Four years of reflection: How (not) to secure Web Applications

@JulianBerton
Part of OWASP Foundation – 81 groups

OWASP Melbourne - Application Security

📍 Melbourne, Australia
👥 1,629 members · Public group
🔗 Organized by OWASP F. and 1 other
OWASP AppSec Day 2019
Australia's biggest software security conference for technology professionals
Training 30th-31st October | Conference 1st November
Melbourne, Australia
DevSecQAFinOps
In the last 6 months who has felt like this?
Julian Bright  10:33 AM
@here Doing a bit of a language census, please react with the languages you pushed to production in last 2 weeks.

~150 tools, languages, platforms and frameworks
Dear Developers,

2019 called and said security is everyone's job…

Sooooooo here is a report with 2000 unvalidated issues for you to fix.

Kthxbye
58% Believe security is an inhibitor to DevOps agility.
No. of data breaches

No. of security controls

Source: My brain
Make security controls easy to adopt…

Sometimes a hacker’s best friend is an employee just trying to do their job more efficiently.
Developer Happiness™

- Easy to adopt controls
- Clear actionable information
- Works with dev flow
- Low disruption
- Real prioritised risks
A journey back in time to the year 2014...
2014

- < 70 developers
- 1 office building
- Simple software stack
- 1 physical data centre
- ~4 monolith applications
- < 100 git repositories
- ~10 deploy per day

5 years...

2019

- > 400 developers
- 18 countries
- Complex software stack
- 150+ AWS Cloud accounts
- 100’s of microservices
- > 2000 git repositories
- > 100 deploys per day
Restaurant Manager at Twofortythree Morley
Nov 13 to Nov 14 | 1 year

Employment status
Current company industry -
Availability -

Work type FullTime

Current location -

Location found in CV

Skills & Qualifications
Highest qualification Not specified
Skills -

Keyword found in CV
wa tax file number super fund macquarie super member fund id maq personal bank account cba complete access account bsb acc
Police checks
Order a national police check for employment purposes.

Right to work
Verify Australian work rights as a visa holder or citizen.

Driver Licence
Prove your right to drive with a valid Australian licence.
Shift Left Right?
If you thought .au's largest jobs site, @seekjobs, was a good place to store personal CV details, its probably not...
Fenrir
@semibogan

Fenrir @semibogan · 15 Jan 2018
Fuck this mess.
Less than a day later...

Andrew Hatch @Hatchman76 · 11 Sep 2015
Replying to @semibogan
@semibogan Check again :)

Fenrir @semibogan · 11 Sep 2015
@Hatchman76 that's pretty ace. Excellent response!
this should be obvious but don't use @seekjobs at work. They don't use SSL, anything you do can be monitored, thus risking employment status
6 months later...

Summary

Overall Rating

A+

Certificate: 95
Protocol Support: 97
Key Exchange: 98
Cipher Strength: 97

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Renegotiation test has been disabled temporarily due to an Apache httpd 2.4.37 bug. MORE INFO »

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »
Little bit too far right...

What about from random internet people instead!?
Open Bug Bounty Community helped fix 186,394 vulnerabilities

- 317,593 coordinated disclosures
- 186,394 fixed vulnerabilities
- 372 bug bounties with 810 websites
- 8,801 researchers, 316 honor badges
<table>
<thead>
<tr>
<th>Domain</th>
<th>Researcher</th>
<th>Date</th>
<th>Status</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>seek.com.au</td>
<td>dim0k</td>
<td>06.03.2016</td>
<td>patched</td>
<td>Cross Site Scripting</td>
</tr>
<tr>
<td>seek.com.au</td>
<td>dim0k</td>
<td>04.03.2016</td>
<td>patched</td>
<td>Cross Site Scripting</td>
</tr>
<tr>
<td>Affected Website:</td>
<td>seek.com.au</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Bug Bounty Program:</td>
<td>Create your bounty program now. It's open and free.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerable Application:</td>
<td>Custom Code</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Type:</td>
<td>XSS (Cross Site Scripting) / CWE-79</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVSSv3 Score:</td>
<td>6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:L/S:C/C:L/I:L/A:N]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```javascript
seek.com.au/jobs/searchFrom=Australia'-alert(document.cookie);
```
Attackers exploit SEEK via XSS vulnerability.
Hi Dimtry,

If you find vulnerabilities in the future, please disclosure them to us via

security@seek.com.au

Unfortunately as you publicly disclosed the issues we cannot offer you any reward as per our policy.

SEEK Security Team
<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Reported</th>
</tr>
</thead>
<tbody>
<tr>
<td>XSS</td>
<td>March 2016</td>
</tr>
<tr>
<td>HTML Injection</td>
<td>March 2016</td>
</tr>
<tr>
<td>XSS</td>
<td>April 2016</td>
</tr>
<tr>
<td>XSS</td>
<td>April 2016</td>
</tr>
<tr>
<td>XSS</td>
<td>May 2016</td>
</tr>
<tr>
<td>XSS</td>
<td>July 2016</td>
</tr>
</tbody>
</table>
Hi Dimtry,

Thank you for reporting these issues.

As a result we would like to offer you $550 USD. Could you please send us your Paypal details?

SEEK Security Team
Hello,

Email of my PayPal account is
dmitry.ivasf128@gmail.com

Thanks

d1n0ck
SEEK’s Vulnerability Disclosure Policy...

SEEK

SEEK is a diverse group of companies that have a unified purpose to help people live more fulfilling and productive working lives and help organisations succeed.

-$50 - $10,000 per vulnerability

Managed by Bugcrowd

https://bugcrowd.com/seek
Bug Bounty Program Metrics (2016 to 2019)

- Total: $115,000 (USD)
- Average: $845
- Highest: $10,000

Bar chart showing the distribution of bug bounty payments over different severity levels:
- Critical: 0
- Severe: 23
- Moderate: 46
- Low: 69
Part 5 — A Comprehensive Guide to Running a Bug Bounty Program

https://medium.com/@berton.julian
Just-In-Time Security Education...
54% of technology teams see security pros in the role of “nag”
Part 3 — Tackling Security Culture and Awareness

Julian Berton
Jul 16, 2017 · 10 min read

https://medium.com/@berton.julian
JIT Security Education

● Clear guidance around the “why”
● Relevant information only
● Getting help?
Part 4 — Delivering an Application Security Training Course

Julian Berton
Jul 16, 2017 · 14 min read

https://medium.com/@berton.julian
Bugcrowd 4:27 PM
pamoshea left a note.

*sql injection in events.seek.com.au*

Note
Created Jira ticket: [https://seek-jira.atlassian.net/browse/SEC-395](https://seek-jira.atlassian.net/browse/SEC-395)

Bugcrowd 12:03 PM
Zac set a reward amount of $3,000.

*sql injection in events.seek.com.au*

Researcher QA6Y0YLQ4RE8LPJ - 93.27%  
Priority P1 - critical
SQL Injection in events.seek.com.au

- Description of the issue
- Impact to SEEK
- Likelihood of attack

- Proof of concept
- Metrics and ownership tags
FYI Over the last week we've had a few "must fix" submissions to our bug bounty program (#bug-bounty-alerts) about a several vulnerabilities in events.seek.com.au. These vulnerabilities allowed the researcher to access the contact details (name, surname, phone) of who had RSVP'd for SEEK events.

More information here:
- XSS vulns: https://seek-jira.atlassian.net/browse/SEC-391
- SQLi: https://seek-jira.atlassian.net/browse/SEC-395

@servicemanagement could we please setup a PIR for this issue? Will be someone from the security team, internal systems ( ), and marketing ( or similar)
Post Incident Review (PIR)

- Problem
- Mitigating strategies
- What could we do differently?
- Risks & Data
- What made it not nearly as bad as it could have been?
- Root cause
- What are the positives?
- High Fives!
Scalable, alignment of technical patterns and standards…

Via Request For Comments (RFC)
2014

- < 70 developers
- 1 office building
- Simple software stack
- 1 physical data centre
- ~4 monolith applications
- < 100 git repositories
- ~10 deploy per day

5 years...

2019

- > 300 developers
- 18 countries
- Complex software stack
- 150+ AWS Cloud accounts
- 100’s of microservices
- > 2000 git repositories
- > 100 deploy per day
Security Change through Feedback

@Riot

engineering.riotgames.com/news/evolution-security-riot
• RFC process is used for internet standards (OAuth, TLS).

• Not an approval process.
This Source Control - GitHub RFC is designed to gain consensus and adoption of the guidance within, to help solve the problem described below:

The control, ownership, quality, searchability and security of our source code is vital for allowing teams at SEEK to effectively collaborate with each other. By sharing ideas, code and providing feedback to better the products we create for our customers.

The main idea behind this RFC is the following:

To achieve this level of collaboration in a secure fashion, ALL of SEEK's product related source code SHOULD be under source control, use Git and be stored within the SEEK-Jobs or SEEK-OSS GitHub organisations.
RFC 0003 - Source Control - GitHub

Status: ADOPTED

Tags: security, standard, source-code

Owner(s): Security Team, Platform Engineering, Architecture

Scope: All product development
GitHub Auditor 3:05 PM
WARNING: repository SEEK-Jobs/indirect-job-apply has been created as public by @mjohnson

GitHub Auditor 8:16 AM
⚠️ GitHub repo indirect-job-apply has no team admin
A current repo admin should add a team with admin rights cc: @mjohnson

November 28th, 2018
Open the gate for Secure-by-Default
High performing teams spend 50% less time fixing security issues.
Buildkite @ SEEK
Our current build system....
Secure-by-Default

- Comes out of the box
- Will not inhibit “innovation”
- Support when things don’t work
RFC014 - CICD Tool Requirements

- Secure Secret Storage
- Key Rotation
- Local Build Agents
- SSO SAML Support
- Audit Logging
- Zero Vendor Trust

- Build Reporting
- Event Notifications
- Codified Build Pipelines
- Native Docker Builds
- Low Latency Build Start
steps:
  - name: "Snyk testing"
plugins:
  - seek-oss/aws-sm#v0.0.5:
    env:
      SNYK_TOKEN: snyk-service-user-api
  - seek-oss/snyk#v0.0.4:
    block: true
    language: package.json
    path: package.json
Scan PR’s for issues

Some checks were not successful
1 failing and 1 successful checks

security/snyk — 1 vulnerable dependency path

security/snyk-verify — Verified pull request

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

Merge pull request
You can also open this in GitHub Desktop or view command line instructions.
Insecure Randomness

Vulnerable module: crypto-browsifier
Introduced through: aws-sdk@2.168.0

Fix this vulnerability

Detailed paths and remediation
- Introduced through: dotme-aggregator@1.0.0 > aws-sdk@2.168.0 > crypto-browsifier@1.0.9
- Remediation: Upgrade to aws-sdk@2.178.0.
Insecure Randomness

Vulnerable module: crypto-browserify
Introduced through: aws-sdk@2.168.0

Fixable

Detailed paths and remediation

- Introduced through: dotme-aggregator@1.0.0 > aws-sdk@2.168.0 > crypto-browserify@1.0.9
- Remediation: Upgrade to aws-sdk@2.178.0.

Overview

crypto-browserify is implementation of crypto for the browser.

Affected versions of the package are vulnerable to Insecure Randomness due to using the cryptographically insecure Math.random(). This function can produce predictable values and should not be used in security-sensitive context.

More about this issue
Uninitialized Memory Exposure

New vulnerability in package https-proxy-agent at the seek-poc organisation.

Severity
High

Package
https-proxy-agent

Issue ID
npm:https-proxy-agent:20180402
A macro view of your software maturity
116 Activities
12 Practices
4 Domains
Example Activities

- Educate executives on security.
- Use centralized reporting.
- Track bugs through the fix process.
- Operate a bug bounty program.
- Include security awareness.
<table>
<thead>
<tr>
<th>Activity</th>
<th>Firms (120)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black-box security tools into QA processes.</td>
<td>25%</td>
</tr>
<tr>
<td>Use automated &amp; manual code review tools.</td>
<td>63%</td>
</tr>
<tr>
<td>Identify gate locations and gather artifacts.</td>
<td>84%</td>
</tr>
<tr>
<td>Provide awareness training.</td>
<td>88%</td>
</tr>
</tbody>
</table>
Activity Change (%)

2% Overall Positive Change
Part 2—Building an Application Security Programme

Julian Berton
Jul 16, 2017 · 11 min read

https://medium.com/@berton.julian
Questions?

Twitter: @JulianBerton
Medium: @berton.julian
https://appsecday.io/