Eric Audit, Daniel McNair, Martin Williams

E-commerce Honeypot

Purpose

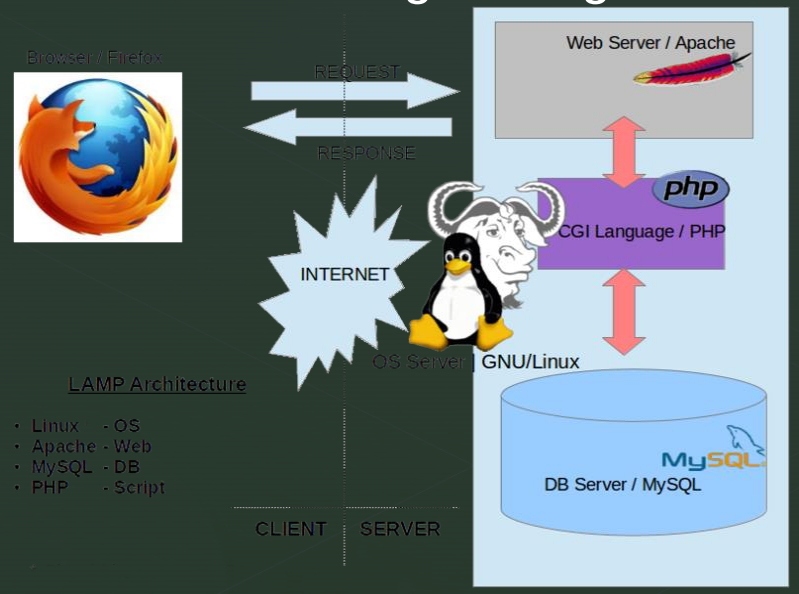
- This presentation will describe the design, implementation, and documentation relevant to Jackal’s e-commerce Honeypot.

Environment Structure

- The ecommerce store is hosted on an AWS Linux 2 EC2 t2.micro (free) instance
- Added software: Apache Tomcat 9, Apache Struts 2.5, MATE desktop, Firefox, Tigervnc, MariaDB 10.2, PHP 7.2.

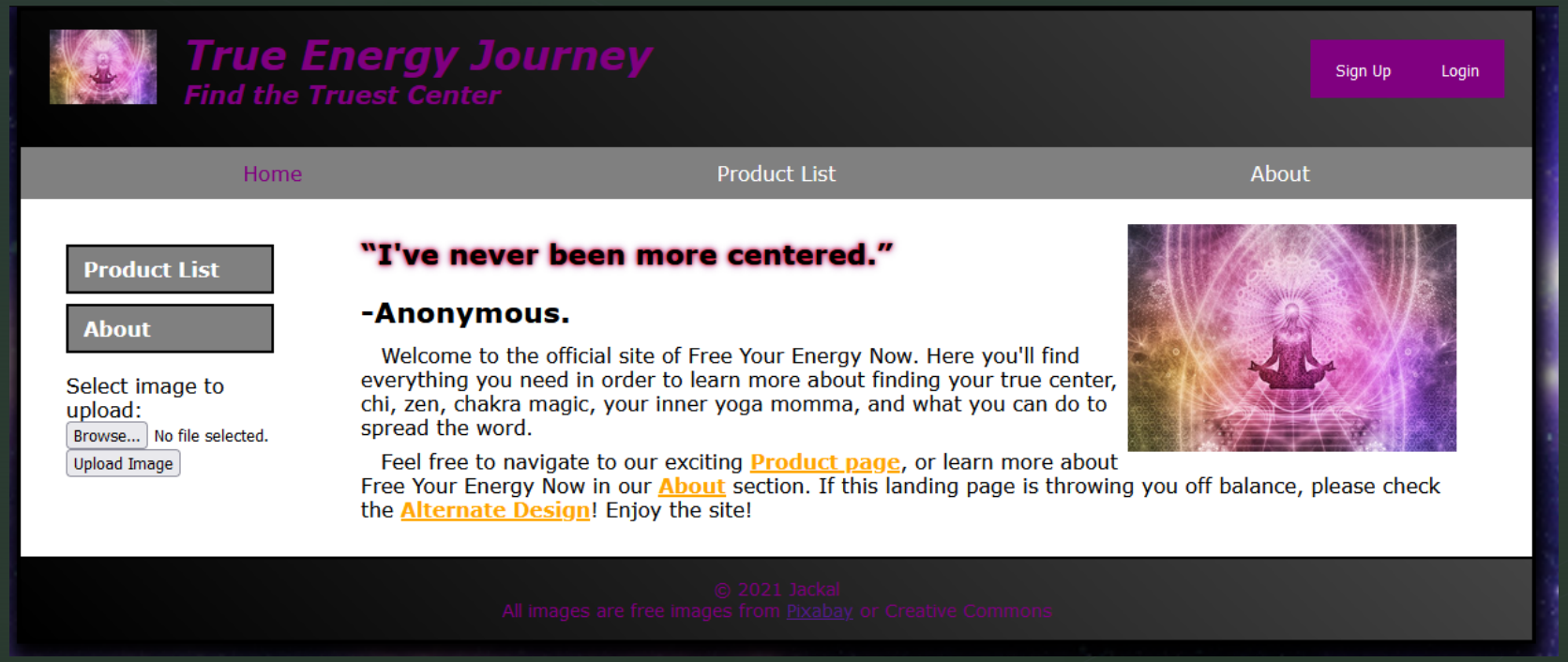
Backend Systems

- Daniel configured the majority of the backend systems that support the e-commerce honeypot. The most important of these systems is the Apache 2.4.33 webserver that contains our HTML, CSS, and PHP files. The database and log management was also configured by Daniel.



User Interface

- The user interface of the site consists of three webpages: index.html, products.html, and about.html and four php scripts upload.php, xss.php, login.php, and signUp.php.

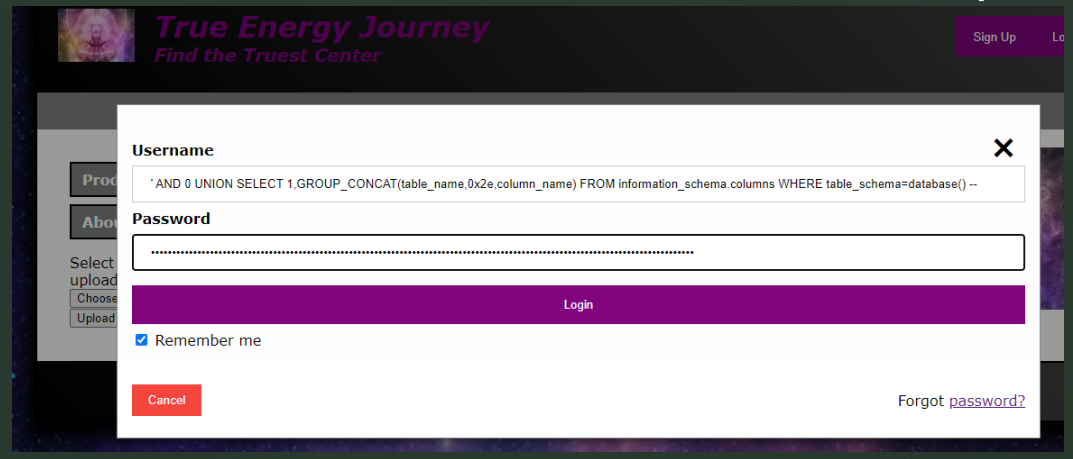


Vulnerability Objectives

- While the specifics of how each vulnerability was implemented and the methods used to test them will be discussed in their own sections in the following slides.
- For each vulnerability Jackal used a well-known CVE with documented POC.

A1:2017-Injection

- SQL is one of the most common attacks on the web and often results in the most damage to organizations and its users.
- The e-commerce site contains an SQL injection vulnerability in its Login function in which a threat actor can escape the initial SQL query and place their own SQL statements.
  This vulnerability is present due to a lack of utilizing prepared SQL statement that can not be escaped.



A2:2017-Broken Authentication

- Broken Authentication can include user authentication methods that do not protect users from password complexity related account compromise or password brute forcing attacks.
- The sign-up function does not restrict the types of passwords users can enter and stores passwords in plain text in the database. The login function also does not limit the number of login attempts which allows for password brute forcing.

A3:2017-Sensitive Data Exposure

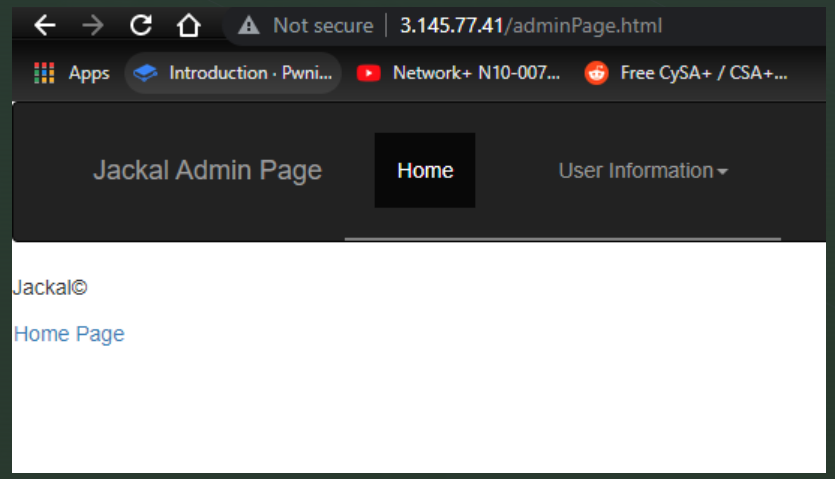
- HTTPS not enforced on infrastructure. HTTP allows data to be transmitted in plain text which can be dangerous when users are transmitting login or purchasing data(name, address, credit card number, etc.) on the website.

A4:2017-XML External Entities (XXE)

- No input validation on upload.php.
- Files placed in 'BadFiles' directory with 777 perms on webserver.
- Attack would to be like CVE-2015-0250 and involve xml payload inside SVG file.
- Xml parser never worked.
- Upload(good).php fixes Input validation errors.

A5:2017-Broken Access Control

- Hidden admin page which does not authenticate which user is logged in(available to all users instead of just the admin user) or presents a password request, no direct links on server to this page so it would require directory brute forcing to find.



A6:2017-Security Misconfiguration

- Apache Tomcat 9 uses default accounts and passwords.
- 'BadFiles' Directory has 777 perms unnecessarily.

A7:2017-Cross-Site Scripting

- Cross-Site Scripting is an attack vector that injects malicious code into a vulnerable website.
- The webserver blindly accepts input from the user then renders the input in the client browser
- Without some sort of input validation or sanitization, a malicious script can reflect off our website onto the users browser
- CVE-2012-4558

Source: Dr. Armin Tabari

A8:2017-Insecure Deserialization

- Vulnerability was implemented as described in CVE-2017-9805.
- Apache Struts 2.5 is used on the infrastructure.
- struts2-rest-showcase.war used as included.

```
root
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
libstoragemgmt:x:999:997:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rngd:x:998:996:Random Number Generator Daemon:/var/lib/rngd:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
ec2-instance-connect:x:997:995::/home/ec2-instance-connect:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
chrony:x:996:994::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
ec2-user:x:1000:1000:EC2 Default User:/home/ec2-user:/bin/bash
nginx:x:995:993:Nginx web server:/var/lib/nginx:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
polkitd:x:994:992:User for polkitd:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
tomcat:x:91:91:Apache Tomcat:/usr/share/tomcat:/sbin/nologin
```

A9:2017-Using Components with Known Vulnerabilities

- The Apache version 2.4.33 on the EC2 instance contains an out of bound read vulnerability that can cause a denial of service. According to CVE-2021-36160 “A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS)”. Mod_proxy_uwsgi should not be enabled on this server so patching would involve disabling this package.
- Apache Struts 2.5 is vulnerable to insecure deserilization

Logging

- In order to log the traffic going to the EC2 instance, AWS CloudWatch was used to aggregate logs in ten-minute intervals. AWS utilizes flow logs that are generated by the instance and sends them to CloudWatch so that the logs and system resource monitoring can be done on the same service.

```
2 474199228591 eni-0d3558096b7c87e11 80.82.65.247 172.31.18.18 60738 1717 6 1 40 1638627142 1638627183 REJECT OK
2 474199228591 eni-0d3558096b7c87e11 89.248.165.72 172.31.18.18 48650 34957 6 1 40 1638627142 1638627183 REJECT OK
2 474199228591 eni-0d3558096b7c87e11 89.248.165.72 172.31.18.18 48650 32349 6 1 40 1638627142 1638627183 REJECT OK
2 474199228591 eni-0d3558096b7c87e11 162.142.125.149 172.31.18.18 34782 3307 6 1 44 1638627142 1638627183 REJECT OK
2 474199228591 eni-0d3558096b7c87e11 162.142.125.159 172.31.18.18 16632 8014 6 1 44 1638627142 1638627183 REJECT OK
2 474199228591 eni-0d3558096b7c87e11 92.118.161.9 172.31.18.18 59570 37777 6 1 44 1638627142 1638627183 REJECT OK
2 474199228591 eni-0d3558096b7c87e11 162.142.125.152 172.31.18.18 60995 12186 6 1 44 1638627184 1638627243 REJECT OK
2 474199228591 eni-0d3558096b7c87e11 45.134.26.42 172.31.18.18 44553 41496 6 1 40 1638627184 1638627243 REJECT OK
2 474199228591 eni-0d3558096b7c87e11 221.181.185.151 172.31.18.18 24739 22 6 6 2062 1638627184 1638627243 ACCEPT OK
2 474199228591 eni-0d3558096b7c87e11 89.248.165.72 172.31.18.18 48650 25775 6 1 40 1638627184 1638627243 REJECT OK
2 474199228591 eni-0d3558096b7c87e11 162.142.125.151 172.31.18.18 41970 10943 6 1 44 1638627184 1638627243 REJECT OK
2 474199228591 eni-0d3558096b7c87e11 192.241.207.12 172.31.18.18 33469 443 6 1 40 1638627184 1638627243 REJECT OK
2 474199228591 eni-0d3558096b7c87e11 172.31.18.18 221.181.185.151 22 24739 6 11 9069 1638627184 1638627303 ACCEPT OK
2 474199228591 eni-0d3558096b7c87e11 45.134.26.238 172.31.18.18 44679 24210 6 1 40 1638627254 1638627303 REJECT OK
2 474199228591 eni-0d3558096b7c87e11 162.142.125.151 172.31.18.18 36900 12153 6 1 44 1638627254 1638627303 REJECT OK
2 474199228591 eni-0d3558096b7c87e11 45.134.26.231 172.31.18.18 44603 61804 6 1 40 1638627254 1638627303 REJECT OK
```