**Combinatorial Testing Methods for XSS Vulnerabilities**

Dimitris E. Simos, Bernhard Garn, Jovan Zivanovic, Manuel Leithner, Josip Bozic, Franz Wotawa

**XSSInjections**
- Unsanitized user input displayed on web application.
- Malicious users can add HTML-Script element.
- JavaScript gets executed in client machine.

**Attack Model**

```
(function (r) { [r].concat([1, 3, 1, 3, 1, 3, 1, 3], r); })
```

**XSSInjector**
- Prototype tool for executing CT generated attack vectors.
- Browser Oracle for checking executed JavaScript.

**Case Study**
- WAVSEP: Well known verification framework with known vulnerabilities, used to evaluate automated web application vulnerability scanners.
- Piwigo: A PHP-based photo gallery software.
- MyBB: Self-hosted bulletin board application.
- Koha: An integrated library system written in Perl.
- W3C tidy service: Online tool for validating and fixing HTML code.

**Found Vulnerabilities**

**Evaluation**

**WAVSEP Injection Range (Browser Oracle)**

<table>
<thead>
<tr>
<th>SUT</th>
<th>Grammar 1</th>
<th>Grammar 2</th>
<th>Grammar 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAVSEP</td>
<td>2</td>
<td>57</td>
<td>516</td>
</tr>
<tr>
<td>Piwigo</td>
<td>2</td>
<td>48</td>
<td>115</td>
</tr>
<tr>
<td>MyBB</td>
<td>2</td>
<td>46</td>
<td>51</td>
</tr>
<tr>
<td>Koha</td>
<td>2</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>29</td>
<td>0</td>
</tr>
</tbody>
</table>