Test Driven Security
In Continuous Integration

Julien Vehent - @jvehent - Enigma 2017
I HAVE FOUND SOURCE CODE DISCLOSURE ON WWW.MOZILLA.ORG!!!

RIGHT CLICK VIEW SOURCE AND YOU CAN STEAL ALL SOURCE CODE OF THE SERVER!!!

THIS IS A MAJOR VULNERABILITY!!!

Can I have a bounty now?
“Dear security researcher, we appreciate your participation to Mozilla’s bug bounty program, however this is not a vulnerability but simply a feature of the web, and thus not available for a bounty reward.”

“WHY DON’T YOU PAY A BOUNTY??! IT’S A MAJOR VULNERABILITY! I HAVE HACKED THE NSA WITH IT. YOU MUST PAY ME A BOUNTY!

Or maybe a t-shirt. Can I have a tshirt?”
User Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
Build ID: 20161208153507

Steps to reproduce:
Hello I found a reflected xss affecting hg.mozilla.org
Just visit the link to reproduce

https://hg.mozilla.org/integration/fx-team/pushloghtml?user="</script>alert(/XSS/)</script>


Actual results:
Reflected XSS with Iframe injection
Web vulns on Mozilla sites (2016)

Bug count by vulnerability type

- wsec-other
- wsec-selfxss
- wsec-disclosure
- wsec-xss
- wsec-http-header-inject
- wsec-impersonation
- wsec-authorization
- wsec-csrf
- wsec-authentication
- wsec-redirect
- wsec-servermisconfig
- wsec-session
- wsec-objref
- wsec-injection
- wsec-appmisconfig
- wsec-tls
- wsec-dos
- wsec-sql
- wsec-bruteforce
- wsec-input
- wsec-csrf, wsec-xss
- wsec-crossdomain, wsec-xss
- wsec-fileinclusion
- wsec-http
- wsec-errorhandling
- wsec-traversal
- wsec-oscmd
- wsec-headers
- wsec-crypto
- wsec-crossdomain
- wsec-xml
Bug Bounty payments

- Average is $2,400
- Paid only on high and critical issues (~25%)
- Bounty program cost is coming close to a full time employee.
Can we increase applications security by finding these issues **BEFORE** they reach our production systems?
DevOps
**DevOps** is the process on continuously improving software products.

- **Rapid release cycles**
- **Global automation of integration & delivery pipelines**
- **Close collaboration between teams**
A DevOps pipeline
Can we integrate security testing directly into DevOps pipelines?

To allow Devs & Ops to detect issues as code travels through the pipeline.
Test Driven Security

1. Define a baseline
2. Write tests
3. Run tests in CI/CD
4. Socialize requirements
5. Require tests to pass to deploy prod
# 1. Defining a Security baseline

**Test Scores**

<table>
<thead>
<tr>
<th>Test</th>
<th>Pass</th>
<th>Score</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Security Policy</td>
<td>✔</td>
<td>0</td>
<td>Content Security Policy (CSP) implemented with unsafe sources inside style-src.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This includes 'unsafe-inline', data: or overly broad sources such as https:</td>
</tr>
<tr>
<td>Contribute.json</td>
<td>✔</td>
<td>0</td>
<td>Contribute.json implemented with the required contact information</td>
</tr>
<tr>
<td>Cookies</td>
<td>✔</td>
<td>0</td>
<td>All cookies use the Secure flag and all session cookies use the HttpOnly flag</td>
</tr>
<tr>
<td>Cross-origin Resource Sharing</td>
<td>✔</td>
<td>0</td>
<td>Content is not visible via cross-origin resource sharing (CORS) files or headers</td>
</tr>
<tr>
<td>HTTP Public Key Pinning</td>
<td>✔</td>
<td>+5</td>
<td>Preloaded via the HTTP Public Key Pinning (HPKP) preloading process</td>
</tr>
<tr>
<td>HTTP Strict Transport Security</td>
<td>✔</td>
<td>+5</td>
<td>Preloaded via the HTTP Strict Transport Security (HSTS) preloading process</td>
</tr>
<tr>
<td>Redirection</td>
<td>✔</td>
<td>0</td>
<td>All hosts redirected to are in the HTTP Strict Transport Security (HSTS) preload list</td>
</tr>
<tr>
<td>Referrer Policy</td>
<td></td>
<td>0</td>
<td>Referrer-Policy header not implemented (optional)</td>
</tr>
<tr>
<td>Subresource Integrity</td>
<td>✗</td>
<td>-5</td>
<td>Subresource Integrity (SRI) not implemented, but all external scripts are loaded over https</td>
</tr>
<tr>
<td>X-Content-Type-Options</td>
<td>✔</td>
<td>0</td>
<td>X-Content-Type-Options header set to nosniff</td>
</tr>
<tr>
<td>X-Frame-Options</td>
<td>✔</td>
<td>0</td>
<td>X-Frame-Options (XFO) header set to SAMEORIGIN or DENY</td>
</tr>
<tr>
<td>X-XSS-Protection</td>
<td>✔</td>
<td>0</td>
<td>X-XSS-Protection header set to 1; mode=block</td>
</tr>
</tbody>
</table>
Custom tests are built on top of **ZAP**, NSP, eslint, Mozilla Observatory, ...
3. Running tests in CI/CD

- GitHub
- Travis CI
- Circle CI
- Docker Hub
- Jenkins
- Amazon Web Services
3. Running tests in CI/CD

Add more commits by pushing to the `testpr` branch on `Securing-DevOps/invoicer`.

- **Some checks haven’t completed yet**
  - 1 pending check

  - `ci/circleci` — CircleCI is running your tests

- **This branch has no conflicts with the base branch**
  - Merging can be performed automatically.

Merge pull request or view command line instructions.
3. Running tests in CI/CD

```yaml
$ cat circle.yml
[...

test:
  override:
    # start the application container
    - docker run mozilla/cutefox &

    # retrieve the ZAP container
    - docker pull owasp/zap2docker-weekly

    # run the ZAP scan against the application
    - >
      docker run -t owasp/zap2docker-weekly
      zap-baseline.py -t http://172.17.0.2:8080/
```
PASS: Strict-Transport-Security Header Scanner
PASS: Absence of Anti-CSRF Tokens
PASS: Secure Pages Does Not Include Mixed Content

FAIL: Web Browser XSS Protection Not Enabled x 2
http://172.17.0.2/account/preferences/
http://172.17.0.2/sitemap.xml

FAIL: Cookie Without SameSite Site Attribute x 1
http://172.17.0.2/en-GB/firefox/
4. Socialize requirements

[tracker] Security checklist #1482

- jvehent opened this issue on Sep 29, 2016 - 5 comments

jvehent commented on Sep 29, 2016 - edited

Risk Management

- The service must have performed a Rapid Risk Assessment and have a Risk Record bug (SVC-RRA).

Infrastructure rules

- Use Intermediate TLS (INFRA-TLS)
- Set HSTS to 31536000 (1 year) (INFRA-HSTS)
- Set HPKP to 5184000 (60 days) (INFRA-HPKP)
  - Public-Key-Pins: max-age=300;
    - pin-sha256="wo1wRy10VNah9iBc1RSC7XhI1Y9VwJGOIud4PB18="; pin-sha256="r/MIkJ3eEpVdm+u/k0/cwxzOMoibk4TYHIlBly1biA5E=";
    - Start with max-age set to 5 minutes and increase gradually
    - Pin to the EV and DV roots of Digicert
- If the service is not hosted under services.mozilla.com, it must be manually added to Firefox's preloaded pins.

mzl.la/2kN2dO3
5. Require tests to pass
5. Require tests to pass

<table>
<thead>
<tr>
<th>Average stage times:</th>
<th>BUILD</th>
<th>DEPLOY</th>
<th>ZAP Scan</th>
<th>INVALIDATE CACHE</th>
</tr>
</thead>
<tbody>
<tr>
<td>#71</td>
<td>4min 15s</td>
<td>23s</td>
<td>23s</td>
<td>10min 7s</td>
</tr>
<tr>
<td>Jan 12</td>
<td>4min 24s</td>
<td>22s</td>
<td>28s</td>
<td>10min 0s</td>
</tr>
<tr>
<td>17:38</td>
<td>8 commits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#70</td>
<td>1min 15s</td>
<td>27s</td>
<td>25s</td>
<td>9min 28s</td>
</tr>
<tr>
<td>Jan 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13:31</td>
<td>6 commits</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. Require tests to pass

- Run tests in CD (jenkins)
- Block **stage** deploy on FAIL
- Send feedback to Devs
- Don’t ever block prod!

$ cat pipeline.groovy

```groovy
[...]

stage('ZAP Scan') {
  checkpoint 'zap'
  catchError {
    test('https://url')
  }
}
```
Does it work?

On addons.mozilla.org...

- 2010 to 2015: 106 bugs, inc. 63 XSS
- 2016: enabled baseline
- Since 2016: 8 bugs, 0 XSS
Want secure applications?

1. Define baseline security
2. Drive testing from the DevOps pipeline
3. Never deploy sub-standard code
4. Empower DevOps teams to fix issues
5. Save time to work on the complex stuff
Questions?