Clubbing Seals: Exploring the Ecosystem of Third-party Security Seals

Tom Van Goethem, Frank Piessens, Wouter Joosen, Nick Nikiforakis
Security Conscious Alice

Security Seal Provider

Webshop

Vulnerability Scanner

Security is OK?
Outline

• Ecosystem entities
• Security evaluation
• Attacks
Security Conscious Alice

Webshop

Security Seal Provider

Vulnerability Scanner

Security is OK?
Scans for vulnerabilities in dynamic web applications, such as SQL injection, to verify websites that safeguard consumer data.

The badge only appears when a website has passed intensive security scans. The scans test sites in the way a hacker would most likely attack, protecting you from data loss or breach of information.
Security Seal Providers

- 10 seal providers evaluated
- Large security companies - startups providing security seals
- Yearly cost: $84 - $2,388 per year
- All offer vulnerability scan
- Half offer malware scan
Security Seal Providers

• Differences in offered security services
  – Server-side file access (FTP)
  – Server-side authentication (login-form)

• Differences in security seal visibility
  – Vulnerability may lead to invisible seal
  – Grace period (0 days - 1 week)
Security Conscious Alice

Security is OK?

Webshop

Security Seal Provider

Vulnerability Scanner
Security Seal Customers

- Found by crawling Alexa top 1M
  - Security seal images, links
- Google snippets
  - site:scanverify.com/siteverify.php
- 8,302 websites (~74% from Alexa top 1M)
- Mainly e-commerce
Security Evaluation

• Should Alice trust seal providers?
• Security evaluation on various dimensions
  – Comparison to non-sealed websites
  – Manual penetration test
  – Vulnerable webshop experiment
Comparison to non-sealed websites

• Sealed sites interested in security → implement security mechanisms?

• Compare with equivalent websites
  – Same category
  – Similar Alexa ranking (10 ranks above or below)

• Compare presence of security indicators
  – HSTS, Secure/HttpOnly cookies, CSP, XFO, ...
<table>
<thead>
<tr>
<th>Security Mechanism</th>
<th>Sites w/ Seal (%)</th>
<th>Sites w/o Seal (%)</th>
<th>Significantly different (p-value)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSTS</td>
<td>1.05</td>
<td>1.06</td>
<td>✗</td>
</tr>
<tr>
<td>Secure Cookies</td>
<td>1.83</td>
<td>0.42</td>
<td>✗</td>
</tr>
<tr>
<td>SSL Stripping</td>
<td>15.45</td>
<td>15.64</td>
<td>✗</td>
</tr>
<tr>
<td>X-Frame Options</td>
<td>3.71</td>
<td><strong>5.14</strong></td>
<td>✓</td>
</tr>
<tr>
<td>HttpOnly Cookies</td>
<td><strong>42.27</strong></td>
<td>29.98</td>
<td>✓</td>
</tr>
<tr>
<td>Content-Security-Policy</td>
<td>0.00</td>
<td>0.00</td>
<td>–</td>
</tr>
<tr>
<td>Anti-CSRF tokens</td>
<td>6.39</td>
<td><strong>11.89</strong></td>
<td>✓</td>
</tr>
<tr>
<td>X-Content-Type-Options</td>
<td>0.00</td>
<td>0.00</td>
<td>–</td>
</tr>
<tr>
<td>iframe sandbox</td>
<td>0.18</td>
<td>0.04</td>
<td>✗</td>
</tr>
</tbody>
</table>
Manual Penetration Test

- Security scan by seal provider → no easily discoverable vulnerabilities?

- Contact 1,000 sealed websites
  - Only 9 agreed to penetration test

- During 8 hours, check for SQL injection, XSS, CSRF, ...

- 7 out of 9 websites vulnerable
  - 6 websites contain easily discoverable vulnerabilities (XSS, textbook SQL injection)
Vulnerable webshop experiment

• Evaluate accuracy of tools used by seal providers
• Setup webshop with severe vulnerabilities
  – Reflect realistic website
  – Outdated PrestaShop
  – Add 12 vulnerabilities spanning various classes
    • XSS, SQL Injection, sensitive files, ...
Attacks

- Security seals are part of an attacker's toolset
  - Find vulnerable websites
  - Identify vulnerability
  - Improve phishing campaigns
# Attacks

*Find vulnerable websites*

<table>
<thead>
<tr>
<th></th>
<th>Day 1</th>
<th>Day 2</th>
<th>Day 3</th>
<th>Day 4</th>
<th>Day 5</th>
<th>Day 6</th>
<th>Day 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website 1</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
</tr>
<tr>
<td>Website 2</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
</tr>
<tr>
<td>Website 3</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
</tr>
<tr>
<td>Website 4</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
</tr>
<tr>
<td>Website 5</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
</tr>
<tr>
<td>Website 6</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
</tr>
<tr>
<td>Website 7</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
<td>![Green Shield]</td>
</tr>
</tbody>
</table>
Attacks
Identify vulnerabilities

Security Seal Provider

Vulnerability Scanner

Attacker's proxy

Setup

Scan proxy

Report vulnerabilities

Target

Exploit vulnerabilities!

OWASP AppSecEU 15
Amsterdam, The Netherlands
Attacks

Improve phishing campaigns

• Include security seal on phishing page
  – Hide Referer header
• Leads to increased credibility on phishing page
Attacks

Improve phishing campaigns

Clone

OWASP AppSecEU 15
Amsterdam, The Netherlands
Conclusion

• Security seals often used on webshops
• Presence of seal not trustworthy
  – Sealed sites not more secure than non-sealed
  – Vulnerability scanners insufficient
• Various attacks on security seals
  – Sealed sites = valuable target for attackers