activeScan++

Augmenting manual testing with attack proxy plugins

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- Security Consultant – ContextIS
  - Web app hacking
  - Tool development
- Vulnerability bounty hunting vs Google&Mozilla
  - Hit #6 on Google 0x0A list
  - Host header attack research
  - Author of hackxor
  - Twitter: @albinowax

Agenda

OWASP
The Open Web Application Security Project

- The proxy-plugin approach
- Automating esoteric attacks
  - Host header injection
  - DNS rebinding
  - Relative path overwrite
- Generic injection detection

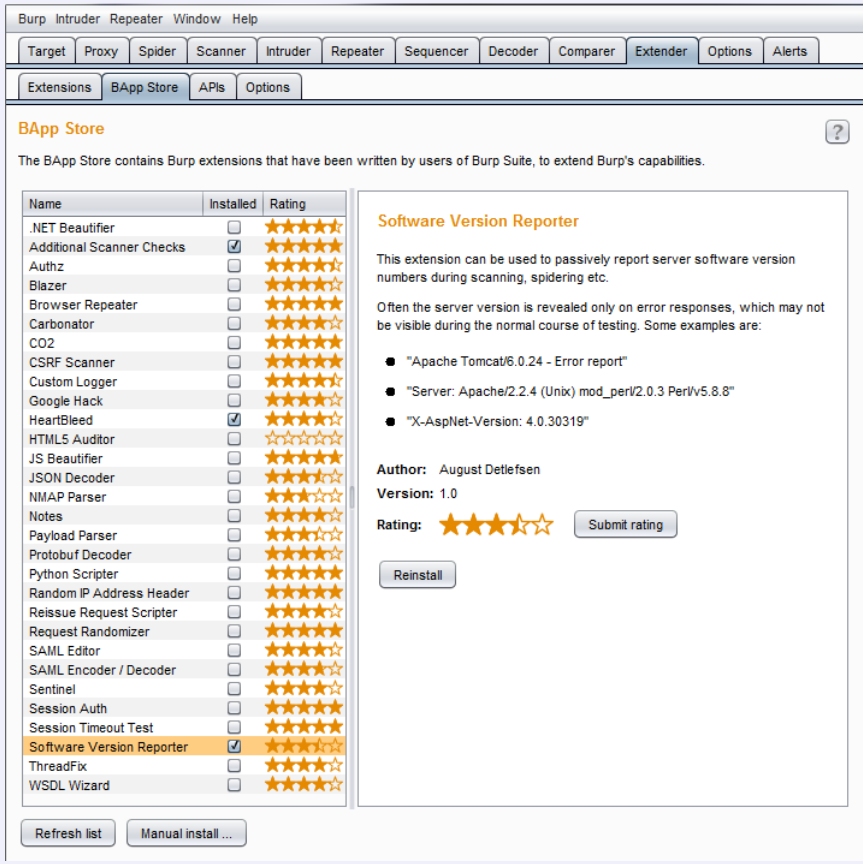
OWASP
The Open Web Application Security Project

The proxy-plugin approach

Scanner objectives

OWASP
The Open Web Application Security Project

- Identify vulnerabilities
- Guide manual testing
  - Identify suspect behaviour
  - Flag vulnerability components
  - Collate useful information



Scanner headaches

OWASP
The Open Web Application Security Project

- Classical scanner headaches
  - State-driven sites
  - JS-heavy functionality
  - Hazardous forms
- Proprietary Proxy-plugin headaches
  - Entirely API-bound
  - Restricted view
- Zed Attack Proxy plugin headaches?

OWASP
The Open Web Application Security Project

It's easy:

```
self._payloads = {
    # eval() injection
    'php':['{$${sleep($time)}}', "'.sleep($time).'", '".sleep($time)."',
'sleep($time)'],
    'perl':["'.sleep($time).'", '".sleep($time)."', 'sleep($time)'],
    'ruby':["'+sleep($time)+'", '"+sleep($time)+"'],

    # Shell command injection into '$input' on linux and "$input" on windows:
    'any':['"&timeout $time&\'`sleep $time`\''],
}
...
# Time how long each response takes compared to the baseline
for payload in payloads:
    if(self._attack(basePair, insertionPoint, payload, 10)[0] > baseTime+6):
        print "Suspicious delay detected. Confirming it's consistent..."
```

OWASP
The Open Web Application Security Project

Automating esoteric attacks

Host header overview

OWASP
The Open Web Application Security Project

- HTTP Host Header
- Intended for virtual hosting
  - Defines which vhost you're talking to
- People trust it:

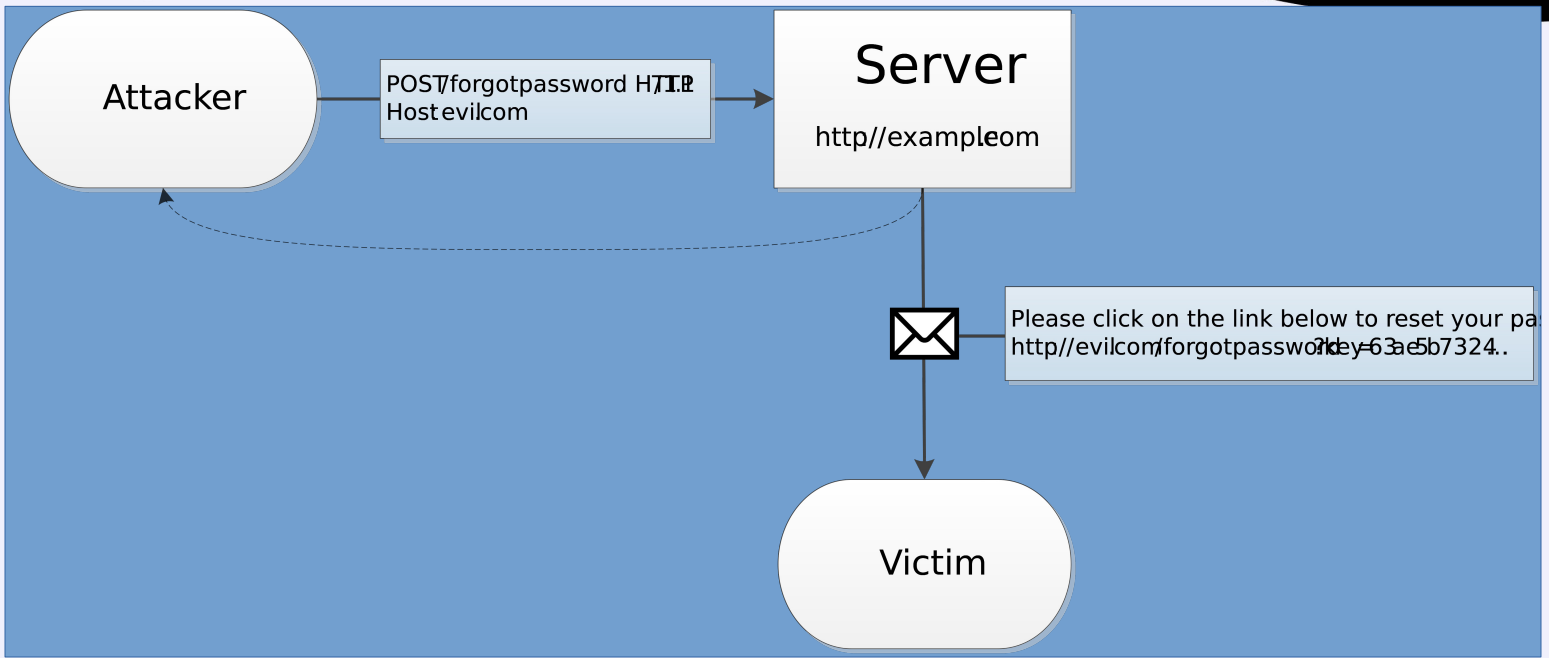
```
if($_SERVER['SERVER_NAME']=='localhost'){
    $ENV='DEVELOPMENT';
}
else {
    $ENV='PRODUCTION';
}
```

Host header attacks

- How do you attack other users?
  - Not like this:

Host header attacks

OWASP
The Open Web Application Security Project



TYPO3
django
PIWIK
Open Analytics Platform
Drupal
Symfony

Your new password

Apache [apache@localhost.localdomain] on behalf of no-reply@localhost.localdomain [no-reply@localhost.localdomain]

Sent: 23 May 2014 16:23
To: James Kettle

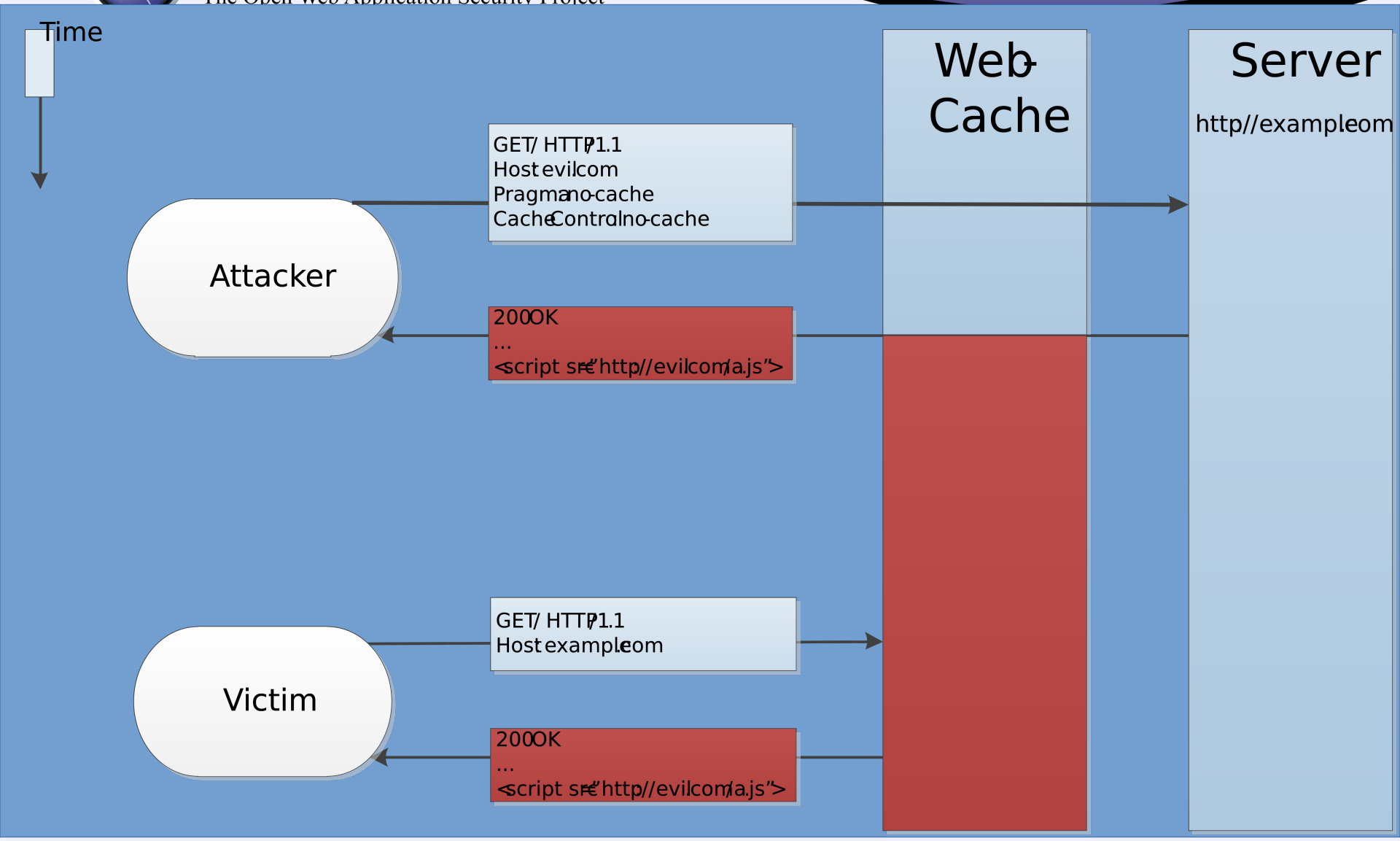
Dear user01,

This email was sent in response to your request to reset your password. Please click on the link below.
http://evil.com/typo3/?tx_felogin_pi1%5Buser%5D=1&tx_felogin_pi1%5Bforgothash%5D=1400901783%7C8d52bc03c0ff6116f95b075054fccc1b

For security reasons, this link is only active until 2014-05-24 03:23. If you do not visit the link before then, you will need to repeat the password reset steps.

Cache poisoning

OWASP
The Open Web Application Security Project



OWASP
The Open Web Application Security Project

Automated detection:

GET /typo3/ HTTP/1.1
Host: evil.com
Referer: http://evil.com/

GET http://example.com/typo3/ HTTP/1.1
Host: evil.com
Referer: http://evil.com/

GET /typo3/ HTTP/1.1
Host: example.com
X-Forwarded-Host: evil.com
Referer: http://evil.com/

Typo3 Demo

OWASP
The Open Web Application Security Project

- Typo3 CMS
  - May 22, 2014: TYPO3-CORE-SA-2014-001

"TYPO3 CMS is susceptible to host spoofing. TYPO3 uses the HTTP host-header to generate absolute URLs in several places like 404 handling, http(s) enforcement, password reset links and many more. Since the host header itself is provided by the client it can be forged to any value, even in a name based virtual hosts environment."

- Demo

DNS Rebinding

OWASP
The Open Web Application Security Project

- Same Origin Policy
  - Origins based on hostnames, not IP addresses
- Serve the user malicious.html
- Claim you've moved to 127.0.0.1 ('rebind')
  - malicious.html can now access 127.0.0.1
- Proxy through user's web browser

DNS Rebinding

OWASP
The Open Web Application Security Project

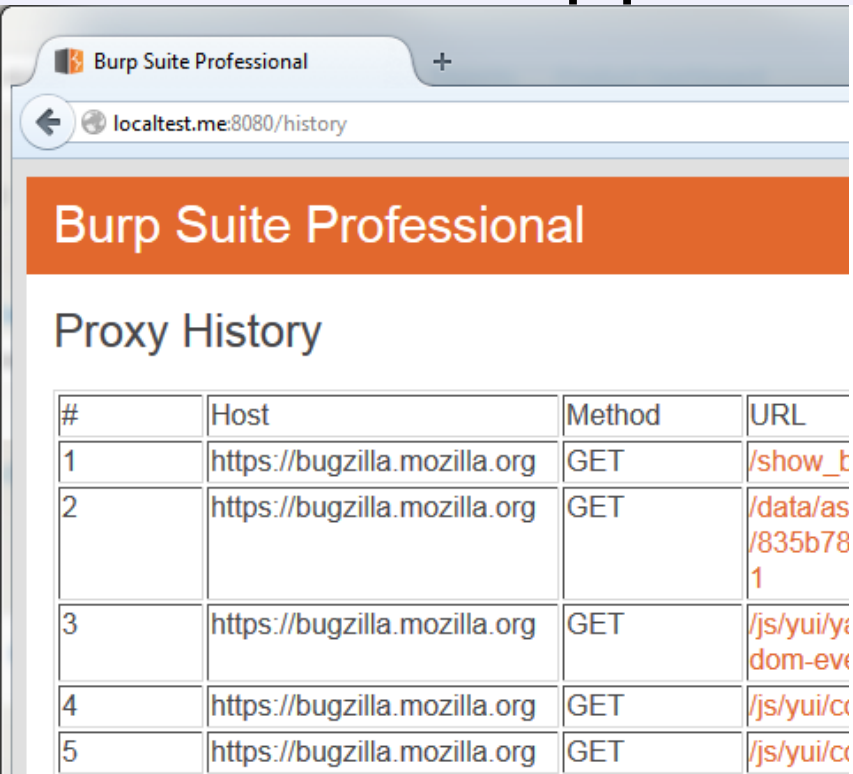
- Partially fixed by DNS pinning
- DNS pinning bypass via cached resources
  - Google Chrome
    - **Status: WontFix**

    https://code.google.com/p/chromium/issues/detail?id=98357
  - Mozilla Firefox
    - *“It's not feasible for the browser to protect the user from DNS rebinding attacks. Servers need to protect themselves by validating the Host header and firewalls need to protect themselves by preventing external names from resolving to internal IP addresses.”*
    - https://bugzilla.mozilla.org/show_bug.cgi?id=689835
- This attack will not go away

DNS Rebinding

OWASP
The Open Web Application Security Project

- Detected during other host header attacks
- Affects applications close to home:



Burp Suite Professional - Release Notes

Wednesday, June 11, 2014

v1.6.01

This release contains various enhancements to existing functionality:

- The Spider's link-discovery engine has been enhanced, and now achieves a WIVET score of 50%. There is more work to do in this area, and improved crawling of JavaScript-driven navigation is in the pipeline.
- There are new hotkeyable actions to go back and forwards in the Repeater history for the currently displayed tab. Hotkeys can be assigned to these actions at Options / Misc / Hotkeys.
- The "valid from" time on Proxy-generated CA-signed host certificates has been changed to be 30 days in the past, to reduce problems that can arise when using multiple test machines with different system times.
- Handling of non-HTTP-compliant messages that use \n instead of \r\n as header delimiters has been improved.
- A new option has been added to prevent access to the in-browser Proxy interface using a fully-qualified DNS name, to hinder DNS rebinding attacks against it.

Host header defence

OWASP
The Open Web Application Security Project

- Define trusted hosts
- Wildcard with care
  - Expands attack surface
  - No server compromise necessary:
    - Token accessible with XSS via document.history
    - Leaked to external resources via Referer
- Minimise configuration burden
  - Allow /etc/hostname, ‘localhost’

Host header defence

OWASP
The Open Web Application Security Project

- Treat Host as typical user input
  - Validate, encode, escape
- Cache with care
  - Include host in the cache ID
  - Reject duplicate host headers

Relative Path Overwrite

OWASP
The Open Web Application Security Project

Relative Path Overwrite (RPO) attack by @garethheyes

On https://example.com/en/index.jsp:

- <link href="https://contextis.co.uk/style/main.css" (absolute)
  - Browser loads https://contextis.co.uk/style/main.css

- <link href="/style/main.css" (root-relative)
  - Browser loads https://example.com/style/main.css

Relative Path Overwrite

OWASP
The Open Web Application Security Project

https://example.com/en/index.jsp;foo/bar

- Page content: <link href="style/main.css"
- Browser loads: https://example.com/en/index.jsp;foo/style/main.css

– Imports the current page
– CSS parsing is extremely lax
– CSS can extract page content
  - See ‘Scriptless Attacks - Stealing the Pie Without Touching the Sill’

Detecting RPO

OWASP
The Open Web Application Security Project

- RPO requirements:
  - Relative CSS include
  - Missing/malformed <!DOCTYPE
    - Or missing X-Frame-Options, X-Content-Type
  - Malleable path
  - Injection vector
    - Persistent input
    - Path
    - Referer
    - Cookie

OWASP
The Open Web Application Security Project

Generic injection detection

Classic payload limitations

OWASP
The Open Web Application Security Project

- Directory traversal:

```
include('includes/modules/pdf/' .
$_REQUEST['pdf'] . '.php');
```

- Classic scanner payload:

  pdf=../../../../../../../../../../../../etc/passwd%00

  Requirements:
  - /etc/passwd exists
  - ../ isn’t filtered
  - No input length limit
  - Null bytes don’t break anything
  - The file read is displayed back

- Solution: more payloads?

Minimal payload sets

OWASP
The Open Web Application Security Project

- Keep it simple
- /pdf.php?pdf=573
  - ./573 vs /.573
    - Almost any directory traversal
  - 575-2 vs 576-2
    - Almost any numeric evaluation
  - 57'+'3 vs 57''+3
    - Java, MSSQL, Python
  - 573\'a vs 573'\a
    - Almost any string injection

Identifying equivalent responses

OWASP
The Open Web Application Security Project

- Confounding factors:
  - Reflected input
  - Timestamps
  - Apparently random input
- Solutions:
  - Fingerprint document structure
  - Fuzzy point detection

Fuzzy point detection

OWASP
The Open Web Application Security Project

```
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: close
Content-Length: [length]
Content-Type: text/html; charset=utf-8
Date: Sat, 19 Apr 2014 [timestamp]  GMT
Expires: Thu, 19 Nov 1981 [timestamp] GMT
Pragma: no-cache
Set-Cookie: PHPSESSID=[???] ; path=/
Vary: Accept-Encoding
X-Powered-By: PHP/5.3.2-1ubuntu4.5

<body onload="sf();">
<div id="header">
      <!-- TODO: Please change with your custom logo! -->
      <div id="getbootitle"><a href="http://owaspbwa/getboo/"><img src="images/getboologo.png" alt="GetBoo Logo" title="GetBoo Logo" width="222"
height="29"></a></div>
      <p id="navigation"></p>
      <p id="access">
            <a href="about.php" title="What is getboo about?">About</a><span> / </span>          <a href="http://wiki.getboo.com/help/helpindex" title="Get help with
getboo">Help</a><span> / </span>
                                    <a href="newuser.php" title="Register an account">Register</a><span> / </span>
                        <a href="login.php" title="Login into your account">Log In</a>
            </p>
</div><h2>Forgot password</h2>
<p class="error">The username and the email don't match, or the user does not exist</p><p>You must enter your username <b>and</b> your email to get your password
hint question.<br>
If it doesn't help you recover your password, you will get the possibility to receive a new password.</p>
<form method="post" action="forgotpass.php">
<table>
      <tr>
            <td><span class="formsLabel">Username</span></td>
            <td><input type="text" name="aname" maxlength="20" value="[???]" class="formtext" onfocus="this.select()" /> <b style="text-decoration:underline;
cursor:pointer;" onmouseover="return overlib('20 chars max');" onmouseout="return nd();">?</b></td>
      </tr>
      <tr>
            <td><span class="formsLabel">Email address</span></td>
            <td><input type="text" name="email" size="40" maxlength="150" value="[???]" class="formtext" onfocus="this.select()" /> <b style="text-
decoration:underline; cursor:pointer;" onmouseover="return overlib('150 chars max');" onmouseout="return nd();">?</b></td>
      </tr>
      <tr>
            <td></td>
            <td><input type="submit" name="submitted" class="genericButton" value="Hint question" /></td>
      </tr>
</table></form>
<p><a href="newuser.php">New User?</a></p>
```

Take-home

OWASP
The Open Web Application Security Project

- Proxy plugin-in scanning:
  - Existing solutions imperfect
  - Vast potential
  - Almost painless

References

OWASP
The Open Web Application Security Project

- ActiveScan++ code repository:
  - <tbd>
- Relative path overwrite:
  - http://www.thespanner.co.uk/2014/03/21/rpo/
  - http://www.nds.rub.de/media/emma/veroeffentlichungen/2012/08/16/scriptlessAttacks-ccs2012.pdf
- Host header attacks:
  - http://www.skeletonscribe.net/2013/05/practical-http-host-header-attacks.html
  - https://drupal.org/node/1992030
- DNS rebinding:
  - http://www.adambarth.com/papers/2009/jackson-barth-bortz-shao-boneh-tweb.pdf

OWASP
The Open Web Application Security Project

Questions?