WEB APP 101:
GETTING THE LAY OF THE LAND

Mike Saunders
mike@redsiege.com
@hardwaterhacker
slides: redsiege.com/wa101
DISCLAIMER
WHY?
SCOPING - GOALS

- Most important step - informs the rest of the test
- What’s important to the client?
  - May not be traditional XSS/SQLi/CSRF/etc.
  - Lateral user to user attacks
  - Horizontal user to admin attacks
  - Logic flaws
  - Protecting sensitive resources (DB, back end infrastructure...)
- Sometimes we need to decide for the client
SCOPING LARGE APPS

- Client budget may not support thorough testing
- ID functions with high impact
  - Financial transactions
  - User management
  - State changes
- Areas using custom code instead of built-in security functions
- Interviews with developers can help
- Code review
PRE-AUTHENTICATION PROCESS

- Enumeration
  - sslscan
  - nikto
- nmap script scans
- dirbusting
- robots.txt and sitemap.xml
- Google dorks
- Wayback machine
A WORD ABOUT GOBUSTER / DIRBUSTING

- Tune status codes with -s
- Provide a wordlist with -w
  - directory-list-2.3-medium
  - RobotsDisallowed
  - SecLists Discovery/Web-Content
- Check for file extensions with -x
- Change user agents with -a
- Pay attention to status codes (401/403/500)
EFFECTIVE ENUMERATION

- Manually browse to every link/function *before* testing
  - Make note of dangerous/sensitive functions
    - Logout / modify/delete
- Work with client to get proper data for testing inputs
  - If data isn’t correct, likely can’t exercise all functions
  - Walkthrough of app with client expert is helpful
- Run crawler *after* manual enumeration and excluding dangerous functions
**METHODOLOGY**

- Always two windows open - browser and proxy
  - Review every request and response
  - Make note of anything significant or out of the ordinary
- Always be enumerating
  - Enumeration in background during manual crawl
- Make sure your scope in Burp is correct
CRAWLING CONSIDERATIONS

- Did you exclude sensitive functions?
- Burp spider can be useful
  - Don’t be Peter Winter - change your defaults in Burp
- Burp Discover Content tool can be unwieldy
  - Pros - it can find lots of stuff, but so can other tools
  - Cons - It can take forever
FORCED BROWSING

- Can be tested manually using Repeater
- Right click in scope - copy all links
  - Copy links to a file
  - Loop: curl -sk -x http://127.0.0.1:8080 $url
    - Review results in proxy, ensure auth is required
TIPS & TRICKS

- Use Intruder to target specific parameters for scanning (Tim Tomes)
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are inserted to payload positions – see help for full details.

Attack type: Sniper

GET /vulnerabilities/brute/?username=$admin$&password=$1234$&Login=Login HTTP/1.1
Host: 172.16.127.167
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:57.0) Gecko/20100101 Firefox/57.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.127.167/vulnerabilities/brute/
Cookie: PHPSESSID=bu6l7ns4jihj729ev2ilkdjgd7; security=high
Connection: close
Upgrade-Insecure-Requests: 1

Send to Repeater

Actively scan defined insertion points

Convert selection
URL-encode as you type
Cut
Copy
Paste
TIPS & TRICKS

▪ Use Intruder to target specific parameters for scanning (Tim Tomes)
▪ You can rename tabs in repeater (Tim Tomes)
▪ Useful for keeping track of identified issues, areas for follow-up
Double-click on tab to rename
TIPS & TRICKS

- Use Intruder to target specific parameters for scanning (Tim Tomes)
- You can rename tabs in repeater (Tim Tomes)
  - Useful for keeping track of identified issues, areas for follow-up
- Use color-coding in proxy tab
<table>
<thead>
<tr>
<th>#</th>
<th>Host</th>
<th>Method</th>
<th>URL</th>
<th>Params</th>
<th>Edt</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td><a href="http://gip.su.gov">http://gip.su.gov</a></td>
<td>GET</td>
<td>/erups/wilume/2017/nmng-hand...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td><a href="http://172.16.127.167">http://172.16.127.167</a></td>
<td>GET</td>
<td>/vulnerabilities/brute/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td><a href="http://172.16.127.167">http://172.16.127.167</a></td>
<td>GET</td>
<td>/vulnerabilities/brute/?username=...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td><a href="http://172.16.127.167">http://172.16.127.167</a></td>
<td>GET</td>
<td>/vulnerabilities/exec/</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>21</td>
<td><a href="http://172.16.127.167">http://172.16.127.167</a></td>
<td>POST</td>
<td>/vulnerabilities/exec/</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>22</td>
<td><a href="http://172.16.127.167">http://172.16.127.167</a></td>
<td>POST</td>
<td>/vulnerabilities/exec/</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>23</td>
<td><a href="http://172.16.127.167">http://172.16.127.167</a></td>
<td>POST</td>
<td>/vulnerabilities/exec/</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>23</td>
<td><a href="http://172.16.127.167">http://172.16.127.167</a></td>
<td>GET</td>
<td>/vulnerabilities/view_source.php?i...</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

```
vulnerabilities/exec/  HTTP/1.1
172.16.127.167
agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:57.0) Gecko/20100113
Content-Type: application/x-www-form-urlencoded
```
TIPS & TRICKS

- Use Intruder to target specific parameters for scanning (Tim Tomes)
- You can rename tabs in repeater (Tim Tomes)
  - Useful for keeping track of identified issues, areas for follow-up
- Use color-coding in proxy tab
- Testing “nested” parameters
POST /vulnerabilities/xss_r/ HTTP/1.1
Host: 172.16.127.167
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:57.0) Gecko/201
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.127.167/vulnerabilities/xss_r/
Cookie: PHPSESSID=$bu6l7ns4jihj729ev2ilkdjgd7$; security=$high$
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 8

regularparameter=$true$&nestedparameter=$1%72%73%74%75%76%77%78%79$
TIPS & TRICKS

- Use Intruder to target specific parameters for scanning (Tim Tomes)
- You can rename tabs in repeater (Tim Tomes)
  - Useful for keeping track of identified issues, areas for follow-up
- Use color-coding in proxy tab
- Testing “nested” parameters
- Keeping state with macros
- Read Web Application Hacker’s Handbook