Hacking for Fun and Profit

W3Lc0me to Th3 Fu1ur

💀 How to break stuff
💀 How to trade
💀 How to hide
💀 Help!
Knowing the enemy
E1 - Who am I

^ Ivan Bütler, Uznach, 31.12.1970

^ Speaker at **Blackhat** 2008 Las Vegas

^ Lecturing at University of Applied Science Rapperswil

^ Lecturing at University of Applied Science Lucerne

^ Founder of Compass Security AG

^ Founder of **Swiss Cyber Storm II / Wargames / Hacking-Lab**

^ Passionate Swiss Security Researcher

^ Husband of Cornelia and father of Tim and Nick (7 & 9)
Compass Security – Swiss Pentesters
Welcome @ BYOL - IT Underground

This BOYL Topics – **Web Security**

- Bypass Authorization
- Session Fixation
- Cross Site Scripting
- SQL Injection
- Xpath Injection
- XSRF
- JSON Hijacking
- Click Jacking
- Observation Plugin
- XML Attack
- Applet Hacking
- Java Script Malware Analysis
- Oracle Wargame
- URL Redirection Attack
Hacking-Lab

- Remote Security Lab
- Swiss Cyber Storm II
- Computer Wargames / BYOL
Hacking for Fun and Profit

How does it work?

- **Register** a Hacking-Lab Account
- Choose your favorite Wargame
- **Exploit** the vulnerability
- Get **Points** from the Jury
- Improve your Ranking
Hacking-Lab Infrastructure

Compass Security E-Lab Infrastructure

- glocken.hacking-lab.com
- xssshell.hacking-lab.com
- myspace.hacking-lab.com

OpenVPN Gateway

192.168.200.0/24

Internet PC
Wargame Testing Webapplications
Wargame Testing Webapplication

- The education applications are developed by Compass Security
- The applications are vulnerable
- Please don't perform a Denial of Service Attack (this is easy)
- Please don't drop databases (this is easy too)
- Important URLs
  - glocken.hacking-lab.com (vulnerable app)
  - www.hacking-lab.com (lab cases)
- Login Accounts for the Wargames
  - UserID's: hacker10....hacker40
  - Passwords: compass
Registered -> Choose your Wargame

### Event Cases

#### IT Underground Warsaw 2009

<table>
<thead>
<tr>
<th>Name</th>
<th>Level</th>
<th>Duration</th>
<th>Details / Solved</th>
<th>Solved by</th>
<th>Pt.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2101 Web Security: Bypassing Authorization</td>
<td>1</td>
<td>30</td>
<td>Details / Send Solution</td>
<td>0</td>
<td>⭐</td>
</tr>
<tr>
<td>2202 Web Security: Session Fixation Attack</td>
<td>1</td>
<td>10</td>
<td>Details / Send Solution</td>
<td>0</td>
<td>⭐</td>
</tr>
<tr>
<td>2300 Web Security: Cross Site Scripting with Input Val</td>
<td>1</td>
<td>10</td>
<td>Details / Send Solution</td>
<td>0</td>
<td>⭐</td>
</tr>
<tr>
<td>2310 Web Security: SQL-Injection Login Form</td>
<td>1</td>
<td>15</td>
<td>Details / Send Solution</td>
<td>0</td>
<td>⭐</td>
</tr>
<tr>
<td>2310 Web Security: SQL-Injection with UNION</td>
<td>1</td>
<td>15</td>
<td>Details / Solved</td>
<td>0</td>
<td>⭐</td>
</tr>
<tr>
<td>2320 Web Security: URL Redirection Attack</td>
<td>1</td>
<td>15</td>
<td>Details / Send Solution</td>
<td>0</td>
<td>⭐</td>
</tr>
<tr>
<td>2605 Web Security: XPath Injection</td>
<td>1</td>
<td>15</td>
<td>Details / Send Solution</td>
<td>0</td>
<td>⭐</td>
</tr>
</tbody>
</table>
Who is being exploited?

- I will play the **victim**!
- Talk to me once you are ready
- I will click on every link you want
- swisscyberstorm@gmail.com
Global Ranking Page – Get Points

![Hacking Lab Image]

### Global Ranking

**My Ranking**

<table>
<thead>
<tr>
<th>Rank</th>
<th>Nickname</th>
<th>Team</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CrypTom</td>
<td>🇨🇭</td>
<td>405</td>
</tr>
<tr>
<td>2</td>
<td>allotria</td>
<td>🇨🇭</td>
<td>405</td>
</tr>
<tr>
<td>3</td>
<td>Disenchant and Baboo</td>
<td>🇨🇭</td>
<td>325</td>
</tr>
<tr>
<td>4</td>
<td>remove</td>
<td>🇨🇭</td>
<td>315</td>
</tr>
<tr>
<td>5</td>
<td>rebel</td>
<td>🇨🇭</td>
<td>275</td>
</tr>
<tr>
<td>6</td>
<td>Disenchant</td>
<td>🇨🇭</td>
<td>260</td>
</tr>
<tr>
<td>7</td>
<td>stefan.wenigmann</td>
<td>🇨🇭</td>
<td>250</td>
</tr>
<tr>
<td>8</td>
<td>wip81</td>
<td>🇨🇭</td>
<td>250</td>
</tr>
<tr>
<td>9</td>
<td>Simone</td>
<td>🇨🇭</td>
<td>250</td>
</tr>
<tr>
<td>10</td>
<td>Tommy27</td>
<td>🇨🇭</td>
<td>250</td>
</tr>
<tr>
<td>11</td>
<td>Andi</td>
<td>🇨🇭</td>
<td>250</td>
</tr>
<tr>
<td>12</td>
<td>ers</td>
<td>🇨🇭</td>
<td>200</td>
</tr>
<tr>
<td>13</td>
<td>rac83</td>
<td>🇨🇭</td>
<td>185</td>
</tr>
<tr>
<td>14</td>
<td>skskillL</td>
<td>🇨🇭</td>
<td>180</td>
</tr>
</tbody>
</table>
How to prepare for the Wargames?

- **Bring** your own laptop
- Use **web inspection proxies**
- Use your brain
- Have your **landing** page available
  - Your personal web server on your laptop
  - Your personal tomcat server on your laptop
- **Tools that are recommended for the Wargames**
  - Wireshark, Paros, Burp, WebScarab, LiveHttpHeader, Add N Cookie Editor, Tamper Data, Editor, Local web server, netcat, jad, malzilla,
What is a landing page?

Landing Page: your own web server

Example JSON Hijacking

```
JSON Object
( confidential data)
```

glocken.hacking-lab.com
Compass Security AG, Switzerland
Ethical Hacking & Penetration Testing

Sign-Up a Hacking-Lab Account
Choose your Lab
Solve your Lab
Get Points
Ask – if required
What are the Wargames about?

Short Introduction
Introduction Wargames

Available Wargames

- Bypass Authorization
- Session Fixation
- Cross Site Scripting
- SQL Injection
- Xpath Injection
- XSRF
- JSON Hijacking
- Click Jacking
- Observation Plugin
- XML Attack
- Applet Hacking
- Java Script Malware Analysis
- Oracle Wargame
- URL Redirection Attack
Bypassing Authorization

- Authenticate with hacke10, hacker11, hacker12 ... hacker40 with the password "compass"

- Every user has a credit-card number

- Find a way to get other users profile information by manipulating the request where the profile is shown

- Test your own profile first, then get other profiles
Session Fixation

- Authenticate with hacke10, hacker11, hacker12 ... hacker40 with the password „compass“

- Use the application URL from the lab description! (important)

- Perform a session fixation attack.

- You have solved this exercise if you are authenticated to the web app, without entering the password – the victim entered the password for you

- Hacking-Lab plays the role of the victim!
Cross Site Scripting

- Authenticate with hacke10, hacker11, hacker12 ... hacker40 with the password „compass“

- Use the application URL from the lab description! (important)

- Perform a XSS Attack

- You have solved this exercise if you have stolen the victim’s session information

- Hacking-Lab plays the role of the victim!
SQL Injection (Simple)

- Don't authenticate with a password – authenticate with an SQL injection attack
- Use the application URL from the lab description! (*important*)
- Perform a SQLi
- You have solved this exercise if you can login to any account without knowing the password
SQL Injection (Advanced)

- Find the second SQL injection vulnerability (not the login page from the case before)
- Use the application URL from the lab description! (important)
- Perform a SQLi attack
- You have solved this exercise if you can extract name, surname, creditcard with one single sql injection exploit
Xpath Injection

- Find the Xpath injection vulnerability (transaction id)
- Use the application URL from the lab description! (important)
- Perform a Xpath injection attack
- You have solved this exercise if you can extract others than your own transaction within the shop (other transactions disclose other users credit card information)
JSON Hijacking

- The vulnerable cow-bell shop has a JSON interface. The interface returns profile information of the authenticated user.

- Use the application URL from the lab description! (important)

- Perform a JSON hijacking attack

- You have solved this exercise if you can store the victim’s profile information to your landing page

- Hacking-Lab plays the role of the victim (required)
Click Jacking

- Create a click jacking web app that hides cow-bell shopping
- Use the application URL from the lab description! (important)
- Perform a Click Jacking attack
- Hacking-Lab plays the role of the victim (required)
Observation Plugin

- Develop a Firefox Plugin based on LiveHttpHeader that observes the users sessions and stores them to your landing page
- Use the application URL from the lab description! (important)
- Compile the observation plugin for firefox
- Hacking-Lab plays the role of the victim (required)
XML Attack

- Exploit the XML search functionality in the cow-bell show

- Extract /etc/passwd and /etc/shadow from the cow-bell server and crack them

- Use the application URL from the lab description! (important)

- You have solved this wargame once you have cracked the accounts
Applet Hacking

- Applets use serialized objects in between the browser and the application. They can’t be analyzed with an inspection proxy.
- But the server does not check the price when ordering cow-bells.
- Use the application URL from the lab description! (important)
- You have solved this wargame if you can buy cow-bells with any price you want (1 EURO per bell).
Java Script Malware Analysis

- Hacker‘s are injecting obfuscated java scripts into vulnerable web apps

- Use the application URL from the lab description! (important)

- De-Obfuscate the java script. Show the result to Hacking-Lab

- Explain the malware – get Points
Oracle Wargame

- Advanced SQL Injection Wargame provided by Alexander Kornbrust – Red Database Security
- Use the application URL from the lab description! (important)
- Exploit the application with advanced sql injection techniques
- Get points
URL Redirection Attack

- Find the url redirection vulnerability in the cow-bell shop
- Exploit the redirection and fool the Hacking-Lab victim
- Use the application URL from the lab description! (important)
- You have solved this wargame if you can hijack the victim‘s identity
- Hacking-Lab play‘s the role of the victim
Thank you for Reading

Compass Security AG, Switzerland
Ethical Hacking & Penetration Testing

E1

ivan.buetler@csnc.ch
e1@hacking-lab.com

Compass Security AG
Swiss Ethical Hacking
www.csnc.ch