Security pitfalls of client-side cross-domain HTTP requests

Martin Johns
SAP Research
What are client-side cross-domain requests?

They are
- Initiated by JavaScript via XMLHttpRequest
- Directed at cross-domain hosts
What are client-side cross-domain requests?

They are
• Initiated by JavaScript via XMLHttpRequest
• Directed at cross-domain hosts

Forbidden by the Same-Origin Policy
Security implications

http://kittypics.org

Browser

http://kittypics.org

JavaScript (kittypics.org)

Cookie for mail.google.com

http://mail.google.com
Security implications

1. Leakage of sensitive information
   - The adversary can request sensitive web resources

2. Circumvention of CSRF protection
   - Token-based CSRF protection relies on the fact, that the adversary cannot read cross-domain data

1. + 2. = XSS-based Session hijacking
   - Chaining requests & reading responses -> capabilities equal to XSS session hijacking
Opt-in model for client-side cross-domain requests

http://b.net

Browser

http://b.net

CrossDomain.swf (b.net)

Cookie for c.net

http://c.net

Policy <b.net>

data
Opt-in model for client-side cross-domain requests

```xml
<cross-domain-policy>
  <allow-access-from domain="google.com" />
  <allow-access-from domain="facebook.com" />
</cross-domain-policy>
```
Opt-in model for client-side cross-domain requests

http://b.net

Browser

http://b.net

Cookie for c.net

Policy

<b.net>

<data>

<xhtml>

<cross-domain-policy>
<allow-access-from domain="*"/>
</cross-domain-policy>

</xhtml>

</data>
Survey

Mission statement
Find out if cross-domain policies are used insecurely in the wild

Method
Examine the policies of the Alexa top 1,000,000

1,093,127 domains scanned

<table>
<thead>
<tr>
<th></th>
<th>Total</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flash</td>
<td>82,052</td>
<td>8%</td>
</tr>
<tr>
<td>Silverlight</td>
<td>995</td>
<td>0.09%</td>
</tr>
<tr>
<td>CORS</td>
<td>215</td>
<td>0.02%</td>
</tr>
</tbody>
</table>
Results
Penetration / Security - Flash

Wildcard policy

31,011 files (37.7% of all crossdomain.xml) resulting in 2.8% potentially insecure sites

When checking for authentication

15,060 sites (1.3% of all analyzed sites)
Conclusion

Check your site’s crossdomain.xml files
  • You might be surprised…

Only allow trusted domains

Or even better – Use CORS (cross-origin resource sharing)
  • However, that is a topic for another talk
Thank You!

Contact information:

Martin Johns
SAP Research
martin.johns@sap.com