Common Security Flaws in JavaScript based Applications

Paul Muntean
paul@sec.in.tum.de

Chair for IT Security / I20
Prof. Dr. Claudia Eckert
Technical University of Munich

25.01.2016
Outline

1. Organization and Requirements
2. Grading
3. Time Table
4. Seminar Topics
5. Literature Research
6. Next Steps
7. Q&A
The seminar will be organized as a scientific conference:

1. Familiarization phase (approx. 2 Week)
2. Manufacturing phase (approx. 6 Week)
3. Review phase (approx. 2 Week)
4. Improvement phase (approx. 2 Week)
5. Talk preparation (approx. 1 Week)
6. Talk and Discussion
## Requirements

### Report Elaboration
- Delivery of a scientific paper with about $\geq 10$ pages in length
- Usage of \LaTeX\ is mandatory for all
- Formatting with the \LaTeX-Style of Springer (LNCS)

### Reviews
- Each one of you creates two anonymous reviews about other two Reports
- Size of the one review: approx. one page in \LaTeX
- Additionally each of you will get an review from us

### Presentation
- Preparing of a presentation (Tool free choice)
- 30 Minutes presentation
- Afterwards 15 minutes discussion
The Grading is comprised of all personal contributions of this seminar and is composed of:

- Report (50%)
- Presentation (25%)
- Delivered review (15%)
- Participation and discussion (10%)
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.04.</td>
<td>Kick-off</td>
</tr>
<tr>
<td>18.04. - 27.06.</td>
<td>Regular meetings (Presence mandatory)</td>
</tr>
<tr>
<td>02.05.</td>
<td>Delivery of the literature research and Outline of the report</td>
</tr>
<tr>
<td>09.05. - 27.06.</td>
<td>Presentations</td>
</tr>
<tr>
<td>Bis 30.06.</td>
<td>Delivery of the 1. version of the report and End of the presentation phase</td>
</tr>
<tr>
<td>04.07.</td>
<td>Distribution of the review topics</td>
</tr>
<tr>
<td>Bis 07.07.</td>
<td>Delivery of the reviews</td>
</tr>
<tr>
<td>08.07.</td>
<td>Return of the reviews</td>
</tr>
<tr>
<td>Bis 11.07.</td>
<td>Delivery of the final version of the report</td>
</tr>
<tr>
<td>16.07.</td>
<td>End of lectures</td>
</tr>
<tr>
<td>April</td>
<td>Mai</td>
</tr>
<tr>
<td>-------</td>
<td>-----</td>
</tr>
<tr>
<td>1 2 3</td>
<td>1 8</td>
</tr>
<tr>
<td>4 5 6 7 8 9 10</td>
<td>2 3 4 5 6 7 14 15 16 17 18 19 20 21 22</td>
</tr>
<tr>
<td>11 12 13 14 15 16 17</td>
<td>9 10 11 12 13 14 15 16 17 18 19</td>
</tr>
<tr>
<td>18 19 20 21 22 23 24</td>
<td>23 24 25 26 27 28 29</td>
</tr>
<tr>
<td>25 26 27 28 29 30</td>
<td>30 31</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Juni</th>
<th>Juli</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 2 3 4 5</td>
<td>1 2 3</td>
</tr>
<tr>
<td>6 7 8 9 10 11 12</td>
<td>4 5 6 7 8 9 10</td>
</tr>
<tr>
<td>13 14 15 16 17 18 19</td>
<td>11 12 13 14 15 16 17</td>
</tr>
<tr>
<td>20 21 22 23 24 25 26</td>
<td>18 19 20 21 22 23 24</td>
</tr>
<tr>
<td>27 28 29 30</td>
<td>25 26 27 28 29 30 31</td>
</tr>
</tbody>
</table>
Before we go to the topics...
Questions, comments, need for discussion?
Seminar Topics

Overview

1. Prevention of JIT-ROP attacks using JIT generated code relocation
2. Randomization based protection
3. Fine-grained object-level access control protection against third-party web browser scripts
4. CFI based protection of JIT compiled code
5. CFI based protection against JIT-ROP attacks based on modularity
6. Per-input based protection against JIT-ROP attacks
7. CFI based protection against JIT-ROP attacks for JIT generated code
8. Cross-Site Script inclusion prevention
9. Randomization based security against JIT-ROP attacks for commonly used JavaScript engines
10. Malicious JavaScript based ROP attack on commonly used JavaScript engines
11. Prevention of privilege escalation attacks based on third-party web scripts
12. JavaScript based extension to the last-level cache attack
Prevention of JIT-ROP attacks using JIT generated code relocation


Randomization based protection


Fine-grained object-level access control protection (defence) against third-party web browser apps

CFI based protection (defence) of JIT compiled code in order to protect from ROP attacks,


CFI based protection (defence) against JIT-ROP attacks based on modularity


Per-Input Control-Flow Integrity per input based protection (defence) against JIT-ROP attacks

CFI based protection (defence) against JIT-ROP attacks for JIT generated code based on a fine-grained Control Flow Graph (CFG)


Cross-Site Script Inclusion prevention (defence)


malicious JavaScript based ROP attack on commonly used JavaScript engines

Seminar Topics (4)

prevention (defence) of privilege escalation based on third-party web scripts


JavaScript based extension to the last-level cache attack


randomization based protection (defence) w.r.t. to JIT-ROP attacks for the Google V8 engine

Who wants which topic?
Goal:

- To find relevant Literature
- Main arguments, Techniques or Approaches...
  1. find,
  2. understand,
  3. explain,
  4. prove them
- Structure Topics
  - Report structure
Literature Research & Sources

Good

- Books, Library
- http://portal.acm.org/
- http://www.springerlink.com/
- http://www.computer.org/
- http://citeseer.ist.psu.edu/
- http://scholar.google.com/

Wrong

- Heise-Newsticker
- Wikipedia
- e.g., Website XYZ
Access to Literature

Through the Authors Website
- Authors publish the papers mostly on their websites
- Other resources can be found through Google Scholar

Through Springer, ACM, IEEE
- Download of papers costs
- TUM has full rights to download papers
- Usage on an Proxy-Server required: www.lrz.de
- Access through the proxy in the TUM web is restricted
Next Steps

\textbf{LaTeX-Introduction}

- Is there the need?
- Schedule a date?

\textbf{ToDos in the Familiarization phase}

1. Literature research
2. Create report structure