AutoCSP: Automatically Retrofitting CSP to Web Applications

Mattia Fazzini, Prateek Saxena, Alessandro Orso
Web Applications
Web Applications

The New York Times

amazon.com
Web Applications

The New York Times

YouTube

amazon.com
Web Applications

The New York Times

YouTube

amazon.com

facebook
Web Applications

Taobao.com

PayPal

The New York Times

Yahoo!

GitHub

YouTube

Google

Amazon

LinkedIn

Facebook

Wikipedia
Web Applications

Popular

Taobao.com
PayPal
The New York Times
Yahoo!
GitHub
YouTube
Google
Amazon
Windows Live
LinkedIn
Facebook
Wikipedia
Web Applications

- Taobao.com
- Twitter
- PayPal
- Baidu
- The New York Times
- Yahoo!
- Sina
- GitHub
- YouTube
- Google
- Amazon
- Windows Live
- LinkedIn
- Facebook
- Wikipedia

Popular

Target
Cross-Site Scripting (XSS)
Cross-Site Scripting (XSS)

Hydara et. al., 2014

XSS Publications
Cross-Site Scripting (XSS)

Hydara et. al., 2014

XSS Publications

18 Sep 2014
“eBay Under Fire After Cross Site Scripting Attack”

16 Sep 2013
“NASDAQ Website Vulnerable to XSS Attacks”

28 May 2013
“PayPal vulnerable to cross-site scripting again”
Cross-Site Scripting (XSS)

Hydara et. al., 2014

XSS Publications

Vulnerability Classes (2014)

WhiteHat Security, 2014

- 18 Sep 2014
  “eBay Under Fire After Cross Site Scripting Attack”

- 16 Sep 2013
  “NASDAQ Website Vulnerable to XSS Attacks”

- 28 May 2013
  “PayPal vulnerable to cross-site scripting again”
Content Security Policy (CSP)
Content Security Policy (CSP)
Content Security Policy (CSP)
Content Security Policy (CSP)
Content Security Policy (CSP)

Server

Client

Name

Content-Security-Policy

Directives

script-src  style-src  img-src  frame-src  ...

W3C®
Content Security Policy (CSP)

Server

Client

W3C®

Name

Content-Security-Policy

Directives

script-src  style-src  img-src  frame-src  ...

Values

Content Security Policy (CSP)

Server

Client

Name

Content-Security-Policy

Directives

script-src

style-src

img-src

frame-src

Values

Content Security Policy (CSP)

<table>
<thead>
<tr>
<th>Directives</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>script-src</td>
<td>'none', 'self', domain, 'unsafe-inline', 'unsafe-eval'</td>
</tr>
<tr>
<td>style-src</td>
<td></td>
</tr>
<tr>
<td>img-src</td>
<td></td>
</tr>
<tr>
<td>frame-src</td>
<td></td>
</tr>
</tbody>
</table>

Server

Client
Motivating Example

Server-side Code

```php
<?php
print("<html><head>");
...
$out="<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>
print($out);
print("<a href='javascript:grades();'>Grades</a>");
while($assignment=mysql_fetch_row($query)){
  print("<td style='text-align:left;'>
  $assignment[5].
  </td>");
}
print("</html>"; ?>
```

Web Page

```html
<html>
<head>
...
</head>
<body>
...
<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>
<a href='javascript:grades();'>Grades</a>
...
while($assignment=mysql_fetch_row($query)){
  print("<td style='text-align: left;'>
    <script>alert('XSS');</script>
  </td>");
}
</body>
</html>
```
Motivating Example

Server-side Code

```php
<?php
print("<html>
 <head>");
...

$out = "<script>
function grades(){
  document.student.page2.value=3;
  document.student.submit();
 }
</script>
print($out);
...

print("<a href='javascript:grades();'>Grades</a>");
...

while($assignment = mysql_fetch_row($query)){
...

print("<td style='text-align:left;'>"
$assignment[5].
"</td>");
...

print("</html>"); ?>
```

Web Page

```html
<html>
<head>
...
<body>
...
<script>
function grades(){
  document.student.page2.value=3;
  document.student.submit();
 }
</script>
<a href='javascript:grades();'>Grades</a>
...
<td style='text-align: left;'>
<script>alert('XSS');</script>
</td>
...
</body>
</html>
```
Motivating Example

Server-side Code

```php
<?php
print("<html>
<head>");
...
$out="<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>"
...
print($out);
...
print("<a href='javascript:grades();'>Grades</a>"
...
while($assignment = mysql_fetch_row($query)){
...
print("<td style='text-align:left;'>
.$assignment[5].
"</td>"));
...
print("</html>"); ?>
```

Web Page

```html
<html>
<head>
...
</head>
<body>
...
<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>
...
<a href='javascript:grades();'>Grades</a>
...
<td style='text-align: left;'>
<script>alert('XSS');</script>
</td>
...
</body>
</html>
```
Motivating Example

Server-side Code

```php
<?php
print("<html>\n<head>\n...
$Out="<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>"
print($out);
print("<a href='javascript:grades();'>Grades</a>"
while($assignment = mysql_fetch_row($query)){
print("<td style='text-align:left;'>".$assignment[5]."</td>".Promise prom })
```

Web Page

```html
<html>
<head>
...
</head>
<body>
<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>
<a href='javascript:grades();'>Grades</a>
while($assignment = mysql_fetch_row($query)){
print("<td style='text-align:left;'>".$assignment[5]."</td>";Promise prom })
```
Motivating Example

Server-side Code

```php
<?php
print("<html>
 <head>
 ... ...
 $out="<script>
 4  function grades(){
 5   document.student.page2.value=3;
 6   document.student.submit();
 7 }
 8  </script>"
 9 ... ...
10 print($out);
11 ...
12 print("<a href='javascript:grades();'>
13   Grades</a>"");
14 ...
15 while($assignment =
16   mysql_fetch_row($query)){
17    ...
18    print("<td style='text-align: left;'>"$
19      .$$assignment[5].
20    "</td>");
21    ...
22 } ...
23 print("</html>"; ?>
```
Motivating Example

Server-side Code

```php
<?php
  print("<html>
  <head>");
  ...
  $out="<script>
  ...
  function grades(){
    document.student.page2.value=3;
    document.student.submit();
  };
  ...
  print($out);
  ...
  print("<a href='javascript:grades();'>Grades</a>");
  ...
  while($assignment = mysql_fetch_row($query)){
    ...
    print("<td style='text-align: left;'>"
    ...
    $assignment[5].
    "</td>"可谓);
    ...
  
  print("</html>"; ?>
```

Web Page

```html
<html>
  <head>
    ...
    function grades(){
    ...
    document.student.page2.value=3;
    document.student.submit();
  }
  ...
  <a href='javascript:grades();'>Grades</a>
  ...
  <td style='text-align: left;'>
    <script>alert('XSS');</script>
  </td>
  ...
</body>
</html>
```
Motivating Example

Server-side Code

```php
<?php
  print("<html>
    <head>
      ...
    </head>
    $out="<script>
      function grades(){
        document.student.page2.value=3;
        document.student.submit();
      }
    </script>"
    ...
  print("</html>"');

while($assignment = mysql_fetch_row($query)){
  print("<td style='text-align: left;'>")
  $assignment[5]."</td>");
  ...
print("</html>"); ?>
```

Web Page

```html
<html>
  <head>
    ...
  </head>
  <body>
    ...
  </script>
    function grades(){
    document.student.page2.value=3;
    document.student.submit();
  }
</script>
  ...
  <a href='javascript:grades();'>Grades</a>
  ...
  <td style='text-align: left;'>"
  $assignment[5]."</td>");
  ...
</html>
```
Motivating Example

Server-side Code

```php
<?php
print("<html>\n <head>");
...
$out="<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>"
print($out);
...
print("<a href='javascript:grades();'>Grades</a>"
while($assignment = mysql_fetch_row($query)){
  ...
  print("<td style='text-align:left;'>\n  .$assignment[5].\n  "</td>"
  ...
  print("</html>"; ?>
```

Web Page

```html
<html>
<head>
...
</head>
<body>
...
<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>
<a href='javascript:grades();'>Grades</a>
while($assignment = mysql_fetch_row($query)){
  ...
  print("<td style='text-align: left;'\n  .alert('XSS')\n  "</td>"
  ...
  print("</html>"
```
Motivating Example

Server-side Code

```php
<?php
print("<html>
 <head>");
...
$out = "<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>
...
print($out);
...
print("<a href='javascript:grades();'>Grades</a>");
...
while($assignment = mysql_fetch_row($query)){
...
print("<td style='text-align:left;'>",
 $assignment[5].
 "</td>");
...
print("</html>"); ?>
```

Web Page

```html
<html>
<head>
...
</head>
<body>
...
<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>
...
<a href='javascript:grades();'>Grades</a>
...
<td style='text-align: left;'>
<script>alert('XSS');</script>
</td>
...
</body>
</html>
```
Motivating Example

Server-side Code

```php
<?php
print("<html>
<head>");
...
$out="<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>"
print($out);
...
print("<a href='javascript:grades();'>Grades</a>"
while($assignment = mysql_fetch_row($query)){
...
print("<td style='text-align:left;'>"
$assignment[5]."</td>";}
print("</html>"); ?>
```

Web Page

```html
<html>
<head>
...
</head>
<body>
...
<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>
<a href='javascript:grades();'>Grades</a>
...
</body>
</html>
```
Motivating Example

Server-side Code

```php
<?php
print("<html>
 <head>");
...
$out = "<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}

while($assignment = mysql_fetch_row($query)){
    print("<td style='text-align:left;'>"
        . $assignment[5].
    "</td>");
...
print("</html>"); ?>
```

Web Page

```html
1 <html>
2 <head>
3 ...
4 </head>
5 <body>
6 ...
7 <script>
8 function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>
8 function grades(){
document.student.page2.value=3;
document.student.submit();
}
9 <a href='javascript:grades();'>
10 Grades
11 </a>
12 ...
13 ...
14 <td style='text-align: left;'>
15 <script>alert('XSS');</script>
16 </td>
17 ...
18 ...
19 <td style='text-align: left;'>
20 <script>alert('XSS');</script>
21 </td>
22 ...
23 </body>
24 </html>
```
Motivating Example

Server-side Code

```php
<?php
print("<html>
<head>"
);
...
3 $out="<script>
4 function grades(){
5    document.student.page2.value=3;
6    document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a href='javascript:grades();'>Grades</a>"
);
13 ...
14 while($assignment = mysql_fetch_row($query)){
15    ...
16    print("<td style='text-align:left;'>"
17        . $assignment[5].
18    "</td>");
19    ...
20 } print("</html>" ); ?>
```

Web Page

```html
<html>
<head>
...
3 ...
4 </head>
5 <body>
6 ...
7 </script>
8 function grades(){
9    document.student.page2.value=3;
10   document.student.submit();
11 }
12 </script>
13 ...
14 <a href='javascript:grades();'>Grades</a>
15 ...
16 <script>alert('XSS');</script>
17 </a>
18 ...
19 <td style='text-align: left;'>
20   $assignment[5].
21 </td>
22 ...
23 </td>
24 </body>
24 </html>

Content-Security-Policy:
script-src: ‘unsafe-inline’
style-src: ‘unsafe-inline’
Motivating Example

Server-side Code

```php
<?php
print("<html>
 <head>");
...
$out = "<script>
  function grades(){
    document.student.page2.value=3;
    document.student.submit();
  }
}
</script>"
...
print($out);
...
print("<a href='javascript:grades();'>Grades</a>"
...
while($assignment = mysql_fetch_row($query)){
  ...
  print("<td style='text-align:left;'>"
    .$assignment[5].
  "</td>";
  ...
  }
print("</html>"; ?>
```

Web Page

```html
<html>
<head>
...
</head>
<body>
...
<script>
  function grades(){
    document.student.page2.value=3;
    document.student.submit();
  }
</script>
...
<a href='javascript:grades();'>Grades</a>
...
</body>
</html>
```
Motivating Example

Server-side Code

```php
<?php
print("<html>
<head>
...
</head>
<body>

$out="<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>

print($out);

print("<a href='javascript:grades();'>Grades</a>";

while($assignment = mysql_fetch_row($query)){
...
print("<td style='text-align: left;'>
.$assignment[5].
"</td>";
...
print("</td>";

print("</body>
</html>?

?>
```

Web Page

```html
<html>
<head>
...
</head>
<body>

function grades(){
document.student.page2.value=3;
document.student.submit();
}

<a href='javascript:grades();'>Grades</a>

while($assignment = mysql_fetch_row($query)){
...
$assignment[5].
"</td>";
...
$assignment[5].
"</td>";

print("</body>
</html>
```

Motivating Example

Server-side Code

```php
<?php
print("<html>
<head>
...
</head>
<body>

$out="<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>

print($out);

print("<a href='javascript:grades();'>Grades</a>";

while($assignment = mysql_fetch_row($query)){
...
print("<td style='text-align: left;'>
.$assignment[5].
"</td>";
...
print("</td>";

print("</body>
</html>?
```

Web Page

```html
<html>
<head>
...
</head>
<body>

function grades(){
document.student.page2.value=3;
document.student.submit();
}

<a href='javascript:grades();'>Grades</a>

while($assignment = mysql_fetch_row($query)){
...
$assignment[5].
"</td>";
...
$assignment[5].
"</td>";

print("</body>
</html>
```
Motivating Example

Server-side Code

```php
<?php
print("<html>
<head>");
...
$out="<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>"
print($out);
print("<a href='javascript:grades();'>Grades</a>");
while($assignment = mysql_fetch_row($query)){
  print("<td style='text-align:left;'>
  .$assignment[5].
  "</td>");
}
print("</html>"); ?>
```

CSP-enabled Web Page

```html
<html>
<head>
<script src='uri.js'></script>
<link rel='stylesheet' type='css' href='style.css'/>
</head>
<body>
<a id='uri' href='#'>Grades</a>
<td id='style'><script>alert('XSS');</script></td>
</body>
</html>
```
Motivating Example

**Server-side Code**

```php
<?php
print("<html>
 <head>");
 ...
$out=":<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>"
print($out);
print("<a href='javascript:grades();'>Grades</a>"
while($assignment = mysql_fetch_row($query)){
 print("<td style='text-align:left;'>
.$assignment[5].
"</td>");
 ...
print("</html>"; ?>
```

**CSP-enabled Web Page**

```html
<html>
 <head>
 ...
 <script src='uri.js'>
 </script>
 <link rel='stylesheet' type='css' href='style.css'/>
 ...
 <body>
 ...
 <script src='external.js'>
 </script>
 <a id='uri' href='#'>Grades</a>
 ...
 <td id='style'>
 <script>alert('XSS');</script>
 </td>
 ...
</body>
</html>
```

**Content-Security-Policy:**

script-src: ‘domain’
style-src: ‘domain’
Motivating Example

Server-side Code

```php
<?php
print("<html>
<head>");
...
$out = "<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>"
print($out);
print("<a href='javascript:grades();'>Grades</a>"
while($assignment = mysql_fetch_row($query)){
print("<td style='text-align:left;'>

$assignment[5]
</td>";
}
print("</html>"; ?>
```

CSP-enabled Web Page

```html
<html>
<head>
...
<script src='uri.js'></script>
<link rel='stylesheet' type='css' href='style.css'/>
</head>
<body>
...<script src='external.js'></script>
<a id='uri' href='#'>Grades</a>
...<td id='style'>
<script>alert('XSS');</script>
</td>
</body>
</html>
```

Content-Security-Policy:
- script-src: ‘domain’
- style-src: ‘domain’
Motivating Example

Server-side Code

```
<?php
print("<html>
 <head>");
...
$out="<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>
print($out);
...
print("<a href='javascript:grades();'>Grades</a>");

while($assignment = mysql_fetch_row($query)){
    print("<td style='text-align:left;'>"
    .$assignment[5].
    "</td>");
}
print("</html>"); ?>
```

CSP-enabled Web Page

```
<html>
<head>
...
<script src='uri.js'></script>
<link rel='stylesheet' type='css' href='style.css'/>
</head>
<body>
<script src='external.js'></script>
<a id='uri' href='#'>Grades</a>
<td id='style'><script>alert('XSS');</script></td>
</body>
</html>
```

Content-Security-Policy:
script-src: ‘domain’
style-src: ‘domain’
Motivating Example

Server-side Code

```php
<?php
print("<html>
 <head>");
...
$out="<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>"
print($out);
...
print("<a href='javascript:grades();'>Grades</a>";
while($assignment = mysql_fetch_row($query)){
    print("<td style='text-align:left;'>
    .$assignment[5].
    '</td>");
    ...
print("</html>"; ?>
```

CSP-enabled Web Page

```html
<html>
 <head>
 ...
 <script src='uri.js'>
 </script>
 <link rel='stylesheet' type='css' href='style.css'/>
 ...
 <a id='uri' href='#'>Grades</a>
 ...
 <td id='style'>
 <script>alert('XSS');</script>
 </td>
 ...
 </body>
</html>
```

Goal

Automatically change server-side code to generate CSP-enabled web pages.
AutoCSP Overview
AutoCSP Overview

Inputs

Web App
AutoCSP Overview

Inputs

Web App

Transformed Web App

CSP

WebApp
AutoCSP Overview

Inputs

Web App

Dynamic Tainting

Transformed Web App

CSP
AutoCSP Overview

Inputs

Web App

Dynamic Tainting

Web Page Analysis

Transformed Web App
AutoCSP Overview

Inputs

Web App

Transformed Web App

Dynamic Tainting

Web Page Analysis

CSP Analysis
AutoCSP Overview

Inputs
Web App

Dynamic Tainting

Web Page Analysis

Transformed Web App

Source Code Transformation

Source Code

CSP Analysis
AutoCSP Overview

Inputs

Web App

Transformed Web App

Dynamic Tainting

Source Code Transformation

Source Code

CSP Analysis

CSP

Web Page Analysis

HTML

SCRIPT

STYLE

HTML

SCRIPT

STYLE

CSP

CSP

CSP

CSP

CSP
3 $out="<script>
4 function grades(){
5 document.student.page2.value=3;
6 document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>")
20 .$assignment[5].
21 "</td>");
(1) Dynamic Tainting

```javascript
... 3 $out="<script>
  4  function grades(){
  5    document.student.page2.value=3;
  6    document.student.submit();
  7  }
  8  </script>"
...
 10 print($out);
...
 16 while($assignment =
 17  mysql_fetch_row($query)){
 18    ...
 19  print("<td style='text-align:left;'>".$assignment[5].
 20    "</td>");
```
(1) Dynamic Tainting

```javascript
$\text{3}\$\text{out} = "\text{<script>}
4\text{ function grades()}{
5\text{ document.student.page2.value=3;}
6\text{ document.student.submit();}
7\text{ }$
8\text{ </script>"}
9\text{ }
10\text{ print($out);}
11\text{ }
12\text{ while($assignment =}
13\text{ mysql_fetch_row($query))}{
14\text{ }$
15\text{ print("<td style='text-align:left;'>"}
16\text{ $assignment[5].}
17\text{ "</td>"});
```
(1) Dynamic Taints

```php
function grades() {
    document.student.page2.value = 3;
    document.student.submit();
}
```
(1) Dynamic Tainting

```plaintext
...
3 $out="<script>
4   function grades(){
5     document.student.page2.value=3;
6     document.student.submit();
7   }
8 </script>"
...
10 print($out);
...
16 while($assignment =
17   mysql_fetch_row($query)){
18   ...
19   print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
```
(1) Dynamic Tainting

```php
3 $out="<script>
4 function grades(){
5     document.student.page2.value=3;
6     document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
16 while($assignment =
17     mysql_fetch_row($query)){
18     ...
19     print("<td style='text-align:left;'>".
20     $assignment[5].
21     "</td>";
```

Positive Dynamic Tainting

HTML buffer

Taint buffer

Source buffer
(1) Dynamic Taintng

```
3 $out="<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 print($out);
...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"$assignment[5].
20 "</td>"};
```

**HTML buffer**
```
.. <script> func..
```

**Taint buffer**
```
```

**Source buffer**
```
```
(1) Dynamic Tainting

```javascript
3 $out="<script>
4   function grades(){
5     document.student.page2.value=3;
6     document.student.submit();
7   }
8 </script>"
9
10 print($out);
11 ...
12
15   while($assignment =
16     mysql_fetch_row($query)){
17     ...
18   print("<td style='text-align:left;'>".
19     $assignment[5].
20     "</td>");
21 
```
1) Dynamic Tainting

```
3 $out=":<script>
4 function grades(){
5   document.student.page2.value=3;
6   document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
13 while($assignment =
14   mysql_fetch_row($query)){
15   ...
16   print("<td style='text-align:left;'>"$
17   .$assignment[5].
18   "</td>");
```

<table>
<thead>
<tr>
<th>HTML buffer</th>
<th>. . . &lt; s c r i p t &gt; f u n c . . &gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taint buffer</td>
<td>. . T T T T T T T T T T T T T T</td>
</tr>
<tr>
<td>Source buffer</td>
<td>. . 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10</td>
</tr>
</tbody>
</table>
(1) Dynamic Tainting

```
3 $out="<script>
4     function grades(){
5         document.student.page2.value=3;
6         document.student.submit();
7     }
8 </script>"
9
10 print($out);

16 while($assignment =
17     mysql_fetch_row($query)){
18     ...
19     print("<td style='text-align:left;'>".
20     .$assignment[5].
21     "</td>");
```
(1) Dynamic Tainting

```
3 $out="<script>
4   function grades(){
5     document.student.page2.value=3;
6     document.student.submit();
7   }
8 </script>"
9
10 print($out);
11
16 while($assignment =
17     mysql_fetch_row($query)){
18   ...
19 print("<td style='text-align:left;'>"
20   .$assignment[5].
21   "</td>");
```
(1) Dynamic Tainting

```
3 $out = "<script>
4   function grades(){
5     document.student.page2.value=3;
6     document.student.submit();
7   }
8 </script>"
9
10 print($out);
...
16 while($assignment =
17   mysql_fetch_row($query)){
18   ...
19  print("<td style='text-align:left;'>".
20  . $assignment[5].
21  "</td>");
```

<table>
<thead>
<tr>
<th>HTML buffer</th>
<th>. . &lt;script&gt; func . . &gt; . . &lt;script&gt; alert . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taint buffer</td>
<td>. . T T T T T T T T T T T T T T T T T T . .</td>
</tr>
<tr>
<td>Source buffer</td>
<td>. . 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 . .</td>
</tr>
</tbody>
</table>
## (2) Web Page Analysis

<table>
<thead>
<tr>
<th>Buffer Type</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML buffer</td>
<td>.. &lt;script&gt;func. .. &lt;script&gt;alert ..</td>
</tr>
<tr>
<td>Taint buffer</td>
<td>.. TTTTTTTTTTTTTT ..</td>
</tr>
<tr>
<td>Source buffer</td>
<td>.. 10101010101010101010101010101010 ..</td>
</tr>
</tbody>
</table>
(2) Web Page Analysis

**HTML buffer**
```
.. <script> function .. > .. <script> alert ..
```

**Taint buffer**
```
.. T T T T T T T T T T T T ..
```

**Source buffer**
```
.. 10 10 10 10 10 10 10 10 10 10 10 ..
```

Diagram:
- Document
  - <html>
    - <head>
    - <body>
      - <script> func..
      - <script> alert..
(2) Web Page Analysis

HTML buffer: `..<script>func..</script>..</script>...`  
Taint buffer: `...TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT TT
(2) Web Page Analysis

HTML buffer: \[
\text{.. <script> func .. > .. <script> alert ..}
\]

Taint buffer: \[
\text{.. T T T T T T T T T T T T T T ..}
\]

Source buffer: \[
\text{.. 10 10 10 10 10 10 10 10 10 10 10 ..}
\]
(2) Web Page Analysis

Annotated DOM Tree

HTML buffer: .. <script> func .. > .. <script> alert ..
Taint buffer: .. T T T T T T T T T T T T T ..
Source buffer: .. 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 ..
(3) CSP Analysis
(3) CSP Analysis

Content-Security-Policy: default-src 'none'
(3) CSP Analysis

Content-Security-Policy: default-src ‘none’
(3) CSP Analysis

Content-Security-Policy: default-src ‘none’
(3) CSP Analysis

Content-Security-Policy: default-src ‘none’
(3) CSP Analysis

Content-Security-Policy: default-src ‘none’

```html
<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>
```
(3) CSP Analysis

Content-Security-Policy: default-src ‘none’

```html
<head>
  <script src='external.js'></script>
</head>
<body>
  <script>
    function grades(){
      document.student.page2.value=3;
      document.student.submit();
    }
    </script>
</body>
</html>
```
(3) CSP Analysis


```html
<html>
<head>
<body>
<script>
func;
document.student.page2.value=3;
document.student.submit();
</script>
<script src='external.js'>
</script>
</body>
</html>
```
(3) CSP Analysis


```html
<head>

<body>
  <script>
    function grades()
    {
      document.student.page2.value=3;
      document.student.submit();
    }
    </script>
  <script src='external.js'>
  </script>
</body>
</html>
```
(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'

```html
<script>
function grades(){
  document.student.page2.value=3;
  document.student.submit();
}
</script>

<script src='external.js'></script>

<external.js>

<document>
  <html>
    <body>
      e_script_10
    </body>
  </html>
</document>
```
(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'

```html
<html>
<head>
<body>
<script>
function grades(){
document.student.page2.value=3;
document.student.submit();
}
</script>
<script src='external.js'></script>
</body>
</html>
```
(3) CSP Analysis


```
<script>
    function grades(){
        document.student.page2.value=3;
        document.student.submit();
    }
</script>

<script src='external.js'></script>

external.js

```

```
<script>
    function grades(){
        ...
    }
</script>

```

```
<script src='external.js'></script>

```

```
e_script_10

```
(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'

Edit Set e_script_10
(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'; style-src 'self'

Edit Set e_script_10
(3) CSP Analysis


Edit Set  e_script_10  e_a_12  e_td_19
(3) CSP Analysis

Content-Security-Policy: default-src 'none', script-src 'self'; style-src 'self'

Edit Set  |  e_script_10  |  e_a_12  |  e_td_19
(3) CSP Analysis

(3) CSP Analysis

1 <?php print("<html><head>");
2 ...
3 $out="<script>
4 function grades(){
5  document.student.page2.value=3;
6  document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a href='javascript:grades();'>Grades</a>"上海的);
13 ...
14 while($assignment =
15 mysql_fetch_row($query)){
16  ...
17  print("<td style='text-align:left;'>"
18  $assignment[5].
19  "/td">"上海的);
20  ...
21  "/td">"上海的);
22  ...
23 }
24 print("</html>"); ?>
```php
<?php
   print("<html>
   <head>");

   ...

   $out="<script>
   function grades(){
   document.student.page2.value=3;
   document.student.submit();
   }
   </script>"
   ...

   print($out);
   ...

   print("<a href=javascript:grades();>Grades</a>";

   ...

   while($assignment = mysql_fetch_row($query)){
      ...

      print("<td style='text-align:left;'>".$assignment[5]."</td>");
   ...

   print("</html>"; ?>
```
<?php
print("<html>
<head>");
...
$out = "<script>
function grades()
    document.student.page2.value=3;
    document.student.submit();

</script>"
...
print($out);
...
print("<a href='javascript:grades();'>Grades</a>"
...
while($assignment = mysql_fetch_row($query))
    ...
print("<td style='text-align:left;'>" . $assignment[5]. "</td>";
...
print("</html>"); ?>

function filter_script_10($out){}
function filter_script_10($out){

    $newOut=$out;
    $newScript="<script>function grades(){..}</script>";
    $newScript=str_replace("<script>function grades(){..}</script>",
    "<script src='external.js'></script>",
    $newScript);

    function grades(){
        document.student.page2.value=3;
        document.student.submit();
    }
}

while($assignment = mysql_fetch_row($query)){
    $assignment[5].
    "</td>";
}

print("</html>"); ?>
function filter_script_10($out) {

    $newOut = $out;

    $newScript = "<script>function grades(){..}</script>";

    $newScript = str_replace("<script>function grades(){..}</script>", "<script src='external.js'></script>", $newScript);

    $newOut = str_replace("<script>function grades(){..}</script>", $newScript, $newOut);

    return $newOut;
}

<?php
print("<html>
 <head>\n <head>");
...
3 $out = "<script>
function grades(){
    document.student.page2.value=3;
    document.student.submit();
}
</script>"
...
11 print($out);
12 ...
13 print("<a href='javascript:grades();'>Grades</a>");
14 ...
15 while($assignment = mysql_fetch_row($query)){
...
19 print("<td style='text-align:left;'>".$assignment[5]."</td>");
20 ...
23 }
24 print("</html>"); ?>
(4) Source Code Transformation

Edit Set

<table>
<thead>
<tr>
<th>e_script_10</th>
<th>e_a_12</th>
<th>e_td_19</th>
<th>e_csp_1</th>
</tr>
</thead>
</table>

```php
1 <php print("<html>
  <head>

2 ...

3 $out="<script>
4  function grades(){
5    document.student.page2.value=3;
6    document.student.submit();
7  }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>"
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>".
20 $assignment[5].
21 "</td>");
22 ...
23 }
24 print("</html>"; ?>
```

```php
1 <php print("<html>
  <head>

2 ...

3 $out="<script>
4  function grades(){
5    document.student.page2.value=3;
6    document.student.submit();
7  }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>"
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>".
20 $assignment[5].
21 "</td>");
22 ...
23 }
24 print("</html>"; ?>
```
(4) Source Code Transformation

```php
<?php
print("<html>\n<head>\n...

$out = "<script>
function grades(){
document.student.page2.value = 3;
document.student.submit();
}
</script>

print($out);

print("<a href='javascript:grades();'>Grades</a>");

while($assignment = mysql_fetch_row($query)){
...
print("<td style='text-align:left;'>".$assignment[5]."</td>"第三人
...
print("</html>"; ?>
```
(4) Source Code Transformation

```
1 <?php print("<html>
 <head>");
2 ...
3 $out="<script>
4  function grades(){
5    document.student.page2.value=3;
6    document.student.submit();
7 }
8 </script>"
9 ...
10 print($out);
11 ...
12 print("<a
13 href='javascript:grades();'>
14 Grades</a>"");
15 ...
16 while($assignment =
17 mysql_fetch_row($query)){
18 ...
19 print("<td style='text-align:left;'>"
20 .$assignment[5].
21 "</td>");
22 ...
23 }
24 print("</html>"); ?>
```

```
1 <?php header("Content-Security-Policy:...");...
2 ...
3 $out="<script>
4  function grades(){
5    ...
20    .$assignment[5].
21    "</td>");
22  ...
23  }
24 print("</html>"); ?>
```

```
1 <?php header("Content-Security-Policy:…");…
2 ...
3 $out="<script>
4  function grades(){
5    ...
20    .$assignment[5].
21    "</td>");
22  ...
23  }
24 print("</html>"); ?>
```
Implementation

Dynamic Tainting

CSP Analysis

Web Page Analysis

Source Code Transformation

Java

php
Implementation

Dynamic Tainting
- Zend

CSP Analysis
- Java

Web Page Analysis
- J

Source Code Transformation
- PHP
Implementation

Dynamic Tainting

CSP Analysis

Web Page Analysis

Source Code Transformation

Java

php
Implementation

Dynamic Tainting

CSP Analysis

Web Page Analysis

Source Code Transformation

Zend

Java

php
Implementation

Dynamic Tainting

Web Page Analysis

CSP Analysis

Source Code Transformation

zend

Java

J

php
Empirical Evaluation

Research Questions:
Empirical Evaluation

Research Questions:

**RQ1:** Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?
Empirical Evaluation

Research Questions:

**RQ1:** Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?

**RQ2:** What is the effect of AutoCSP on the performance of the retrofitted web applications?
Empirical Evaluation

Research Questions:

**RQ1:** Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?

**RQ2:** What is the effect of AutoCSP on the performance of the retrofitted web applications?

**RQ3:** How dependent is AutoCSP’s performance on the input used for its taint analysis?
Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?

RQ2: What is the effect of AutoCSP on the performance of the retrofitted web applications?

RQ3: How dependent is AutoCSP’s performance on the input used for its taint analysis?

RQ4: Is automation actually needed to retrofit CSP to web applications?
Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?

RQ2: What is the effect of AutoCSP on the performance of the retrofitted web applications?

RQ3: How dependent is AutoCSP’s performance on the input used for its taint analysis?

RQ4: Is automation actually needed to retrofit CSP to web applications?
### Subjects

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Type</th>
<th>Version</th>
<th>KLOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallery</td>
<td>Photo Sharing</td>
<td>1.5</td>
<td>34.5</td>
</tr>
<tr>
<td>LinPHA</td>
<td>Photo Sharing</td>
<td>1.3</td>
<td>59.6</td>
</tr>
<tr>
<td>MyBB</td>
<td>Forum</td>
<td>1.6</td>
<td>105.9</td>
</tr>
<tr>
<td>OpenEMR</td>
<td>Medical Management</td>
<td>4.1</td>
<td>480</td>
</tr>
<tr>
<td>phpList</td>
<td>Newsletter management</td>
<td>2.10</td>
<td>35.4</td>
</tr>
<tr>
<td>Schoolmate</td>
<td>School Management</td>
<td>1.5</td>
<td>6.5</td>
</tr>
<tr>
<td>Serendipity</td>
<td>Blogging</td>
<td>0.8</td>
<td>49.6</td>
</tr>
</tbody>
</table>
# Subjects

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Type</th>
<th>Version</th>
<th>KLOC</th>
<th>MI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallery</td>
<td>Photo Sharing</td>
<td>1.5</td>
<td>34.5</td>
<td>4</td>
</tr>
<tr>
<td>LinPHA</td>
<td>Photo Sharing</td>
<td>1.3</td>
<td>59.6</td>
<td>4</td>
</tr>
<tr>
<td>MyBB</td>
<td>Forum</td>
<td>1.6</td>
<td>105.9</td>
<td>4</td>
</tr>
<tr>
<td>OpenEMR</td>
<td>Medical Management</td>
<td>4.1</td>
<td>480</td>
<td>4</td>
</tr>
<tr>
<td>phpList</td>
<td>Newsletter management</td>
<td>2.10</td>
<td>35.4</td>
<td>4</td>
</tr>
<tr>
<td>Schoolmate</td>
<td>School Management</td>
<td>1.5</td>
<td>6.5</td>
<td>4</td>
</tr>
<tr>
<td>Serendipity</td>
<td>Blogging</td>
<td>0.8</td>
<td>49.6</td>
<td>4</td>
</tr>
</tbody>
</table>

Malicious Inputs (MI)

CVE Details

OWASP

HTML5 Security Cheatsheet
# Subjects

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Type</th>
<th>Version</th>
<th>KLOC</th>
<th>MI</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallery</td>
<td>Photo Sharing</td>
<td>1.5</td>
<td>34.5</td>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>LinPHA</td>
<td>Photo Sharing</td>
<td>1.3</td>
<td>59.6</td>
<td>4</td>
<td>43</td>
</tr>
<tr>
<td>MyBB</td>
<td>Forum</td>
<td>1.6</td>
<td>105.9</td>
<td>4</td>
<td>63</td>
</tr>
<tr>
<td>OpenEMR</td>
<td>Medical Management</td>
<td>4.1</td>
<td>480</td>
<td>4</td>
<td>113</td>
</tr>
<tr>
<td>phpList</td>
<td>Newsletter management</td>
<td>2.10</td>
<td>35.4</td>
<td>4</td>
<td>77</td>
</tr>
<tr>
<td>Schoolmate</td>
<td>School Management</td>
<td>1.5</td>
<td>6.5</td>
<td>4</td>
<td>90</td>
</tr>
<tr>
<td>Serendipity</td>
<td>Blogging</td>
<td>0.8</td>
<td>49.6</td>
<td>4</td>
<td>65</td>
</tr>
</tbody>
</table>

Malicious Inputs (MI)

Inputs (I)

CVE Details

[OWASP](https://owasp.org)

HTML5 Security Cheatsheet
RQ1(1): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?
RQ1(1): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?
RQ1(1): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?
### RQ1(2)

**RQ1(2):** Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks **without disrupting the applications’ functionality?**

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Inputs</th>
<th>None</th>
<th>Self</th>
<th>AutoCSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallery</td>
<td>16</td>
<td>175</td>
<td>68</td>
<td>0</td>
</tr>
<tr>
<td>LinPHA</td>
<td>43</td>
<td>231</td>
<td>136</td>
<td>0</td>
</tr>
<tr>
<td>MyBB</td>
<td>63</td>
<td>598</td>
<td>364</td>
<td>2</td>
</tr>
<tr>
<td>OpenEMR</td>
<td>113</td>
<td>699</td>
<td>533</td>
<td>11</td>
</tr>
<tr>
<td>phpList</td>
<td>77</td>
<td>1224</td>
<td>273</td>
<td>1</td>
</tr>
<tr>
<td>Schoolmate</td>
<td>90</td>
<td>16</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Serendipity</td>
<td>65</td>
<td>476</td>
<td>385</td>
<td>6</td>
</tr>
</tbody>
</table>
**RQ1(2):** Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks **without disrupting the applications’ functionality?**

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Inputs</th>
<th>None</th>
<th>Self</th>
<th>AutoCSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallery</td>
<td>16</td>
<td>175</td>
<td>68</td>
<td>0</td>
</tr>
<tr>
<td>LinPHA</td>
<td>43</td>
<td>231</td>
<td>136</td>
<td>0</td>
</tr>
<tr>
<td>MyBB</td>
<td>63</td>
<td>598</td>
<td>364</td>
<td>2</td>
</tr>
<tr>
<td>OpenEMR</td>
<td>113</td>
<td>699</td>
<td>533</td>
<td>11</td>
</tr>
<tr>
<td>phpList</td>
<td>77</td>
<td>1224</td>
<td>273</td>
<td>1</td>
</tr>
<tr>
<td>Schoolmate</td>
<td>90</td>
<td>16</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Serendipity</td>
<td>65</td>
<td>476</td>
<td>385</td>
<td>6</td>
</tr>
</tbody>
</table>
RQ1(2): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks **without disrupting the applications’ functionality?**

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Inputs</th>
<th>None</th>
<th>Self</th>
<th>AutoCSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallery</td>
<td>16</td>
<td>175</td>
<td>68</td>
<td>0</td>
</tr>
<tr>
<td>LinPHA</td>
<td>43</td>
<td>231</td>
<td>136</td>
<td>0</td>
</tr>
<tr>
<td>MyBB</td>
<td>63</td>
<td>598</td>
<td>364</td>
<td>2</td>
</tr>
<tr>
<td>OpenEMR</td>
<td>113</td>
<td>699</td>
<td>533</td>
<td>11</td>
</tr>
<tr>
<td>phpList</td>
<td>77</td>
<td>1224</td>
<td>273</td>
<td>1</td>
</tr>
<tr>
<td>Schoolmate</td>
<td>90</td>
<td>16</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Serendipity</td>
<td>65</td>
<td>476</td>
<td>385</td>
<td>6</td>
</tr>
</tbody>
</table>
**RQ1(2):** Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks *without disrupting the applications’ functionality?*

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Inputs</th>
<th>None</th>
<th>Self</th>
<th>AutoCSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallery</td>
<td>16</td>
<td>175</td>
<td>68</td>
<td>0</td>
</tr>
<tr>
<td>LinPHA</td>
<td>43</td>
<td>231</td>
<td>136</td>
<td>0</td>
</tr>
<tr>
<td>MyBB</td>
<td>63</td>
<td>598</td>
<td>364</td>
<td>2</td>
</tr>
<tr>
<td>OpenEMR</td>
<td>113</td>
<td>699</td>
<td>533</td>
<td>11</td>
</tr>
<tr>
<td>phpList</td>
<td>77</td>
<td>1224</td>
<td>273</td>
<td>1</td>
</tr>
<tr>
<td>Schoolmate</td>
<td>90</td>
<td>16</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Serendipity</td>
<td>65</td>
<td>476</td>
<td>385</td>
<td>6</td>
</tr>
</tbody>
</table>
**RQ1(2):** Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks **without disrupting the applications’ functionality?**

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Inputs</th>
<th>None</th>
<th>Self</th>
<th>AutoCSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallery</td>
<td>16</td>
<td>175</td>
<td>68</td>
<td>0</td>
</tr>
<tr>
<td>LinPHA</td>
<td>43</td>
<td>231</td>
<td>136</td>
<td>0</td>
</tr>
<tr>
<td>MyBB</td>
<td>63</td>
<td>598</td>
<td>364</td>
<td>2</td>
</tr>
<tr>
<td>OpenEMR</td>
<td>113</td>
<td>699</td>
<td>533</td>
<td>11</td>
</tr>
<tr>
<td>phpList</td>
<td>77</td>
<td>1224</td>
<td>273</td>
<td>1</td>
</tr>
<tr>
<td>Schoolmate</td>
<td>90</td>
<td>16</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Serendipity</td>
<td>65</td>
<td>476</td>
<td>385</td>
<td>6</td>
</tr>
</tbody>
</table>
**RQ1(2):** Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks **without disrupting the applications’ functionality?**

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Inputs</th>
<th>None</th>
<th>Self</th>
<th>AutoCSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallery</td>
<td>16</td>
<td>175</td>
<td>68</td>
<td>0</td>
</tr>
<tr>
<td>LinPHA</td>
<td>43</td>
<td>231</td>
<td>136</td>
<td>0</td>
</tr>
<tr>
<td>MyBB</td>
<td>63</td>
<td>598</td>
<td>364</td>
<td>2</td>
</tr>
<tr>
<td>OpenEMR</td>
<td>113</td>
<td>699</td>
<td>533</td>
<td>11</td>
</tr>
<tr>
<td>phpList</td>
<td>77</td>
<td>1224</td>
<td>273</td>
<td>1</td>
</tr>
<tr>
<td>Schoolmate</td>
<td>90</td>
<td>16</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Serendipity</td>
<td>65</td>
<td>476</td>
<td>385</td>
<td>6</td>
</tr>
</tbody>
</table>
RQ1(2): Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Inputs</th>
<th>None</th>
<th>Self</th>
<th>AutoCSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallery</td>
<td>16</td>
<td>175</td>
<td>68</td>
<td>0</td>
</tr>
<tr>
<td>LinPHA</td>
<td>43</td>
<td>231</td>
<td>136</td>
<td>0</td>
</tr>
<tr>
<td>MyBB</td>
<td>63</td>
<td>598</td>
<td>364</td>
<td>2</td>
</tr>
<tr>
<td>OpenEMR</td>
<td>113</td>
<td>699</td>
<td>533</td>
<td>11</td>
</tr>
<tr>
<td>phpList</td>
<td>77</td>
<td>1224</td>
<td>273</td>
<td>1</td>
</tr>
<tr>
<td>Schoolmate</td>
<td>90</td>
<td>16</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Serendipity</td>
<td>65</td>
<td>476</td>
<td>385</td>
<td>6</td>
</tr>
</tbody>
</table>

E1: client-side execution of eval.
```
var x = eval('...');
```

E2: client-side creation on inline script nodes.
```
document.write('<script>...</script>');
```

E3: client-side creation on inline style nodes.
```
document.write('<style>...</style>');
```
RQ4: Is automation actually needed to retrofit CSP to web applications?

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>$E_{csp}$</th>
<th>$E_e$</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallery</td>
<td>2</td>
<td>76</td>
<td>12</td>
</tr>
<tr>
<td>LinPHA</td>
<td>2</td>
<td>67</td>
<td>11</td>
</tr>
<tr>
<td>MyBB</td>
<td>5</td>
<td>97</td>
<td>6</td>
</tr>
<tr>
<td>OpenEMR</td>
<td>31</td>
<td>319</td>
<td>52</td>
</tr>
<tr>
<td>phpList</td>
<td>1</td>
<td>33</td>
<td>8</td>
</tr>
<tr>
<td>Schoolmate</td>
<td>1</td>
<td>328</td>
<td>26</td>
</tr>
<tr>
<td>Serendipity</td>
<td>5</td>
<td>103</td>
<td>16</td>
</tr>
</tbody>
</table>
RQ4: Is automation actually needed to retrofit CSP to web applications?

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>$E_{csp}$</th>
<th>$E_e$</th>
<th>$F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallery</td>
<td>2</td>
<td>76</td>
<td>12</td>
</tr>
<tr>
<td>LinPHA</td>
<td>2</td>
<td>67</td>
<td>11</td>
</tr>
<tr>
<td>MyBB</td>
<td>5</td>
<td>97</td>
<td>6</td>
</tr>
<tr>
<td>OpenEMR</td>
<td>31</td>
<td>319</td>
<td>52</td>
</tr>
<tr>
<td>phpList</td>
<td>1</td>
<td>33</td>
<td>8</td>
</tr>
<tr>
<td>Schoolmate</td>
<td>1</td>
<td>328</td>
<td>26</td>
</tr>
<tr>
<td>Serendipity</td>
<td>5</td>
<td>103</td>
<td>16</td>
</tr>
</tbody>
</table>

$E_{csp}$: number of CSP edits.
RQ4: Is automation actually needed to retrofit CSP to web applications?

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>$E_{csp}$</th>
<th>$E_e$</th>
<th>$F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallery</td>
<td>2</td>
<td>76</td>
<td>12</td>
</tr>
<tr>
<td>LinPHA</td>
<td>2</td>
<td>67</td>
<td>11</td>
</tr>
<tr>
<td>MyBB</td>
<td>5</td>
<td>97</td>
<td>6</td>
</tr>
<tr>
<td>OpenEMR</td>
<td>31</td>
<td>319</td>
<td>52</td>
</tr>
<tr>
<td>phpList</td>
<td>1</td>
<td>33</td>
<td>8</td>
</tr>
<tr>
<td>Schoolmate</td>
<td>1</td>
<td>328</td>
<td>26</td>
</tr>
<tr>
<td>Serendipity</td>
<td>5</td>
<td>103</td>
<td>16</td>
</tr>
</tbody>
</table>

$E_{csp}$: number of CSP edits.

$E_e$: number of modified HTML elements.
RQ4: Is automation actually needed to retrofit CSP to web applications?

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>$E_{csp}$</th>
<th>$E_e$</th>
<th>$F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gallery</td>
<td>2</td>
<td>76</td>
<td>12</td>
</tr>
<tr>
<td>LinPHA</td>
<td>2</td>
<td>67</td>
<td>11</td>
</tr>
<tr>
<td>MyBB</td>
<td>5</td>
<td>97</td>
<td>6</td>
</tr>
<tr>
<td>OpenEMR</td>
<td>31</td>
<td>319</td>
<td>52</td>
</tr>
<tr>
<td>phpList</td>
<td>1</td>
<td>33</td>
<td>8</td>
</tr>
<tr>
<td>Schoolmate</td>
<td>1</td>
<td>328</td>
<td>26</td>
</tr>
<tr>
<td>Serendipity</td>
<td>5</td>
<td>103</td>
<td>16</td>
</tr>
</tbody>
</table>

$E_{csp}$: number of CSP edits.

$E_e$: number of modified HTML elements.

$E_{csp}$: number of modified files.
Evaluation Summary

**RQ1:** Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?

- AutoCSP offers effective protection against XSS.
- AutoCSP introduces low number of false alarms.

**RQ4:** Is automation actually needed to retrofit CSP to web applications?

- Automation is needed.
Related Work

Content Security Policy

Doupé et al., Stamm et al., and Weinberger et al.

Web Page Security Policies

Jim et al. and Louw et al.

Dynamic Tainting in Web Applications Security

Halfond et al., Nguyen-Tuong, and Pietraszek et al.
Related Work

Content Security Policy

Doupé et al., Stamm et al., and Weinberger et al.

Web Page Security Policies

Jim et al. and Louw et al.

Dynamic Tainting in Web Applications Security

Halfond et al., Nguyen-Tuong, and Pietraszek et al.
Related Work

Content Security Policy

Doupé et al., Stamm et al., and Weinberger et al.

Web Page Security Policies

Jim et al. and Louw et al.

Dynamic Tainting in Web Applications Security

Halfond et al., Nguyen-Tuong, and Pietraszek et al.
Related Work

**Content Security Policy**

Doupé et al., Stamm et al., and Weinberger et al.

**Web Page Security Policies**

Jim et al. and Louw et al.

**Dynamic Tainting in Web Applications Security**

Halfond et al., Nguyen-Tuong, and Pietraszek et al.
Summary

Cross-Site Scripting (XSS)

Content Security Policy (CSP)

AutoCSP

Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?

RQ2: What is the effect of AutoCSP on the performance of the nonmodified web applications?

RQ3: How dependent is AutoCSP’s performance on the input used for its input analysis?

RQ4: Is automation actually needed to retrofit CSP to web applications?
Summary

Cross-Site Scripting (XSS)

Content Security Policy (CSP)

Empirical Evaluation
Research Questions:

RQ1: Can autoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?

RQ2: What is the effect of autoCSP on the performance of the retrofit web applications?

RQ3: How dependent is autoCSP’s performance on the input used for its taint analysis?

RQ4: Is automation actually needed to retrofit CSP to web applications?
Summary

Cross-Site Scripting (XSS)

- XSS Publications
  - 04, 05, 06, 07, 08, 09, 10, 11, 12

- Vulnerability Classes (2014)
  - XSS 58%

Content Security Policy (CSP)

- Server
  - GSP

- Client
  - 11, 37, 47, 87, 77

AutoCSP

- Test Inputs
- Dynamic Tainting
- Web Page Analysis
- Source Code Transformation
- CSP Analysis

Empirical Evaluation

Research Questions:

- RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?
- RQ2: What is the effect of AutoCSP on the performance of the retrofit web applications?
- RQ3: How dependent is AutoCSP’s performance on the input used for its benign analysis?
- RQ4: Is automation actually needed to retrofit CSP to web applications?
Summary

Cross-Site Scripting (XSS)

Content Security Policy (CSP)

AutoCSP

Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?

RQ2: What is the effect of AutoCSP on the performance of the normalized web applications?

RQ3: How dependent is AutoCSP’s performance on the input used for its fault analysis?

RQ4: Is automation actually needed to retrofit CSP to web applications?
Summary

Cross-Site Scripting (XSS)

- XSS Publications
- Vulnerability Classes (2014)

Content Security Policy (CSP)

- Server CSP
- Client CSP

AutoCSP

- Test Inputs
- Web App
- Dynamic Tainting
- Web Page Analysis
- Source Code Transformation
- CSP Analysis

Empirical Evaluation

Research Questions:

RQ1: Can AutoCSP retrofit CSP to web applications and offer an effective protection against XSS attacks without disrupting the applications’ functionality?

RQ2: What is the effect of AutoCSP on the performance of the retrofitted web applications?

RQ3: How dependent is AutoCSP’s performance on the input used for its taint analysis?

RQ4: Is automation actually needed to retrofit CSP to web applications?