YGN ETHICAL HACKER GROUP

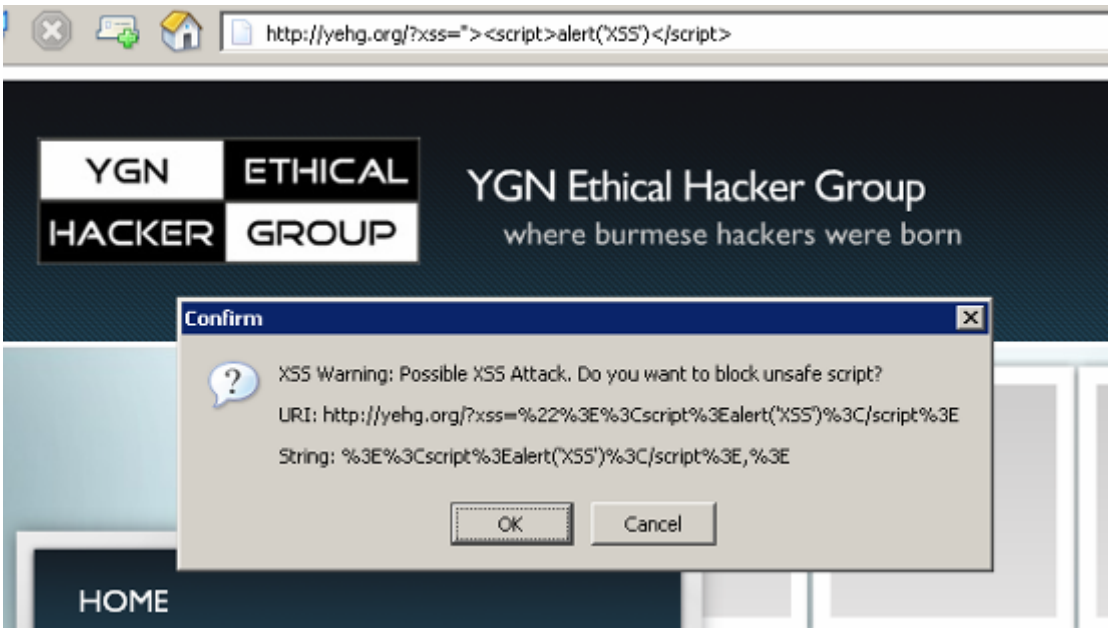
Security Advisory

XSS Filter Bypass VUNERABILITY IN XSS-Warning Add-on

Discovered by: d0ubl3_h3lix
Date: March 2008
Product: Gecko Browser extension/add-on XSS-Warning
URL: http://www.gianniamato.it/project/extension/xsswarning/
Vulnerability Type: Broken Filter
Risk: **high**
Threats: XSS-0wnage

Note:

XSS-Warning is a nice add-on for gecko browsers such as Firefox, Netscape. It searches a XSS attack patterns in URL string while users are surfing the web. If found, it alerts users as a possible XSS attack. Then, it completely disables the XSS-affected page if users click 'OK' to block unsafe script.

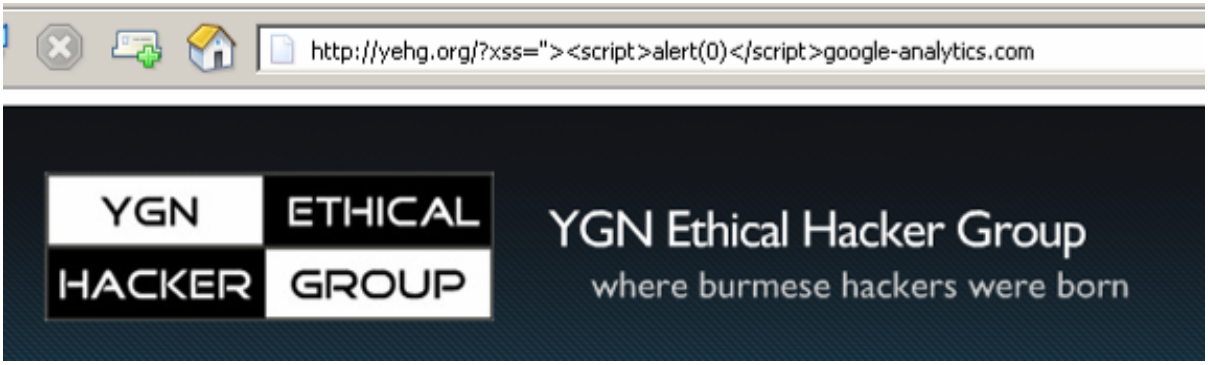


Proof-Of-Vulnerability:

Since its release, XSS-Warning can't check very advanced XSS-Bypass attack payload. What I have discovered is that attackers don't have to use even such advanced payloads to bypass XSS-Warning protection. After checking its source code, I found XSS-Warning white lists as follow:

```
(^http\:\/\/suggestqueries.google.com|^http\:\/\/toolba
 pagead2.googlesyndication.com|google-analytics.com|.tr
.revsci.net|.shinystat.com|^http\:\/\/www.frappr.com|^h
```

The above regular expression filter has logic flaws. Attackers can bypass it with their desired malicious XSS payloads together with any keyword of ***google-analytics.com*** or ***pagead2.googlesyndication.com*** or ***.shinystat.com***. Here is a proof screenshot:



It no longer gives me xss-warning at all. If users trust this add-on at all and surf the web with over-confidence, this poses significant risks to their security. There is no perfect security. One protection closes one gap.

Fix:

The fix is pretty simple:

1. Just extract only domain from URL string – i.e . Use document.domain Not document.location
2. Match it with white lists. In our case, match the domain name yehg.org with white lists.
3. If no matches, issue XSS Warning to users.