Pure Hacking:

Practical ModSecurity: Beyond the Core Rule Set

by Josh Amishav-Zlatin

PureHacking

Outline

- Introduction
- ModSecurity Rules Language Primer
- Practical Use Cases

"If you give someone a program, you will frustrate them for a day; if you teach them how to program, you will frustrate them for a lifetime."

Introduction

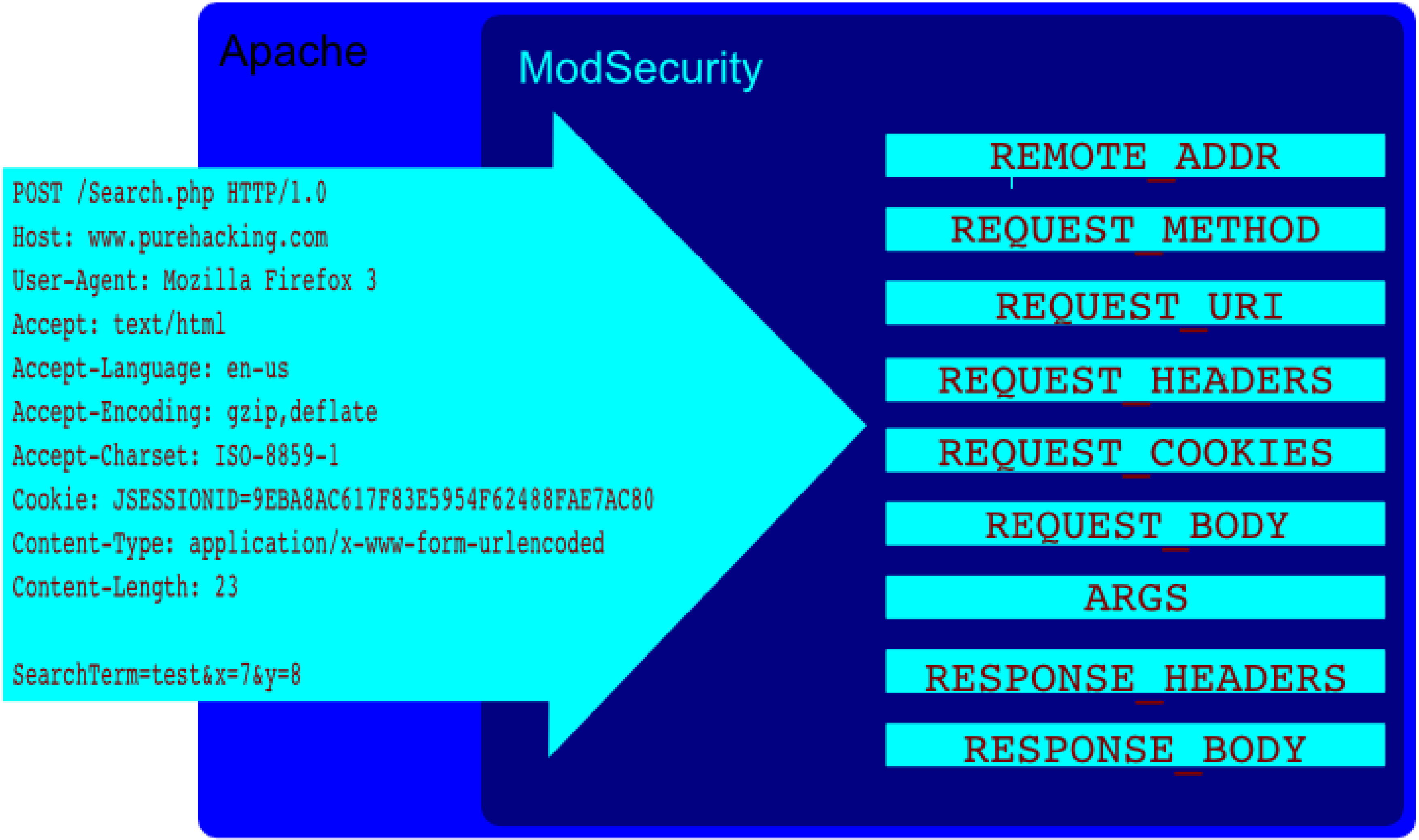
- Why
- How
- What

"Technology makes it possible for people to gain control over everything, except over technology"

ModSecurity Rules Primer
The Five Stages

- Request Header Parsing
- Request Body Parsing
- Response Header Parsing
- Response Body Parsing
- Logging

“Lisp in action is like a finely choreographed ballet. Basic in action is like a waltz of drugged elephants. C in action is like a sword dance on a freshly waxed floor.”



Apache

ModSecurity

```
POST /Search.php HTTP/1.0
Host: www.purehacking.com
User-Agent: Mozilla Firefox 3
Accept: text/html
Accept-Language: en-us
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1
Cookie: JSESSIONID=9EBA8AC617F83E5954F62488FAE7AC80
Content-Type: application/x-www-form-urlencoded
Content-Length: 23

SearchTerm=test&x=7&y=8
```

REMOTE_ADDR

REQUEST_METHOD

REQUEST_URI

REQUEST_HEADERS

REQUEST_COOKIES

REQUEST_BODY

ARGS

RESPONSE_HEADERS

RESPONSE_BODY

ModSecurity Rules Primer

- SecRule VARIABLES OPERATOR [ACTIONS]
  - Expands the variables
  - Applies the operator
  - A match either executes the per-rule action or performs the default action

"To err is human... to really foul up requires the root password."

ModSecurity Rules Primer

- SecRule REQUEST_URI ppp
- SecRule REQUEST_URI p{3}
- SecRule REQUEST_URI|ARGS “pure”

"If Python is executable pseudocode, then Perl is executable line noise."

ModSecurity Rules Primer

- SecRule ARGS:ph “@rx attack”
- SecRule ARGS|!ARGS:q owasp
- SecRule &ARGS:/^Q/“ “@eq 1”

“I code in vi because I don’t want to learn another OS.”

ModSecurity Rules Primer

- SecRule ARGS p1 log,auditlog,deny
- SecRule ARGS p2 phase:2,pass
- SecRule ARGS p3 chain,deny,status:404

  SecRule REMOTE_ADDR “!@beginsWith 10.1.1.”

"A computer lets you make more mistakes faster than any invention in human history - with the possible exceptions of handguns and tequila"

ModSecurity Rules Primer

- Variable Names
  - e.g. ARGS, GEO, QUERY_STRING
- Supported Operators
  - e.g. @rx, @rbl, @contains
- Disruptive Actions
  - e.g. deny, drop, redirect

"Programmers are tools for converting caffeine into code."

Pure Hacking Leaders in Internet Security

ModSecurity Rules Primer

- Meta-data Actions
  - e.g. id, msg, severity
- Flow Actions
  - e.g. allow, chain, pass
- Data Actions
  - e.g. capture, status, t

"The great thing about Object Oriented code is that it can make small, simple problems look like large, complex ones."

ModSecurity Rules Primer

- Audit Log Sanitisation Actions
  - – e.g. sanitiseArgs. sanitiseMatches, sanitiseRequestHeader
- Variable Actions
  - – e.g. setenv:name=value, setenv:!name
- Built-in Collection Variables
  - – e.g. initcol, setuid, setsid

"... one of the main causes of the fall of the Roman Empire was that, lacking zero, they had no way to indicate successful termination of their C programs." - Robert Firth

ModSecurity Rules Primer

- SecRule REQUEST_COOKIES:/^ASP/
  ^(.+)$ “phase:2,capture,log,auditlog, \
    pass,setsid:%{TX.1}, \
    msg:'captured sessid %{TX.1}”
- SecRule SESSION:IS_NEW “eq 1” \
    “phase:2,nolog,pass, \
      setvar:SESSION.timeout=86400”

"If at first you don't succeed; call it 1.0”

Pure Hacking Leaders in Internet Security

Access Control

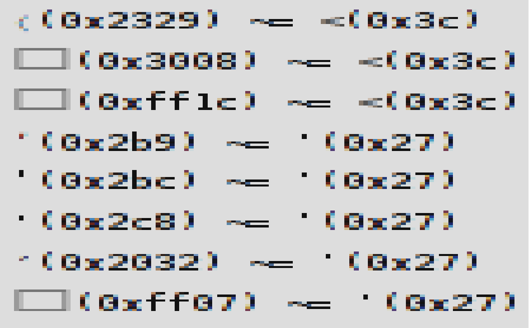
- Parameter Rotation
- Permissions Matrix
- Demo

Inter-Module Communication

- Insecure Cookies Demo

Lost in Translation

- Impedance Mismatch Demo



```
〈(0x2329) ~= <(0x3c)
□(0x3008) ~= <(0x3c)
□(0xff1c) ~= <(0x3c)
ʹ(0x2b9) ~= '(0x27)
ʼ(0x2bc) ~= '(0x27)
ˈ(0x2c8) ~= '(0x27)
′(0x2032) ~= '(0x27)
□(0xff07) ~= '(0x27)
```

http://hackademix.net/2010/08/17/lost-in-translation-asps-homoxssuality/

Pure Hacking Leaders in Internet Security

Lost in Translation

- %u3008scr%u0131pt %u3009%u212fval(%uFF07al %u212Frt(%22XSS%22)%u02C8) %u2329/scr%u0131pt%u2A
- ▯ scrıpt □ℯ val(▯ alℯrt(”XSS”)') □ /scrıpt □
- <script>eval('alert("XSS")')</script>

Pure Hacking ✓ Leaders in Internet Security

Weak Password Recovery

- Demo

Questions?

Email: jzlatin@purehacking.com

Blog: https://www.purehacking.com/portal/

Pure Hacking ✓ Leaders in Internet Security