Web App Pentests

- Very much a grey area
- Absolutely used in pentesting
- But..
- It is also its own full test
- Usually used as a means to an end
  - Access….
- Never proport to be a full assent of a web server
- How to report this?

Web App Objectives

- Check all input fields for input validation
- Identify SQL injection
- Identify cross-site scripting (XSS)
- Identify known command injection vulnerabilities
- Identify known vulnerabilities in common commercial and open-source web application software
- Identify business logic errors in applications
- Exploit each flaw in an effort to gain access to the target host and pivot to the internal environment

Web App Pentests

- System Infrastructure Scanning
  - Validate that only required ports, protocols and services are exposed
  - Excess exposure should be documented
- SSL/TLS Configuration Analysis
  - Enumeration of
    - Protocols
    - Cipher suites
    - Hashing Algorithms
    - Certificate Details
  - ***Important for PCS-DSS***

Web App Pentests 2

- HTTP Security Header Analysis
- Application Component Analysis
  - Third party components should be enumerated and tested
- Authentication Controls Analysis
  - Username enumeration
  - Single use tokens
  - Password policy strength
  - Password change mechanism
  - Account lockout
  - Rate limiting
  - ***SSO and MFA***

Web App Pentests 3

- Session Handling Analysis
  - Token determination
  - Token analysis
  - Token attacks
  - Token replacement
  - Session termination
- Input Tampering
  - Script injection
  - Data Layer manipulation
  - External system interaction
    - Collaborator
    - Cross-Origin Resource Sharing CORS
  - Cryptographic analysis

Web App Pentests 4

- Input Enumeration
  - Determine Identifier Patterns
  - Attempt access of unauthorized information
- Vertical Privilege Separation
- Horizontal Privilege Separation
- Automated Web Application Scanning
- API's
  - ***Getting API documentation before start of testing <-THIS!!!!***

"Look at me!
I'm a hacker!"

Red Team

- We are now mimicking what an attacker does
- Takes longer and is ***more expensive***
- Like a Pentest.. But slower and quieter
- Starting to get stealthy
- A lot of the methodology covered to this point is still used and in play

Red Team Objectives

- Harvest Sensitive Data
- Lateral Movement
- Data Exfiltration
- Defeat or disable alarm systems or other security monitoring or reporting devices
- Be Stealthy

Then.... We report as we go...

Red Team 2

- **Weaponization**
  - Using reconnaissance, craft software to evade defenses and that will entice employees to execute
  - Example Activities
    - Forge identity documents, contracts, and authorization letters
    - Develop custom attacks focused specifically on the customer's actual assets and defenses
    - Develop methods to defeat or bypass physical security measures, such as unsecured or poorly monitored ingress points

Totally not the same guy

Red Team 2

- **Delivery**
  - Delivery mechanisms may include: email attachments, USB sticks, social media or other public facing input points
- Exploitation
  - Exploitation of human, server, hardware or physical assets
  - Exploitation of vulnerable systems/service

Red Team 4

- **Command and Control (C2)**
  - Establish a two-way communication channel between Red Team controlled infrastructure and the target environment.
    - Use of common protocols with unconventional techniques (DNS tunneling, Fake TLS.
    - A wireless access point on a hardwired network, which may be accessed from a parking lot or other unsecured location

Purple Team

- Working with the blue team
- Step-by-step
- The goal is getting caught
- Improving detects
- Not stealthy
- Stimulus and response

Let's hug it out!

Black Team??

- The biggest issue with Red Teams is time
  - We just do not have enough
- Real attacks fail... A lot
- Give the team time to try lots of different attacks
- Much larger timeframe
- Pricing
- Lots of failure

I have..
Very...
Bad posture..

Scope Creep

- This always happens
  - Not a bad thing
  - If it is managed
  - Why does this happen? The customer trusts you
- Manage Expectations
  - Please see the Scope and RoE sections
- Constant communication with a customer
  - Document!!!!!!!
  - Change midstream and mad we did not deliver the initial contract
- Almost never a problem to ask for more money <- Change order!!
- Notify management early and often

When The Customer is Not Ready

- Most common issue ever..
- Note it in the report
  - CYA
- Notify management there is an issue
- Management can often get the customer moving
- Let the customer know not being ready impacts their report
- DO NOT BREAK YOURSELF

BAD TIMING

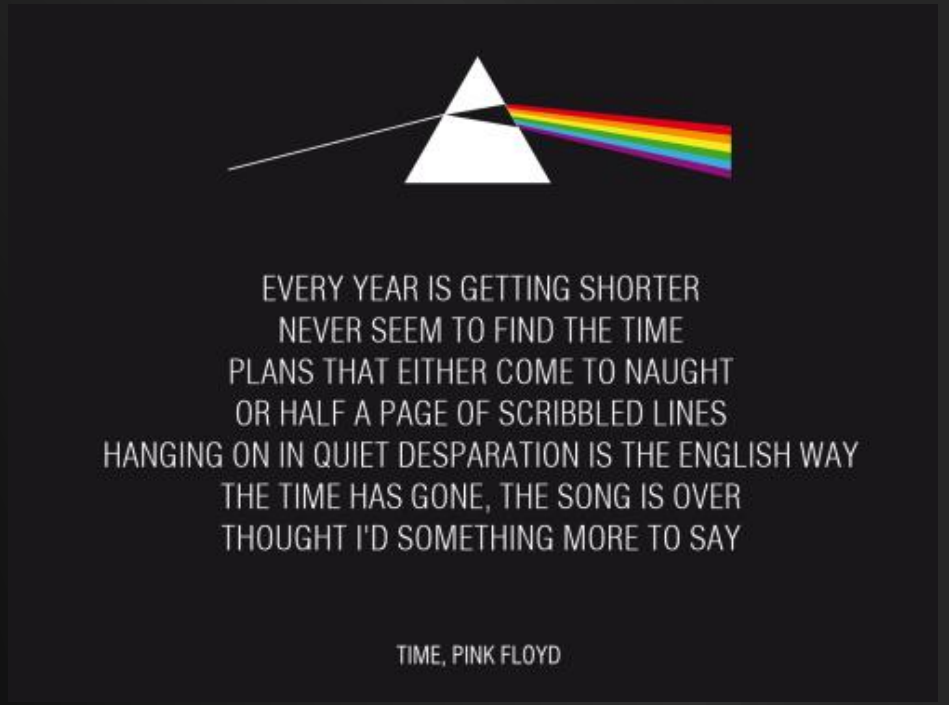
Tester Burnout

- It is real
- Two problems
  - Things going great!!!!
  - The test is kicking my ass!!!
- Learn to leave things behind
- Exercise
- Get a hobby
- Have a family
- Have friends
- Have a life

"I love what I do!"
"I would do this on my own time!"
"Don't worry about me!"

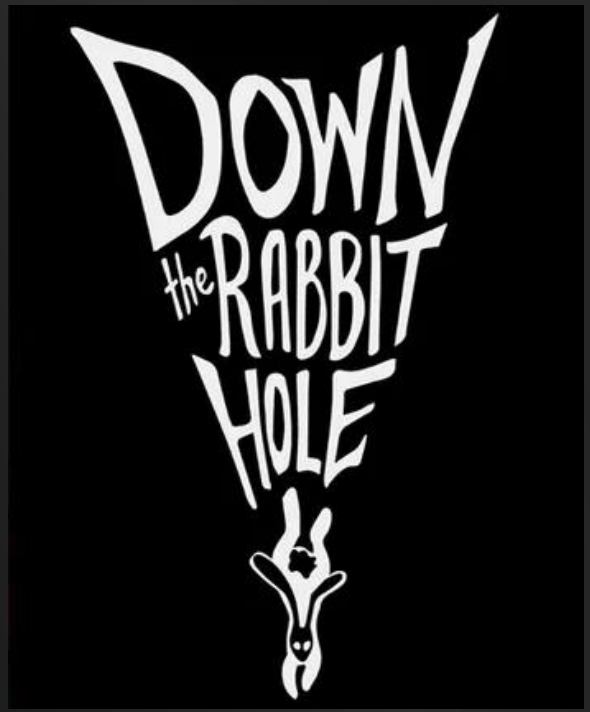
Tester Burnout: Timebox

- Customers are paying for your time
- No test is ever over!!!
- If you work a lot of overtime you are just hurting yourself
- "We pride ourselves on working 60 hour weeks!"
  - A tale of a testing company that no longer exists
- Keep your days about 8 hours
- Burnout is real and real expensive



Rabbit Holes

- 5 and 5 rule
  - Five things, five min each, move on
- Too easy to get distracted
- Coverage is far more important
- Get coverage, then circle back on some possible holes



New People…

- Getting up and running will take more time….
- You may be working a bit more than 8 hours a day
  - Sorry
- Look to get training and strive for some level of mentorship
  - What Does Mentorship look like?
- There is a learning curve
- It will get better
- Knowledge pull vs. push

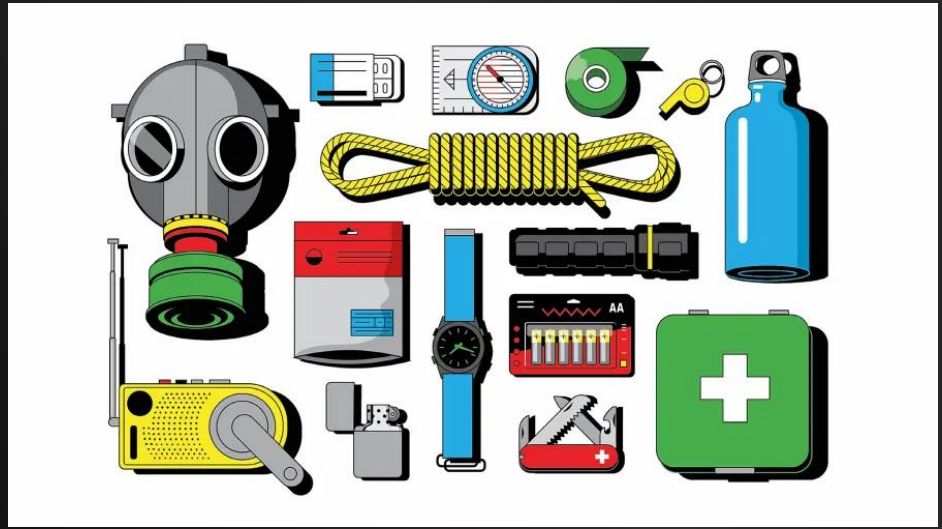
"Welcome aboard!"

What We Do Not Test

- Personal phones*
- Cloud Services*
- Third-Parties*
- Family Members*
- Other Personal Devices*
- ***DDoS***
- ISP*
- * = Without permission

Scope

- Share screen when meeting
- Everyone should see the same things
- Email Followup
  - No Exceptions
  - Confirm receipt
- Beginning of the "Doomsday File"
- CYA



For when things go real bad.

A Special Note On Communication

- Document everything
- Email, Email, Email
- Call with the customer? Email a follow-up
- Called and missed them? Voice Mail and an Email Followup
- "I called them last week"
- "I emailed them last week"
- These are things that enrage John
- In Person > Video > Phone > Email > Text > Anything > Twitter

MITRE... Always MITRE

- Everything is mapping to MITRE ATT&CK
- Expect this as a request
- Easy if you report as you go
- Very, very hard if you don't
- Tie to Risk Assessments and Threat Modeling
- "Is this what APT 22322 would do??"
- "You say yes!!!!"

Recon

- Do not touch
- Scope Validation
- IP and Domain Range validation… And Russia…. And Iran….. And DoD….. And the Wrong Casino….. And half of Canada

Vulnerability Scanning

- Same as it was 10+ years ago
- Vendors have not changed with the times
- Test and scan for external vulnerabilities
- Some companies are moving towards credentialed scans
- Very little in actual innovation

Vulnerability Prioritization

- New focus on prioritization
- Address the most critical issues first
- While prioritization can be a great approach it can also be a crutch
- Addressing only the High and Critical issues
  - Many attackers will exploit Low and Informational issues
- Very difficult for vendors to do this without organizational and service context

Low and Informational Blind Spots: Example

10.10.10.133 (tcp/23)

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------
Login:

------------------------------ snip ------------------------------
```

10.10.10.134 (tcp/23)

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------
Login:

------------------------------ snip ------------------------------
```

10.10.10.135 (tcp/23)

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------
router>

------------------------------ snip ------------------------------
```

Addressing Vulnerabilities: The Wrong Way

- Many organizations address vulnerabilities by IP address
- For example: 1,000 IP addresses x ~25 vulnerabilities per IP = 25,000 issues to address
- This can be daunting
- Because of this we can see why so many companies focus on prioritization
- However, this approach is almost always wrong

Addressing Vulnerabilities: The Correct Way

- Stop focusing on IP addresses and ranges
- Focus on the vulnerabilities
- Instead of 25,000 total vulnerabilities you will be dealing with a few hundred that repeat on multiple systems
- Use automation and address them as groups of issues
- This approach works regardless of the tool you use
- With this method BHIS testers have addressed over 1 million IP address, all vulnerabilities in less than 3 weeks

MITRE ATT&CK

Enterprise Matrix

Below are the tactics and technique representing the MITRE ATT&CK Matrix™ for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Distributed Component Object Model	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Logon Scripts	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CMSTP	Exploitation for Credential Access	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code Signing	Forced Authentication	Network Sniffing	Pass the Ticket	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Exploitation for Privilege Escalation	Compile After Delivery	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Compiled HTML File	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Fallback Channels	Transfer Data to Cloud Account	Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Firmware	Input Capture	Permission Groups Discovery	Remote Services	Input Capture	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Screen Capture	Multiband Communication		Service Stop

Exploit Public-Facing Application

External Remote Services

Getting Caught

Client malware detection and countermeasures			
HTTP viewstate covert channel - VSAgent; Port 443	2/1/2018 9:33	blocked	required authenticated proxy which is not compiled into client agent
DNSCat C2 channel; Port 53	2/1/2018 9:37	blocked	McAfee signature fired, and deleted malware
Metasploit HTTPS Meterpreter Shell code injected into memory via PowerShell; Port 443	1/31/2018 15:30	blocked	script would not seem to execute. No shell connection received
Metasploit TCP Meterpreter Shell code injected into memory via PowerShell (obfuscated with Unicorn); Port 443	2/1/2018 9:35	blocked	McAfee signature fired, and deleted malware
PowerShell Empire PowerShell code injected into memory; Port 443	2/1/2018 9:48	allowed	Command shell active
Raw malware EXE - Metasploit; Port 443; templated using write.exe	2/1/2018 9:56	allowed	Command shell active
Encoded malware EXE - Metasploit; Port 443; templated using write.exe	2/1/2018 9:57	allowed	Command shell active
MS-Office Document malicious macro; HTTPS port 443	2/1/2018 14:28	allowed	Command shell active
MS-Office Document malicious macro; TCP Port 8080	2/1/2018 14:34	blocked	McAffee Detected Malware
Cleartext communication with Netcat tool; Port 8443	2/1/2018 10:00	allowed	Anything that communicates with a TLS port such as 443 or 8443 is allowed through the perimeter without inspection
Metasploit Reverse TCP single stage EXE file.	2/1/2018 14:40	allowed	Command shell active
Metasplot Reverse TCP single stage Visual Basic file.	2/1/2018 14:39	blocked	McAffee Detected Malware
ICMP C2 Channel	2/1/2018 10:52	allowed	ICMP command shell established

Getting Caught 2

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Command-Line Interface	Audio Capture	Automated Exfiltration	Commonly Used Port
AppCert DLLs	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Data Compressed	Communication Through Removable Media
AppInit DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Vulnerability	Execution through API	Browser Extensions	Data Encrypted	Connection Proxy
Application Shimming	AppInit DLLs	Code Signing	Credentials in Files	Network Service Scanning	Logon Scripts	Execution through Module Load	Clipboard Data	Data Transfer Size Limits	Custom Command and Control Protocol
Authentication Package	Application Shimming	Component Firmware	Exploitation of Vulnerability	Network Share Discovery	Pass the Hash	Graphical User Interface	Data Staged	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Bootkit	Bypass User Account Control	Component Object Model Hijacking	Forced Authentication	Peripheral Device Discovery	Pass the Ticket	InstallUtil	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Browser Extensions	DLL Search Order Hijacking	DLL Search Order Hijacking	Hooking	Permission Groups Discovery	Remote Desktop Protocol	LSASS Driver	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Change Default File Association	Exploitation of Vulnerability	DLL Side-Loading	Input Capture	Process Discovery	Remote File Copy	Mshta	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Component Firmware	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	Query Registry	Remote Services	PowerShell	Email Collection	Scheduled Transfer	Fallback Channels
Component Object Model Hijacking	File System Permissions Weakness	Disabling Security Tools	Network Sniffing	Remote System Discovery	Replication Through Removable Media	Regsvcs/Regasm	Input Capture		Multi-Stage Channels
Create Account	Hooking	Exploitation of Vulnerability	Password Filter DLL	Security Software Discovery	Shared Webroot	Regsvr32	Man in the Browser		Multi-hop Proxy
DLL Search Order Hijacking	Image File Execution Options Injection	Extra Window Memory Injection	Private Keys	System Information Discovery	Taint Shared Content	Rundll32	Screen Capture		Multiband Communication
External Remote Services	New Service	File Deletion	Replication Through Removable Media	System Network Configuration Discovery	Third-party Software	Scheduled Task	Video Capture		Multilayer Encryption
File System Permissions Weakness	Path Interception	File System Logical Offsets	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Scripting			Remote File Copy

Key Takeaways

- Moving from “Can we be hacked?”
  - To..
- “What can we detect?”
- We (finally) have a framework for this with MITRE
- We also have a large number of tools in their infancy to help automate this
- Start by finding gaps. Fill them. Move on.
- Start with the framework

Scanning Potpourri: Default Scans

- Do them
- Yes, you can tune
- Yes, you can do "better"
- Yes, the default is lame
- But...
- When something goes wrong, what is blamed?
- Default PCI vs. Fragile system
- Hot Rod Scan vs. Fragile system

Scanning Potpourri: Web Checks

- Are horrible
- Burp or ZAP are much, much better
- Slow down the scan
- Turn them on
- A special note on contracts and coverage

Things That Can Kill You

- Password Attacks
- By far the most dangerous thing you can do
- Account Lockout
- Freeze authentication
- Spread out timing
- Slow. Things. Down
- Note on timing and SSH
- Now, some stories
  - Canada.. Again.
  - Insurance company

Things That Can Kill You

- Bandwidth
- Do. Not. Scan. Down. A. VPN.
- Only so much bandwidth
- VPN adapters are fragile
- You will drop packets at best
- You will kill the service at worst
- Even true on older internal networks
- Switches.. Dead Switches..
- "Thats a Finding!"

Things That Can Kill You

- Old Systems
- Please, please ask about this in the RoE/Scope Meeting
- "So, any systems from 2008 we should know about?"
- "What are the top five systems that keep going down?"
- "Have other tests ever crashed something?"
- Document