CMSC389R

Web II

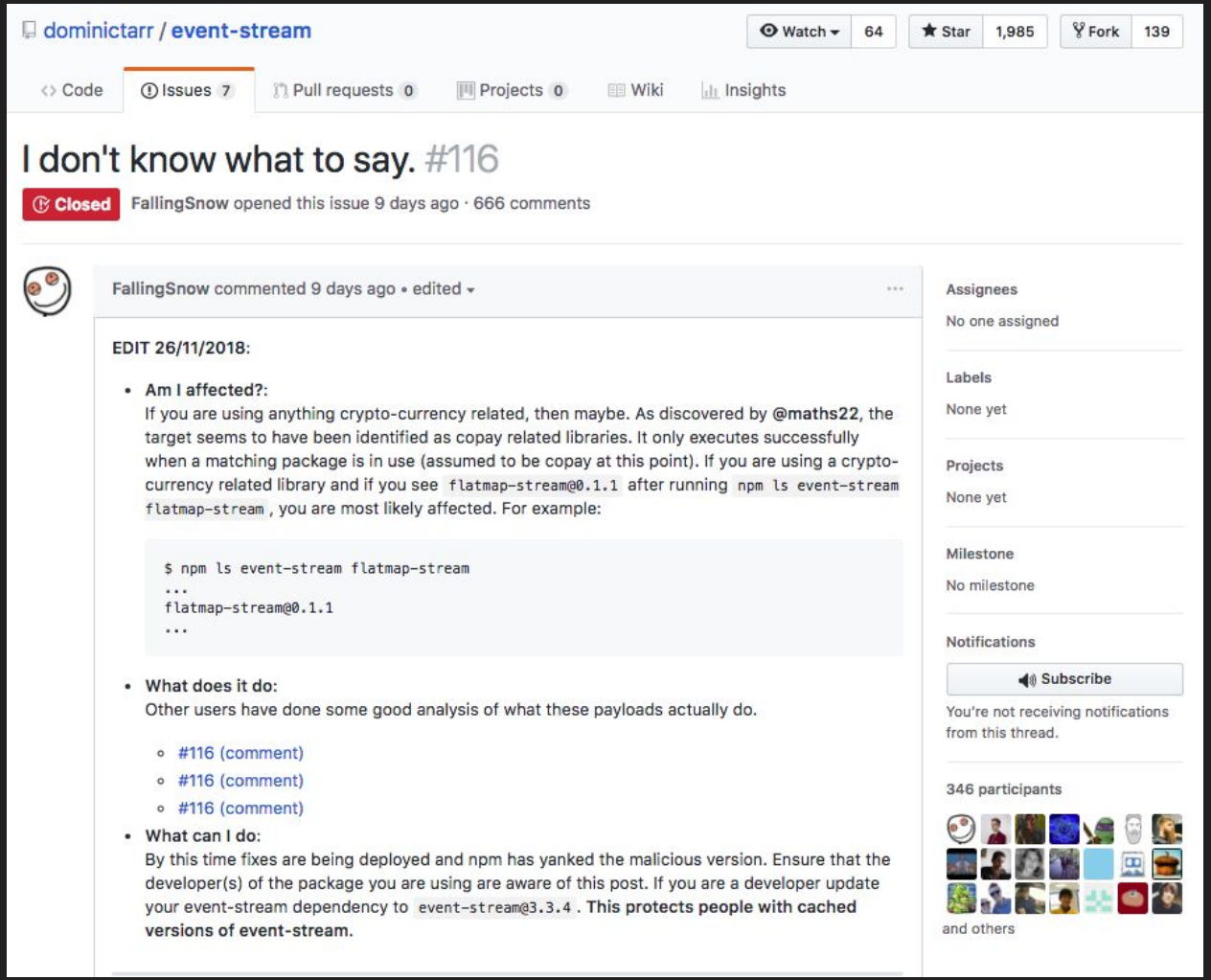
COMPUTER SCIENCE
UNIVERSITY OF MARYLAND

announcements

Any questions so far?

recap

- HTTP requests (ie. GET/POST)
- Maintaining state (ie. cookies, etc)
- Some common vulns
  - XSS
  - SQLi



dominictarr / event-stream

Watch 64 | Star 1,985 | Fork 139

Code | Issues 7 | Pull requests 0 | Projects 0 | Wiki | Insights

I don't know what to say. #116

Closed FallingSnow opened this issue 9 days ago · 666 comments

FallingSnow commented 9 days ago • edited

EDIT 26/11/2018:

- **Am I affected?:**
  If you are using anything crypto-currency related, then maybe. As discovered by **@maths22**, the target seems to have been identified as copay related libraries. It only executes successfully when a matching package is in use (assumed to be copay at this point). If you are using a crypto-currency related library and if you see `flatmap-stream@0.1.1` after running `npm ls event-stream flatmap-stream`, you are most likely affected. For example:

```
$ npm ls event-stream flatmap-stream
...
flatmap-stream@0.1.1
...
```

- **What does it do:**
  Other users have done some good analysis of what these payloads actually do.
  - #116 (comment)
  - #116 (comment)
  - #116 (comment)
- **What can I do:**
  By this time fixes are being deployed and npm has yanked the malicious version. Ensure that the developer(s) of the package you are using are aware of this post. If you are a developer update your event-stream dependency to `event-stream@3.3.4`. **This protects people with cached versions of event-stream.**

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Notifications
Subscribe
You're not receiving notifications from this thread.

346 participants
and others

The event-stream npm package was originally created and maintained by Dominic Tarr. However, this popular package has not been updated for a long time now. According to Thomas Hunter's post on Medium, "Ownership of event-stream, was transferred by the original author to a malicious user, right9ctrl. The malicious user was able to gain the trust of the original author by making a series of meaningful contributions to the package."

The malicious owner then added a malicious library named flatmap-stream to the events-stream package as a dependency. This led to a download and invocation of the event-stream package (using the malicious 3.3.6 version) by every user. The malicious library download added up to nearly 8 million downloads since it was included in September 2018.

The malicious package represents a highly targeted attack and affects an open source app called bitpay/copay. Copay is a secure bitcoin wallet platform for both desktop and mobile devices. "We know the malicious package specifically targets that application because the obfuscated code reads the description field from a project's package.json file, then uses that description to decode an AES256 encrypted payload", said Thomas in his post.

OWASP Top 10

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

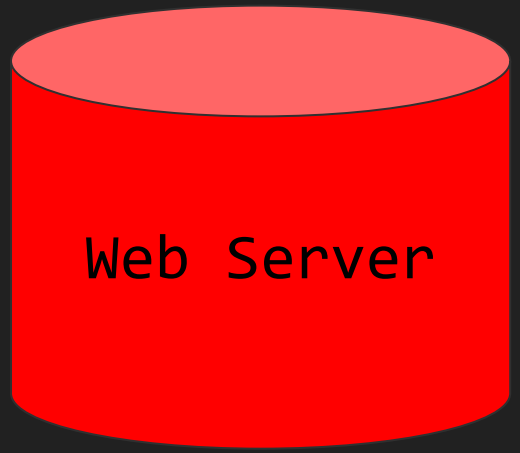
https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Local File Inclusion

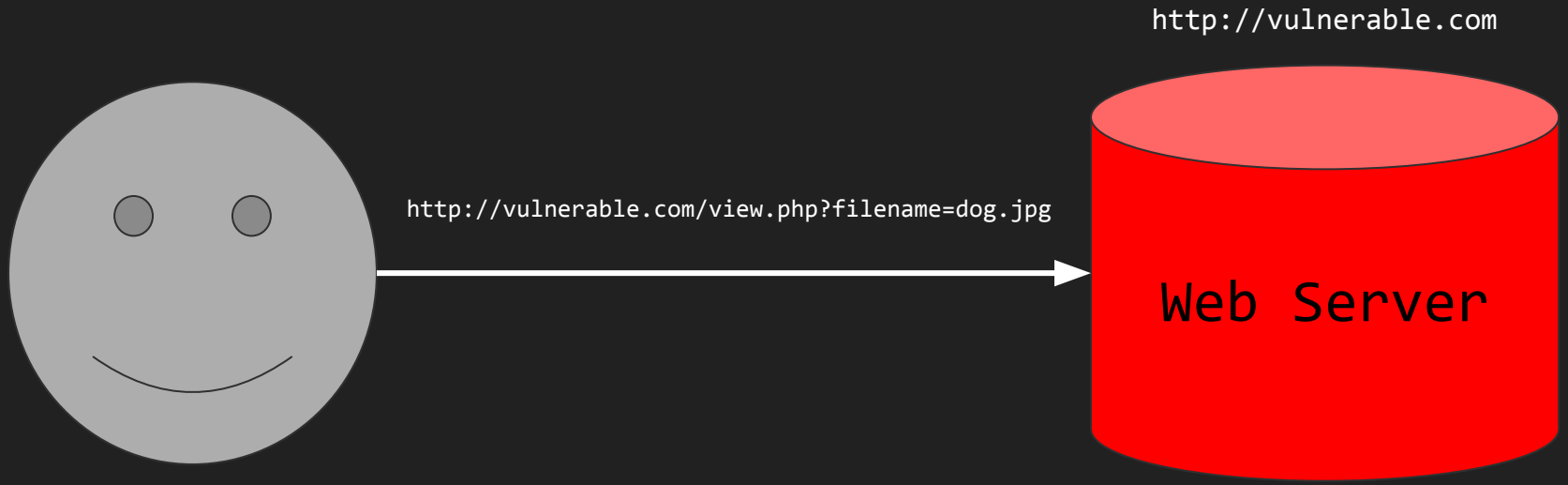
- Attacker includes a file path local to the server as input to a vulnerable field
- Can lead to:
  - Code execution (server & client)
  - DoS
  - Sensitive Information Disclosure

Local File Inclusion

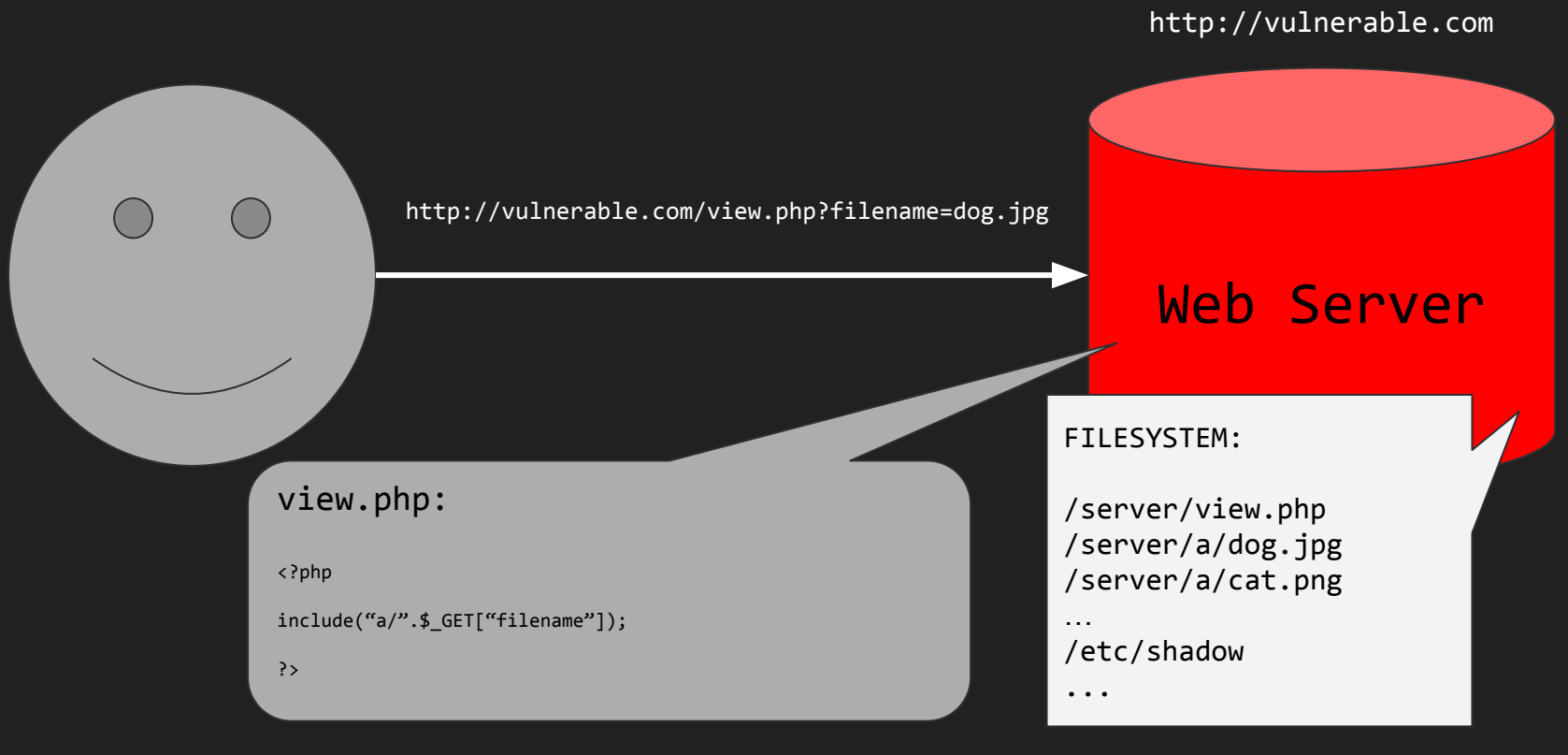
http://vulnerable.com



Local File Inclusion



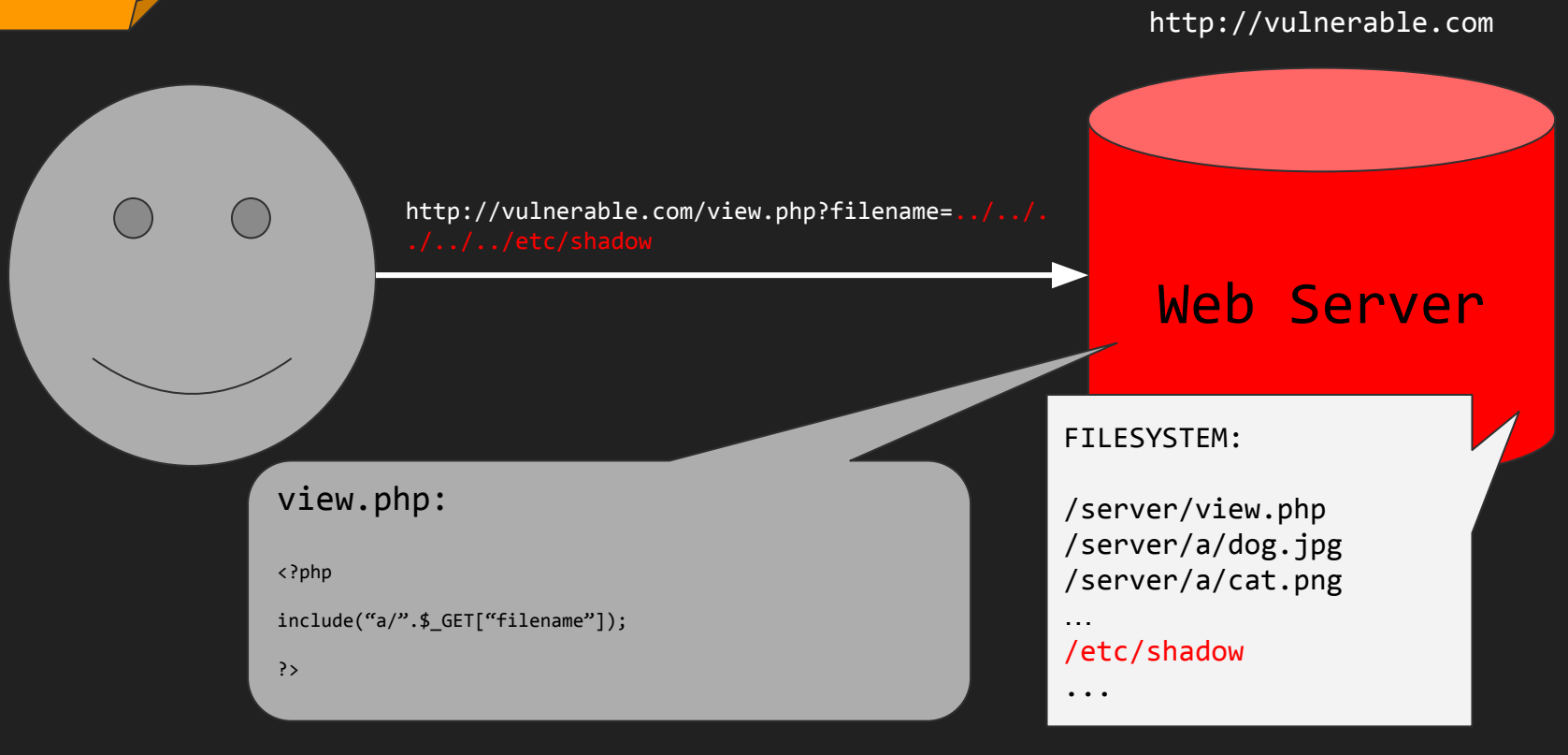
Local File Inclusion



Local File Inclusion

Directory Traversal Attack

Local File Inclusion (ATTACK)



Remote File Inclusion

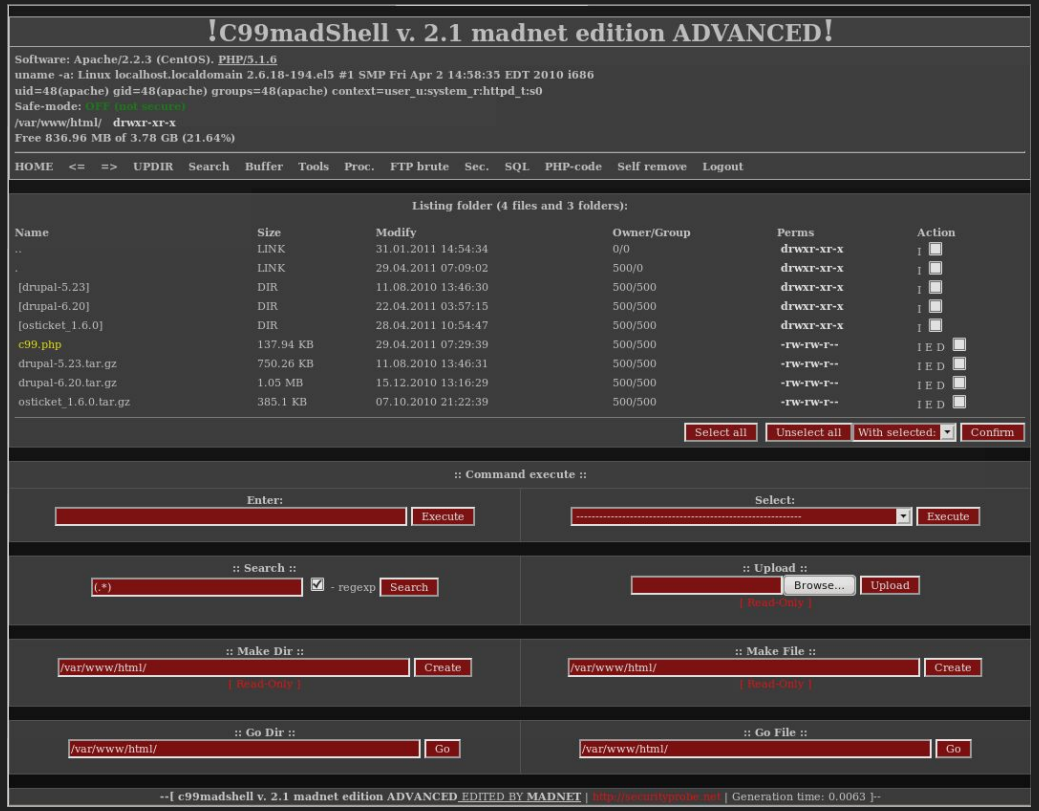
- Similar to LFI, but attacker includes a remote path as input to a vulnerable field
- Can lead to:
  - Code execution (server & client)
  - DoS
  - Sensitive Information Disclosure

Remote File Inclusion

Remote File Inclusion

Remote File Inclusion (ATTACK)

0wned


!C99madShell v. 2.1 madnet edition ADVANCED!
Software: Apache/2.2.3 (CentOS). PHP/5.1.6
uname -a: Linux localhost.localdomain 2.6.18-194.el5 #1 SMP Fri Apr 2 14:58:35 EDT 2010 i686
uid=48(apache) gid=48(apache) groups=48(apache) context=user_u:system_r:httpd_t:s0
Safe-mode: OFF (not secure)
/var/www/html/ drwxr-xr-x
Free 836.96 MB of 3.78 GB (21.64%)
HOME <= => UPDIR Search Buffer Tools Proc. FTP brute Sec. SQL PHP-code Self remove Logout
Listing folder (4 files and 3 folders):
Name Size Modify Owner/Group Perms Action
.. LINK 31.01.2011 14:54:34 0/0 drwxr-xr-x I
. LINK 29.04.2011 07:09:02 500/0 drwxr-xr-x I
[drupal-5.23] DIR 11.08.2010 13:46:30 500/500 drwxr-xr-x I
[drupal-6.20] DIR 22.04.2011 03:57:15 500/500 drwxr-xr-x I
[osticket_1.6.0] DIR 28.04.2011 10:54:47 500/500 drwxr-xr-x I
c99.php 137.94 KB 29.04.2011 07:29:39 500/500 -rw-rw-r-- I E D
drupal-5.23.tar.gz 750.26 KB 11.08.2010 13:46:31 500/500 -rw-rw-r-- I E D
drupal-6.20.tar.gz 1.05 MB 15.12.2010 13:16:29 500/500 -rw-rw-r-- I E D
osticket_1.6.0.tar.gz 385.1 KB 07.10.2010 21:22:39 500/500 -rw-rw-r-- I E D
Select all Unselect all With selected: Confirm
:: Command execute ::
Enter: Execute
Select: Execute
:: Search ::
(.*) - regexp Search
:: Upload ::
Browse... Upload
[Read-Only]
:: Make Dir ::
/var/www/html/ Create
[Read-Only]
:: Make File ::
/var/www/html/ Create
[Read-Only]
:: Go Dir ::
/var/www/html/ Go
:: Go File ::
/var/www/html/ Go
--[c99madshell v. 2.1 madnet edition ADVANCED EDITED BY MADNET | http://securityprobe.net | Generation time: 0.0063]--

Web Application Firewalls (WAF)

- Used by webapps prevent attacks such as XSS, SQLi, RFI/LFI, misconfigs, etc
- Typically rule-based
- Can be implemented in:
  - Server code (Apache ModSecurity, etc)
  - Appliance between network and server (Barracuda, etc)
  - Cloud (AWS WAF, Cloudflare, etc)

(Some) Approaches to WAF Bypasses

- How does WAF normalize input data?
  - Decode HTML entities?
  - Escape characters?
  - Enforce null byte string termination?
- Is it using regex to match signatures?
  - Blocks ‘OR ‘1’=’1’
  - Allows ‘ || 0x50 is not null

challenges

http://142.93.136.81:8893/

Wreak havoc

resources

- Natas OverTheWire
- JuiceShop
- Gruyere
- Ringzer0team
- OWASP Top 10

homework #12

Will not be posted.

Get ready for the final!