- Use automatic configuration script

Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

- Address: 127.0.0.1
- Port: 5000

Bypass proxy server for local addresses

OK

Local Area Network (LAN) settings
LAN Settings do not apply to dial-up connections. Change Settings above for dial-up connections.
Proxy Server Setting Chrome Browser
Proxy Server Setting
Chrome Browser
Proxy Server Setting
Chrome Browser
Setting Paros Local Proxy: Tools >> Options >> Local Proxy

Address (e.g., localhost, 127.0.0.1) : localhost
Port (e.g., 8080) : 5000

Set your browser proxy settings using the above. The http port and https port must be the same port as above.
Web Port Number ➔ Jump to Pertinent Service Program
**Web Port Number (16bits-64k) → Assigned Service Handler**

**IANA:**
Internet Assigned Numbers Authority

<table>
<thead>
<tr>
<th>Label on Column</th>
<th>Service Name</th>
<th>UDP and TCP Port Numbers Included</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>Domain Name Service – UDP</td>
<td>UDP 53</td>
</tr>
<tr>
<td>DNS TCP</td>
<td>Domain Name Service – TCP</td>
<td>TCP 53</td>
</tr>
<tr>
<td>HTTP</td>
<td>Web</td>
<td>TCP 80</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Secure Web (SSL)</td>
<td>TCP 443</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transport</td>
<td>TCP 25</td>
</tr>
<tr>
<td>POP</td>
<td>Post Office Protocol</td>
<td>TCP 109, 110</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management</td>
<td>TCP 161,162 UDP 161,162</td>
</tr>
<tr>
<td>TELNET</td>
<td>Telnet Terminal</td>
<td>TCP 23</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td>TCP 20, 21</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell (terminal)</td>
<td>TCP 22</td>
</tr>
<tr>
<td>AFP IP</td>
<td>Apple File Protocol/IP</td>
<td>TCP 447, 548</td>
</tr>
</tbody>
</table>
Paros Scanning

HTTP Request
HTTP Response

Crawl Structure

Header part

Body part

Crawl Information

URL/URI

Web Log Information
Paros modify HTTP Data

A Simple Form with JavaScript Validation

```
<title>A Simple Form with JavaScript Validation</title>

<script type="text/javascript">

/*

Function validate_form ()
{
    var valid = true;

    if ( document.contact_form.contact_name.value == "" )
    {
        alert ( "Please fill in the 'Your Name' box." );
        valid = false;
    }

    return valid;

}*/
```

Please Enter Your Name

Your Name: [ ]

Send Details
Paros intercept & modify HTTP Data
Paros intercept & modify HTTP Data
Paros Demonstration!

http://www.skku.edu/index_pc.jsp >> global
http://www.skku.edu/eng_home/index.jsp

GET http://admission-global.skku.edu/admission/about/welcome.jsp HTTP/1.1

GET http://admission-global.skku.edu/admission/undergraduate/schedule.jsp HTTP/1.1

Hack
http://admission-global.skku.edu/admission/about/contact.jsp
Wrap Up!

1. Stateless Web Programming
2. Cookie
3. HTTP GET and POST Method
4. Paros Proxy Server Capability
WWW Web Service Overview – Look Around!
#1 SQL Injection
#2 Broken Authentication and Session Management
#3 XSS: Cross-Site Scripting
#4 Insecure direct object reference
#5 Security misconfiguration
#6 Sensitive data exposure
#7 Missing function level access control
#8 Cross-site request forgery
#9 Using components with known vulnerabilities
#10 Invalidated redirects and forwards
FAILED OWASP TOP 10

How many apps fail the OWASP Top 10 upon initial risk assessment?

Financial: 58%
Financial Services: 61%

Manufacture: 65%
Manufacturing: 68%

Technology: 68%
Technology: 68%

Healthcare: 69%

Retail: 70%
Retail + Hospitality: 70%

Government: 76%