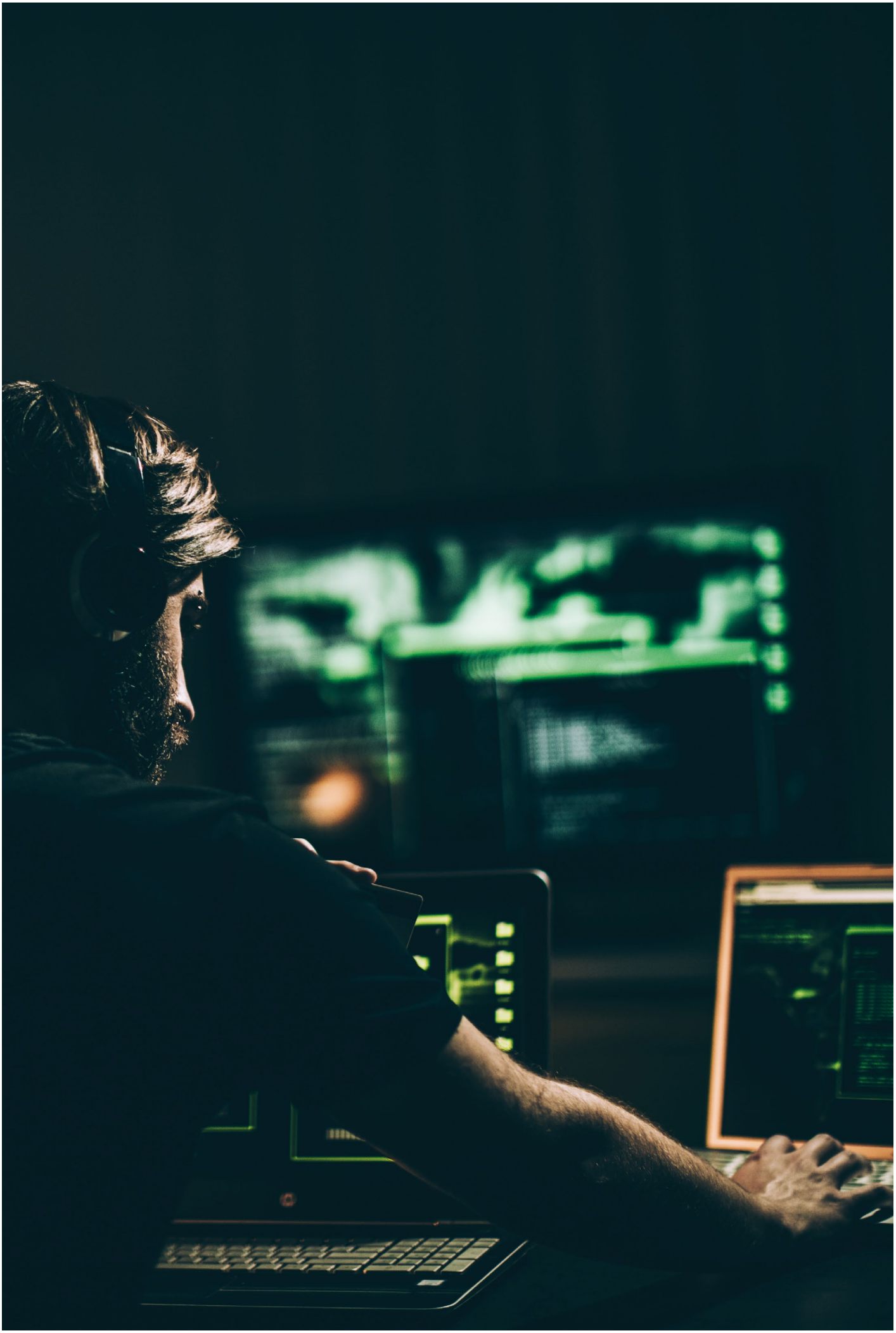
itlab

A Buyer's Guide to Penetration Testing

2018 Edition

Perspective Risk
an itlab company

CREST CHECK IT Health Check Service QMS ISO 9001 REGISTERED QMS ISO 27001 REGISTERED



Contents

Introduction

Zia Rehman
Technical Director

By downloading this guide, you have taken the first step towards one of the most powerful tools you can use to help strengthen your company's cybersecurity: a penetration test.

Over the next few pages, you will gain a solid understanding of the value of a penetration test. Crucially, you'll also be able to make sense of the noise out there and commission a test wisely.

The guide was created by a respected and popular figure in the cybersecurity industry – Zia Rehman. Rehman is an accredited CREST CCT Infrastructure and CREST CCT Application penetration tester with almost 20 years' experience in IT security.

Rehman and his business partner Pravesh Kara founded Perspective Risk (PR) in 2010 and went on to build an elite team of some of the best talent in information security. PR rapidly gained a reputation for delivering high quality and responsive services to its clients, spanning government, defence, automotive, financial services, charities, technology providers and beyond.

Today IT Lab - incorporating Perspective Risk - offers a range of cybersecurity services led by Cyber and Managed Services Director Michael Bateman. These cover defensive capabilities including Security Operations Centre (SOC) services, to offensive penetration testing engagements supported by assurance, risk and consulting capabilities.

Perspective Risk continues to deliver world class, independent penetration testing across an expanding client base. The combined portfolio of solutions and services are keeping organisations large and small safer from cyber criminals.

We hope you find the following advice beneficial.

What is a Penetration Test?

A penetration test, often shortened to pentest, is conducted by ethical hackers to simulate a real-world attack against your organisation. Their mission is to:

01 **Robustly test your defences** by deploying various techniques and tools ranging in sophistication.

02 **Reveal your organisation's security vulnerabilities** – in systems and people.

03 **Show what the consequences of a successful attack** could look like.

A quality penetration test will help you to see your vulnerabilities in context with the risks, empowering you to:

- Make informed decisions regarding potential remedial actions.
- Justify any additional investment in your cybersecurity.
- Identify possible gaps in your security policies and processes.

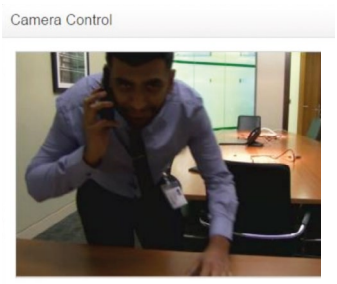
Your penetration tester will liaise with your IT team or developers to set up the test. Sometimes this affords useful insights into their mindset and behaviours.

YOUR ELECTRONIC ENVIRONMENT'S DEFENCES

You can choose to have any system or element of your infrastructure tested, including:

- Your network
- Web applications - often seen as the Achilles' heel of cybersecurity
- Your wireless solutions
- Mobile applications

As necessary - and with the appropriate permissions in place - testing can be extended to encompass your supply chain and third-party solutions.

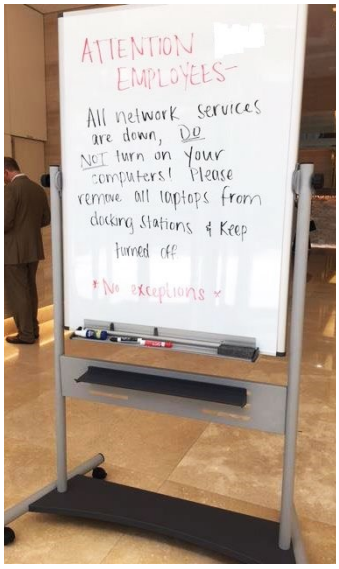


Another successful PR physical breach

YOUR PHYSICAL ENVIRONMENT'S DEFENCES

Depending on your specific concerns, a penetration test can include attempts to breach your physical perimeters. The goal is to gain access to your building, devices, servers etc.

Why is a Penetration Test Crucial?



A report by the National Cyber Security Centre and the National Crime Agency - The cyber threat to UK business - makes for sobering reading. Finding include:

- The cyber threat to UK business is significant and growing.
- The rise of internet connected devices is giving attackers greater opportunities.
- The threats are varied and adaptable, ranging from attacks which are:
  - Colossal, opportunistic and indiscriminate to;
  - Persistent, sophisticated, and deploy bespoke malware designed to compromise a specific target.
- The past year (2016-2017) has been punctuated by cyber-attacks on a scale and boldness never seen before.

Clearly there's an abundance of guidance on the internet to help security conscious organisations. The challenge is how – as a busy multi-tasking professional – can you keep abreast of it, particularly in an ever-changing threat landscape?

Good cyber-hygiene is essential, and the generic advice will assist you. However, every organisation is unique, with a distinct environment, controls and culture. Consequently, every organisation's security vulnerabilities are different.

Many companies employ talented and dedicated IT professionals. Realistically however, their teams are unlikely to possess the same depth of knowledge as those who specialise in information security.

Simply put, a penetration test will furnish you with an **expert report specific to your business.**

By taking a proactive approach to your security, you will help to:

- Reduce the risk of a data breach and associated fines (e.g. the ICO).
- Minimise service interruption / loss.
- Protect your reputation and brand.
- Safeguard your assets, e.g. cash and IP.
- Meet the standards of organisations you'd like to do business with.
- Increase the confidence of your stakeholders, customers etc.
- Comply with regulations (e.g. GDPR).
- Increase your resiliency in the event of a successful attack; contain it and recover faster.
- Ensure your users can keep working.

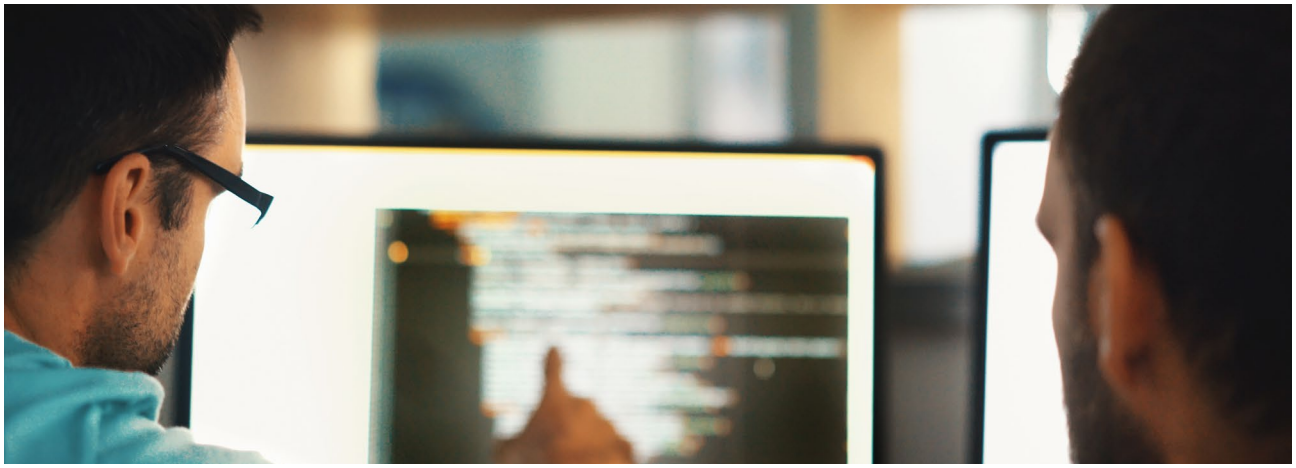
What's the Difference between a Penetration Test and a Vulnerability Scan?

A vulnerability scan is - for the most part - an automated way of assessing computers, networks and applications etc. for security weaknesses.

While a penetration tester will also deploy tools, it is a skilful human process. By their nature, penetration testers are inquisitive and creative. They will apply their knowledge and experience and adopt the mindset of a determined cybercriminal.

Ask your potential provider for their penetration testing methodology or a summary of their process. This will ensure you are signing up for a comprehensive threat-based penetration test and not a vulnerability scan dressed up as one.

Beware of 'appliances' promising efficiencies and savings as you may well receive a vulnerability scan in a pretty report.



Penetration Testing Providers – What Should You Look For?

CREDENTIALS AND PEOPLE

Providers that take the quality of their penetration testing seriously will demonstrate this by undergoing independent verification.

In the UK, this means allowing CREST - a not-for-profit information security standards authority - to scrutinise their testing and supporting processes. To maintain standards, CREST assesses its approved providers annually.

For those of you in the public sector, or who supply to government, look for a company accredited by the National Cyber Security Centre (NCSC) as a CHECK Green Light service provider. As with CREST, the NCSC CHECK scheme will reassure you that the provider's penetration testing services have been measured against rigorous standards.

You will find links to the CREST and CHECK websites at the end of this guide.

ISO 27001 certification is another quality standard to look for. The provider's certificate should expressly state penetration testing services.

Ultimately of course, you will be interacting with a person, not a company. Your penetration tester will have access to your sensitive data, so your trust and confidence in them is essential. You can validate your tester's credentials via the CREST and NCSC CHECK schemes.

Ask your potential provider how its employees are vetted. Are they checked by independent screening companies or in-house? Third party screening avoids bias. Include all personnel involved in the delivery of the test; don't confine your enquiries to the tester alone.

Above all, this should include a criminal record check, together with employment records, educational certificates and professional qualifications. If you are a supplier to government, this should extend to verifying the government Security Clearance (SC) of individuals. If your needs require it, you may want to look for a tester with Developed Vetting (DV) clearance, over and above SC.

Another consideration is the status of your tester. Are they an employee or a contractor? Some providers are mere sales fronts, reliant on contractors to deliver penetration testing. How can they mandate the quality, ethos and ethics of their agents?

A more abstract quality to gauge is passion. Ask if your tester has published blogs or articles. In our experience, good testers are generous with their knowledge and active in the information security community.

ETHICS AND APPROACH

Ask for references, testimonials and case studies. Confident providers seek and share feedback because they are committed to delivering a quality service. At IT Lab, we've also found it's a great motivator for our testers, who take pride in their work and read all feedback avidly.

To ensure your security objectives are met, your provider should furnish you with a scoping document: the blueprint for the penetration test.

A fluffy scope could end up being a costly mistake. Your provider should detail your expectations and requirements and capture relevant impacts and potential threats. Without knowing these values, risk cannot be accurately calculated.

It should be clear and understood as to:

- What is being tested
- How it is being tested
- Why it is being tested
- Who is doing the testing
- Where and when the testing is taking place

Sound penetration testing is a collaborative exercise. If it's delivered in an uncontrolled or unprofessional fashion it could leave you with a lot of cleaning up to do afterwards.

Your provider will require assistance to set up your system or network in readiness for the test and informing the relevant personnel. These requirements and prerequisites should be formally captured and set out in the scope document.

The Results of the Test: Key Things to Look For

The penetration test report is the tangible deliverable you will receive after the test. There are many penetration testers who can hack into most systems. However, they should also be able to communicate their findings plainly and meaningfully.

Your Report and the Key things to Look for:

01 Is there a management summary directed at non-technical people? The results should not be limited to technical speak about the threats and vulnerabilities. The report should enable your company to hold a wider discussion about risk and the impact of risk. It should help you to make a measured decision about what vulnerabilities you are prepared – or not prepared – to tolerate.

02 Conversely, some reports describe vulnerabilities without any technical terminology. Consequently, the value of the penetration test is lost on those in IT roles and who may have been able to act on more comprehensive information.

03 Is there a technical summary giving an aerial view of the overall threat and vulnerability landscape for the target systems? Is it meaningfully set out?

04 The threats your organisation is vulnerable to should be prioritised. This is sometimes done in tabulated form with a RAG (Red, Amber, Green) system.

05 Are the vulnerabilities reported in sufficient detail? Is there enough information for you to understand their level of risk and impact? Are steps included to allow you to recreate them or is the provider hiding behind a 'black art'?

06 Is there detailed remediation information? Is it customised to your environment, or is it a generic one-line statement along the lines of "provider recommends you fix it"?

A quality provider of penetration testing services should be willing to provide you with sample reports. They are necessary for the independent annual accreditation process for penetration testing, so will be on hand.

To protect their intellectual property and the information you exchange with them, good providers will request a mutual non-disclosure agreement.

What Costs Can You Expect?

Expect them to vary. Penetration Testing is usually sold by the day. Essentially, you are purchasing the time and skills of a penetration tester to provide the information you need.

A tester's daily rate typically ranges between £600 and £3,000. Travel and accommodation expenses may also apply.

Anything above £1,500 per day and you will be paying a premium for the brand. If you have sensitive stakeholders, you may decide it's worth it if a well-known name reassures them.

Need to verify the quotes you have received? Obtain prices from three reputable providers. The content of their quotes or proposals will give you an idea of how much care they have taken to listen and understand your requirements.

Use our buyer's checklist templates at the end of this guide to record your notes and price comparisons.

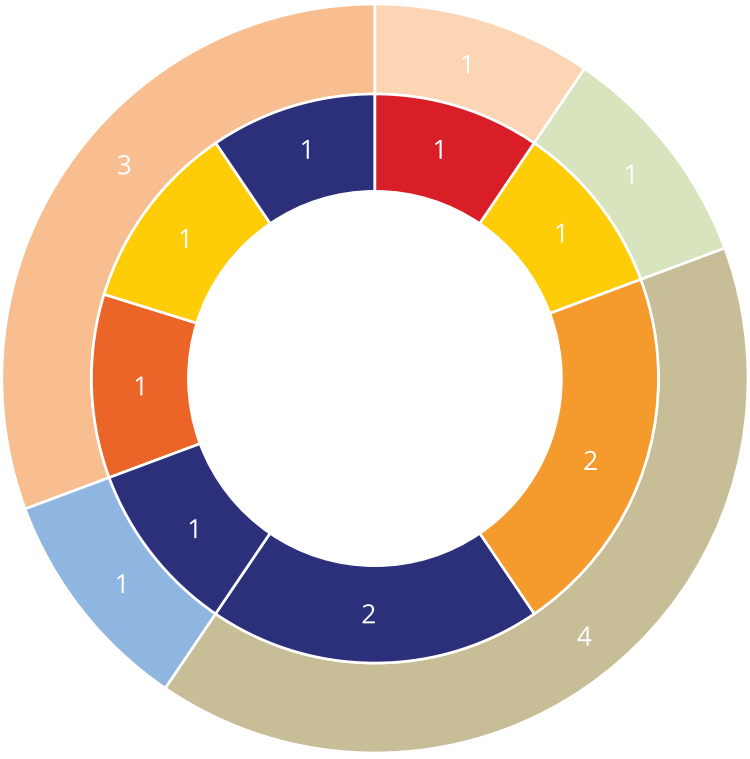
Example Penetration Test Reports

To wrap around your needs, IT Lab's reports are customisable. You may have explicit security concerns and require us to test specific systems. Deficiencies against particular standards can be highlighted, together with remediation advice.

Perhaps you have broader concerns and you'd like our testers to identify and prioritise the vulnerabilities across your infrastructure and show you what the key threats are.

Please see below for a small sample of what is included in our reports:

Categorised Vulnerability Summary



Technical and Remediation Summary

Reference	Vulnerability	Risk	Remediation
4.1	Application Authentication Mechanism Flaw	Critical	It is recommended that server side validation routines be reviewed to ensure that the server validates all data sent by the client and only accepts password data it was expecting
4.2	Session Information Transmitted without Encryption	High	All authentication session token should be transmitted over SSL and the Secure cookie should be configured on all authentication tokens
4.3	Inadequate User Authorisation	Medium	Users should be only granted access to specific resources that they are authorised to access and all access control decisions should be derived from a user's session
4.4	Emails Stored Unencrypted on File System	Medium	All sensitive databases retained on mobile devices should be encrypted using Apple File Protection APIs
4.5	Soap Credentials Easily Retrieved from Application Binary	Medium	Application code should be modified so that credentials are not permanently hard coded
4.5	Screen Lockout Mechanism not Implemented	Medium	It is recommended that the Acme mobile application locks after a 20 minute period of inactivity
4.7	Insecure Storage of Authentication Key	Low	Any authentication keys stored on the device should be encrypted with a unique encryption key prior to storing in the Apple key store
4.8	Error Message Exposes Technical Configuration Details	Low	All errors should always return the same generic error message informing the user that an error has occurred
4.9	Cookie without HttpOnly Flag Set	Low	Ensure that all Set-Cookie directives contain the HttpOnly flag
4.10	Weak SSL Ciphers	Low	Mandate the use of encryption ciphers of 128 bits in length or more

Detailed Risk Description

4.2 Session Information Transmitted without Encryption

Control Session Management

Targets Supporting Web Services

High

4.2.1 Impact

The supporting Acme web services offer functionality over both HTTP (unencrypted) and HTTPS (encrypted) connections. As the same cookie is used for both these connection types it would be possible for an attacker in a position to observe network traffic to intercept the unencrypted HTTP cookie transmissions and use the cookie to gain access to authenticated sections of the application, whereby personal and financial data can be viewed.

4.2.2 Probability

As mobile devices are commonly used over shared Wi-Fi connections such as hotels, airports etc., intercepting data becomes trivial and thus the probability of this attack being realised is high. Tools are freely available for the interception of data over Wi-Fi and little or no skill is required for their use. Once session tokens are obtained by these means an attacker must have a degree of knowledge to use them to steal a user session however attacks of this nature are well publicised on the Internet.

4.2.3 Remediation

If feasible it is recommended that the entire application including unauthenticated pages, such as news, events and help pages be transmitted over HTTPS and the HTTP service be disabled. If this is not possible and a HTTP service is functionally required the application should redirect any requests for sensitive content back to the HTTPS service.

Furthermore, the Secure cookie attribute should be implemented on all authenticated cookies to prevent them being sent to HTTP pages, such as the news, event and help pages. This should be reinforced using cookie scope instructions to prevent tokens being submitted for these resources.

The following instructions relate to configuring the Secure cookie flag in the PHP technology in use on the application:

Cookie parameters can be configured framework wide within the php.ini file or they can be configured on a per script basis.

Setting the Secure flag in the php.ini file is as simple as inserting the following directive:

```
session.cookie_Secure = True
```

To set the Secure flag on a per script basis, i.e. before each session_start() call:

```
void session_set_cookie_params  ( int $lifetime  [, string $path  [, string $domain
                                  [, bool $secure= true  [, bool $HttpOnly= true  ]]]] )
```

4.2.4 Technical Details

Initial access to the application does not require authentication allowing for a user to browse the latest news, events and product offerings and view help files. This communication takes place over HTTP:

```
URL being accessed: http://x.x.x.x/xxxx/xxxxxx/Events
Cookie set: Acmesession=7g6jtcft8p8oe2rnbu7o8f1ga9
```

After authentication, which is conducted over SSL, a new cookie is set and access to all personal and financial data is transmitted encrypted:

```
URL being accessed: https://x.x.x.x/xxxx/xxxxxx/Message
Cookie set: Acmesession=3f76jlet877nqe2rnb56rbr27q1
```

However, browsing back to a HTTP section of the application resends the now authenticated cookie which may be intercepted:

```
URL being accessed: https://x.x.x.x/xxxx/xxxxxx/News
Cookie sent: Acmesession=3f76jlet877nqe2rnb56rbr27q1
```

4.2.5 References

OWASP guide to Secure flag: https://www.owasp.org/index.php/SecureFlag

Compare Providers with our Buyer's Guide Template Checklists

Feel free to use these templates to record and compare your findings.

Penetration Test

Buyer's Guide Checklist

Provider:_____

Provider Contact Details:_____

Provider Contact Name:_____

Date:_____

Question	Hints	Checked	Notes
Provider's credentials	Membership of CREST and CHECK	☐	
Provider's credentials	ISO certifications – ISO 27001 and ISO 9001	☐	
Provider's reputation and experience	Testimonials, references, case studies	☐	
Penetration testers credentials	CREST and CHECK qualifications, educational and professional qualifications	☐	
Vetting of penetration testers	Independent vetting certificates and security clearances	☐	
Status of penetration testers	Employee or contractor	☐	
The test	Penetration test or vulnerability scan? Ask if approach is manual or automated	☐	
Your requirements / scoping document	Ask how these will be documented. The provider should understand your risk profile and concerns	☐	
The penetration test report	Ask for sample reports. Are they: Comprehensive? | Can you understand them? | Management summary? | Supporting technical information? | Detailed remediation advice? |	☐	
Price quoted	A penetration tester's day rate typically ranges between £600 and £3,000, exclusive of VAT and travel expenses. Accommodation expenses may also apply	☐	

Penetration Test

Buyer's Guide Checklist

Provider:_____

Provider Contact Details:_____

Provider Contact Name:_____

Date:_____

Question	Hints	Checked	Notes
Provider's credentials	Membership of CREST and CHECK	☐	
Provider's credentials	ISO certifications – ISO 27001 and ISO 9001	☐	
Provider's reputation and experience	Testimonials, references, case studies	☐	
Penetration testers credentials	CREST and CHECK qualifications, educational and professional qualifications	☐	
Vetting of penetration testers	Independent vetting certificates and security clearances	☐	
Status of penetration testers	Employee or contractor	☐	
The test	Penetration test or vulnerability scan? Ask if approach is manual or automated	☐	
Your requirements / scoping document	Ask how these will be documented. The provider should understand your risk profile and concerns	☐	
The penetration test report	Ask for sample reports. Are they: Comprehensive? | Can you understand them? | Management summary? | Supporting technical information? | Detailed remediation advice? |	☐	
Price quoted	A penetration tester's day rate typically ranges between £600 and £3,000, exclusive of VAT and travel expenses. Accommodation expenses may also apply	☐	

Penetration Test

Buyer's Guide Checklist

Provider:_____

Provider Contact Details:_____

Provider Contact Name:_____

Date:_____

Question	Hints	Checked	Notes
Provider's credentials	Membership of CREST and CHECK	☐	
Provider's credentials	ISO certifications – ISO 27001 and ISO 9001	☐	
Provider's reputation and experience	Testimonials, references, case studies	☐	
Penetration testers credentials	CREST and CHECK qualifications, educational and professional qualifications	☐	
Vetting of penetration testers	Independent vetting certificates and security clearances	☐	
Status of penetration testers	Employee or contractor	☐	
The test	Penetration test or vulnerability scan? Ask if approach is manual or automated	☐	
Your requirements / scoping document	Ask how these will be documented. The provider should understand your risk profile and concerns	☐	
The penetration test report	Ask for sample reports. Are they: Comprehensive? | Can you understand them? | Management summary? | Supporting technical information? | Detailed remediation advice? |	☐	
Price quoted	A penetration tester's day rate typically ranges between £600 and £3,000, exclusive of VAT and travel expenses. Accommodation expenses may also apply	☐	

Useful Links

- CREST website
- CREST UK Approved Member Companies Supplying Penetration Testing Services
- National Cyber Security Centre (NCSC) CHECK service providers
- NCSC Using a CHECK provider

itlab

Perspective Risk
an itlab company

London
1 East Poultry Avenue
London
EC1A 9PT

Manchester
Riverside, Agecroft Road
Manchester
M27 8SJ

www.itlab.com