New Year, New Skills

Web Application Pentesting

Jennifer Shannon

- Senior Security Consultant at Secure Ideas
  - Jacksonville HQ office
- Industry Experience
  - Started as SOC Analyst
  - Reverse engineering malware & threat intelligence
  - Pentesting, Security Consulting, & Training
- Other Interesting Facts
  - All around geek
  - Collector of things
  - Lockpick enthusiast
  - The city of Jacksonville stole my driveway once

Secure Ideas
professionally evil®

What is *Professionally Evil*?

professionally evil®

We need to think "evil" so we can understand **how** an attacker will behave and **what** they will attack.

And we are Professional:

- Provide clients the best penetration test experience
- Educate clients on how to improve their security posture
- **Permission**: Penetration Testing is always under contract
- Establish and **follow** rules of engagement

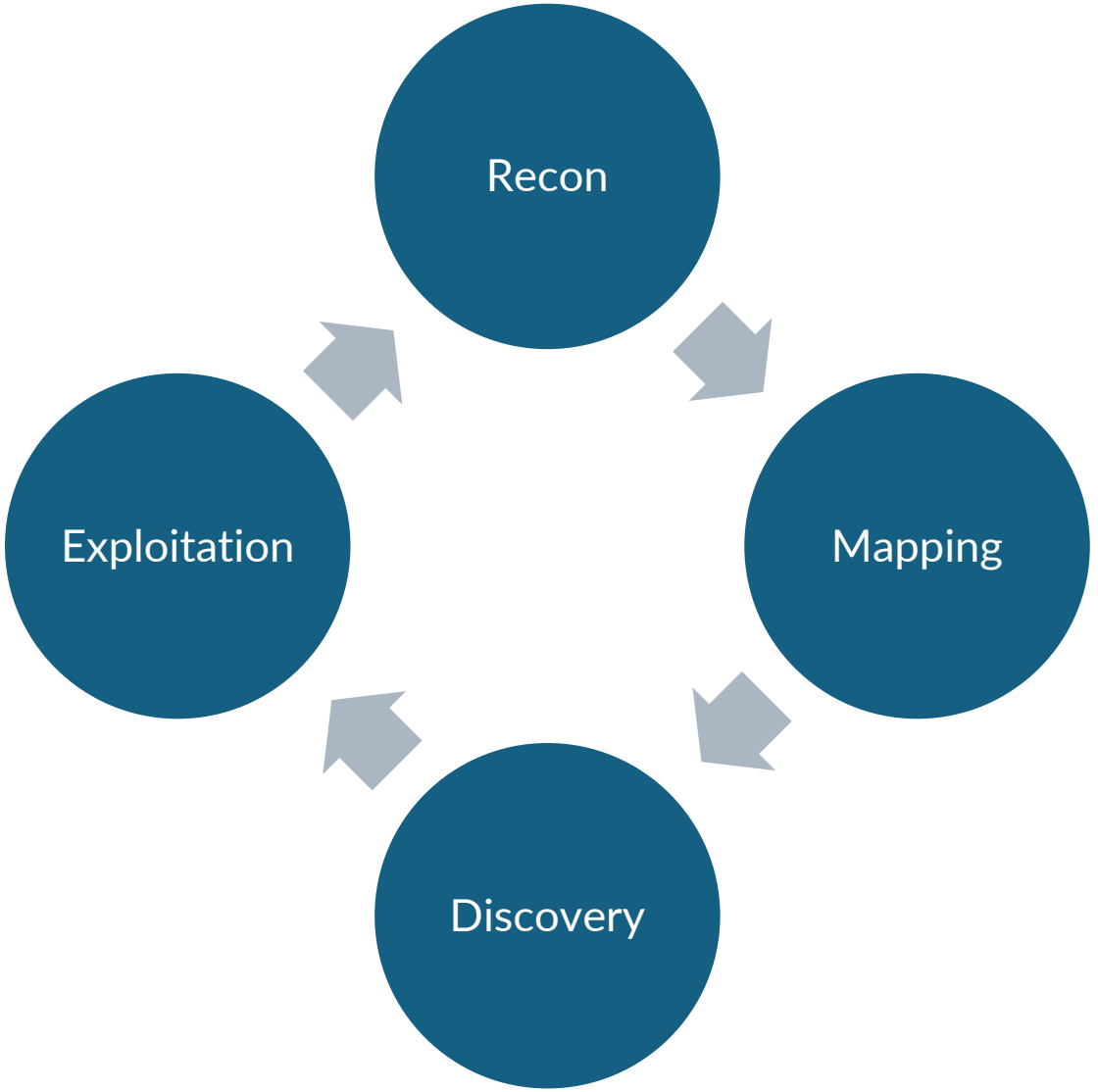
Copyright © 2021 Secure Ideas LLC

Why this matters?

Copyright © 2021 Secure Ideas LLC

Secure Ideas
professionally evil®

Methodology



Copyright © 2021 Secure Ideas LLC

Reconnaissance

Information gathering

- Search of public sources
- Information regarding the target organization and its infrastructure, systems, and applications.

Gathered information can include both technical and non-technical details such as:

- Possible target IP address ranges
- Associated domains and subdomains
- Employee names and email addresses
- Usernames and passwords from previous breaches

First phase of the penetration testing methodology meant to

- Provides insight for subsequent phases
- May be shortened due to test type

Copyright © 2021 Secure Ideas LLC

Mapping Tasks

- Initial stage that touches the application
- Recon may, but typically recon is external to the application
- Focuses on determining how the application works
  - Unauthenticated visitor
  - Authenticated user
  - Administrator?
- It is critical to build this foundation
  - Guides the entire rest of the testing
  - Ensures the tester understands the application

Copyright © 2021 Secure Ideas LLC

Discovery

Discovery is the longest part of a test

- Focused on finding potential flaws and issues

Based on recon and mapping

- Testing techniques can find multiple types

Focus on context

- Application context
  - What the application does
  - How the application works
- Vulnerability context
  - Server or client focused
  - Technology boundaries
- Exploit context
  - For the next step
  - Where does your payload land

Copyright © 2021 Secure Ideas LLC
Secure Ideas professionally evil®

Exploitation!

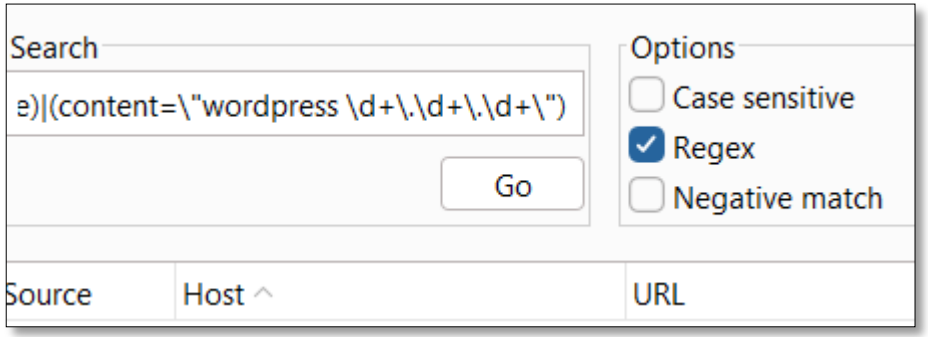
- This is the final step!
- Uses information gathered during early stages
- Depending on flaws discovered:
  - This may be limited to just a Proof-of-Concept Attack
  - Not performed if potentially damaging
    - Ex: DDOS
- If access to underlying system access is granted this restarts the whole process

Tips and tricks

- A few of my favorite things

Copyright © 2021 Secure Ideas LLC

Regex to search!



Copyright © 2021 Secure Ideas LLC

Regex: Information Disclosure

- (Server:)|(X-Powered-By:)|(ASP.Net)|(Microsoft-IIS)|(Microsoft-HTTPAPI)|(X-AspNet-Version)|(nginx)|(X-Collaborator-Version)|(Vmware)|(content=\"wordpress \d+\.\d+\.\d+\")

```
GET /success.txt?ipv6 HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (Windows
NT 10.0; Win64; x64; rv:120.0)
Gecko/20100101 Firefox/120.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
```

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Content-Length: 8
4 Via: 1.1 google
5 Date: Thu, 30 Nov 2023 03:14:08
  GMT
6 Age: 76777
7 Content-Type: text/plain
```

- Why?
  - Can help identify underlying services/infrastructure
  - Allows for more tailored attacks

Copyright © 2021 Secure Ideas LLC
Secure Ideas professionally evil®

Regex: CORS

- (Access-Control-Allow-Credentials: true)|(Access-Control-Allow-Origin: (?!.*(*)))|(Access-Control-Allow-Methods:)

```
HTTP/2 200 OK
Access-Control-Allow-Origin:
https://accounts.google.com
Access-Control-Allow-Methods: GET,
 POST, OPTIONS
Access-Control-Max-Age: 86400
Access-Control-Allow-Credentials:
true
```

- Why?
  - Helps to find screenshot material quickly!

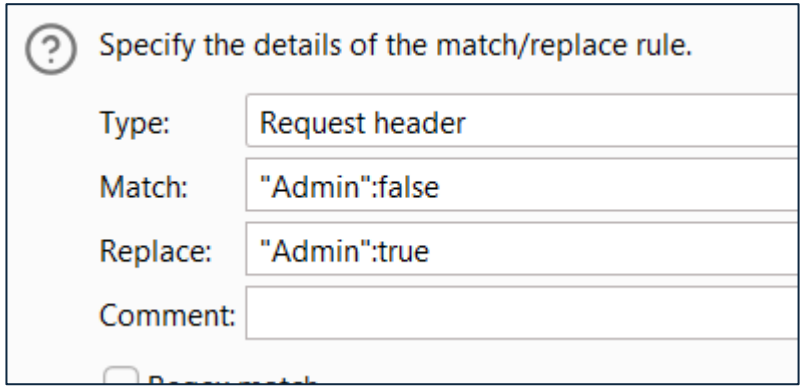
Copyright © 2021 Secure Ideas LLC
Secure Ideas professionally evil®

Search and Replace?

- In Burp there are default Match/Replace rules
  - Disabled by default
  - Perform some basic tasks to save time

Enabled	Item	Match	Replace	Type	Comment
☐	Request header	^User-Agent.*$	User-Agent: Mozilla/4.0 (compatibl...	Regex	Emulate IE
☐	Request header	^User-Agent.*$	User-Agent: Mozilla/5.0 (iPhone; CP...	Regex	Emulate iOS
☐	Request header	^User-Agent.*$	User-Agent: Mozilla/5.0 (Linux; U; A...	Regex	Emulate Android
☐	Request header	^If-Modified-Since.*$		Regex	Require non-cached res

- But wait, there's more!
  - Create custom rules for each application

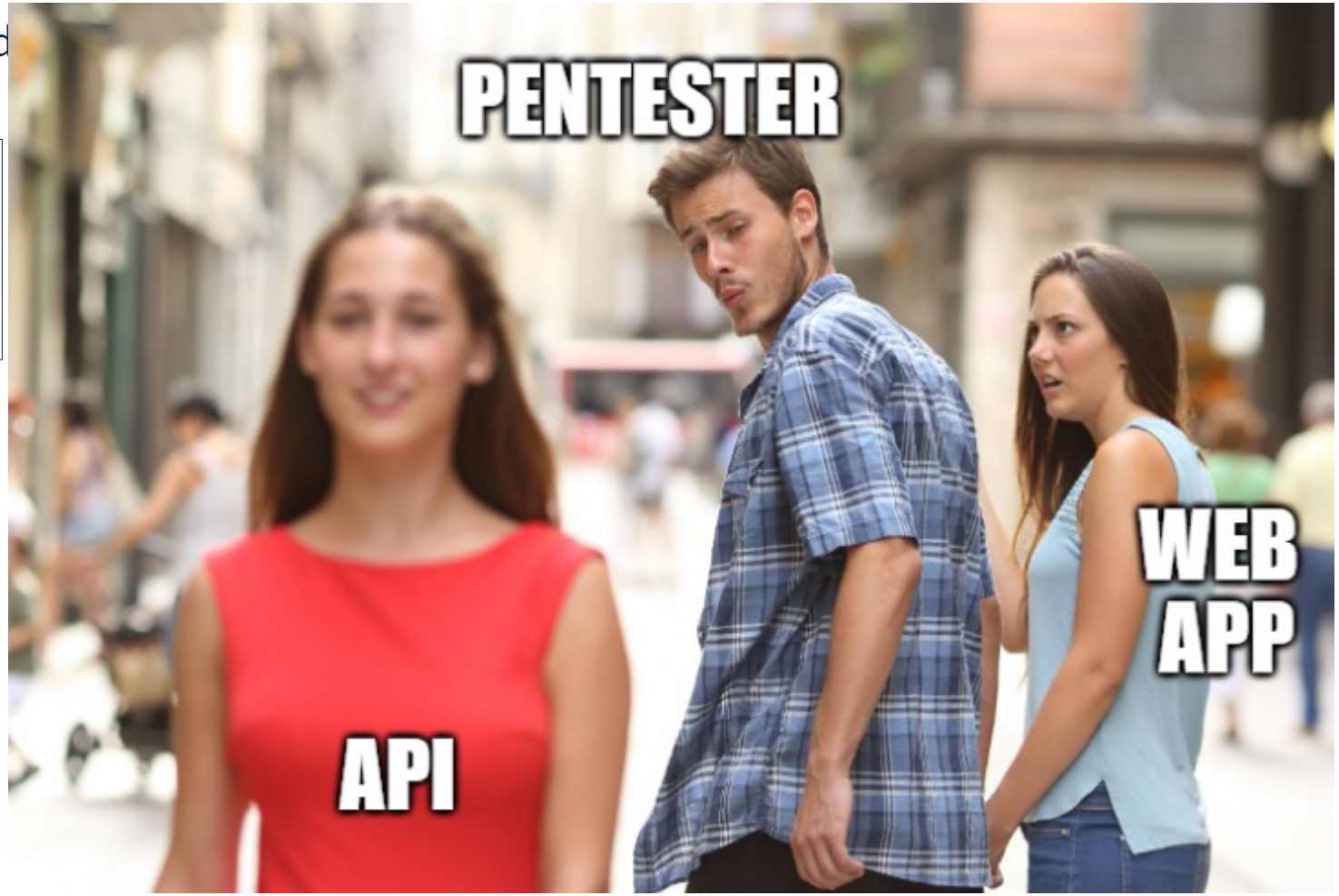


Copyright © 2021 Secure Ideas LLC

Undocumented API? Find References!

- Find where Endpoint is first mentioned

Engagement tools	Search
Compare site maps	Find comments
Expand branch	Find scripts
Expand requested items	Find references
Collapse branch	Analyze target



Copyright © 2021 Secure Ideas LLC

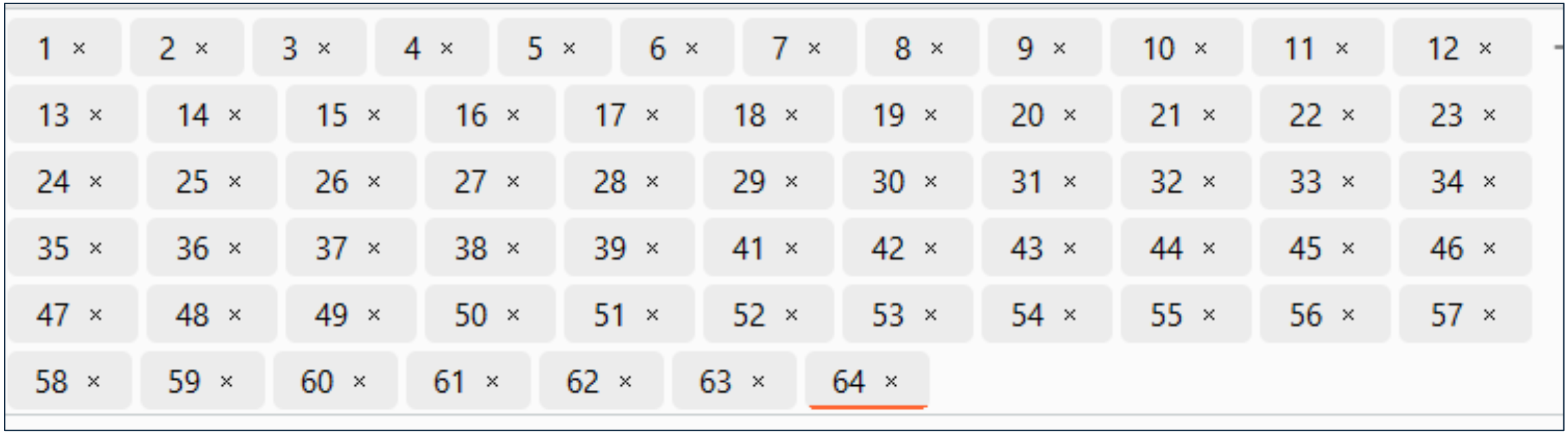
Hotkeys!

- Settings > User Interface > Hotkeys
- My favorite hotkeys
- Ctrl + R
  - Sends to Repeater
- Ctrl + Shift + R
  - Jumps to Repeater
- Ctrl + F
  - Forward intercepted Proxy message

Toggle Proxy interception	Ctrl+T
Open embedded browser	
Issue Repeater request	Ctrl+Space
Go back in Repeater history	
Go forward in Repeater history	
Start Intruder attack	
Switch to Dashboard	Ctrl+Shift+D
Switch to Target	Ctrl+Shift+T
Switch to Proxy	Ctrl+Shift+P
Switch to Intruder	Ctrl+Shift+I
Switch to Repeater	Ctrl+Shift+R
Switch to Collaborator	
Switch to Sequencer	
Switch to Decoder	
Switch to Comparer	
Switch to Logger	Ctrl+Shift+L
Switch to Organizer	Ctrl+Shift+O
Switch to Extensions	
Show settings	
Go to previous tab	Ctrl+Minus

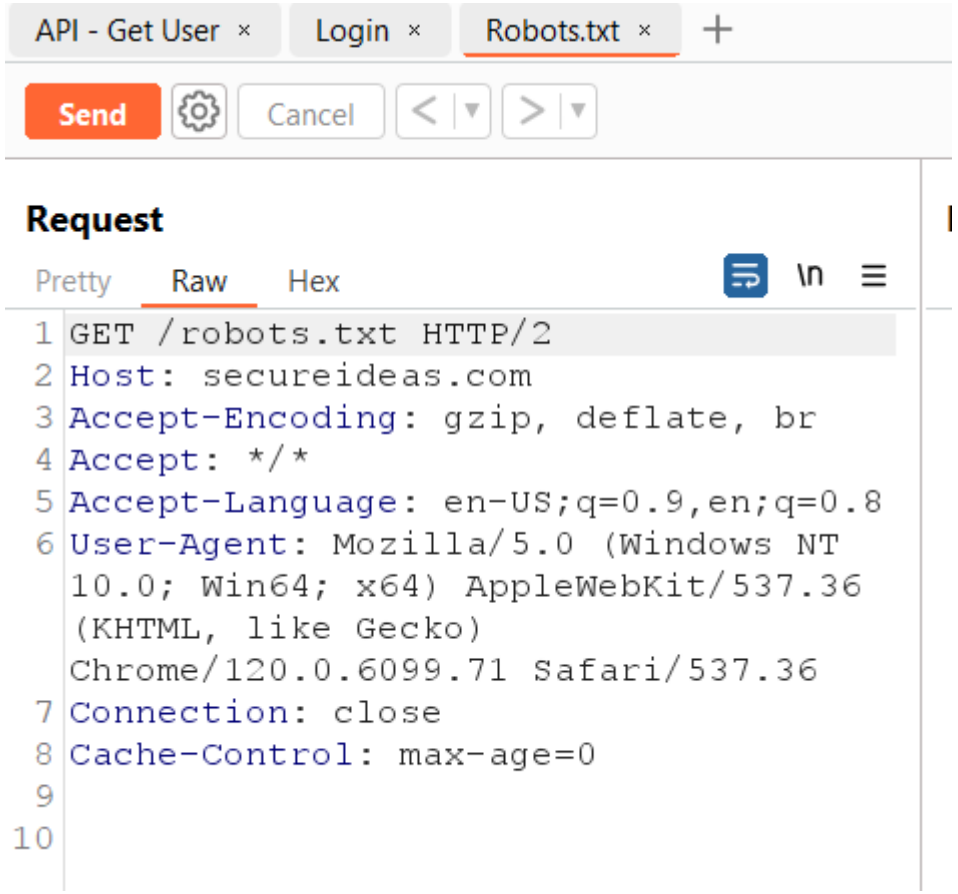
Copyright © 2021 Secure Ideas LLC

Old Me – Repeater Tabs



Copyright © 2021 Secure Ideas LLC

New Me – Renamed Repeater Tabs!



Copyright © 2021 Secure Ideas LLC

Happy Hacking!

Copyright © 2021 Secure Ideas LLC