NEST Kali Linux Tutorial:
OWASP Zed Attack Proxy

“The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications”

Melissa Berghmans
Colin Williams
November 2013

Zed Attack Proxy

• ZAP is an intercepting proxy
  – Sits between your browser and the internet and listens to all web pages you visit
• ZAP makes it easy to test web application security
• ZAP is a project by the Open Web Application Security Project
ZAP Setup

• Start ZAP:
  – Applications → Kali Linux → Top 10 Security Tools → owasp-zap
ZAP Setup

- Open Iceweasel
  - Edit → Preferences → Advanced → Network
ZAP Setup

• Configure Proxy  
  – Settings  
    → Manual Proxy Configuration

• Close Settings

• ZAP is now ready!
Choose a Target

- Navigate to http://www.webscantest.com/
Choose a Target

- Click ‘DB Inject Tests’
- Click ‘Pretty wide open against an int value that has no quotes around it’
Choose a Target

• Click ‘search’

1 | 1 | Rake | clean up leaves | $50 | ![Picture of a rake]

The form based credentials are testuser/testpass, and the HTTP Basic credentials are htestuser/htestpass.
Choose a Target

- Switch back to ZAP
Choose a Target

- Expand ‘http://www.webscantest.com’, ‘datastore’
- Click on the ‘POST’, and select the ‘Request’ tab
Fuzz!

- Select the parameter value (e.g. ‘1’)
- Right click, select ‘Fuzz’
Fuzz!

- Select Fuzz Category: ‘jbrofuzz / SQL Injection’
- Select Fuzzer: ‘MySQL Injection 101’
Fuzz!

- Click ‘Fuzz’, and watch the results at the bottom
• Click on a fuzz attempt, and look at the HTML source:

```
HTTP/1.1 200 OK
Date: Sat, 02 Nov 2013 03:32:01 GMT
Server: Apache
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache

"padding:15px; vertical-align:top ">
<form method="POST"> <input name="id" value="a"> <input type="submit" value="search"></form> Invalid Product<br/>
Error 1054: Unknown column &#039;id' in &#039;where clause' of SELECT * FROM inventory WHERE id = a </td>
</tr>
<tr style='height:20%; vertical-align:top'>
<td align="center"> The form based credentials are testuser/testpass, and the HTTP Basic credentials are btestuser/btestpass. </td>
</tr>
```
Exploit

• Go back to Iceweasel, enter ‘1 OR 1=1’ into search field, and click search:
References

- http://www.youtube.com/watch?v=Xp_PBH7wjiw